SESIONES EXTRAORDINARIAS

2016

ORDEN DEL DÍA Nº 1244

Impreso el día 15 de diciembre de 2016
Término del artículo 113: 26 de diciembre de 2016

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas para regularizar las situaciones observadas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Ministerio del Interior y Transporte, cuyo objeto fue el análisis de la gestión informática en la Dirección Nacional de Migraciones (DNM). (265-S.-2016.)

Buenos Aires, 2 de noviembre de 2016.

Al señor presidente de la Honorable Cámara de Diputados de la Nación.

Tengo el honor de dirigirme al señor presidente, a fin de comunicarle que el Honorable Senado, en la fecha, ha sancionado el siguiente

Proyecto de resolución

El Senado y la Cámara de Diputados de la Nación

RESUELVEN:

1) Dirigirse al Poder Ejecutivo nacional solicitándole informe sobre las medidas adoptadas para regularizar las situaciones observadas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Ministerio del Interior y Transporte, cuyo objeto fue el análisis de la gestión informática en la Dirección Nacional de Migraciones (DNM).

2) Comuníquese al Poder Ejecutivo nacional y a la Auditoría General de la Nación, juntamente con sus fundamentos.

Saludo a usted muy atentamente.

FEDERICO PINEDO.
Juan P. Tunessi.

FUNDAMENTOS

La Auditoría General de la Nación (AGN), por resolución AGN 172/15, efectuó un examen en el ámbito del Ministerio del Interior y Transporte, cuyo objeto fue el análisis de la gestión informática en la Dirección Nacional de Migraciones (DNM).

Período auditado: del 1°/1/13 al 30/6/14. Las tareas de campo se desarrollaron de marzo a septiembre/14.

La AGN, en el apartado "Alcance del examen", señala que el examen fue realizado de conformidad con las normas de auditoría externa de la misma, aprobadas por la resolución 145/93, dictadas en virtud de las facultades conferidas por el artículo 119, inciso *d)* de la ley 24.156.

La tarea abarcó el nivel de controles aplicados a la tecnología informática (TI) en la DNM en base a la información obtenida, a la identificación de los temas de mayor exposición al riesgo, y a las pruebas sustantivas y de cumplimiento realizadas. Asimismo, se enfocó en el marco de trabajo de TI del organismo, con énfasis en las aplicaciones de control migratorio (SICAM + Sigeram) y de regularización de la residencia de extranjeros (SADEX), debido a la importancia que revisten para el cumplimiento de la función del organismo.

La AGN se basó en la verificación de los objetivos de control establecidos por el marco de referencia de buenas prácticas de TI COBIT (Control Objectives in Information Technologies) versión 4.1.

La AGN, en el apartado "Aclaraciones previas", realiza una breve descripción del contexto general de las migraciones; de la Dirección Nacional de Migraciones, sus misiones y funciones, y su organización institucional; de los sistemas de información de la misma: Sigeram v7 (Sistema de Gestión de Registro de Aptitud Migratoria), SICAM (Sistema Integral de Captura Migratoria) y SADEX (Sistema de Admisión de Extranjeros).

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

1. Planificar y organizar

1.1. Definir un plan estratégico para TI

Observaciones: en febrero de 2012 se aprobó un plan de tecnologías de la información 2012-2014, elabora-

do a partir de una evaluación realizada por la propia DGSyTI, y en función del lineamiento estratégico de la Dirección Nacional orientado a tomar el control administrativo sobre los pasos fronterizos administrados por otros organismos (Prefectura Naval Argentina, Gendarmería Nacional) o a mejorar la infraestructura de TI. También se plantea la actualización de la infraestructura de *data center* con una contratación llave en mano (2012-2014), el rediseño de la página web, mantenimiento de sistemas aplicativos SADEX, SICAM, Sigeram, SACER, capacitaciones con aula virtual, a los usuarios, innovación en materia de digitalización, tecnologías biométricas e infraestructura de firma digital. En tal sentido, cabe señalar que el plan de TI 2012-2014 no cuenta con los planes tácticos que lo respalden, donde se detallen tiempos, recursos afectados, costos, hitos intermedios a alcanzar o riesgos relacionados, que permitan inferir cómo se lograrán los objetivos planteados. Al cierre de trabajos de campo de la auditoría, habían transcurrido veinticinco meses desde su última actualización.

Nivel de riesgo: alto. Nivel de madurez: repetible.

1.2. Definir la arquitectura de información

Observaciones: la DGSyTI estableció un modelo no formalizado de arquitectura de la información. En ese sentido, se establecieron algunas pautas en cuanto al desarrollo de los aplicativos (siempre desarrollos propios) y el equipamiento que se distribuyó a lo largo del país en la red propia de datos. No obstante, no se formalizó el modelo, como tampoco se definieron formalmente pautas que aseguren la integridad y la consistencia de toda la información almacenada, tales como un diccionario de datos de la organización, un esquema de clasificación de datos de acuerdo a la criticidad y la sensibilidad, los procedimientos para definir datos nuevos y esquemas de funciones estándar de tratamiento de los datos (biblioteca de funciones). La propiedad de los datos y de los sistemas no se encuentra formal y claramente definidas.

Nivel de riesgo: alto. Nivel de madurez: repetible.

1.3. Determinar la dirección tecnológica

Observaciones: la Dirección General de Sistemas y Tecnologías de la Información ha implementado una infraestructura tecnológica en los puestos de control de migraciones y en delegaciones migratorias del país consistente en una red de comunicaciones con enlaces punto a punto y aplicaciones específicas desarrolladas e implementadas internamente. Adicionalmente, cuenta con una red de celulares corporativos para uso del personal. No obstante, no se tuvo a la vista documentación respaldatoria de las decisiones sobre la infraestructura tecnológica y los estándares adoptados.

Falta un plan de infraestructura que esté de acuerdo con los planes estratégicos y tácticos de TI alineados con los de la organización, con establecimiento de estándares, dirección tecnológica, un planeamiento de la capacidad instalada y las posibles necesidades futuras. La organización utiliza los Estándares Tecnológicos para la Administración Pública (ETAP) solamente para las adquisiciones. En el caso de las versiones de SICAM con servidor local, el motor de base de datos se encuentra sin soporte técnico por parte del fabricante del producto. Esta situación podría comprometer la continuidad del servicio brindado por el aplicativo en caso de una falla imprevista.

Nivel de riesgo: alto. Nivel de madurez: repetible.

1.4. Definir los procesos, organización y relaciones de TI

Observaciones: al momento de los trabajos de campo, se encontraba aprobada la estructura organizativa hasta el tercer nivel operativo del organismo (dirección general, direcciones –anteriormente denominadas coordinaciones–, y departamentos). Adicionalmente, la segregación de tareas, roles y responsabilidades se encuentran definidos. No obstante, el organigrama no contempla posiciones importantes como administración de proyectos, aseguramiento de la calidad, seguridad (física y lógica), monitoreo de la infraestructura y gestión de riesgos, entre otras. Asimismo, la administración de la seguridad no está definida en el organigrama. Ante su ausencia, la función está asignada a funcionarios de diversas áreas, dependiendo del ámbito de aplicación: en el caso de los vínculos de comunicaciones, y accesos a la red, las tareas las lleva a cabo el Departamento de Enlaces y Comunicaciones; para acceso y seguridad de servidores, la responsabilidad recae en el Departamento de Tecnología, mientras que los accesos a las aplicaciones corresponden al Departamento de Soporte Operativo. Por último, cabe destacar que el representante de la seguridad de la información ante el Comité de Seguridad de la Información, es el director de Aplicaciones Informáticas, lo cual vulnera el control por oposición.

En relación a la infraestructura de TI, a cuyo cargo se encuentra la Dirección de Tecnología y Comunicaciones, y dada la expansión geográfica a la que se vio sometida el organismo producto de la disposición DNM 2.980/2013, la misma, además de una dotación interna, cuenta con referentes informáticos (RI) en el interior del país que llevan a cabo tareas de soporte técnico solicitadas desde la administración central. Considerando que estos agentes deben desplazarse físicamente hasta el lugar del incidente para proceder a su solución in situ, cabe señalar que, en algunos casos, los RI son insuficientes (las regiones VI y IX) y en otros inexistentes (región VIII y las provincias de Córdoba, La Pampa, San Luis y Tucumán) para garantizar la continuidad del servicio.

Sobre el rol de cada RI cabe destacar que:

– No se encuentran definidas formalmente ni las misiones ni las responsabilidades de la función. Su dependencia funcional no está claramente definida por cuanto debe responder a su mando superior (delegado, coordinador de la región, encargado del PCF y otros) y a las directivas emanadas por la DGSyTI.

– En la mayoría de las zonas asignadas, son las únicas personas a cargo de esta tarea, con lo cual existe una dependencia crítica ante su eventual ausencia.

– Algunos agentes se encuentran bajo una modalidad contractual no compatible con la criticidad de sus responsabilidades.

– En algunos casos deben recorrer distancias que en tiempo superan la mitad del horario de atención al público o tienen más de 40 puestos de trabajo para atender o la dotación no les permite solucionar más de un incidente en la misma jornada laboral.

– No pueden realizar un programa preventivo que evite una posible discontinuidad del servicio.

Nivel de riesgo: alto. Nivel de madurez: parcialmente definido.

1.5. Administrar la inversión en TI

Observaciones: la asignación presupuestaria de los recursos de TI no está imputada a las áreas usuarias de los servicios de TI, sino a la Dirección General de Sistemas y Tecnología de la Información (DGSyTI).

Falta la implementación a nivel de la organización de un enfoque orientado a la administración por centros de costos de los recursos de TI. Dentro de este marco de trabajo, la DGSyTI no presenta un proceso presupuestario propio de los programas de inversión de TI incluyendo los costos de operar y mantener la infraestructura actual. Este proceso debería permitir su monitoreo para determinar la contribución esperada de TI a los objetivos estratégicos del organismo.

En relación a la formulación presupuestaria, el presupuesto total del organismo se incrementó en un 37,53 % en términos nominales entre 2012 y 2013; sin embargo, la inversión en TI prevista, se mantuvo constante en términos nominales pero se redujo en términos porcentuales del 6,08 % en 2012 al 4,42 % en 2013 (en relación al presupuesto total del organismo).

Nivel de riesgo: medio. Nivel de madurez: repetible.

1.6. Comunicar las aspiraciones y la dirección de la gerencia

Observaciones: el ambiente de control de TI es incompleto. Existen algunas disposiciones pero no todas se cumplen. Faltan políticas formalizadas del ambiente de control que se puedan tomar como marco de referencia y que sean parte de un programa de comunicación continua al personal relevante, referidas a Planificación de Proyectos y su seguimiento, Programa de Aseguramiento de la Calidad, Administración de riesgos, y Documentación en general, que tenga como objetivo maximizar la entrega de valor de TI a los objetivos estratégicos del organismo, mientras se minimizan los riesgos.

Nivel de riesgo: medio. Nivel de madurez: repetible.

1.7. Administrar los recursos humanos de TI

Observaciones: la ley 25.164, Ley Marco de Regulación de Empleo Público Nacional, determina diferentes modalidades de contratación: con sujeción al régimen de estabilidad, con sujeción al régimen de contrataciones por tiempo determinado, y con sujeción al régimen para el personal de gabinete o ad honórem. La DNM adhiere al Convenio Colectivo General para la Administración Pública Nacional (decreto 214/2006).

Al momento de los trabajos de campo, en el organismo el 89,55 % del personal pertenece a la planta transitoria. En este orden, el personal de la DGSyTI en su mayoría es contratado bajo la modalidad "transitorio/permanente". La perpetuidad en esta modalidad de contratación, pensada para situaciones transitorias o estacionales, desvirtúa la naturaleza jurídica de la misma, provocando situaciones desfavorables para los agentes dentro del organismo. La percepción del plus informático sólo es exclusiva del personal de planta permanente. La falta de personal y de formalización de los marcos de trabajo (políticas, procedimientos, documentaciones varias) genera una alta exposición a dependencias críticas sobre individuos clave.

Nivel de riesgo: medio. Nivel de madurez: repetible.

1.8. Administrar la calidad

Observaciones: no existen políticas ni un sistema de administración de calidad relacionado con TI que establezca estándares para medirla y monitorearla. Esto impide identificar desviaciones, aplicar acciones correctivas (en caso de detectarlas), informar a los usuarios involucrados y conocer la entrega de valor de TI a los objetivos estratégicos del organismo.

Nivel de riesgo: medio. Nivel de madurez: inicial.

1.9. Evaluar y administrar los riesgos de TI

Observaciones: no existe un marco de administración de riesgos que permita identificarlos para tomar una acción para prevenirlos, asumirlos, mitigarlos, evitarlos o resolverlos en caso de un incidente, cuantificando costos y probabilidades de ocurrencia. Informalmente los riesgos tecnológicos se conocen, pero falta la formalización del contexto de riesgo y su evaluación formal de manera tal de contemplar las fortalezas, las oportunidades, las debilidades y las amenazas. El organismo se encuentra expuesto a la ocurrencia de hechos inesperados que pueden generar perjuicios, sin que estén analizadas las medidas a tomar para cada caso.

Nivel de riesgo: alto. Nivel de madurez: inicial.

1.10. Administrar proyectos

Observaciones: se ha formalizado un manual de procedimientos de proyectos informáticos, pero no se lo aplica en todos los casos.

El marco de trabajo actual no permite inferir cómo se abordan aspectos tales como costos, plazos, hitos a cumplir, alcance, recursos afectados; parámetros definidos en el sistema de administración de la calidad; el control de cambios de modo tal que todas las modificaciones a la línea base se revisen, aprueben e incorporen al plan integrado de acuerdo al marco de

trabajo; el monitoreo del desempeño contra los criterios clave previamente definidos en el sistema de calidad.

Nivel de riesgo: medio. Nivel de madurez: repetible.

2. Adquirir e implementar

2.1. Identificar soluciones automatizadas

Observaciones: se ha formalizado un Manual de Procedimientos de Proyectos Informáticos (MPPI) que contempla etapas del ciclo de vida de desarrollo de sistemas, tales como: la administración de los requerimientos, estudios de factibilidad, evaluación de los distintos cursos alternativos posibles de acción, análisis de riesgo, asignación de prioridades, recursos y consentimiento de los usuarios relevantes, pero no se aplica en todos los casos.

En el MPPI, contempla un formulario estándar para realizar un requerimiento a ser evaluado, pero no siempre se lo utiliza en la práctica. Otros medios tales como correo electrónico, notas u otros suelen ser también admitidos para cambios considerados menores. Falta establecer un marco de trabajo que sirva para la administración de requerimientos informáticos, que permita organizarlos, clasificarlos, otorgar prioridades, asignar recursos y calcular costos. Las áreas solicitantes o usuarias participan en la etapa de prueba sin quedar registros de ello, ya que no hay un procedimiento que determine cómo se documentarán las mismas.

Nivel de riesgo: medio. Nivel de madurez: parcialmente definido.

2.2. Adquirir o desarrollar y mantener software aplicativo

Observaciones: se ha formalizado un Manual de Procedimientos de Proyectos Informáticos (MPPI) que contempla cuestiones que hacen a esta etapa del ciclo de vida de desarrollo de sistemas (CVDS) incorporando documentaciones tales como: alcance, requerimientos, diseño, pruebas, e implementación, pero no se aplica en todos los casos y el marco de trabajo es incompleto, ya que no se definieron estándares de documentación como los protocolos de aceptación a aplicar en cada etapa. Por lo tanto, se infiere que es una formulación de una política a aplicar pero no un manual de procedimiento.

A falta de un sistema de administración de calidad (SAC), no se realiza gestión de aseguramiento de ésta en las distintas etapas del CVDS.

En relación al control y la posibilidad de auditar los desarrollos de aplicaciones, existe un débil cumplimento de la política formulada, sumada a la falta de especificidad de ésta en temas tales como: la documentación en las distintas etapas de los proyectos, reportes de seguimiento, pistas de auditoría, el control del código fuente, mediciones sobre la satisfacción de usuarios y una definida metodología de desarrollo.

La documentación existente se encuentra desactualizada e incompleta. La falta de un entorno de desarrollo integrado permite que existan redundancias o inconsistencias de datos. No está definido el marco de trabajo de los pases de entorno de desarrollo, a pruebas, y de ésta última a producción.

Nivel de riesgo: alto. Nivel de madurez: inicial.

2.3. Adquirir y mantener infraestructura tecnológica

Observaciones: no hay un plan de infraestructura tecnológica que considere aspectos tales como adquisiciones, implementaciones, planeamiento de la capacidad para necesidades futuras, costos de transición, riesgo tecnológico y vida útil de la capacidad existente como contribución de TI para alcanzar los objetivos estratégicos del organismo.

Los sistemas principales están sostenidos por una infraestructura tecnológica instalada en los diferentes pasos fronterizos, delegaciones y administración central conectados a través de una red MPLS (Multi-Protocol Label Switching) para intercambio de datos. Esta infraestructura comprende la administración de 62 servidores en sede central, 111 servidores en el interior del país, switches, estaciones de trabajo, impresoras y *scanners*.

No hay un plan de mantenimiento preventivo sobre la infraestructura detallada del equipamiento instalado en los distintos puntos mencionados anteriormente, en base a un diagnóstico previo que incluya las garantías de los proveedores de tecnología. Otro aspecto relevante es la ausencia de un sistema de stock y registro de repuestos.

Nivel de riesgo: alto. Nivel de madurez: inicial.

2.4. Facilitar la operación y el uso

Observaciones: existen manuales de usuario y hay coordinación con las áreas de Recursos Humanos para la capacitación del usuario final. Sin embargo, para los casos de cambios o actualizaciones de los aplicativos, falta un procedimiento que determine la forma en que el usuario tome conocimiento. En ese sentido, la comunicación de cambios es informal. En relación a la transferencia de conocimientos al personal de operaciones y soporte, se basa en información de calidad variable no estandarizada.

Nivel de riesgo: medio. Nivel de madurez: parcialmente definido.

2.5. Adquirir recursos de TI

Observaciones: el organismo cumple con las normas jurídicas correspondientes al Régimen de Contrataciones de la Administración Pública Nacional. Sin embargo, falta formular un marco de trabajo que permita medir el grado de cumplimiento de los contratos y que en relación a este análisis, contribuya a mejorar, modificar o concluir contratos que apliquen a todos los proveedores, que abarque: responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, así como obligaciones y cláusulas de penalización por incumplimiento cuando no cumplan los acuerdos de niveles de servicios previamente establecidos.

Nivel de riesgo: medio. Nivel de madurez: parcialmente definido.

2.6. Administrar cambios

Observaciones: no hay procedimientos formales para la administración de cambios que establezcan un tratamiento estandarizado de todas las solicitudes de mantenimiento y actualizaciones, en aplicaciones, procesos, servicios y parámetros de sistema. Tampoco existe un procedimiento alternativo y formal para atender situaciones de emergencia. Cuando se realizan cambios o actualizaciones no se genera la documentación pertinente. Pueden surgir errores a partir de cambios no autorizados y/o no probados a los sistemas de información. No se ha contemplado el tratamiento de cambios producidos por cuestiones no funcionales, tales como cuestiones técnicas (performance y otros) o de seguridad.

Nivel de riesgo: alto. Nivel de madurez: inicial.

2.7. Instalar y acreditar soluciones y cambios

Observaciones: se ha formalizado un Manual de Procedimientos de Proyectos Informáticos (MPPI) que contempla cuestiones que hacen a esta etapa del ciclo de vida de desarrollo de sistemas (CVDS) con documentaciones tales como: alcance, requerimientos, diseño, pruebas, e implementación, pero no se aplica en todos los casos. Además, el marco de trabajo es incompleto, ya que no se encuentran definidos los estándares de documentación, como los protocolos de aceptación a aplicar en cada etapa. En consecuencia, el manual constituye una política a implementar más que un catálogo de procedimientos.

No existe un marco de trabajo (procedimientos formales) para realizar las pruebas donde estén definidos los roles, responsabilidades y criterios aceptados. La política establecida en el MPPI sugiere la posibilidad de pasar del entorno de desarrollo al de producción, sin pasar por el de pruebas.

Por otra parte, las pruebas se llevan a cabo mediante la duplicación de datos, sin que se tomen los debidos recaudos para enmascarar o convertir los datos sensibles sobre las personas. Tampoco se especifica quiénes son los responsables del pasaje de las aplicaciones y los datos entre los distintos entornos (desarrollo, prueba y producción).

Nivel de riesgo: alto. Nivel de madurez: repetible.

3. Entregar y dar soporte

3.1. Definir y administrar los niveles de servicio

Observaciones: existe un marco de trabajo que define formalmente los niveles de servicio entre el usuario y la DGSyTI. Dicho marco mantiene una alineación con los requerimientos y las prioridades del organismo y facilita el entendimiento común. El marco cuenta con definiciones de servicio, acuerdos de niveles de operación (especificaciones técnicas del servicio a recibir), las fuentes de financiamiento y los acuerdos de niveles de servicio. No incluye, sin embargo, procesos para la creación de futuros requerimientos de servicio.

No hay personal dedicado al seguimiento del cumplimiento de la prestación del servicio, ni una política y procedimientos específicos sobre qué hay que medir (disponibilidad, desempeño, carga de trabajo, capacidad), ni las acciones que se deben tomar con el propósito de minimizar el riesgo de interrupciones. Estos atributos no están organizados en un catálogo de servicios.

Nivel de riesgo: medio. Nivel de madurez: inicial.

3.2. Administrar servicios de terceros

Observaciones: no existe un marco de trabajo para administrar los servicios de terceros. Esto comprende la formalización del proceso de administración de relaciones con proveedores, su clasificación y el monitoreo de la prestación brindada en base a los niveles de servicio acordados.

No hay personal dedicado a esta función, para asegurar que el proveedor está cumpliendo con los requerimientos convenidos y que adhiere continuamente a los acuerdos del contrato.

En relación a mantener un efectivo servicio de entrega en forma segura, no se encuentran identificados los riesgos de no cumplimiento, lo que no permite definir las acciones a seguir con el fin de mitigarlos.

Nivel de riesgo: alto. Nivel de madurez: inicial.

3.3. Administrar el desempeño y la capacidad

Observaciones: la planeación del desempeño y la capacidad es intuitiva. No resulta de un proceso de monitoreo de la infraestructura de TI presente y su proyección futura.

No hay personal dedicado al monitoreo de la infraestructura, ni una política y procedimientos específicos sobre lo que hay que medir (disponibilidad, desempeño, carga de trabajo, capacidad), ni la fijación de acuerdos de nivel de servicios, ni las acciones que se deben tomar para balancear la carga de trabajo, dar prioridad a ciertas tareas o reasignar de recursos con el propósito de minimizar el riesgo de interrupciones del servicio.

No se elaboran informes de control asociados entre la capacidad y el desempeño. Éstos se transmiten a través de canales informales (reuniones de evaluación entre los equipos de la Dirección de Tecnología y Comunicaciones y la Dirección de Aplicaciones Informáticas). Esta situación no permite planificar con precisión las necesidades futuras, ni tomar acciones preventivas para evitar la degradación del servicio ante los posibles incrementos en la demanda.

Nivel de riesgo: alto. Nivel de madurez: repetible.

3.4. Garantizar la continuidad del servicio

Observaciones: no existe un plan de contingencia formalizado que garantice la continuidad de servicios de TI diseñado para reducir el impacto de la interrupción

de procesos críticos. La disposición DNM 19.057 del 9/5/06 instruye sobre la garantía que debe existir en la continuidad del servicio y la necesidad de la existencia de un plan de contingencia, pero al momento de los trabajos de campo dichos planes no se habían formalizado para la administración central. Tampoco hay planes de contingencia formalizados en las delegaciones y en los puestos de control fronterizos. El organismo no se encuentra preparado ante el riesgo de acontecimientos no previstos que pudieran ocasionar la interrupción de los servicios.

Nivel de riesgo: alto. Nivel de madurez: inicial.

3.5. Garantizar la seguridad de los sistemas

Observaciones: el organismo no ha definido la administración de Seguridad a un nivel jerárquico apropiado que permita, a partir de roles y responsabilidades adecuadamente definidos, el establecimiento de un marco de trabajo de manera tal de mantener la integridad de la información y de la infraestructura de procesamiento, así como minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

La función del responsable de seguridad no está formalmente definida en el organigrama del organismo. Actualmente está a cargo de un funcionario afectado a otras tareas críticas e incompatibles con esta función. Esta superposición de tareas también produce que el responsable de seguridad no participe ni esté comunicado en la definición y autorización de los accesos de los usuarios.

De tal modo se debilitan los aspectos centrales que refieren a la seguridad y eficiencia, derivando en la falta de desarrollo o mejora de procedimientos específicos de control tales como: derechos de acceso y sus perfiles, la existencia única de ingreso a la red y aplicativos por parte de los usuarios, la definición del responsable de los datos e información almacenada en las bases de datos, revisiones de las cuentas y privilegios, inhabilitación de tiempo sin actividad, *testing* de penetración, uso de puertos USB, entre otros.

Los "Términos y condiciones de uso" que se encuentran en la página web institucional refieren al acceso a los diversos sistemas, y plasma recomendaciones para el uso de las cuentas de usuarios, explicita las mejores prácticas en el uso de correo electrónico y realiza recomendaciones para evitar el *phishing*. No obstante, falta formalizar la lectura y consentimiento del usuario.

A pesar de la integración en 2006 del Comité de Seguridad Informática, aún no se han generado informes de control referentes a la seguridad lógica o accesos indebidos a la red, tanto de usuarios comunes como de personal de la DGSyTI.

En cuanto a los servidores Linux, su administrador está designado en el Departamento de Enlace y Comunicaciones siendo que la responsabilidad por la administración de los servidores recae sobre el Departamento de Tecnología.

De las pruebas realizadas sobre el servidor de producción donde está alojada la página web institucional, se verificó la existencia de los siguientes perfiles de usuarios: desarrolladores de aplicaciones con perfiles de administrador de base de datos en el ambiente de producción, genéricos con perfil administrador de base de datos con acceso al ambiente de producción, y otros usuarios genéricos.

Nivel de riesgo: alto. Nivel de madurez: repetible.

3.6. Identificar y asignar costos

Observaciones: no hay un marco de trabajo de administración por centro de costos, en función del uso de TI para cada una de las dependencias del organismo, que esté alineado con los procedimientos de contabilización y medición financiera que incluya costos directos, indirectos, fijos y variables, y que garantice que los cargos para los distintos servicios sean identificables para su monitoreo.

El aplicativo contable en uso (SIDIF) no prevé una clasificación de cuentas específica para las partidas aplicadas a TI. En consecuencia, se debe recurrir a procesos manuales por fuera de este sistema para obtener la información que las refleje. En el caso del Sistema de Patrimonio, se identificó equipamiento fuera de uso y pendiente de baja asignados a TI, lo que brinda información inexacta sobre los activos asignados al área.

Nivel de riesgo: medio. Nivel de madurez: inicial.

3.7. Educación y capacitación de los usuarios

Observaciones: la planificación de la capacitación se lleva a dos niveles: hay un Plan Anual de Capacitación (PAC) que forma parte de un Plan Estratégico de Capacitación Trianual (PEC). Las necesidades que exponen las distintas direcciones del organismo constituyen parte del PAC. El criterio de elección de los cursos a ser brindados es definido por el Área de Capacitación y de la Dirección de Recursos Humanos. En relación a la capacitación de las aplicaciones informáticas, los conocimientos son impartidos por analistas funcionales de la Dirección General de Sistemas y Tecnologías de Información.

Nivel de riesgo: medio. Nivel de madurez: definido.

3.8. Administrar la mesa de servicio y los incidentes

Observaciones: no existe un marco estructurado y formalizado para el tratamiento de incidentes. La atención se encuentra concentrada en la administración central. Para incidentes en el interior (delegaciones, puestos fronterizos) que requieran la presencia física de personal técnico, se dispone de una estructura conformada con personal de estas características a nivel de las nueve regiones en las que se encuentra dividido el país. Los requerimientos llegan por distintos medios: correos electrónicos, llamados telefónicos, notas y otros. Se cargan en una planilla de cálculo y se procede a derivar al personal correspondiente.

Nivel de riesgo: medio. Nivel de madurez: inicial.

3.9. Administrar la configuración

Observaciones: los bienes de TI se registran parcialmente a través de un Sistema de Patrimonio de uso exclusivo de la Dirección General de Administración y que abarca solamente bienes adquiridos a terceros con recursos presupuestarios, aunque no las licencias de software. Paralelamente, la DGSyTI mantiene información similar en una planilla de cálculo, sin acceso al sistema de patrimonio antes mencionado. En esta planilla de cálculo se registran los servidores centrales, como así también los que están en los pasos fronterizos. En el caso específico de las estaciones usadas para control migratorio se asigna la responsabilidad patrimonial a cada delegación local. En este sentido, también está a su cargo el mantenimiento, reparación y reconfiguración del equipo por parte de los informáticos locales. Sin embargo, no está previsto algún procedimiento que registre el evento, justifique la acción sobre el equipo y el eventual reemplazo de componentes internos. No existe un sistema de control de stock de repuestos a nivel central, con control de la DGSyTI.

No se constató que se mantenga una biblioteca de las aplicaciones desarrolladas internamente como parte de los activos organizacionales de TI.

Nivel de riesgo: alto. Nivel de madurez: inicial.

3.10. Administración de problemas

Observaciones: el proceso de resolución de problemas no se encuentra bajo un marco estructurado y formalizado para su tratamiento. Al igual que para el caso del tratamiento de incidentes, faltan procedimientos aprobados formalmente que contemplen las distintas etapas de la administración de problemas: evaluación de impacto, asignación de prioridad, escalabilidad, tratamiento, rastreo, resolución, conformidad de usuario y monitoreo.

Nivel de riesgo: alto. Nivel de madurez: inicial.

3.11. Administración de datos

Observaciones: falta formalizar un marco de trabajo para administrar datos. Las tareas se llevan a cabo en forma intuitiva. No existen procedimientos formalizados para administrar las bibliotecas de medios de almacenamiento, respaldo, retención, recuperación y eliminación de datos; resguardar la seguridad en relación al recibo, procesamiento, almacenamiento y salida de datos, para que cumpla con las políticas de seguridad de la organización y los requerimientos regulatorios; determinar una clasificación por criticidad, impacto o requerimientos de seguridad alineados al plan de continuidad.

Nivel de riesgo: alto. Nivel de madurez: repetible.

3.12. Administración del ambiente físico

Observaciones: se hace necesario diferenciar en este punto entre la situación del Centro de Procesamiento de Datos de la Administración Central y los servidores locales y controladores de comunicaciones instalados en los distintos puntos del país. En cuanto a los últimos, se presentan diversos problemas producto de que deben funcionar en emplazamientos antiguos, de baja calidad de mantenimiento, sin las dimensiones apropiadas y, en algunos casos, compartiendo el espacio con agentes de la Dirección Nacional de Aduanas y el Servicio Nacional de Sanidad y Calidad Agroalimentaria (SENASA). Se presentan también circunstancias en las cuales las instalaciones edilicias son suministradas por organismos de migraciones de los países fronterizos. En ese sentido, el ambiente de TI presenta vulnerabilidades que en ocasiones están sujetas a decisiones multijurisdiccionales.

Las principales observaciones de algunos PCF visitados son:

– Cortes de energía. Gran parte se encuentran sometidos a cortes de energía frecuentes. En tal sentido, no todos tienen instalación eléctrica apropiada que cumpla con las normas y reglamentaciones de seguridad, como la existencia de llaves térmicas y disyuntores. No se estableció un estándar para las instalaciones eléctricas. Se observaron elementos en mal estado, empalmes inapropiados y la existencia de prolongadores. Tampoco tienen grupo electrógeno propio que permita la continuidad de la operatividad de los aplicativos, más un sistema de baterías que permita el cierre ordenado de las aplicaciones ante un corte. En muchos casos dependen de los servicios brindados por los otros organismos con los que comparten el lugar. Tampoco existe energía eléctrica estabilizada y luces de emergencia.

− Ubicación física de los equipos. No en todos los PCF los equipos están en lugares aislados y debidamente refrigerados; suelen estar en locales inadecuados, como cocinas o lugares de tránsito de personas.

– Sistemas contra incendios. No cuentan con detectores de humo, y los matafuegos no son los adecuados para tratar focos de fuego en lugares con componentes electrónicos.

− Presencia de material inflamable: cajas de cartón, papeles, elementos plásticos, anafes, garrafas, instalaciones de gas, estufas, cortinas, pisos y puertas de madera.

En relación al Centro de Procesamiento de Datos de la Administración Central, se detectaron las siguientes debilidades:

– No se cuenta con un plan de contingencia formal. No obstante, la disposición DNM 19.057/06 hace mención a que debe ser realizada la confección del mismo.

− No se cuenta con un sitio alternativo de procesamiento para situaciones de contingencia. Si bien hay un lugar alternativo en el Centro de Documentación Rápida, no cuenta con infraestructura de red de datos y su procesamiento. Sólo se utiliza este sitio para el resguardo del *back-up*.

− Los matafuegos no se encuentran emplazados en el lugar correcto.

− Se halló material inflamable (cajas de cartón, puertas y ventanas de madera).

− Las ventanas del *data center* carecen de protección.

− Para cubrir faltantes de los paneles del cielo raso, se recurre a soluciones precarias.

− No se realizan pruebas periódicas de verificación del funcionamiento de los detectores de humo, ni se efectúa su mantenimiento preventivo.

− El cableado de los servidores no se encuentra identificado bajo una nomenclatura estructurada y se encuentran desprolijidades en las conexiones.

− El caño de escape del grupo electrógeno carece de ventilación a los cuatro vientos.

− El mantenimiento del grupo electrógeno está tercerizado y no se lleva registro de los días y horarios que se efectúa.

Cabe señalar que el Plan de Tecnologías de la Información 2012-2014, en su punto 5 menciona que se realizará una actualización de la infraestructura del data center a los efectos de proporcionar un ambiente de máxima seguridad. Al momento de cierre de los trabajos de campo, la ejecución del plan se encuentra atrasada respecto de la planificación original.

Nivel de riesgo: alto. Nivel de madurez:

− Centro de Procesamiento de Datos de la Administración Central y Delegaciones: repetible.

− Pasos de Control Fronterizos (PCF): no conforma.

3.13. Administración de operaciones

Observaciones: no hay políticas ni procedimientos formales de operación, necesarios para una efectiva administración del procesamiento. En tal sentido, faltan procedimientos estándar para operaciones de TI que garanticen que el personal de operaciones esté familiarizado con todas las tareas de su responsabilidad; para monitorear la infraestructura de TI y los eventos relacionados; y para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o disminución del desempeño.

En relación al mantenimiento de infraestructura de TI instalada en el interior del país, a cuyo cargo se encuentran los referentes informáticos, no se cuenta con procedimientos formales para atender las fallas más frecuentes y darles un tratamiento estandarizado. Tampoco cuentan con un stock de los repuestos de los componentes más sensibles que permitan subsanar un probable incidente. Esto puede provocar la discontinuidad del servicio hasta tanto llegue el repuesto de la administración central.

Nivel de riesgo: alto. Nivel de madurez: repetible.

4. Monitorear y evaluar

4.1. Monitorear y evaluar el desempeño de TI

Observaciones: falta establecer un marco de trabajo de monitoreo general que abarque a todas las áreas de TI y un enfoque que defina el alcance, la metodología y el proceso a seguir para medir la calidad en la entrega de servicios integrado con un sistema de administración de gestión (tablero de control con indicadores) que permita comparar en forma periódica el desempeño contra métricas establecidas en un sistema de aseguramiento de la calidad (SAC), realizar análisis de la causa origen e iniciar medidas correctivas para resolver los desvíos que puedan presentarse. No hay personal dedicado al monitoreo. Se utilizan herramientas tales como el Nagios y el System Center Operations Manager (SCOM) que monitorean el estado de la red y que emiten alarmas cuando los parámetros previamente definidos por el administrador de red exceden los valores establecidos. Éstas son recibidas por el personal en sus estaciones de trabajo o en sus teléfonos inteligentes (fuera del horario de trabajo, donde se establecen guardias rotativas) y en función del criterio de quien esté a cargo del incidente, procede a su solución. Las acciones son mayormente reactivas.

La falta de un marco de trabajo de monitoreo de la infraestructura y del respectivo personal afectado a esta tarea imposibilita el análisis de datos orientado a la toma de acciones correctivas oportunas. La falta de un marco de trabajo de Mesa de Ayuda se suple con un esquema de trabajo de guardias pasivas rotativas del personal, que genera un estado de situación similar al de una contingencia permanente, con el consiguiente desgaste del personal afectado. Del análisis de datos relevados sobre la actividad de la red de datos de casi un semestre provista por el organismo, se desprenden que la tasa de caída de los enlaces de comunicaciones entre los puestos fronterizos, tales como el puente Tancredo Neves (2.082 hs), Puerto Pilcomayo (1.377 hs), el aeropuerto de Ushuaia (1.130 hs), Posadas (697,73 hs) y Bariloche (341 hs), y la Sede Central provocando que la base de datos contra la que se controla la aptitud migratoria no se encuentre actualizada en tiempo real al momento de realizarse los controles.

Nivel de riesgo: medio. Nivel de madurez: inicial.

4.2. Monitorear y evaluar el control interno

Observaciones: no se ha implantado un marco de trabajo formal de control interno de TI que pueda evaluarse posteriormente; por lo tanto, se carece de métricas que permitan verificar el logro de los objetivos de control interno para los procesos de TI (básicamente eficacia/eficiencia), identificar las acciones de mejoramiento y reportar sus excepciones. Las auditorías internas son llevadas a cabo por un único funcionario, que realiza controles a algunos objetivos de auditoría puntuales pero que no puede abarcar un programa más completo.

Nivel de riesgo: medio. Nivel de madurez: repetible.

4.3. Garantizar el cumplimiento con requerimientos externos

Observaciones: se puede determinar las siguientes debilidades

– Resolución 48 de SIGEN: se elaboró un Plan de Tecnologías de la Información 2012/2014; no obstante ello, no cuentan con planes tácticos que lo respalden ta-

les como tiempos, recursos, costos, hitos intermedios a alcanzar o riesgos relacionados, que permitan inferir el logro de los objetivos planteados. Asimismo, a la fecha de las tareas de campo, no se había actualizado el plan. No existe un modelo de arquitectura de la información formal con pautas que aseguren la integridad y la consistencia de toda la información almacenada, tales como un diccionario de datos de la organización, un esquema de clasificación de datos de acuerdo a la criticidad y la sensibilidad, procedimientos para definir datos nuevos y esquemas de funciones estándar de tratamiento de los datos (biblioteca de funciones). Faltan definir políticas y procedimientos de algunos procesos claves, ej.: Plan de Continuidad. No se adoptó una metodología de administración de proyectos informáticos encarados, el que, mínimamente debería contemplar entre otros: a) documentación, justificación y aprobación que origina el proyecto; b) definición clara del plan, determinando sus objetivos, alcances y asignación de misiones y funciones del grupo de trabajo; c) presupuesto de los recursos a ser utilizados. En orden al método, también resultaría necesario la elaboración del Plan de Prueba y de Capacitación. No existe un método formal para las actividades de desarrollo, mantenimiento o adquisición de sistemas, el que debe estar documentado y aprobado, y de aplicación complementaria a las normas relativas a la administración de proyectos. No hay una definición del marco de trabajo para el monitoreo de procesos, por el cual y a partir de indicadores de desempeño se pueda llevar a cabo el objetivo de control de la infraestructura de TI, debiendo en consecuencia presentar informes periódicos de gestión a la dirección de la organización, con el fin de que esta última supervise el cumplimiento de los objetivos planteados.

– Marco de la ley 26.653, "Accesibilidad de la información de las páginas web". La DNM cumple con lo prescripto por la norma; no obstante ello, en cuanto a criterios de usabilidad, existen principios tales como: comprensibilidad y navegabilidad por y entre las distintas secciones de la página que debieran mejorarse a fin de obtener una integración completa de las personas con discapacidad (sobre todo visual) por ejemplo: gráficos y botones etiquetados, inclusión de textos alternativos en las imágenes, asociación de celdas de encabezado con celda de datos, etc. Se verificó el cumplimiento del decreto 375/2005 de gobierno electrónico, la ley 25.506 de firma digital y el Régimen de Contrataciones de la Administración Nacional.

Nivel de riesgo: Alto. Nivel de madurez: repetible.

4.4. Proporcionar gobierno de TI

Observaciones: faltan cubrir posiciones funcionales claves como Administración de la Seguridad; Monitoreo de la Infraestructura de TI; Administración de Gestión de Aseguramiento de la Calidad; Administración de Riesgos; Administración de Proyectos.

Falta establecer el gobierno de TI con un entorno de control que incluya marcos de trabajo definidos y formalizados para asegurar el tratamiento uniforme para la administración de todos los proyectos de TI; el seguimiento de la gestión, mediante un programa de calidad que establezca indicadores a partir de metas y objetivos definidos previamente, de modo de medir la contribución de TI a los objetivos estratégicos del organismo y posibilite la rendición de cuentas; administración de costos, donde se identifiquen los distintos costos y que garantice los cargos para que los distintos servicios sean identificables para su monitoreo y una correcta administración de los programas de inversión; esquema de monitoreo que permita medir el desempeño y la correcta asignación de los recursos y si los objetivos perseguidos son alcanzados o no, y que permitan acciones correctivas; administración de riesgos, que permitan reportar aquellos relacionados con TI y su impacto en la posición de riesgos de la organización.

Nivel de riesgo: alto. Nivel de madurez: inicial.

El proyecto de informe de auditoría por nota 71/15-A06 fue enviado en vista al organismo auditado para que formule las aclaraciones y/o comentarios que estime pertinentes. La DNM, mediante la nota 426/15 del 5/7/15 envía el descargo respectivo. Como resultado del análisis realizado, se modifica parcialmente el texto de la observación 4.1. sin incidencia en su nivel de madurez.

Finalmente, la AGN arriba a las siguientes conclusiones:

Los movimientos migratorios internacionales han representado para la Argentina un elemento relevante en materia sociocultural, política y económica, constituyendo aportes fundamentales en su configuración histórica y actual. Más allá de la histórica inmigración europea de finales de siglo XIX y principios del XX, el país constituye un polo de atracción para los migrantes del cono sur latinoamericano, tal como surge de las estadísticas de radicación, que arrojan un promedio anual de más de 200.000 personas por año para el período 2004/2014 (con picos de 336.987 y 304.251 en 2006 y 2012), y las estadísticas de movimiento de personas, que ascienden a más de 56 millones para 2014 –considerando ingresos y egresos–. Esto ocurre en un territorio con fronteras extensas y en ocasiones permeables, cuyo control estricto resulta complejo.

La Dirección Nacional de Migraciones (DNM) es el organismo responsable de controlar el ingreso, permanencia y egreso de personas al país y ejerce el poder de policía de extranjeros en todo el territorio de la República. A partir de la sanción de la ley 25.871, su rol cobró relevancia en el control de los trámites migratorios al asumir funciones que anteriormente estaban asignadas a otros organismos, tales como Gendarmería Nacional o Prefectura Naval Argentina. Este proceso de crecimiento institucional no fue acompañado por un desarrollo acorde de la estructura de la Dirección General de Sistemas y Tecnologías de la Información (DGSyTI).

Como consecuencia de esto, se observan falencias en la planificación y la organización que, dada la depen-

dencia crítica que representa la TI para el organismo, conducen a una gestión basada en acciones reactivas.

La ausencia de marcos de trabajo formalizados no permite generar información a partir de la cual se puedan obtener los indicadores cuantitativos y cualitativos necesarios para la conformación de un tablero de control de gobierno de TI y medir la entrega de valor.

Mientras que la infraestructura de TI creció en forma exponencial, algunas funciones sensibles tales como la planificación, el monitoreo de la infraestructura, la administración de la seguridad, la gestión de riesgos o el aseguramiento de la calidad del servicio no han sido formalmente definidas.

Además, para el mantenimiento de la infraestructura de TI en el interior, la DGSyTI no cuenta con una estructura funcional propia. Lo hace a través de referentes informáticos que dependen jerárquicamente de los funcionarios de rango superior del lugar de asiento. Esto provoca una dicotomía en relación al principio de unidad de mando, cuando en presencia de incidentes varios, debe responder por este principio a su inmediato superior.

Por otra parte, la política de retención de recursos humanos resulta poco apropiada atento que el 94,03 % del personal se encuentra bajo una modalidad de contrato que no permite un plan de carrera en el organismo e introduce un factor de riesgo de inestabilidad laboral al tener que renovar el vínculo anualmente.

Respecto de la información en las aplicaciones informáticas de control de tránsito migratorio, debe considerarse que:

– No todos los pasos fronterizos se encuentran informatizados. En estos casos, la registración de los datos de los migrantes se hace en forma manual y se cargan en las aplicaciones en forma diferida, proceso que está sujeto a las siguientes debilidades: a) los pasos no cuentan con el control de aptitud migratoria, b) los datos son factibles de errores o faltantes en su manipulación, c) producto del punto anterior, pueden generarse inconsistencias tales como casos de personas que ingresan por los lugares habilitados que quedan en situación migratoria de irregularidad.

– La base de datos de la DNM no contiene la totalidad de los movimientos de personas.

– La inadecuada infraestructura de TI de algunos PCF provoca caídas del servicio que lo ponen en la misma situación que los que no están informatizados.

La falta de información en el sistema que registra el movimiento de personas en las fronteras no sólo obedece a debilidades en el entorno tecnológico, sino también a debilidades en el control ejercido por el organismo competente, tanto en lugares u horarios no habilitados a través de las policías auxiliares, como en los entornos de los puestos de control fronterizo. La consecuente falta de datos dificulta la identificación y detección de personas cuyo egreso, ingreso o permanencia en el territorio nacional deba ser sancionada y/o prohibida por las razones expuestas en el artículo 29 de la citada ley.

José M. Á. Mayans. – Luis G. Borsani. – Carla B. Pitiot. – Carlos D. Castagneto. – Álvaro G. González. – Julio R. Solanas. – Marcelo J. Fuentes. – Virginia M. García. – Miguel Á. Pichetto.

ANTECEDENTES

1

Dictamen de comisión

Honorable Congreso:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente Senado de la Nación O.V.-309/15, Auditoría General de la Nación comunica resolución 172/15 aprobando el informe de auditoría referido a la evaluación de la tecnología informática de la Dirección Nacional de Migraciones; y, por las razones expuestas en sus fundamentos, os aconseja la aprobación del siguiente

Proyecto de resolución

El Senado y la Cámara de Diputados de la Nación

RESUELVEN:

1) Dirigirse al Poder Ejecutivo nacional solicitándole informe sobre las medidas adoptadas para regularizar las situaciones observadas por la Auditoría General de la Nación con motivo del examen realizado en el ámbito del Ministerio del Interior y Transporte, cuyo objeto fue el análisis de la gestión informática en la Dirección Nacional de Migraciones (DNM).

2) Comuníquese al Poder Ejecutivo nacional y a la Auditoría General de la Nación juntamente con sus fundamentos.*

De acuerdo con las disposiciones pertinentes, este dictamen pasa directamente al orden del día.

Sala de la comisión, 22 de septiembre de 2016.

José M. Á. Mayans. – Luis G. Borsani. – Carla B. Pitiot. – Carlos D. Castagneto. – Álvaro G. González. – Julio R. Solanas. – Marcelo J. Fuentes. – Virginia M. García. – Miguel Á. Pichetto.

2

Ver expediente 265-S.-16.

* Los fundamentos corresponden a los publicados con la comunicación del Honorable Senado.