SESIONES EXTRAORDINARIAS

2016

ORDEN DEL DÍA Nº 1155

Impreso el día 7 de diciembre de 2016
Término del artículo 113: 20 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 de Agricultura, Ganadería y Pesca de la Nación, cuyo objeto fue la evaluación de la Tecnología Informática (TI) del Instituto Nacional de Tecnología Agropecuaria (INTA), Sede Central. (176-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 llevar a su conocimiento 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 de Agricultura, Ganadería y Pesca de la Nación, cuyo objeto fue la evaluación de la Tecnología Informática (TI) del Instituto Nacional de Tecnología Agropecuaria (INTA), Sede Central.

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) efectuó un examen en el ámbito del Ministerio de Agricultura, Ganadería y Pesca de la Nación, cuyo objeto fue la evaluación de la Tecnología Informática (TI) del Instituto Nacional de Tecnología Agropecuaria (INTA), Sede Central.

Período auditado: las tareas de campo abarcaron los meses de septiembre, octubre, noviembre y diciembre del año 2013.

La AGN, en el apartado "Aclaraciones previas", realiza una breve descripción del marco legal e institucional del INTA, destacando que es un organismo estatal descentralizado con autarquía operativa y financiera, dependiente del Ministerio de Agricultura, Ganadería y Pesca de la Nación. Fue creado el cuatro de diciembre de 1956, con el fin de impulsar y vigorizar el desarrollo de la investigación y extensión agropecuarias para el mejoramiento de la empresa agraria y la vida rural.

En el año 1986, habida cuenta las transformaciones operadas en el sector agropecuario respecto de la demanda por tecnología, como por el incremento de participantes en la generación y transferencia tecnológicas, se llevó a cabo un proceso de descentralización operativa y se habilitó a la participación en la conducción de los sectores involucrados. En la actualidad, cuenta con 15 Centros Regionales (CR), 250 Agencias de Extensión Rural (AER) y otras instalaciones con distintas funciones y denominaciones (campo anexo, centro experimental, estación forestal, oficinas de proyecto, laboratorio, agencias de proyecto, oficina de información técnica, campos forestales, unidad de extensión y experimentación adaptativa, oficina de desarrollo) que dependen funcionalmente de los CR y conforman una red de asistencia técnica a lo largo del territorio nacional. Además de estos órganos rectores, la matriz institucional se completa con Programas Na-

cionales (PN) y Áreas Estratégicas (EA). En función de su amplia distribución geográfica, el INTA ha encarado un plan para la interconexión de aproximadamente 420 puntos en red con servicio de disponibilidad las 24 horas del día los 365 días del año.

La AGN señala que el examen se basó en la verificación de los objetivos de control esta-blecidos por el marco de referencia de buenas prácticas de TI COBIT (*Control Objectives in Information Technologies*) versión 4.1. Los objetivos de control describen los resultados que debe alcanzar un organismo implantando procedimientos, basados en las mejores prácticas aplicables, a los procesos de TI. Para cada uno de los objetivos, se menciona el nivel de madu-rez que le corresponde, conforme al modelo de madurez de la capacidad. Luego, se encuentran las recomendaciones para mejorar el ambiente de control y reducir los riesgos. Además, para cada uno de los objetivos de control, se indica qué requerimientos de la información son afec-tados. Asimismo, cada objetivo de control va acompañado de su nivel de riesgo (alto, medio o bajo) que le es propio, poniendo en evidencia el impacto provocado por su incumplimiento y sin estar vinculado con la situación del organismo.

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:

Existen tanto el plan estratégico institucional como su correspondiente de TI, pero sus metas no se encuentran respaldadas por sus correspondientes planes tácticos que detallen cómo se lograrán los objetivos planteados. No hay detalles de tiempos, recursos afectados, costos, hitos intermedios a alcanzar, o riesgos relacionados. Por consiguiente, no se hace posible un correcto control y seguimiento. De hecho, del Plan Estructurante, concebido entre los años 2006 y 2007, gran parte de los objetivos (salvo aquellos relacionados con la infraestructura in-formática) no se han cumplido al momento de los trabajos de campo de la auditoría.

Nivel de riesgo: alto.

Nivel de madurez: inicial. La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza en base a requerimientos específicos. La alineación de los requerimientos de las aplicaciones y tecnología se lleva a cabo de modo reactivo. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.

1.2. Definir la arquitectura de información

Observaciones:

El organismo no estableció un modelo de arquitectura de información integrada que incluya un diccionario y un esquema de clasificación, de acuerdo a la criticidad y la sensibilidad de datos. Tampoco están formalizados procedimientos para definir datos nuevos que aseguren la integridad y la consistencia de toda la información almacenada. Se llevan a cabo desarrollos en distintas unidades del INTA sin seguir ningún lineamiento organizacional dependiente de la administración central. Conviven distintas plataformas de hardware y software, los datos en muchos casos se almacenan localmente, sin seguir una política de seguridad de datos. Esta situación puede generar redundancia de datos, inconsistencias y/o fuga de información fuera el organismo.

Nivel de riesgo: alto

Nivel de madurez: inicial. La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos de sus componentes ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.

1.3. Determinar la dirección tecnológica

Observaciones:

No se desarrolló 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 que engloben a todo el organismo.

Nivel de riesgo: alto.

Nivel de madurez: inicial. La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes son específicos para un fin determinado. La dirección tecnológica está impulsada por los planes evolutivos del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es poco clara.

1.4. Definir los procesos, organización y relaciones de TI

Observaciones:

Falta la aprobación de una estructura formal de TI para las posiciones inferiores a gerentes, que en la actualidad se ejercen ad hoc. Por otra parte, de la estructura de TI depende del departamento de Biblioteca, que es un área usuaria. No existen descripciones formales de políticas, normas y procedimientos de TI. Se observan además desarrollos de software e instalaciones que no cuentan con el control del área de TI, sin misiones y funciones explícitas aprobadas en todos los niveles. Esta situación provoca una disminución de los controles internos. No se estableció un comité estratégico de TI formado por representantes de los niveles decisorios y de TI que determine las prioridades de los programas de inversión alineados con la estrategia y prioridades

del organismo. Existe un Comité de Informática, pero sólo con enfoque hacia la infraestructura. La propiedad de los datos y de los sistemas no se encuentran formal y claramente definidos. Faltan posiciones claves tomo personal que tenga a su cargo la administración de proyectos, análisis funcionales, aseguramiento de la calidad y gestión de riesgos. La función de seguridad está asignada a una sola persona, lo cual dada la magnitud de las instalaciones, se le hace imposible cumplir con las misiones y funciones encomendadas descritas en la política de seguridad. En relación a la infraestructura de TI, a cuyo cargo se encuentra la Gerencia de Informática, la misma cuenta con una dotación interna, además de una estructura informal en el interior del país, de agentes del organismo, que llevan a cabo tareas técnicas solicitadas desde la administración central, que se denominan "Referentes Informáticos" (RI). Tanto la dotación interna como los RI son insuficientes para garantizar un servicio de continuidad.

Sobre el rol de cada RI cabe destacar que:

–No se encuentran definidas formalmente ni las misiones, ni las funciónes ni las respon-sabilidades.

–En muchos casos desempeñan otras tareas además de esta función.

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

–Algunos se encuentran bajo un modo de contratación sin estabilidad en cuanto a la relación de continuidad, no acorde a la criticidad de sus responsabilidades.

–En algunos casos, deben desplazarse muchos kilómetros y tienen demasiados puestos de trabajo para atender.

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

Nivel de riesgo: alto.

Nivel de madurez: inicial. Las actividades y funciónes de TI son reactivas. TI se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizadas.

1.5. Administrar la inversión en TI

Observaciones:

El enfoque presupuestario en relación a TI es en general, por proyecto. Falta la implementación de un enfoque orientado a la administración por centros de costos así como un proceso de monitoreo para determinar la contribución esperada de TI a los objetivos estratégicos del organismo. La asignación de los recursos de TI no está imputada a los usuarios de los servicios de TI, sino en todos los casos a la propia área de TI.

Nivel de riesgo: alto.

Nivel de madurez: repetible. Existe un entendimiento implícito de la necesidad de seleccionar, administrar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.

1.6. Comunicar las aspiraciones y la dirección de la gerencia

Observaciones:

La Dirección Nacional Asistente de Sistemas de Información, Comunicación y Calidad está en un proceso inicial de elaboración de un marco de trabajo de políticas y procedimientos de TI. Faltan algunas políticas y procedimientos relevantes tales como las relacionadas a la formulación y ejecución del plan estratégico de TI, formulación y administración de proyecto de TI, ciclo de vida de desarrollo de sistemas (existe una metodología, pero es incompleta), pruebas e implementacion, plan de contingencia, administración de riesgo y administración de calidad, entre otros.

Nivel de riesgo: medio.

Nivel de madurez: inicial. La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Algunos procesos de elaboración, comunicación y cumplimiento son informales.

1.7. Administrar los recursos humanos de TI

Observaciones:

El personal de TI suele tener a su cargo procesos críticos relacionados con la operatoria de la organización. El instituto tiene un convenio colectivo que promueve la profesionalización de sus empleados. En el mercado laboral, las áreas de TI suelen proveerse mayormente de personal idóneo, en muchos casos no profesional, pero especializado en tecnología, con altos niveles salariales. La rigidez del convenio o su falta de adecuación provoca que los salarios ofrecidos por el organismo estén por debajo del nivel del mercado, con lo cual dificulta el ingreso y la retención del personal. El organismo cuenta con un esquema limitado para gene-rar nuevas vacantes, por lo que se procede a la contratación bajo la modalidad 1.8.7, becarios y otras, que no generan situaciones de estabilidad en los involucrados. Asimismo, carece de una política de retención.

Nivel de riesgo: alto.

Nivel de madurez: repetible. Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.

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: alto.

Nivel de madurez: inicial. Existe conciencia por parte de la dirección de la necesidad de un Sistema de Administración de la Calidad (SAC) en relación a TI. Se realizan juicios informales sobre la calidad.

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 la falta de un inventario completo y detallado de la TI no permite una evaluación formal de éstos que contemple 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 contempladas las medidas a tomar en cada caso.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados. Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales según lo determine cada proyecto. Los riesgos específicos relacionados con TI, tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto.

1.10. Administrar proyectos

Nivel de riesgo: alto.

Nivel de madurez: inicial. El uso de técnicas y enfoques de administración de proyectos dentro de TI no está formalizada. Hay poca participación de los usuarios en las etapas de definición. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración no están definidas. Los cronogramas y objetivos intermedios están vagamente definidos. No se hace seguimiento al tiempo, a los gastos y no se comparan con lo previamente estimado.

Observaciones:

No existe un marco de administración de proyectos centralizado que incluya:

–Costos, plazos, hitos a cumplir, alcance, recursos afectados.

–Parámetros de calidad definidos en el sistema de administración de la calidad.

–Un proceso de administración de control de cambios de modo tal que todas las modifi-caciones a la línea base se revisen, aprueben e incorporen al plan integrado de acuerdo al marco de trabajo.

–Un proceso de monitoreo del desempeño contra los criterios clave previamente definidos en el sistema de calidad.

2. Adquirir e implementar

2.1. Identificar soluciones automatizadas:

Observaciones:

No existe una gestión centralizada del desarrollo de software. Existen políticas y procedimientos formalizados para administrar los requerimientos de soluciones automatizadas, que permitan evaluar factibilidades, cursos de acción alternativos, administrar prioridades, acordar alcances, asignar recursos y determinar un usuario clave que patrocine el proyecto, pero no se aplican en todos los casos. En muchas unidades administrativas se llevan a cabo desarrollos sin control de la Gerencia de Gestión de la Información. Existe una metodología de ciclo de vida de desarrollo de sistemas, pero no se aplica en todos los casos.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Las soluciones automatizadas se analizan de manera informal, y los requerimientos se documentan algunas veces. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.

2.2. Adquirir o desarrollar y mantener software aplicativo

Observaciones:

Hay formalizada una metodología de Ciclo de Vida de Desarrollo de Sistemas (CVDS) que contempla documentaciones tales tomo: alcance, requerimientos, diseño, pruebas, implementación, pero no se aplica en todos los casos y la misma es incompleta ya que no se definieron estándares de documentación a aplicar en cada etapa. No se realiza gestión de aseguramiento de la calidad en los desarrollos ni en la seguridad, tanto propia como para terceros. Existen áreas del organismo, independientes de TI, que llevan a cabo sus propios desarrollos de aplicaciones, sin utilizar la metodología y ni estándares de Seguridad Informática. La misma situación se encuentra en el caso del desarrollo y mantenimiento de las aplicaciones realizadas por terceros.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimiento de software aplicativo varían de un proyecto a otro.

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. Existe la intención de unir 420 puntos en todo el país, pero no se llevó a cabo un análisis de las aplicaciones que se desarrolla-ron en el interior y que pueden transformarse en corporativas. El impacto del aumento del tránsito de datos futuro no se ha contemplado.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Se realizan cambios a la infraestructura sin ningún plan integral. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento se realiza en forma reactiva a necesidades de corto lazo.

2.4. Facilitar la operación y el uso

Observaciones:

Falta un marco para la documentación de los sistemas. No se confecciona una documentación estándar para cada etapa del proceso de ciclo de vida que permita la transferencia de conocimiento. No existe documentación o descripción de los procedimientos de los sistemas de información en producción. Además, se desarrolla software en las distintas unidades administrativas del organismo, que no se encuentran controladas bajo la administración central, por lo que cada una adopta su propio criterio de administración de las aplicaciones.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Existe la percepción de que la documentación de procesos es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Los materiales de entrenamiento tienen calidad variable. No existen procedimientos de integración a través de los diferentes sistemas. No hay aportes de las áreas involucradas en el diseño de programas de entrenamiento.

2.5. Adquirir recursos de TI

Observaciones:

Falta formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores, que abarque: responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión, así como obligaciones y cláusulas de penalización por incumplimiento cuando no cumplan los acuerdos de niveles de servicios previamente establecidos. En el caso de la propiedad intelectual de software desarrollado por la organización no se encuentra preservado, ya sea por debilidades de seguridad (existen desarrollos llevados a cabo en las distintas áreas del organismo y que no están bajo el control de la DNA Sistemas de Información, Comunicaciones y Calidad) y porque no se ha formalizado un documento con los desarrolladores, de respetar esta propiedad.

Nivel de riesgo: alto.

Nivel de madurez: repetible. Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.

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 inadvertidos a partir de cambios no autorizados y/o no probados a los sistemas de información.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio insuficiente. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por la administración de cambios.

2.7. Instalar y acreditar soluciones y cambios

Observaciones:

Existe una metodología de ciclo de vida de desarrollo de sistemas, pero no se aplica en todos los casos. Además, existen desarrollos de aplicaciones en varias unidades administrativas del organismo, donde se siguen criterios propios. Todas las tareas referidas a la implementación de un sistema o su modificación, no siguen criterios estándares preestablecidos. En relación a las pruebas, no se confecciona un ambiente independiente a tal efecto, en el que el usuario pueda llevarlas a cabo. Tampoco se aplica documentación estandarizada para esta etapa.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares, y los enfoques que se toman varían.

3. Entregar y dar soporte

3.1. Definir y administrar los niveles de servicio

Observaciones:

Falta definir un marco de trabajo que brinde un proceso formal de administración de los niveles de servicio entre el usuario y el prestador del servicio, que incluya procesos para la creación de requerimientos, definiciones, acuerdos de niveles de servicio (ANS) para todos los procesos críticos de TI y sus correspondientes fuentes de financiamiento y que, a partir de reportes periódicos, permita monitorear continuamente los criterios de desempeño y revisar periódicamente los ANS para asegurar que son efectivos.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Hay conciencia de la necesidad de administrar los niveles de ser-vicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas para la definición y la administración de servicios no está definidas. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa.

3.2. Administrar servicios de terceros

Observaciones:

No existe un marco de trabajo para administrar los servicios de terceros que incluya formalizar el proceso de administración de relaciones con proveedores; tenerlos catalogados, asegurarse de que los contratos estén de conformidad con los requerimientos legales y regulatorios y monitorear la prestación del servicio en base a los acuerdos de niveles de servicio (ANS).

Nivel de riesgo: alto.

Nivel de madurez: inicial. La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva.

3.3. Administrar el desempeño y la capacidad

Observaciones:

No se ha formalizado un proceso de monitoreo del desempeño y la capacidad de recursos de TI, de modo tal de satisfacer los acuerdos de nivel de servicios (ANS), minimizar el riesgo de interrupciones, balancear la carga de trabajo, analizar ciclos de vida de los recursos de TI y el planeamiento de las necesidades futuras, ante los posibles incrementos en la demanda. En el planeamiento de la capacidad, no se ha tomado en cuenta el proceso de incorporar como corporativos la desarrollos de software realizados en el interior.

Nivel de riesgo: alto.

Nivel de madurez: parcialmente repetible. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria, y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.

3.4. Garantizar la continuidad del servicio

Observaciones:

No hay un plan de continuidad de servicios de TI diseñado para reducir el impacto de la interrupción de procesos críticos. Hay sectores del organismo que llevan a cabo la administración de sus propios resguardos sin intervención y control del área de TI. El organismo no se encuentra preparado ante el riesgo de acontecimientos no previstos que pudieran ocasionar la interrupción de los servicios o pérdida de datos.

Nivel de riesgo: alto.

Nivel de madurez: inicial. Las responsabilidades sobre la continuidad de los servicios son informales, y la autoridad para ejecutar responsabilidades es limitada. La máxima autoridad de TI es consciente de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación.

3.5. Garantizar la seguridad de los sistemas

Observaciones:

Las funciones de seguridad están a cargo de un único funcionario que debe atender una red proyectada de aproximadamente 420 puntos y más de 7.000 usuarios. En julio de 2013, se formalizaron políticas para la administración de usuarios en forma centralizada mediante la utilización de un controlador de dominio único para todas en las plataformas Windows y Linux para los servicios de Internet, aplicaciones y mails.

Se detectaron las siguientes falencias:

– Existen algunos aplicativos accesibles vía intranet con autenticación propia por no tener desarrollado un módulo de autenticación integrada al dominio.

– No hay procedimientos escritos y aprobados que permitan auditar las acciones de los administradores, usuarios externos e internos y casos de emergencia.

– El sistema de RR.HH. permite el acceso a su información, pero no existe un control o proceso automático de validación entre la información registrada en este sistema y los procedimientos de altas o bajas de usuarios en la red.

– Si bien existen políticas para la administración de los *firewalls* que protegen a la red interna de la externa, no se encuentran implementadas políticas individuales en los servidores, que impidan que, por ejemplo, logrando ingresar a un servidor desde la red interna, sería posible desde éste, ganar acceso a servicios no autorizados en otros servidores. En algunos casos hay servidores que utilizan los *firewalls* del sistema operativo con sus configuraciones por defecto.

– Ausencia de procedimientos específicos para desarrollo, actualización y control del plan de contingencia, control de vulnerabilidades de la red informática y base de datos (limitación y control del código SQL).

– No hay políticas de escritorios libres de información, lo que posibilita que información sensible pueda estar expuesta al alcance de personal no autorizado.

Referente a la administración de usuarios:

– No se formaliza la utilización del formulario "Conformidad del Usuario" durante la entrega de la respectiva contraseña.

– Existen aproximadamente 3.200 cuentas de usuarios con más de 6 meses de inactividad habilitadas y cuyos usuarios nunca accedieron a la red informática del organismo. Las políticas de seguridad, aprobadas por resolución 285/2008, indican que deben inhabilitarlas.

– Existe un usuario genérico para la administración local de los servidores Linux cuya contraseña es conocida por más de una persona. Además, en un servidor analizado se encontró usuarios locales con acceso remoto de personal ajeno al departamento de Redes e Infraestructura perteneciente a la Gerencia de Gestión de la Información.

– Se utiliza el usuario privilegiado "root" o "súperusuario" para acceder a los servidores Linux en lugar de hacerlo desde una aplicaciòn, que invoque al usuario "root", de manera tal de que queden los rastros necesarios para realizar los procedimientos de auditoría.

– Si bien las aplicaciones cuentan con usuarios particulares para acceder a las bases de datos, éstos no se encuentran limitados al servidor de aplicación específico, posibilitando la utilización desde ubicaciones remotas dentro de la red.

Nivel de riesgo: alto.

Nivel de madurez: inicial. La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente de las personas. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Los incidentes de seguridad de TI ocasionan respuestas individuales, debido a que las responsabilidades no son claras. Las respuestas a los incidentes de seguridad de TI son impredecibles.

3.6. Identificar y asignar costos

Observaciones:

No hay un marco de trabajo de administración por centro de costos, en función de la TI por cada una de las direcciones nacionales, que esté alineado con los procedimientos de contabilización y medición financiera del organismo; que incluya costos directos, indirectos, fijos y variables, y que garantice los cargos para que los distintos servicios sean identificables para su monitoreo. En el aplicativo contable, denominado e-Siga, no existe una clasificación de cuentas específica de las inversiones de TI. En consecuencia, se debe recurrir a procesos manuales para obtener la información que refleje en forma consolidada la concentración de todas las inversiones en TI.

Nivel de riesgo: alto.

Nivel de madurez: repetible. Hay conciencia general de la necesidad de identificar y asignar costos. La asignación de costos está basada en procedimientos rudimentarios. Los procesos de asignación de costos pueden repetirse. No hay habilitación o comunicación formal sobre la identificación de costos estándar y sobre los procedimientos de asignación. No está asignada la responsabilidad sobre la recopilación o la asignación de los costos.

3.7. Educación y capacitación de los usuarios

Observaciones:

No hay un plan de capacitación de TI que abarque la identificación de las necesidades de capacitación en tecnología en cada una de las diferentes áreas del organismo y en especial la de TI y los mecanismos de impartición, con el correspondiente esquema de evaluación del entrenamiento recibido.

Nivel de riesgo: alto.

Nivel de madurez: inicial. hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.

3.8. Administrar la mesa de servicio y los incidentes

Observaciones:

Hay procedimientos escritos que han sido elaborados, controlados y aprobados por la misma Gerencia de Informática. La mesa de servicios es llevada por el Departamento de Mesa y Ayuda y Soporte Técnico en Buenos Aires. Se atiende en forma centralizada a alrededor de 420 puntos del país. Se registran todos los incidentes, no sólo los referidos a informática, sino también los de telefonía fija y móvil. Transitoriamente, los puntos que todavía no están conectados a la red corporativa se manejan reportando los incidentes telefónicamente, los cuales son cargados en el aplicativo por los operadores de la Mesa de Ayuda.

Se observan las siguientes falencias:

– No se realizan encuestas de satisfacción de usuarios.

– No se realizan acuerdos de niveles de servicios con los usuarios.

Nivel de riesgo: alto.

Nivel de madurez: definido. Los procedimientos se estandarizan y documentan, pero se lleva a cabo entrenamiento informal. Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares. Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte. No se mide la respuesta oportuna a las consultas e incidentes, y los incidentes pueden quedar sin resolución. Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.

3.9. Administrar la configuración

Observaciones:

No hay un repositorio centralizado de inventarios de activos de TI para el organismo que contenga todos los elementos de configuraciones incluyendo hardware, software de base y aplicativos. Sólo existen inventarios parciales que no cubren todas las características para el control de los recursos informáticos. No hay un procedimiento de control de cambios aplicable al mantenimiento de los inventarios.

Nivel de riesgo: alto.

Nivel de madurez: inicial. se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software, pero de manera individual. No están definidas prácticas estandarizadas.

3.10. Administración de problemas

Observaciones:

El organismo se encuentra en un proceso de conexión de todas las unidades distribuidas en todo el país (aproximadamente 420 puntos). Al momento de la auditoría, se encuentran conectados aproximadamente el 78 % de este objetivo. Hay procedimientos escritos que han sido elaborados, controlados y aprobados por la misma Gerencia de Informática. En éstos, está contemplado el escalamiento de los problemas al personal a cargo de solucionarlos. En las unidades que se encuentran conectadas, se dispone de las siguientes formas de comunicar el problema informático o de telecomunicaciones a la Mesa de Ayuda:

– La aplicación de intranet "Gestión de incidentes".

– El link "asistencia.inta.gob.ar".

– Algunas agencias de extensión rural que todavía no disponen de esta aplicación se comunican enviando un correo electrónico o telefónicamente a la Mesa de Ayuda, y los operadores cargan el incidente en el aplicativo.

Se observan las siguientes falencias:

– En relación a los incidentes de TI que se generan en el interior del país, no estando definidas claramente las misiones y funciones de los referentes informáticos, y dada la estructura informal de éstos, existen algunos inconvenientes para asignar la derivación de los problemas para su solución.

– No se realizan encuestas de satisfacción de usuarios.

– No se realizan acuerdos de niveles de servicios con los usuarios.

Nivel de riesgo: alto.

Nivel de madurez: definido. Se cuenta con un sistema integrado de administración de problemas. Los procesos de escalamiento y resolución de problemas están formalizados. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.

3.11. Administración de datos

Observaciones:

Existen aplicaciones corporativas administradas desde la administración central y otras que se administran localmente en las distintas dependencias del organismo. Esto es producto de que las distintas unidades de la organización, distribuidas geográficamente en todo el país, han desarrollado sistemas. De muchos de ellos no se tiene conocimiento en la administración central. Se ha encarado un proyecto de centralización de estos últimos que consiste en almacenarlos en el centro de cómputos del organismo, pero este proceso se encuentra en su etapa inicial en el momento de los trabajos de campo de la auditoría.

En relación a las aplicaciones centralizadas, se observó que:

– Si bien están bajo procedimientos centralizados de resguardo, éste no está formalizado, ni indica qué detalle de las aplicaciones y bases de datos deben estar incluidos, tampoco contiene instructivos para su ejecución, tanto sea para almacenar la información como para su eventual recuperación en caso de incidentes.

– No existe un procedimiento que determine una clasificación por criticidad, impacto o requerimientos de seguridad alineados al plan de continuidad.

– Se observó la falta de un repositorio ignífugo para el resguardo como forma de protección alternativa para casos de desastre. Con respecto a las aplicaciones desarrolladas en las distintas unidades del organismo, se llevan a cabo con procedimientos propios que no están ni regidos ni controlados por la Gerencia de Informatica.

Nivel de riesgo: alto.

Nivel de madurez: inicial. El organismo reconoce la necesidad de una correcta administración de los datos. Existe un método para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación for-

mal. No se lleva a cabo capacitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Existen procedimientos de respaldo y recuperación.

3.12. Administración de instalaciones

Observaciones:

Existen tres centros de procesamiento que denominaremos: Chile, Rivadavia 1, Rivadavia 2 y Alsina.

Además hay una sede con usuarios de aplicaciones en Alsina 1407. Ninguno de ellos satisface los requerimientos de seguridad física adecuados para almacenar la información. No se cuenta con un plan de contingencia formal. Además, la dispersión en estas tres instalaciones genera que tengan que replicarse las medidas de control y seguridad en cada centro. Paralelamente, no cuentan con un sitio alternativo de procesamiento para situación de desastre, cuando bien podrían las instalaciones de un edificio ser el resguardo del otro.

Se efectuaron las siguientes observaciones:

Chile:

– Falta un procedimiento formal de acceso al centro de cómputos donde se detallen las personas autorizadas y sus responsabilidades, y el tratamiento de visitas externas.

– Los matafuegos se encontraban depositados en el piso.

– Presencia de material inflamable (cajas de cartón, amoblamiento de madera, puerta de acceso de madera, sillas de plástico o con tapizado sintético, y piso de goma).

– Se encontraron faltantes de paneles en techo y pared.

– El detector de humo carece de mantenimiento mensual.

– El grupo electrógeno tiene un mantenimiento informal y no se lleva registro de los días y horarios que se lo efectúa. La potencia del grupo es insuficiente, por ese motivo, en casos de corte, sólo se puede acoplar un aire acondicionado.

– Ante un corte de suministro, se actúa de oficio sin tener documentado formalmente que procedimiento utilizar.

– El cableado de los servidores no se encuentra identificado bajo una nomenclatura estructurada.

Rivadavia 1:

– Falta un procedimiento formal de acceso al centro de cómputos donde se detallen las personas autorizadas y sus responsabilidades, y el tratamiento de visitas externas.

– El matafuego se encuentra amurado a una estantería móvil con estantes de aglomerado.

– No posee grupo electrógeno.

– Presencia de material inflamable y objetos que obstaculizan el paso (cajas de cartón, amoblamientos de madera, cablecanal suelto, telgopor, carpetas, biblioratos, resmas de papel y puerta de acceso de madera).

– En la parte superior de la pared existe un agujero por donde cae polvo sobre los servidores pudiendo dañarlos.

– El cableado de los servidores no se encuentra identificado bajo una nomenclatura estructurada y los cables se encuentran colgados por encima de los *racks*.

– Ante un corte de energía eléctrica, las UPS tienen un tiempo máximo de uso de 90 minutos. Superado ese tiempo, comienza el apagado de los servidores. Al no tener un grupo elec-trógeno se discontinúa el servicio.

Rivadavia 2:

– Falta un procedimiento formal de acceso al centro de cómputos donde se detallen las personas autorizadas y sus responsabilidades, y el tratamiento de visitas externas.

– Tiene dos aires acondicionados de los cuales funciona uno solo.

– Presencia de material inflamable (piso de parqué, panel de conexión y distribución con gabinete de madera, cablecanal, cajas de cartón y puerta de acceso de madera).

– El cableado de los servidores no se encuentra identificado bajo una nomenclatura estructurada y los cables se encuentran colgados por encima de los *racks*.

– No posee grupo electrógeno.

– Ante un corte de energía eléctrica, las UPS tienen un tiempo máximo de uso de 120 minutos. Superado ese tiempo, comienza el apagado de los servidores. Al no tener un grupo electrógeno se discontinúa el servicio.

Detalle de la situación encontrada en los tableros de energía eléctrica:

Se han hallado deficiencias en el sistema de suministro eléctrico y se presentan los siguientes riesgos:

Chile:

– No existe un plan de contingencia ante el corte de energía. El mantenimiento del grupo electrógeno está a cargo de la Gerencia de Sistemas en lugar de depender de las áreas de mantenimiento del edificio.

– Los tableros carecen de luces que identifiquen la presencia de energía eléctrica.

– Falta de luces de emergencia en todos los tableros de energía eléctrica.

– El acceso al tablero principal de la planta baja se encuentra obstruido por dos muebles de madera y un exhibidor con folletos del organismo.

– En el primer subsuelo se encuentran las bombas de agua cuyo acceso está obstruido por objetos que interrumpen una rápida acción en caso de emergencia (sillas, cajas, escaleras de madera, papeles, revistas, etcétera).

– Uno de los tableros secundarios de energía eléctrica se encuentra dentro de un baño, otro en la cocina y otro dentro de un depósito con llave, dificultando su manipulación ante una emergencia y aumentando el riesgo por la presencia de caños y llaves de agua.

– El edificio no cuenta con detectores de humo y alarmas contra incendio.

– El caño de escape del grupo electrógeno da a un patio interno pero no ventila a los cuatro vientos.

– El acceso al grupo electrógeno (instalado en el patio del edificio) se encuentra obstruido por objetos que dificultan su acceso. El patio no posee cerradura con llave.

Rivadavia 1:

– Falta grupo electrógeno.

– Falta de luces de emergencia, detectores de humo y alarmas contra incendio.

– Faltan calcomanías en las tapas de los tableros que identifiquen el riesgo de choque eléctrico.

– El frente de los tableros no tiene luces que identifiquen la presencia de energía eléctrica.

Alsina:

– Falta grupo electrógeno.

– Faltan calcomanías en las tapas de los tableros que identifiquen el riesgo de choque eléctrico.

– El acceso a las bombas de agua se encuentra obstruido por objetos (sillas, cajas y plásticos) que dificultan su acceso.

Nivel de riesgo: alto.

Nivel de madurez: inicial. La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo dependen de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.

3.13. Administración de operaciones

Observaciones:

No hay políticas ni procedimientos formales de operación, necesarios para una efectiva administración del procesamiento.

Faltan:

– Procedimientos estándar para operaciones de TI que garanticen que el personal de operaciones esté familiarizado con todas las tareas de su responsabilidad.

– Procedimientos para monitorear la infraestructura de TI y los eventos relacionados.

– Procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o disminución del desempeño.

En relación con la infraestructura 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: inicial. El organismo reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operaciones son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Puede ocurrir que las computadoras, sistemas y aplicaciones que soportan los procesos del negocio no estén disponibles, se interrumpan o retrasen.

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. Este marco debe estar 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 calidad (SAC), realizar análisis de la causa origen e iniciar medidas correctivas para resolver los desvíos que puedan presentarse.

Nivel de riesgo: alto.

Nivel de madurez: inicial. La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos.

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: alto.

Nivel de madurez: repetible. La organización utiliza reportes de control para comenzar iniciativas de acción

correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La Gerencia de Servicios de Información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.

4.3. Garantizar el cumplimiento con requerimientos externos

Observaciones:

– Resolución SIGEN 48/2005 "Pautas de Control Interno de TI":

Se han hallado debilidades en el cumplimiento de aspectos tales como:

a) Organización informática:

– Si bien la responsabilidad por las actividades de Tecnología de la Información (TI) de la organización recaen en un único área, existen numerosos desarrollos y administraciones de datos en las distintas unidades administrativas del organismo que están fuera del control de la DNA Sistemas de Información, Comunicaciones y Calidad.

– No está definida una descripción documentada y aprobada de los puestos de trabajo inferiores a gerentes que conforman la unidad de TI.

b) Plan estratégico de TI:

– Existe un plan estratégico pero no está apoyado en planes tácticos donde detallen cómo se lograrán los objetivos planteados. No hay detalles de tiempos, recursos afectados, costos, hitos intermedios a alcanzar, riesgos relacionados. Por consiguiente, no se hace posible un correcto control y seguimiento.

c) Arquitectura de la información:

– No hay definido un modelo de arquitectura de la información que abarque a la organización íntegra.

d) Administración de proyectos:

– La unidad de TI no dispone de una metodología de administración de proyectos que se aplique en todos los proyectos informáticos

e) Desarrollo, mantenimiento o adquisición de software de aplicación:

– La unidad de TI dispone de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, pero no se aplica en todos los casos.

f) Seguridad:

– Existe una política de seguridad pero no se puede instrumentar completamente por falta de recursos humanos.

– Disposición ONTI – SGP 6/2005 "Modelo de política de seguridad de la información para organismos de la Administración Pública Nacional de la Secretaría de la Gestión Pública".

Ha sido adoptada por el organismo en su totalidad, aunque se destaca que la función de la administración de la seguridad se encuentra a cargo de un único funcionario.

– Decreto 375/2005 Plan Nacional de Gobierno Electrónico.

a) No se presentó ante la Secretaría de Gestión Pública un informe de diagnóstico de la situación del organismo con respecto al Plan Nacional de Gobierno Electrónico.

b) No está formalizado un plan táctico de implementación de la firma digital. El grado de avance de su implantación se encuentra en estado inicial. Al momento de los trabajos de campo de la auditoría, sólo se encontraba en funcionamiento el circuito de viáticos.

– Disposición ONTI 69/2011 "Pautas de accesibilidad para sitios web".

Ha sido adoptada por el organismo en forma aceptable salvo algunas observaciones menores.

Nivel de riesgo: alto.

Nivel de madurez: repetible. Existe el entendimiento de la necesidad de cumplir con los requerimientos externos y la necesidad se comunica. En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente, como en los reglamentos regulatorios o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año tras año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de cumplimiento.

4.4. Proporcionar gobierno de TI

Nivel de riesgo: alto.

Nivel de madurez: inicial. Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. Existen enfoques ad hoc aplicados individualmente o caso por caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación no formal sobre los temas para proceder a su resolución.

Observaciones:

Falta establecer un marco de gobierno de TI con un entorno de control con prácticas inequívocas que aseguren:

– El alineamiento de TI en el cumplimiento de las metas estratégicas del organismo.

– Tratamiento uniforme para la administración de todos los proyectos de TI.

– El cumplimiento de leyes y regulaciones.

– Medir la contribución de TI a los objetivos estratégicos del organismo. Rendición de cuentas.

– 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 permitan acciones correctivas.

– Evaluación periódica de riesgos que permita reportar aquéllos relacionados con TI y su impacto en la posición de riesgos de la organización.

El proyecto de informe de auditoría fue enviado en vista al organismo auditado para que formule las aclaraciones y/o comentarios que estime pertinentes por nota AGN 24/14-AG4 recibida el 12/5/14. El INTA, previa solicitud de prórroga, envía el descargo el 19/6/14, recepcionado por AGN el 16/7/14. Del análisis realizado, se modifican los puntos 3.3, elevando el nivel de madurez de "inicial" a "parcialmente repetible"; 3.8 (administrar la mesa de servicio y los incidentes) en donde se levantó la observación referida a "No se alimenta una base de conocimientos, donde se registren soluciones estándar para determinados problemas en particular que puedan reiterarse a futuro"; y 3.10 (administración de problemas) suprimiendo el párrafo "No hay un repositorio centralizado de inventarios de activos de TI". Como resultado se mantienen todas las observaciones formuladas.

La AGN efectúa las siguientes recomendaciones al INTA:

1. Planificar y organizar

1.1. Definir un plan estratégico para TI

El plan estratégico de TI debe incluir: el presupuesto de la inversión/operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición y los requerimientos legales y regulatorios. Debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

Crear un conjunto de planes tácticos de TI que se deriven del plan estratégico de TI.

Identificar en el organismo las áreas que dependen de forma crítica de TI.

Evaluar el desempeño actual, el de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos estratégicos del organismo, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

1.2. Definir la arquitectura de información

Establecer y mantener un modelo de información que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en el plan estratégico.

Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos y archivos.

1.3. Determinar la dirección tecnológica

Planear la dirección tecnológica. Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es la apropiada para materializar la estrategia de TI y la arquitectura de sistemas del organismo. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de nuevas prestaciones. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

Elaborar un plan de infraestructura tecnológica.

Monitorear tendencias y regulaciónes futuras.

Establecer estándares tecnológicos.

Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento.

1.4. Definir los procesos, organización y relaciones de TI

Ubicar a la función de TI dentro de la estructura organizacional general. En especial, en función de la criticidad que representa para los objetivos estratégicos del organismo y el nivel de dependencia operativa.

Establecer una estructura organizacional de TI interna y externa que refleje las necesidades de la organización.

Definir y comunicar tanto los roles como las responsabilidades para el personal de TI y los usuarios, que delimiten la autoridad entre el personal de TI y los usuarios finales. Definir las responsabilidades y la rendición de cuentas para alcanzar los objetivos estratégicos del organismo.

Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA).

Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel apropiado.

Proporcionar al organismo los procedimientos y herramientas que le permitan asumir sus responsabilidades de propiedad sobre los datos y los sistemas de información.

Evaluar los requerimientos de personal de forma regular o cuando existan cambios impor-tantes en las necesidades estratégicas del organismo, operativos o de TI.

Definir e identificar al personal clave de TI y minimizar la dependencia en ellos.

Establecer un comité estratégico de TI que deberá asegurar que el gobierno de TI asesore sobre la dirección estratégica y revise las inversiones principales.

Establecer un comité directivo de TI para determinar las prioridades de los programas de inversión de TI, dar seguimiento de los proyectos y resolver los conflictos de recursos, y monitorear los niveles y las mejoras del servicio.

1.5. Administrar la inversión en TI

Establecer un marco de administración financiera para TI que impulse la presupuestación, con base en el grupo de proyectos de inversión en bienes y servicios.

Implantar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI contemplando operaciones, proyectos y mantenimiento.

Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en los programas de inversión en TI.

Implantar un proceso de administración de costos que compare los costos reales con los presupuestados.

Implantar un proceso de monitoreo de beneficios que permita medir la contribución esperada de TI a los objetivos estratégicos. Desarrollar un presupuesto por centro de costos y asociado al presupuesto.

1.6. Comunicar las aspiraciones y la dirección de la gerencia de TI

Asegurar que el conocimiento y el entendimiento de los objetivos estratégicos del organismo y de TI se comunican a toda la organización.

Asegurarse que las políticas de TI se implantan comunican a todo el personal relevante de tal forma que estén incluidas y sean parte integral de las operaciones organizacionales.

Definir los elementos de un ambiente de control para TI.

Elaborar a dar mantenimiento a un marco de trabajo que establezca el enfoque del organis-mo hacia los riesgos y hacia el control interno.

Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI.

1.7. Administrar los recursos humanos de TI

Asegurarse de que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales del personal.

Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento.

Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y retribuciones del personal.

Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad.

Minimizar la exposición de dependencias críticas sobre individuos clave por medio de la documentación y divulgación del conocimiento, como también la planeación de la sucesión o rotación de personal.

Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI para el personal que cubra funciones críticas, contratistas y proveedores.

Que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas del organismo, estándares establecidos o responsabilidades específicas del puesto.

Tomar medidas respecto a los cambios en los puestos, en especial, las culminaciones sea por renuncia o despido. Se debe realizar la transferencia del conocimiento, reasignar responsabili-dades y eliminar los privilegios de acceso.

1.8. Administrar la calidad

Se debe establecer un Sistema de Administración de la Calidad (SAC) que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los objetivos estratégicos del organismo. El SAC debe identificar los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades.

Se debe elaborar y comunicar un plan global de calidad que promueva la mejora continua, de forma periódica a través de mediciones para monitorear el cumplimiento continuo del SAC, así como el valor que el SAC proporciona.

1.9. Evaluar y administrar los riesgos de TI

Se debe integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos del organismo.

Se debe establecer el entorno en el cual el marco de trabajo de evaluación de riesgos se aplique para garantizar resultados apropiados.

Se deben identificar todas aquellas amenazas y vulnerabilidades que tengan un impacto po-tencial sobre las metas o las operaciones del organismo, aspectos estratégicos, regulatorios, legales, tecnológicos, de recursos humanos y operativos. Determinar la naturaleza del impacto y dar mantenimiento a esta información.

Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados.

Identificar a los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas que garanticen que los controles y las medidas de seguridad mitigan la exposición de forma continua.

Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos.

Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

1.10. Administrar proyectos

Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado.

Establecer un sistema de control de cambios de modo tal que todas las modificaciones a la línea base o indicadores al inicio del proyecto, se revisen, aprueben e incorporen de manera apropiada al plan integrado, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

Identificar las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado.

Medir el desempeño del proyecto contra los criterios clave tales como el alcance, los tiempos, la calidad, los costos o los riesgos; identificar las desviaciones con respecto al plan; evaluar su impacto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, implantar y monitorear las medidas correctivas.

2. Adquirir e implementar

2.1. Adquirir o desarrollar y mantener software aplicativo: Establecer una metodología de Ciclo de Vida de Desarrollo de Sistemas (CVDS) que contemple:

–Diseño de alto nivel. Traducir los requerimientos a una modificación de diseño de alto nivel para desarrollo de software.

–Diseño detallado. Preparar el diseño detallado y los requerimientos técnicos del software de aplicación.

–Control y auditabilidad de las aplicaciones. Asegurar que los controles se traduzcan correctamente de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable.

–Seguridad y disponibilidad de las aplicaciones. Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados.

–Configuración e implantación de software aplicativo adquirido. Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba.

–Actualizaciones importantes en sistemas existentes. Seguir un proceso de desarrollo si-milar al de desarrollo de sistemas nuevos en el caso de que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales.

–Desarrollo de software aplicativo. Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseños, los estándares de desarrollo y documentación, y los requerimientos de calidad.

–Aseguramiento de la calidad del software. Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de la calidad del software, para cumplir con los estándares especificados en la definición de los requerimientos y en las políticas y procedimientos de calidad del organismo.

–Administración de los requerimientos de aplicaciones. Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estado de los requerimientos particulares, y que las modificaciones se aprueban a través de un proceso establecido de administración de cambios.

–Mantenimiento de software aplicativo. Desarrollar una estrategia y un plan para el man-tenimiento y pase a producción de software de aplicaciones.

2.3. Adquirir y mantener infraestructura tecnológica

–Plan de adquisición de infraestructura tecnológica. Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos funcionales y técnicos, y que esté de acuerdo con la dirección tecnológica del organismo.

–Protección y disponibilidad del recurso de infraestructura. Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

—Mantenimiento de la infraestructura. Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios.

–Ambiente de prueba de factibilidad. Establecer el ambiente de desarrollo y de pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura totalmente independiente del ambiente de producción, en las primeras fases del proceso de adquisición y desarrollo.

2.4. Facilitar la operación y el uso

–Marco para la documentación de sistemas. Desarrollar un plan para identificar y documen-tar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan elaborar procedimientos de administración, de usuario y de operaciones.

–Transferencia de conocimiento. Transferir el conocimiento a niveles gerenciales para permitirles tomar posesión del sistema y los datos, ejercer la responsabilidad por la entrega y calidad del servicio, del control interno y de los procesos administrativos de la aplicación.

–Transferencia de conocimiento a usuarios finales. Transferencia de conocimientos para permitir que los usuarios finales utilicen con efectividad y eficiencia la aplicación como apoyo a los procesos del organismo.

–Transferencia de conocimiento al personal de operaciones y soporte. Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

2.5. Adquirir recursos de TI

–Control de adquisición. Desarrollar y seguir un conjunto de procedimientos y estándares consistente con

el proceso general y la estrategia de adquisiciones del organismo, para garantizar que la compra de infraestructura, instalaciones, hardware, sosftware y servicios relacionados con TI, satisfagan los requerimientos del organismo.

–Administración de contratos con proveedores. Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores.

–Selección de proveedores. Seleccionar proveedores mediante una práctica justa y formal para garantizar la elección del mejor basado en los requerimientos que se han desarrollado.

–Adquisición de sosftware. Garantizar que se protegen los intereses del organismo en todos los acuerdos contractuales de adquisición.

–Adquisición de recursos de desarrollo. Garantizar la protección de los intereses del organismo en todos los acuerdos contractuales de adquisición.

–Adquisición de infraestructura, instalaciones y servicios relacionados. Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación para la adquisición de infraestructura, instalaciones y servicios relacionados.

2.6. Administrar cambios

–Establecer procedimientos de administración de cambios formales para manejar de ma-nera estándar todas las solicitudes, incluyendo mantenimiento y actualizaciones, para cambios y aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

–Evaluación de impacto, priorización y autorización. Garantizar que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en los sistemas y su fun-cionalidad.

–Cambios de emergencia. Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.

–Seguimiento y reporte del estado del cambio. Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes y a los interesados relevantes del cambio, acerca del estado del mismo.

–Cierre y documentación del cambio. Siempre que se implantan cambios al sistema, actualizar el o los sistemas asociados, la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar su implantación completa.

2.7. Instalar y acreditar soluciones y cambios

–Entrenamiento. Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación y modificación de sistemas de información.

–Plan de pruebas. Establecer un plan de pruebas y obtener la aprobación de los principales involucrados.

–Plan de implantación. Establecer un plan de implantación y obtener la aprobación de los principales involucrados.

–Ambiente de prueba. Establecer un ambiente de prueba independiente.

–Conversión de sistema y datos. Garantizar que los métodos de desarrollo del organismo contemplen para todos los proyectos de desarrollo, implantación y modificación, todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, interfaces con otros sistemas, procedimiento, documentación de sistemas, etcétera, y sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se debe desarrollar y mantener pistas de auditoría de los resultados previos y posteriores a la conversión.

–Prueba de cambios. Garantizar que se prueban los cambios de acuerdo con un plan de aceptación definido y en base a una evaluación de impacto y de recursos.

–Prueba final de aceptación. Garantizar que los procedimientos proporcionan una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.

–Transferencia a producción. Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación.

–Liberación de software. Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, seguimiento, procedimientos de respaldo y notificación de usuario.

–Distribución del sistema. Establecer procedimientos de control para asegurar la distri-bución oportuna y correcta, y la autorización de los componentes aprobados de la configuración.

–Registro y rastreo de cambios. Monitorear los cambios a sistemas aplicativos, procedimientos, procesos, sistemas y a las plataformas.

–Revisión posterior a la implantación. Establecer procedimientos para una revisión posterior a la implantación del sistema para evaluar y reportar si el cambio satisfizo los requerimientos del usuario y entregó los beneficios esperados.

3. Entregar y dar soporte

3.1. Definir y administrar los niveles de servicio

Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el usuario y el prestador de servicio.

Definir la estructura organizacional para la administración del nivel de servicio, incluyen-do los roles,

tareas y responsabilidades de los proveedores externos e internos y de los usuarios.

3.2. Administrar servicios de terceros

Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.

3.3. Administrar el desempeño y la capacidad

Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, que asegure su disponibilidad, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los acuerdos de nivel de servicio.

Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares.

3.4. Garantizar la continuidad del servicio

Desarrollar un marco de trabajo de continuidad de TI para soportar los servicios a lo largo de todo el organismo. Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del organismo.

3.5. Garantizar la seguridad de los sistemas

Administrar la seguridad de TI al nivel más apropiado dentro del organismo, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del organismo.

3.6. Identificar y asignar costos

Desarrollar un modelo orientado a los centros de costos. Identificar todos los costos de TI para soportar un modelo de costos transparente.

3.7. Educación y capacitación de los usuarios

Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados.

3.8. Administrar la mesa de servicio y los incidentes

Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimien-tos de servicio y solicitudes de información.

Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI.

Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de manera que el servicio pueda mejorarse de forma continua.

3.9. Administrar la configuración

Establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos de configuración.

3.10. Administración de problemas

Garantizar una adecuada administración de problemas e incidentes. El sistema de admi-nistración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.

3.11. Administración de datos

Establecer mecanismos para garantizar que el proceso reciba los documentos originales correctos, que se procese toda la información recibida, que se preparen y entreguen todos los reportes de salida requeridos y que las necesidades de reinicio y reproceso estén soportadas.

Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera tal que éstos permanezcan accesibles y utilizables.

Probar los medios de respaldo y el proceso de restauración.

3.12. Administración de instalaciones

Definir y seleccionar los centros de datos físicos para los equipos de TI que soportan la estrategia de tecnología ligada a la estrategia del organismo. Debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre, considerando las leyes y regulaciones correspondientes.

Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del ente.

Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos, las especificaciones del proveedor y los lineamientos de seguridad y salud.

Disponer un sitio alternativo de procesamiento.

Incorporar a un plan de contingencia los procedimientos que mitiguen los daños que puedan presentarse en situaciones de exposición al riesgo.

3.13. Administración de operaciones

Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciónes está familiarizado con todas las tareas de operación relativas a ellos.

Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o disminución del desempeño.

4. Monitorear y evaluar

4.1. Monitorear y evaluar el desempeño de TI

Establecer un marco de trabajo de monitoreo general que abarque a todas las áreas y un en-foque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI. Monitorear la contribución de TI a los objetivos estratégicos del organismo.

Comparar en forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar me-

didas correctivas para resolver las causas subyacentes cuando hay desvíos.

Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes.

4.2. Monitorear y evaluar el control interno

Monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos del organismo.

Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI.

Evaluar la completitud y efectividad de los controles de gerencia sobre los procesos, políti-cas y contratos de TI por medio de un programa continuo de autoevaluación.

Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

4.3. Garantizar el cumplimiento con requerimientos externos

Identificar, sobre una base continua, leyes, regulaciones y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI del organismo.

Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios.

4.4. Proporcionar gobierno de TI

Definir, establecer y alinear el marco de gobierno de TI con la visión completa del entorno de control y gobierno corporativo. Basar el marco de trabajo en un adecuado proceso de TI y modelo de control. Proporcionar la transición de cuentas y prácticas inequívocas para evitar la pérdida del control interno. Confirmar que el marco de gobierno de TI asegura el cumplimiento de las leyes y regulaciones y que está alineado a la estrategia y objetivos del organismo. Informar del estado y cuestiones de gobierno de TI.

Facilitar el entendimiento de la alta gerencia sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre las altas gerencias y las funciones de TI sobre la contribución potencial de TI a los objetivos estratégicos del organismo.

La AGN, como resultado de las observaciones efectuadas, análisis del descargo del orga-nismo y de las recomendaciones formuladas, arriba a las siguientes conclusiones:

En el futuro el mundo enfrentará el gran desafío de alimentar a cada vez más población. También es ampliamente conocido quiénes serán los países que podrán ofrecer los alimentos y quiénes fraccionarán el consumo.

El INTA, entre otros, será el responsable de acuerdo con sus misiones y funciones de pro-veer la ciencia, el conocimiento y la gestión para poder desarrollar y aplicar las soluciones sustentables, generando una mayor productividad, cuidando el medio ambiente, optimizando los recursos disponibles y los factores sociales en forma equilibrada.

Una adecuada administración de la TI será indispensable para cumplir con esos objetivos.

La tecnología de comunicaciones ha avanzado desde un nivel en el que los paradigmas organizacionales en los años 80 imponían procesos distribuidos (momento en que el instituto inició el proceso de descentralización administrativa), a un esquema centralizado, de tablero de comando.

Actualmente el organismo, en materia tecnológica, se encuentra en un período de transición. Entre los años 2006 y 2007, se elaboró un proyecto denominado "Plan Estructurante" (PE) donde se detalló el estado de situación en materia tecnológica y las acciones que se iban a adoptar. Desde entonces, hasta el año 2011, donde hubo una renovación en las estructuras orgánicas de TI, no se tomaron acciones relevantes.

A partir de ese año, se encaró un proyecto financiado por el Banco Interamericano de Desarrollo (BID) y el Banco Internacional de Recuperación y Fomento (BIRF–Banco Mundial) en el marco del programa PROSAP por el cual se pretende unir en una red corporativa, aproximadamente 420 puntos hacia fines del 2013. Al momento de los trabajos de campo de la auditoría, se estaba cumpliendo con aproximadamente el 78 % de los objetivos planteados.

Cabe señalar que la tarea se viene desarrollando con muchas limitaciones, principalmente por la falta de:

–Recursos humanos. En la administración central, la Dirección Naciónal Asistente de Información, Comunicaciones y Calidad cuenta con una dotación inferior a las necesidades para cubrir puestos básicos en la gestión de TI. Además, la estructura de referentes informáticos en el interior del país es insuficiente para mantener la infraestructura informática.

–Planificación. Por ejemplo, el tráfico de red, se ha dimensionado sin tomar en cuenta los aplicativos existentes, deserrollados en las distintas unidades del organismo y que de comprobarse su utilidad, deberían adoptarse como corporativos.

Ademàs, algunas situaciones que se diagnosticaron en el PE persisten:

–Las aplicaciones existentes (a excepción del e-SIGA) no están preparadas para obtener indicadores de gestión y no satisfacen todos los requisitos de las áreas involucradas, ya que éstos no se consideraron y, además, los procesos no están completamente sistematizados o, en algunos casos, la tecnología utilizada no lo permite.

–Las distintas unidades de la organización han desarrollado aplicaciones locales, de muchas de las

cuales no se tiene conocimiento en la administración central. Estas aplicaciones se desarrollaron con distintas metodologías de hardware y software, con lo cual existe la posibilidad de que frente a una misma problemática, distintas unidades hayan implementado soluciones similares, que haya redundancia de datos y que la información no esté integrada.

–Producto de lo expresado en el punto anterior, existen falencias en consideraciones que hacen a la seguridad, la integridad y la confiabilidad de la información, lo que posibilita la posible pérdida o fuga.

–Ausencia de documentación de las aplicaciones, lo que genera dependencia crítica sobre individuos.

El modelo genérico de madurez aplicado en la auditoría y los niveles de madurez detecta-dos, indican que los distintos procesos de la gestión de la tecnología informática en el instituto se encuentran principalmente entre el nivel inicial y el nivel repetible.

La adecuada implementación de esta autopista de información, permitirá al organismo, bajo rigurosas normas que tiendan a la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad contar con buena información en tiempo real como base para poder llegar a buenos diagnósticos y a partir de éstas, tomar decisiones oportunas.

A través de aplicaciones corporativas, se podrán compartir datos, experiencias, conocimientos y llegar con nuevas tecnologías al productor.

La alta dirección debe reconocer los beneficios de la tecnología de información y utilizarla para impulsar el beneficio esperado de los objetivos estratégicos, entendiendo los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados, así como el incremento de requerimientos para controlar la información, deben considerarse como elementos clave del gobierno corporativo.

Para el organismo, la información y la tecnología que la soporta, junto con los recursos humanos altamente especializados, son sus más valiosos activos.

Pablo G. González. – Enrique A. Vaquié. – Gerardo R. Morales. – Eric Calcagno y Maillmann. – José M. Díaz Bancalari. – Manuel Garrido. – Julio R. Solanas. – Juan M. Abal Medina. – María E. Labado. – Andrea F. García.

ANTECEDENTES

1

Dictamen de comisión

Honorable Congreso:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas, ha considerado el expediente Senado de la Nación O.V.-365/14 mediante el cual la Auditoría General de la Nación comunica resolución 171/14, aprobando el informe de auditoría referido a evaluación de la Tecnología Informática del Instituto Nacional de Tecnología Agropecuaria (INTA) Sede Central; 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 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 de Agricultura, Ganadería y Pesca de la Nación, cuyo objeto fue la evaluación de la Tecnología Informática (TI) del Instituto Nacional de Tecnología Agropecuaria (INTA), Sede Central.

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, 28 de mayo de 2015.

Pablo G. González. – Enrique A. Vaquié. – Gerardo R. Morales. – Eric Calcagno y Maillmann. – Manuel Garrido. – Nanci M. A. Parrilli. – Julio R. Solanas. – Juan M. Abal Medina. – María E. Labado. – Andrea F. García.

2

Ver expediente 176-S.-2016.

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