MINISTERIO DE RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO

REVISIÓN DE LOS CONTROLES DE LA GESTIÓN INFORMÁTICA

ABRIL DE 2004

CONTENIDO

INFORME EJECUTIVO

El presente informe tiene por objeto sintetizar el resultado de las tareas efectuadas a fin de evaluar los controles de la Tecnología Informática en el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto.

De la evaluación practicada entre los meses de octubre y diciembre de 2003 se observó que el Ministerio presenta falencias de control en lo que respecta a la gestión de la tecnología informática, visibles principalmente en la existencia de diversas áreas informáticas no unificadas, en la ausencia de un plan informático estratégico, en la falta de procedimientos y metodologías adecuados y suficientes para las actividades ejecutadas, en las debilidades en la seguridad informática, en la carencia de un plan de contingencias orientado a garantizar la continuidad de las operaciones, como así también en la ausencia de respaldo documental de los sistemas aplicativos.

En otro orden, se verificó la ausencia de un tratamiento suficiente al informe emitido por esta Sindicatura General de la Nación en octubre de 2001 respecto del proyecto NIC Argentina, por lo cual persisten la mayoría de los hallazgos señalados en esa oportunidad.

A partir de la presente revisión, el área auditada ha elaborado un plan de acción estableciendo las tareas y plazos para la solución de los aspectos observados, por lo que se recomienda establecer un procedimiento de monitoreo y control que permita detectar y corregir desvíos y asegure su cumplimiento.

En función a los hallazgos relacionados con la falta de cumplimiento de la recomendaciones efectuadas por esta Sindicatura General de la Nación en el informe emitido en octubre de 2001 y en la carencia de algunas licencias de productos antivirus, que puede configurar la conducta prevista y reprimida por el art. 71 de la ley 11.723 de Régimen de Propiedad Intelectual, se deberá realizar el pertinente deslinde de responsabilidad.

En el informe analítico adjunto, se describen detalladamente los hallazgos y recomendaciones resultantes de la labor efectuada.

Buenos Aires, 16 de abril de 2004.

INFORME ANALÍTICO

I. OBJETO

Evaluar los controles de la Tecnología Informática en el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto.

II. ALCANCE

El trabajo abarcó el relevamiento y evaluación de los procedimientos de control vinculados a la gestión de la tecnología informática del Ministerio, teniendo en cuenta hallazgos oportunamente informados relativos al proyecto NIC Argentina.

La revisión se llevó a cabo mediante entrevistas y análisis de documentación entre los meses de octubre y diciembre de 2003.

El presente informe se encuentra referido a los hallazgos y conclusiones sobre el objeto de la tarea, hasta la fecha precedentemente indicada y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

Las entrevistas mantenidas se realizaron con personal del Departamento de Informática dependiente de la Dirección de Informática, Comunicaciones y Seguridad.

III. TAREA REALIZADA

El trabajo se desarrolló según la metodología de esta Sindicatura General de la Nación en un todo de acuerdo con las Normas Generales de Control Interno (Resolución SIGEN N° 107/98), Normas de Auditoría Interna Gubernamental (Resolución SIGEN N° 152/02) y las Pautas de Control Interno para Sistemas Computadorizados de Información, aplicables para la evaluación de las actividades de control en el procesamiento de información.

Las tareas abarcaron lo siguiente :

1. Relevamiento de la situación actual de las actividades informáticas del organismo, analizando la evolución producida desde la emisión del informe de SIGEN relativo a NIC Argentina de octubre de 2001 y el informe de la UAI emitido a raíz de lo solicitado

mediante la Circular Nro. 01/02- SGN, examinandose entre otros los recursos informáticos utilizados para el procesamiento de información, la distribución de funciones en el sector informático, los procedimientos relacionados con las actividades informáticas, así como los planes y proyectos vigentes.

2. Evaluación de la situación actual de los controles informáticos analizando los hallazgos que pudieran persistir desde la auditoría practicada en 2001.

IV. HALLAZGOS Y RECOMENDACIONES

Se exponen a continuación los principales hallazgos surgidos del trabajo llevado a cabo, así como las recomendaciones para cada caso :

1. Estructura orgánica

En el análisis de la estructura orgánica del área Informática se observó que, a la fecha de la auditoría, la misma se encuentra definida formalmente sólo hasta el nivel de Departamento, sin detallar los distintos grupos que la componen, así como las responsabilidades y funciones de cada uno de ellos. Cabe destacar que, del relevamiento surgió que existe una estructura propuesta para el área, la que pasará a denominarse Coordinación General, en la cual se definirán los sectores que la integran.

La situación vigente impide la adecuada rendición de cuentas y la implementación de un esquema de control por oposición de intereses, implicando riesgos como la falta de una adecuada separación de funciones, ineficiente distribución de tareas, o desconocimiento, por parte del personal, de sus responsabilidades, entre otros.

Asimismo, existe un grupo dedicado a tareas informáticas en el ámbito del área de Administración, previéndose, según fuera mencionado, su incorporación al ámbito de la Coordinación General en cuestión.

La circunstancia de que existan diversos sectores responsables de actividades informáticas impide alcanzar homogeneidad de criterios y unicidad en los objetivos.

Cabe recordar que la Unidad de Auditoría Interna realizó una observación respecto de la estructura interna del área, en su informe de octubre de 2002, emitido de acuerdo a lo solicitado por esta Sindicatura General de la Nación en su Circular Nº 1/2002-SGN.

Recomendación :
Definir formalmente la estructura interna del Departamento de Informática, asignando las responsabilidades de cada puesto de trabajo. Priorizar el proyecto correspondiente a la unificación de los diversos sectores informáticos a efectos de que exista un único responsable.

Opinión y Plan de Acción del Auditado :
"Se remitió a DIPER un proyecto de estructura que refleja la actual organización del área, a efectos de crearse la Coordinación UNINF en el organigrama."
Fecha de Regularización Prevista : Mayo 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

2. Plan informático

El Ministerio no posee un plan informático aprobado en el cual consten los objetivos a alcanzar en materia informática para el mediano y largo plazo, detallando proyectos, responsables, presupuesto, plazos, etc..

Cabe considerar que, de acuerdo a lo relevado, para el año 2004 se prevén adquisiciones que implican presupuestos de gran envergadura (ej. compras de hardware y software previstas por más de $4 millones sin considerar gastos en personal y otros recursos).

En ese sentido, encarar proyectos aislados que no formen parte de un plan estratégico puede implicar riesgos de una ineficiente asignación de recursos y prioridades, de que se encaren proyectos que no cuenten con la autorización correspondiente, de realizar inversiones en tecnología que no se condigan con la estrategia del organismo, etc.. La ausencia del plan documentado y aprobado dificulta asimismo, el monitoreo de las actividades desarrolladas por el área informática, al no existir un elemento adecuado para medir el cumplimiento de las metas y exigir la correspondiente rendición de cuentas.

Cabe señalar que esta Sindicatura observó en 2001 que el desarrollo de las tareas se realizaba sobre la base de la solución de actividades de coyuntura, sin que existiera un Plan Informático que especificara los objetivos de largo plazo del Ministerio, aspecto que no fue solucionado.

Recomendación :
Desarrollar y aprobar un plan informático, alineado con los objetivos estratégicos globales del organismo, a efectos de guiar el desarrollo de las actividades, permitir la comprobación

del cumplimiento de las metas y optimizar la asignación presupuestaria en función a los proyectos comprometidos.
El plan debe especificar las prioridades, tareas previstas y encaradas actualmente, los plazos y responsables de las mismas, así como los recursos necesarios para llevarlos a cabo.
Debe incluir consideraciones respecto de la estrategia destinada a evitar la obsolescencia tecnológica, así como la estrategia global de administración de las comunicaciones, considerando los procedimientos necesarios para resguardar la confidencialidad e integridad de la información intercambiada en la red del Ministerio, sobre la base de prácticas generalmente aceptadas, tales como firma digital y mecanismos de encripción.

Opinión y Plan de Acción del Auditado :
"Se está diseñando para ser elevado para su aprobación, el Plan Informático 2004. El mismo contempla la determinación de objetivos y responsables, plazos y recursos necesarios, estrategias tecnológicas y de seguridad e integridad de la información. El plan está en concordancia con los objetivos estratégicos del Ministerio."
Fecha de Regularización Prevista : Abril 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

3. Normas, metodologías y procedimientos para las actividades informáticas

El área informática del Ministerio carece de suficientes metodologías y procedimientos documentados y aprobados para el desarrollo de sus actividades.

Dada la envergadura de las operaciones del Ministerio y la sensibilidad de la información procesada, la ausencia de métodos y procedimientos documentados y aprobados adquiere especial relevancia en las siguientes actividades :

- Desarrollo y Mantenimiento de Sistemas (sin una adecuada metodología, no es posible garantizar, por ejemplo, la autorización de todas las modificaciones efectuadas sobre los aplicativos, la adecuada administración de prioridades entre los distintos trabajos de desarrollo o modificación de sistemas, la realización de suficientes controles, el cumplimiento de etapas críticas en el desarrollo de sistemas, como la generación de documentación, la aplicación de estándares de diseño y programación, a adecuada conservación de las distintas versiones de los programas, etc.).

- Administración de la seguridad (sin estos procedimientos, los controles de protección física de los activos informáticos tales como datos, hardware, software, vínculos de comunicaciones, instalaciones, los resguardos para evitar intromisiones de hackers, el otorgamiento de permisos y claves de acceso, la protección contra virus, etc., quedan supeditados al criterio de los funcionarios a cargo, sin asegurar que se efectúen adecuadamente y de manera continua). Actualmente no existe un procedimiento formal para la asignación de los permisos de acceso de los usuarios, que se encuentre sustentado en criterios de clasificación de los sistemas de información, considere el rol desempeñado por el usuario e incluya la autorización correspondiente por parte del propietario responsable de cada sistema.

- Gestión y control de las licencias de software (la ausencia de este procedimiento impide garantizar la adecuada y eficiente administración de los distintos productos de software disponibles, y dificulta el correspondiente monitoreo de la instalación de copias legales).

- Soporte técnico y atención de usuarios (la carencia de procedimientos dificulta la determinación de prioridades de estas tareas y el control de su cumplimiento, e impide la óptima asignación de responsables a la ejecución de las mismas).

La carencia de procedimientos y metodologías de trabajo aprobadas constituye un importante factor de riesgo que afecta la eficiencia de la gestión, la aplicación de métodos y controles uniformes en las operaciones, incrementa la posibilidad de errores y dificulta la capacitación del personal.

Cabe considerar que esta situación ya fue observada por esta Sindicatura en su informe del año 2001, donde se indicó que el Organismo no disponía de un cuerpo normativo formalmente aprobado en el que se especificaran las normas y procedimientos para las tareas del sector informático, mencionándose como ejemplos, que no existían procedimientos documentados para el desarrollo y mantenimiento de sistemas, la administración de cuentas de usuario o las operaciones de procesamiento.

Se observó asimismo que, si bien existían diversas prácticas implementadas respecto de la seguridad informática, estas no se encontraban compiladas en una política documentada y formalizada que definiera la estrategia en cuanto a la seguridad y controles informáticos, que especificara las responsabilidades individuales del personal, y que asegurara el conocimiento y cumplimiento de las medidas, aún ante eventuales cambios en los responsables de las tareas.

Este aspecto también fue observado por la UAI en el informe que elaborara para cumplir lo solicitado mediante la Circular N° 1/2002 SGN.

La situación expuesta implica la transmisión oral de los procedimientos con el consecuente riesgo de errores y dependencia del personal con conocimiento de la operatoria.

En otro orden, cabe señalar que oportunamente se observó que, entre los procedimientos informáticos que no se encontraban documentados, se encontraba el correspondiente a la realización de back ups. Actualmente, el citado procedimiento se encuentra documentado, lo cual denota que, en este aspecto, se ha tenido en cuenta lo recomendado por SIGEN.

No obstante, del análisis del mencionado documento, se observó que las copias de back up se almacenan en una caja ignífuga, sin que exista una copia de resguardo fuera del edificio donde se encuentra el centro de procesamiento.

Recomendación :
Se deberán documentar y aprobar procedimientos para las principales actividades informáticas, encarando en primera instancia, las siguientes :

a) El desarrollo y mantenimiento de sistemas : debe contemplar como mínimo :

- *La utilización de formularios a completar por los usuarios para la solicitud de desarrollos o cambios sobre la aplicación, con el correspondiente instructivo para su confección.*
- *La existencia de un procedimiento para la administración de requerimientos que incluya : priorización de los mismos, personal asignado, control de las tareas realizadas, plazos, etc..*
- *La definición de un procedimiento referido a la realización de pruebas sobre los sistemas desarrollados o modificados, que incluya la participación y aprobación del usuario requeriente.*
- *La documentación de los sistemas y los cambios.*
- *La especificación de estándares de diseño, programación y documentación de aplicaciones*

b) Respecto de la administración de permisos de accesos, teniendo en cuenta la clasificación de la información y los sistemas del MRECIC, se debe documentar un procedimiento que incluya, entre otras cosas, lo siguiente :

- *Un formulario en el que los usuarios dejen constancia de que requieren el otorgamiento de permisos de acceso a la red y/o a los diversos sistemas que se procesan, indicando el tipo de permiso requerido (lectura, modificación, ejecución, etc.). Este formulario deberá incluir la firma autorizante del superior responsable y deberá respetar el nivel de protección asociado a la clasificación asignada a los datos.*
- *La firma de un compromiso por la recepción de una cuenta de usuario, que debe establecer las características que deben cumplir las claves en cuanto a longitud, tiempos de expiración, tipos de caracteres, encriptación, entre otros.*
- *Un formulario por el cual el área de Recursos Humanos informe periódicamente los nombres de los agentes que dejaron de prestar funciones en la Administración, o que cambiaron de dependencia (con lo que deberían modificarse sus permisos de acceso).*

c) En relación con la generación de back ups, se deberá contemplar el almacenamiento periódico de una copia de resguardo, fuera del edificio.

Adicionalmente, documentar procedimientos orientados a la gestión y control de licencias de software (ver sugerencias en Anexo I) y actividades de soporte técnico.

Opinión y Plan de Acción del Auditado :
"Se están diseñando procedimientos, que posteriormente serán elevados para su aprobación siguiendo las recomendaciones en cuanto a: Desarrollo y Mantenimiento de Sistemas, Administración de permisos de Accesos, Generación de Backups, Gestión y Control de Licencias de Software y Soporte Técnico."
Fecha de Regularización Prevista : Octubre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

4. Seguridad lógica

Del análisis de los listados de permisos de acceso otorgados a los usuarios sobre los servidores de la red, se observó lo siguiente :

- En general, los usuarios son identificados mediante una codificación creada por el MRECIC consistente en un "trigrama" único por empleado, conformado por una combinación de 3 letras.
  Cabe señalar que este método para la identificación de los usuarios a través de "trigramas" no es usual, ya que las técnicas habituales consisten, por ejemplo, en identificar a los usuarios mediante el apellido y la inicial del primer nombre, o mediante esta inicial y las primeras cinco letras del apellido.

- El mecanismo de identificación de usuarios mediante trigramas resulta cuestionable asimismo, si se tiene en cuenta que, de acuerdo a lo observado, ya han sido asignadas la gran mayoría de las combinaciones de 3 letras posibles.

- No existe un método de identificación de usuarios homogéneo, ya que si bien en la mayoría se utilizan trigramas, existen casos de denominaciones con nombres propios (ejemplo : "Gustavo", "Corina", "Carlos"), o bien de iniciales del nombre más el apellido (ejemplo : "mgomez") u otros.

- Existen usuarios de carácter genérico, es decir, que no se encuentran asociados a ningún usuario en particular, con lo cual no es posible determinar al responsable de las operaciones llevadas a cabo mediante los mismos (ejemplo : trigramas ZZX - correspondiente a Context EMEXI, ZZY - correspondiente a Context CMIAM y ZZZ - Atención de Reclamos, usuarios popa3d, named, os, nobody, etc.).

Adicionalmente, como ya fuera expuesto precedentemente, no existe un procedimiento formal para la asignación de los permisos de acceso de los usuarios sustentado en la clasificación de los sistemas de información.

Recomendación :
Establecer un mecanismo de identificación de usuarios homogéneo que permita agilizar las tareas de administración de permisos e identificación de los responsables de las operaciones.
Evitar el uso de permisos genéricos.
Elaborar y documentar un procedimiento para el otorgamiento de permisos de acceso de los usuarios, considerando criterios de clasificación de los sistemas de información, el rol desempeñado por el usuario y la autorización correspondiente por parte del propietario responsable de cada sistema.

Opinión y Plan de Acción del Auditado :
"Se están diseñando para su posterior aprobación y aplicación los procedimientos de seguridad solicitados."
Fecha de Regularización Prevista : Agosto 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

5. Política de protección contra virus informáticos

Durante el relevamiento efectuado, se tuvo acceso a un documento del Ministerio denominado Política de Antivirus para Servidores y Clientes, el cual no cuenta con aprobación formal y, según lo manifestado, aún no se encuentra implementado.

La existencia de esta definición constituye un primer paso hacia la solución de la observación efectuada por esta Sindicatura previamente, respecto de que el MRECIC carecía de una política antivirus en los servidores y estaciones de trabajo.

No obstante, del análisis del citado documento surgen algunos aspectos que cabe señalar :

- Se menciona que la realización de diversos controles está siendo llevada a cabo con licencias de productos antivirus de uso limitado, ya que no se dispone de todas las licencias necesarias.

- La actualización de la versión del antivirus en las estaciones de trabajo no se realiza en forma automática, sino que es llevada a cabo por cada usuario de acuerdo a su criterio, atendiendo a los avisos e instrucciones propuestos por la Coordinación General de Informática.

- Como fuera expuesto, el esquema definido aún no se encuentra implementado, y es de carácter informal.

Recomendación :
Elaborar un proyecto que prevea la estrategia de protección contra virus del Ministerio, estableciendo las alternativas respecto de la adquisición y actualización de las correspondientes licencias. En base a esa estrategia, realizar las modificaciones necesarias en el procedimiento disponible actualmente y aprobarlo formalmente.
Implementar mecanismos de actualización automática del antivirus en las estaciones de trabajo.

Opinión y Plan de Acción del Auditado :
"Se encuentra en elaboración un proyecto para evaluar licencias disponibles y actualización de procedimientos de protección contra virus Informáticos, el que posteriormente se elevará para su aprobación formal.
Se prevé actualizar en forma automática los antivirus de las estaciones de trabajo."
Fecha de Regularización Prevista : Agosto 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

6. Plan para afrontar Contingencias

El Ministerio no posee un plan de contingencias y recuperación ante desastres que indique los procedimientos y acciones a llevar a cabo en caso de un eventual siniestro que afecte la continuidad de los servicios de procesamiento de información.

La carencia indicada podría dificultar las tareas de recuperación en caso de posibles interrupciones en el procesamiento de la información involucrada, con los consiguientes riesgos relacionados con la necesaria continuidad de los sistemas críticos (incumplimiento de misiones y funciones designadas, imagen negativa, etc.).

Recomendación
Desarrollar un plan para afrontar contingencias, para lo cual se sugiere determinar, para cada sistema de información, el tiempo aceptable de recuperación ante una eventual interrupción y elaborar el plan sobre esa base. Deben especificarse los recursos necesarios y los responsables de llevar a cabo las tareas, a efectos de asegurar la continuidad de procesamiento de los sistemas críticos.

Opinión y Plan de Acción del Auditado :
"Está en desarrollo el plan para afrontar situaciones de Contingencia en base a lo recomendado."
Fecha de Regularización Prevista : Setiembre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

7. Registros de transacciones (log)

De acuerdo a lo relevado durante la auditoría, el área informática del Ministerio mantiene diversos registros de transacciones o logs, tanto a nivel sistema operativo como para algunas aplicaciones.

No obstante, del análisis de la política de logs obtenida no surgen procedimientos y responsables para la revisión sistemática de tales registros, a efectos de determinar y analizar operaciones de excepción u operaciones no autorizadas.

Recomendación :
Se sugiere documentar y aprobar un procedimiento de revisión de los registros de transacciones implementados, que designe un responsable de su revisión periódica y establezca las actividades anómalas que deben ser analizadas e investigadas.

Opinión y Plan de Acción del Auditado :
"Se está diseñando la política de Registros de Transacciones (log) para ser aprobada formalmente con la asignación de responsables de control y detección periódico."
Fecha de Regularización Prevista : Agosto 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

8. Desactualización tecnológica

En el relevamiento se observó que gran cantidad del equipamiento informático del Ministerio responde a tecnologías obsoletas. Como ejemplo, puede mencionarse que el 40% de las computadoras poseen el sistema operativo Windows 3.11.

En el informe emitido en 2001, esta Sindicatura observó que el procesamiento de NIC Argentina se realizaba sobre una plataforma que no correspondía al volumen de transacciones y relevancia de la información procesada, encontrándose las versiones del software de base, desactualizadas, ocasionando, entre otras cosas, la falta de soporte por parte de los proveedores.

Recomendación :
Se recomienda documentar la estrategia en materia tecnológica incluyendo, entre otros aspectos, un plan de actualización gradual y continua que evite la obsolescencia de los recursos informáticos y distribuya gradualmente los costos relacionados a adquisiciones informáticas en los distintos ejercicios.

Opinión y Plan de Acción del Auditado :
"A través del plan Informático 2004 quedará establecida la estrategia gradual de actualización Tecnológica."
Fecha de Regularización Prevista : Agosto 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

9. Integración de tecnologías

Del relevamiento de las tecnologías relacionadas al procesamiento de los distintos sistemas del Ministerio, se observó que no se ha seguido una estrategia uniforme, sino que coexisten diversas plataformas de bases de datos y lenguajes de programación.

Por ejemplo, existen sistemas con las siguientes tecnologías para almacenamiento de datos : Informix 5.03, Access, MySQL, C-Isam, SQL Base.

Por su parte, se han utilizado los siguientes lenguajes de desarrollo : C, Visual Basic, HTML, PHP, Access, 4GL, SPL, Java, LPI Cobol, Centura.

Cabe destacar, no obstante, que la plataforma de sistemas operativos de los servidores es homogénea (Unix).

La situación observada puede presentar problemas de incompatibilidades, tanto desde el punto de vista de las aplicaciones como de los datos, lo cual trae aparejada una mayor complejidad en el mantenimiento y soporte técnico, y, consecuentemente, un mayor requerimiento de capacitación y recursos de personal especializado en cada una de las tecnologías.

Recomendación :
El plan informático a desarrollar deberá contemplar una estrategia formal procurando estandarizar la plataforma tecnológica del Ministerio.

Opinión y Plan de Acción del Auditado :
"A través del Plan Informático 2004 en elaboración quedará establecida la estrategia para producir la Integración de Tecnologías."
Fecha de Regularización Prevista : Setiembre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

10. Convenios con proveedores ISP (Internet Service Providers)

Durante la auditoría se relevaron los vínculos de comunicaciones existentes en el Ministerio actualmente, observándose que solo para algunos casos existen contratos que avalen la prestación de servicios en cuestión. De acuerdo a lo informado, solo existen contratos para los enlaces a internet de las firmas AT&T y Retina, y los enlaces a los edificios Cascos Blancos y Exportar de las firmas Telecom e Impsat respectivamente. Por su parte, no se tiene constancia de la existencia de contratos para las conexiones a internet con las empresas Telefónica y Telecom, o de los enlaces de los siguientes ISP : Datamarkets, Metrored, Telefónica, entre otros.

Cabe destacar que en el informe emitido por esta Sindicatura en 2001, se observó que en esa oportunidad, 7 proveedores de Internet disponían de conexiones directas con

Cancillería, de los cuales solamente 2 habían sido contratados por el Ministerio. Para los restantes casos no existían convenios ni contratos de ninguna índole, por lo cual podrían existir inconvenientes ante la necesidad de determinar responsabilidades, entre otros motivos: por la mala utilización de los vínculos mencionados o eventuales daños que podrían producirse sobre los dispositivos instalados en el centro de cómputos del MRECIC que eran propiedad de terceros.

De lo expuesto, surge que persiste la situación observada oportunamente.

Recomendación :
Regularizar la situación contractual con todos los proveedores de enlaces de comunicaciones, a efectos de garantizar que el MRECIC disponga de documentos que detallen sus derechos y obligaciones respecto de las empresas en cuestión.

Opinión y Plan de Acción del Auditado :
"Se encuentran en estudio las diferentes posibilidades técnicas para llevar a cabo la actualización de los Convenios con los distintos Proveedores ISP, y regularizar la situación."
Fecha de Regularización Prevista : Setiembre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

11. Documentación de sistemas de aplicación

Se relevó el estado de la documentación de los sistemas informáticos del Ministerio, observándose que diversas aplicaciones carecen de la misma.

Como ejemplos, pueden mencionarse casos como los sistemas Contex Central, Estadística de Comercio Exterior, Pedidos de Cooperación, etc..

Cabe considerar que oportunamente, esta Sindicatura señaló que el sistema de aplicación de NIC con el que se procesaba la información de los dominios ".ar" carecía de documentación técnica y de instructivos o manuales de operación, lo que ocasionaba dependencia hacia el personal que lo desarrolló y que se encargaba del procesamiento, dificultando las tareas de mantenimiento y de capacitación a nuevos operadores. Este aspecto no fue solucionado, ya que, según lo relevado, el sistema en cuestión aún carece de documentación.

Otro ejemplo lo constituye el sistema MovDoc, el cual es utilizado para las comunicaciones formales con las Embajadas. La información que procesa, considerada como crítica para la organización, esta compuesta entre otras cosas, por Memorandos, Circulares y número de cuentas en donde se depositan los sueldos del personal del exterior. Las transmisiones de información se realizan en forma encriptada, utilizándose un algoritmo propio del Ministerio. Cabe señalar, que las características del citado algoritmo no se encuentran documentadas y, según lo manifestado, dada su antigüedad, el personal encargado del mantenimiento del sistema, no conoce detalles de su funcionamiento. Al respecto, cabe cuestionar si los mecanismos de encriptación en cuestión permiten asegurar la confidencialidad e integridad de las comunicaciones.

Recomendación :
Desarrollar un plan para documentar todos los sistemas aplicativos en uso en el Ministerio, designando responsables y plazos para cada caso.
Evaluar los mecanismos utilizados actualmente para encriptar las comunicaciones, analizando si se adecuan a los estándares internacionalmente aceptados, así como su confiabilidad.

Opinión y Plan de Acción del Auditado :
"Se encuentra en elaboración, el plan para la Confección de la Documentación Técnica de los Sistemas Aplicativos.
Se realizará el estudio comparativo del Sistema de Encriptación de Comunicaciones respecto de los estándares Internacionales."
Fecha de Regularización Prevista : Diciembre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

12. Sistema de gestión financiera

De acuerdo a lo relevado, el Ministerio aún se encuentra utilizando el Sistema Conpre (Contabilidad Presupuestaria) para la gestión financiera.

El sistema en cuestión, fue desarrollado por la Secretaría de Hacienda del Ministerio de Economía, para registrar las operaciones financieras y presupuestarias de los distintos organismos, datos que después son compilados por esa Secretaría en el SIDIF Central (Sistema de Información Financiera Central).

El sistema Conpre ha sido reemplazado por nuevas versiones denominadas SIDIF AC (Sistema de Información Financiera para la Administración Central) y más recientemente por el SLU (Sistema Local Único). Estas nuevas versiones incorporan funciones, controles y validaciones que no se encontraban implementadas en la anterior versión Conpre.

Según lo relevado, se está analizando conjuntamente con la Secretaría de Hacienda, la implementación de la nueva versión del sistema.

Recomendación :
Considerando la envergadura de las operaciones financieras y presupuestarias del Ministerio, se sugiere priorizar la implementación de la nueva versión del sistema en cuestión, a efectos de asegurar la realización automatizada de controles y validaciones sobre las operaciones financieras y presupuestarias.

Opinión y Plan de Acción del Auditado :
"La Dirección General de Administración de Cancillería ya ha solicitado a la Secretaría de Hacienda la implementación del sistema SLU. Durante el último trimestre del año pasado se llevaron a cabo reuniones con técnicos de la mencionada Secretaría de Estado, en particular con el equipo de réplica de SLU, con el fin de analizar los elementos a tener en cuenta para dicha instalación, detectándose como un factor relevante las gestiones en múltiples monedas extranjeras que debe realizar la Cancillería en atención a sus particularidades operativas. Esta problemática está siendo evaluada por especialistas de la mencionada Secretaría de Estado."
Fecha de Regularización Prevista : No especificada

Comentario Final de SIGEN :
Atento a la situación actual, se sugiere intensificar las tareas llevadas a cabo conjuntamente con los especialistas de la Secretaría de Hacienda, a efectos de priorizar la automatización de los controles en los procesos presupuestarios y financieros.

13. Falta de solución de observaciones previas

Tal como fuera expuesto en diversos de los puntos precedentes, se ha observado que el Ministerio no ha encarado suficientes acciones tendientes a solucionar los hallazgos volcados en el Informe SIGEN de octubre de 2001 sobre NIC Argentina y en el Informe de la UAI de octubre de 2002 elaborado de acuerdo a lo solicitado en la Circular 01/ 02-SGN.

Recomendación :
Elaborar un plan de acción para la solución de las observaciones formuladas al organismo en las distintas auditorías, designando responsables y plazos para su cumplimiento.

Opinión y Plan de Acción del Auditado :
"Se desarrollará un plan de acción para dar atención a las observaciones de las auditorías SIGEN 2001 y UAI 2002."
Fecha de Regularización Prevista : Diciembre 2004

Comentario Final de SIGEN :
No se formulan nuevos comentarios dado que el plan de acción definido por el auditado, recoge la recomendación de esta Sindicatura.

V. CONCLUSIÓN

De la evaluación practicada surgió que el Ministerio presenta falencias de control en lo que respecta a la gestión de la tecnología informática, visibles principalmente en la existencia de diversas áreas informáticas no unificadas, en la ausencia de un plan informático estratégico, en la falta de procedimientos y metodologías adecuados y suficientes para las actividades ejecutadas, en las debilidades en la seguridad informática, en la carencia de un plan de contingencias orientado a garantizar la continuidad de las operaciones, como así también en la ausencia de respaldo documental de los sistemas aplicativos.

En otro orden, se verificó la ausencia de un tratamiento suficiente al informe emitido por esta Sindicatura General de la Nación en octubre de 2001 respecto del proyecto NIC Argentina, por lo cual persisten la mayoría de los hallazgos señalados en esa oportunidad.

A partir de la presente revisión, el área auditada ha elaborado un plan de acción estableciendo las tareas y plazos para la solución de los aspectos observados, por lo que se recomienda establecer un procedimiento de monitoreo y control que permita detectar y corregir desvíos y asegure su cumplimiento.

En función a los hallazgos relacionados con la falta de cumplimiento de la recomendaciones efectuadas por esta Sindicatura General de la Nación en el informe emitido en octubre de 2001 y en la carencia de algunas licencias de productos antivirus, que puede configurar la conducta prevista y reprimida por el art. 71 de la ley 11.723 de Régimen de Propiedad Intelectual, se deberá realizar el pertinente deslinde de responsabilidad.

Buenos Aires, 16 de abril de 2004

ANEXO I :

ASPECTOS A CONSIDERAR EN EL PROCEDIMIENTO PARA REGULARIZAR LA GESTIÓN DEL SOFTWARE BAJO LICENCIA

1. Elaborar el inventario de licencias y el relevamiento de los productos efectivamente instalados en las máquinas del organismo.
2. Paralelamente, efectuar un relevamiento de los productos que realmente necesitan cada uno de los usuarios.
3. Comparar las licencias disponibles con las necesidades justificadas por los usuarios. Luego distribuir las licencias disponibles.
4. Proceder a eliminar todas las copias ilegales de software surgidas del relevamiento realizado previamente y activar la compra de aquellas que por razones operativas no puedan ser borradas.
5. Emitir una política de utilización de software con licencia para informar a los usuarios sobre sus responsabilidades y establecer las normas respecto del uso de software.
6. Emitir un memorando para obtener el compromiso de los empleados respecto de la utilización de software con licencia.

Establecer un procedimiento para el control permanente de esta situación, que comprenda la realización de auditorías periódicas sobre el tema.