SESIONES ORDINARIAS

2010

ORDEN DEL DÍA Nº 2038

COMISIÓN PARLAMENTARIA MIXTA REVISORA DE CUENTAS

Impreso el día 29 de abril de 2011

Término del artículo 113: 10 de mayo de 2011

SUMARIO: **Pedido** de informes al Poder Ejecutivo sobre las medidas adoptadas a los efectos de regularizar las situaciones observadas por la Auditoría General de la Nación con motivo de su examen en el ámbito del Ministerio de Justicia, Seguridad y Derechos Humanos, con el objeto de evaluar la gestión de la Tecnología de la Información en la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios (DNRPA), para determinar la madurez y los riesgos en su administración de la información.

1. (1.681-D.-2011.)
2. (310-O.V.-2010.)

Dictamen de comisión

Honorable Cámara:

Vuestra Comisión Parlamentaria Mixta Revisora de Cuentas ha considerado el expediente O.V.-310/10, mediante el cual la Auditoría General de la Nación comunica resolución159/10, aprobando el informe referido a evaluar la gestión de la Tecnología de la Información, en la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios, para determinar la madurez y los riesgos en su administración de la información; 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 a los fines de regularizar las situación observadas por la Auditoría General de la Nación, con motivo de su examen en el ámbito del Ministerio de Justicia, Seguridad y Derechos Humanos, con el objeto de evaluar la gestión de la Tecnología de la Información en la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios (DNRPA), organismo descentralizado en la órbita del Ministerio de Justicia, para determinar la madurez y los riesgos en su administración de la información.

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

De acuerdo con las disposiciones pertinentes el presente dictamen pasa directamente al orden del día.

Sala de la comisión, 2 de marzo de 2011.

Heriberto A. Martínez Oddone. – Nicolás A. Fernández. – Luis A. Juez. – Gerardo R. Morales. – Ernesto R. Sanz. – Juan C. Morán. – Gerónimo Vargas Aignasse. – José M. Díaz Bancalari. – Walter A. Agosto.

FUNDAMENTOS

Expediente O.V.-310/10 - Resolución AGN 159/10.

La Auditoría General de la Nación (AGN) efectuó un examen en el ámbito del Ministerio de Justicia, Seguridad y Derechos Humanos, con el objeto de evaluar la gestión de la Tecnología de la Información (TI) en la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios (DNRPA), organismo descentralizado en la órbita del Ministerio de Justicia, para determinar la madurez y los riesgos en su administración de la información. Período auditado: julio 2008 a junio 2009.

Las tareas de campo abarcaron desde septiembre de 2009 hasta diciembre de 2009.

En el apartado 2. "Alcance del examen" la AGN señala lo siguiente:

2.1. En la etapa de planificación identificó los temas de mayor exposición al riesgo mediante la realización de las siguientes actividades:

– Relevamiento de la documentación normativa del área de tecnología informática del organismo.

– Relevamiento de la infraestructura informática del organismo.

– Relevamiento de los sistemas existentes en producción y desarrollo.

– Verificación de la adecuación de los sistemas, la infraestructura y la planificación para lograr las misiones y metas del organismo y cumplir con las leyes y decretos que regulan su actividad.

– Verificación del modelo de arquitectura de la información y su seguridad.

– Relevamiento y análisis del organigrama del área de tecnología informática y su funcionamiento.

– Verificación del cumplimiento de la comunicación de los objetivos y las directivas de la gerencia.

– Análisis de la administración de recursos humanos, el cumplimiento de los requerimientos externos, la evaluación de riesgos, la administración de proyectos, la administración de calidad y las prácticas de instalación y acreditación de sistemas y de administración de cambios.

– Análisis de:

- la definición de los niveles de servicio,
- la administración de los servicios prestados por terceros,
- la administración de la capacidad y el desempeño,
- los mecanismos que garantizan el servicio continuo y la seguridad de los sistemas,
- la imputación de costos,
- la educación y capacitación de los usuarios,
- la asistencia a los clientes de la tecnología de la Información,
- la administración de la configuración de hardware y software,
- la administración de problemas e incidentes,
- la administración de datos, de instalaciones y de operaciones.

Análisis del control de los procesos, la idoneidad del control interno y de su monitoreo.

2.2. En este punto informa sobre las fuentes de las que obtuvo información. En tal sentido indica entrevistas con distintos funcionarios; cuestionario para determinar las necesidades de análisis detallado; cuestionarios para el análisis detallado de los temas que lo requerían; inspecciones directas en el área informática de la Dirección para determinar las condiciones actuales de la administración de la información en el organismo.

2.3. Informa que no fue objeto de la presente auditoría el análisis del aplicativo de la dirección.

2.4. *Metodología:* expresa que la auditoría incluyó dos etapas: la primera, de planificación del análisis detallado; la segunda, de verificación de lo informado en la primera etapa, por medio de pruebas sustantivas y de cumplimiento.

En la etapa de planificación incluyeron las siguientes actividades:

– análisis del marco legal e institucional del funcionamiento de la dirección nacional,

– análisis de los informes de auditoría interna y externa en temas informáticos,

– entrevistas con responsables del área informática de DNRPA,

– análisis de las minutas de reunión para determinar las necesidades de análisis detallado.

Asimismo, en la etapa de verificación se incluyó:

– inspecciones in situ y entrevistas con personal subalterno, realizadas por especialistas en diversas ramas de la informática, a través del trabajo directo en el campo,

– entrevistas con usuarios de los servicios informáticos.

Señala que en función de la información relevada y los niveles de riesgo estimados, se definieron los trabajos de campo convenientes para realizar las verificaciones necesarias.

En el apartado 3. "Aclaraciones previas", se informa sobre el marco legal e institucional de la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios (DNRPA), informando que es un organismo dependiente del Ministerio de Justicia y Derechos Humanos, cuya misión es regular todo lo concerniente al dominio, trasmisión, prueba y crédito prendario de los automotores.

Asimismo, hace saber que existe un convenio de Cooperación técnica y financiera entre la Asociación de Concesionarios de Automotores de la República Argentina (ACARA) y la Secretaría de Justicia mediante el cual la asociación contribuye al mejor funcionamiento y a la modernización de los métodos operativos de la Dirección Nacional de los Registros Nacionales de la Propiedad Automotor y Créditos Prendarios.

En el apartado 4. "Comentarios y observaciones" señala que basó su tarea en la verificación de los objetivos de control establecidos por las normas COBIT (Control Objectives in Information Technologies). Los objetivos de control describen los resultados que debe alcanzar un organismo implantando procedimientos de control en los procesos de TI.

Agrega que para cada una de las observaciones se menciona el nivel de madurez que le corresponde. Además, para cada uno de los objetivos de control, se indica qué requerimientos de la información son afectados.

Destaca que cada objetivo de control va acompañado de su nivel de riesgo genérico (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. Ese nivel genérico es modificado por el índice de madurez correspondiente (dependiente de las observaciones realizadas) para establecer el riesgo específico para ese objetivo, en el caso particular.

En el punto 4.1. "Planificación y organización" efectúa los siguientes comentarios y observaciones:

4.1.1. *Definición de un Plan Estratégico de TI.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la eficiencia.

Nivel de madurez: Inicial. La dirección reconoce la necesidad de una planificación estratégica de TI, pero no hay un proceso de decisión estructurado. La planificación estratégica esta determinada por necesidades puntuales. Por lo tanto, los resultados son esporádicos, no uniformes. La alineación de los requerimientos del organismo, las aplicaciones y la tecnología se realiza en forma reactiva, impulsada por propuestas de los proveedores, y no por una estrategia para toda la organización. La posición de riesgo estratégico se identifica informalmente proyecto por proyecto.

Observaciones: No se recibió el plan estratégico del organismo.

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

4.1.2. *Definición de la arquitectura de la información.*

Objetivo de control: La información debe mantenerse acorde con las necesidades y debe ser identificada, recopilada y comunicada en tiempo y forma de modo de permitir a las personas cumplir sus responsabilidades de manera eficiente y oportuna. Se debe crear y mantener un modelo de arquitectura de información que incluya el modelo de datos del organismo y los sistemas de información relacionados.

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la eficiencia,

– la confidencialidad,

– la integridad.

Nivel de madurez: Inicial. El área de TI reconoce la necesidad de una arquitectura de la información, pero no ha formalizado ni un proceso ni un plan para desarrollarla. Hay un avance aislado y reactivo de los componentes de la arquitectura de la información. Existen implementaciones aisladas y parciales de reglas de sintaxis y diagramas de datos y documentación. Las decisiones se basan en datos aislados, en lugar de basarse en un conjunto organizado de ellos, con un significado que facilita la toma de decisiones.

Observaciones: Existe conciencia de la importancia de la arquitectura de la información pero no se avanzó en el tema, no se ha definido el sector responsable ni se crearon sus misiones y funciones; no existe un modelo al respecto ni políticas y procedimientos al efecto.

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

4.1.3. *Determinación de la Dirección Tecnológica.*

Objetivo de control: Se debe crear y mantener un plan de infraestructura tecnológica que fije y administre expectativas claras y realistas de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de entrega.

Este objetivo de control afecta, primariamente:

– la eficacia,

– y en forma secundaria:

– la eficiencia.

Nivel de madurez: Inicial. No hay políticas ni procesos formales definidos para el tema. Tampoco existen políticas y procedimientos para evaluar y monitorear tendencias, ni para que dichas evaluaciones sean tenidas en cuenta durante el desarrollo y mantenimiento del plan de infraestructura tecnológica. El desarrollo de los componentes y la implementación de nuevas técnicas son realizados ad hoc. Estas tareas no figuran en las misiones y funciones. Las direcciones tecnológicas son manejadas por los planes de evolución de los organismos rectores en la materia y por la oferta de los proveedores de productos de hardware, software de sistemas y software de aplicaciones. No hay análisis ni comunicación normalizados del impacto potencial de los cambios tecnológicos.

Observaciones: No hay plan de infraestructura tecnológica. El organismo no cuenta con estructura aprobada y consecuentemente tampoco con las misiones y funciones de sus sectores internos. Se tiene conciencia de la importancia que la planificación de infraestructura reviste para el organismo pero no se ha definido formalmente un área para determinar la dirección tecnológica. A la fecha, no existe normativa para la función.

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

4.1.4. *Definición de la organización y las relaciones de TI.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la eficiencia.

Nivel de madurez: Inicial. Las actividades y funciones de TI son reactivas y no hay uniformidad en la implementación. No hay una estructura organizacional definida, los roles y responsabilidades están asignados informalmente y no hay líneas claras de responsabilidad. La función de TI se considera una función de soporte y carece de una perspectiva como organización global.

Observaciones: El organismo no cuenta con estructura aprobada de informática en general y consecuentemente tampoco con sus misiones y funciones ni con las de sus sectores internos. No existe el comité de planificación de servicios de información, ni su estructura con misiones y funciones formalizadas.

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

4.1.5. *Administración de la inversión en tecnología de información.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la confiabilidad.

Nivel de madurez: Repetible. Hay un entendimiento implícito de la necesidad de selección y presupuestación de la inversión de TI. Se ha comunicado la necesidad de establecer un proceso a tal fin. El cumplimiento queda librado a la iniciativa de las distintas personas del organismo. Aparecen técnicas comunes para desarrollar los componentes del presupuesto de TI. Se toman decisiones de presupuestación reactivas. Comienzan a enunciarse expectativas basadas en tendencias de la tecnología y a considerarse en las decisiones de inversión su impacto sobre la productividad y los ciclos de vida de sistemas.

Observaciones: No existe en el organismo una política formal ni un procedimiento de formulación presupuestaria que garanticen el establecimiento de un presupuesto operativo anual y su aprobación. Tampoco existen los planes estratégicos del organismo y de TI que permitan orientar la inversión. No se hace un seguimiento o monitoreo de las inversiones y los gastos de TI.

La totalidad de las contrataciones de TI que realiza el organismo, se efectúan a través del ente cooperador constituido por la Asociación de Concesionarios Automotor de la República Argentina, (ACARA), por lo cual no resulta necesario satisfacer las normas de contrataciones vigentes para la administración pública nacional.

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

4.1.6. *Comunicación de los objetivos y directivas de la gerencia.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– el cumplimiento.

Nivel de madurez: Inicial. La dirección es reactiva en el abordaje de los requerimientos del ambiente de control de la información. Las políticas, procedimientos y normas se desarrollan y comunican en forma ad hoc, en función de las necesidades, impulsadas principalmente por problemas. Los procesos de desarrollo, comunicación y cumplimiento son informales y no siguen criterios uniformes.

Observaciones:

No hay:

– políticas formales que impongan un comportamiento de los funcionarios vinculado a la ética, áreas responsables de la formulación de políticas y procedimientos,

– un marco de referencia y un proceso de revisión periódica de estándares, políticas, directrices y procedimientos,

– una política de calidad ni de minimización de riesgos,

– una política formal de seguridad,

– sanciones disciplinarias definidas para la falta de cumplimiento de las políticas de seguridad y control interno,

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

4.1.7. *Administración de los recursos humanos de TI.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia.

Nivel de madurez: Inicial. La dirección reconoce la necesidad de la administración de los recursos humanos pero no ha formalizado ningún proceso o plan. El proceso de administración de los recursos humanos de TI es informal y tiene un enfoque reactivo y concentrado en las operaciones para la contratación y administración del personal.

Observaciones: Los roles y responsabilidades de las distintas funciones del área informática no están formalmente definidos. Todo el personal del área es contratado con excepción del coordinador del área. No existe una política formal de reclutamiento y promoción. No hay un proceso adecuado de evaluación de desempeño del personal que ocupa los cargos del área informática.

La totalidad de los contratos del personal de TI del organismo, se efectúa a través de ACARA en su calidad de ente cooperador.

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

4.1.8. *Garantía del cumplimiento de los requisitos externos*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– el cumplimiento,

y en forma secundaria:

– la confiabilidad.

Nivel de madurez: Inicial. Se ha tomado conciencia de la importancia de cumplir las regulaciones, los contratos y la legislación que afectan al organismo. Se siguen procesos informales para mantener el cumplimiento, pero solo a medida que surge una necesidad en nuevos proyectos o en respuesta a auditorías o revisiones.

Observaciones: No existen políticas y procedimientos formales para:

– garantizar que se adopten en forma oportuna las medidas correctivas para evaluar los requisitos externos,

– diseñar los resguardos y objetivos de seguridad e higiene,

– garantizar el cumplimiento de las exigencias de los contratos de seguros.

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

4.1.9. *Evaluación y administración de riesgos*

Objetivo de control: La máxima autoridad debe definir un proceso por el cual el organismo se ocupa de identificar los riesgos de tecnología de la información y analizar su impacto, involucrando funciones multidisciplinarias y adoptando medidas eficaces en función de costos a fin de mitigar los riesgos.

Este objetivo de control afecta, primariamente:

– la confidencialidad,

– la integridad,

– la disponibilidad,

y en forma secundaria:

– la eficacia,

– la eficiencia,

– el cumplimiento,

– la confiabilidad.

Nivel de madurez: Inicial. El organismo conoce sus responsabilidades legales y contractuales, pero considera los riesgos de TI en forma ad hoc, sin seguir procesos o políticas definidas. Se llevan a cabo evaluaciones informales del riesgo de los proyectos. Es poco probable que se identifiquen evaluaciones de riesgo dentro de un plan. El departamento informático no especifica la responsabilidad por la administración de riesgos en las descripciones de puestos u otros medios. Los riesgos como la seguridad, disponibilidad e integridad, se consideran sobre la base de cada proyecto. Los riesgos relacionados que afectan las operaciones diarias son un tema tratado informalmente en reuniones de gestión. En los casos en que se tienen en cuenta los riesgos, no hay una mitigación uniforme.

Observaciones: No existe un marco formal de identificación y evaluación de riesgos.

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

4.1.10. *Administración de proyectos*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia.

Nivel de madurez: Repetible. El área de TI tomó conciencia y comunicó a su personal la necesidad de una gestión de los proyectos. La organización está en el proceso de aprender y repetir ciertas técnicas y métodos de un proyecto a otro. Sus objetivos institucionales y técnicos están definidos informalmente. Las partes interesadas en la administración participan de manera limitada. Se desarrollaron algunas pautas para la mayoría de los aspectos de su gestión, pero la aplicación queda a discreción de cada participante.

Observaciones: No hay un marco formal de administración de proyectos ni procedimientos de monitoreo de sus plazos y costos. No se da participación formal a los usuarios

externos al organismo. No existe una normativa formal para el desarrollo y mantenimiento de software. No hay una política de costos, ni normas para asegurar la calidad.

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

4.1.11. *Administración de la calidad*

Objetivo de control: Se debe elaborar un sistema de administración de calidad con procesos y estándares probados de desarrollo y de adquisición. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de errores y la comunicación de los resultados a los interesados.

Este objetivo de control afecta, primariamente:

–la eficacia,

–la eficiencia,

–la integridad

y en forma secundaria:

–la confiabilidad.

Nivel de madurez: Inicial. El organismo carece de un proceso de planificación de garantía de calidad y de una metodología de ciclo de vida de desarrollo de sistemas. La alta gerencia ha tomado conciencia de la necesidad de una garantía de la calidad pero los proyectos y las operaciones de TI, en general, no se controlan desde esta perspectiva.

Observaciones: No se aplican criterios de calidad y no existe metodología formal del ciclo de vida del desarrollo y mantenimiento de sistemas.

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

En el punto 4.2. "Administración e implementación", efectúa los comentarios y observaciones qen en cada caso se indican:

4.2.1. *Identificación de Soluciones Automatizadas.*

Objetivo de control: La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que las misiones del Organismo se satisfacen con un enfoque efectivo y eficiente. Este proceso debe cubrir la definición de las necesidades, considerar las fuentes alternativas, realizar una revisión de la factibilidad tecnológica y económica, ejecutar un análisis de riesgo y de costo-beneficio y concluir con una decisión final sobre desarrollar o comprar. Todos estos pasos permiten minimizar el costo para adquirir e implantar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos de la organización.

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la eficiencia.

Nivel de madurez: Repetible. Existen algunos enfoques intuitivos para identificar soluciones de TI y éstos varían según los temas. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de algunos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.

Observaciones: El organismo no posee políticas y procedimientos para identificar requerimientos funcionales y operativos para desarrollar, implementar y modificar las soluciones de sistemas. No hay políticas definidas que satisfagan los requerimientos de desempeño, confiabilidad, compatibilidad y legislación. No existen políticas para la identificación de alternativas a las soluciones de tecnología ni de la evaluación de la tercerización para la programación de software en comparación con los desarrollos propios.

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

4.2.2. *Adquisición y mantenimiento del software de aplicación*

Objetivo de control: Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del organismo. Este proceso cubre su diseño, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad de sus objetivos, de forma apropiada con las aplicaciones automatizadas correctas.

Se deben establecer estrategias de adquisición de software y evaluación de requerimientos y especificaciones para la contratación de terceros proveedores de servicios.

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

Este objetivo de control afecta, primariamente:

–la eficacia,

–la eficiencia,

y en forma secundaria:

–la integridad,

–el cumplimiento,

–la confiabilidad.

Nivel de madurez: Inicial. Se tomó conciencia de que se necesita un proceso para adquirir y mantener las aplicaciones. Sin embargo, los enfoques varían de proyecto a proyecto sin uniformidad y en general, en forma aislada de otros proyectos. No existe una metodología de adquisición formal, aceptada, entendida y aplicada. No existen políticas ni procedimientos que aseguren que la instalación y el mantenimiento del software se realice de acuerdo con un marco de desarrollo y mantenimiento definido y debidamente aprobado.

Observaciones: No existe una metodología común para el desarrollo y mantenimiento de sistemas para la organización.

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

4.2.3. *Adquisición y mantenimiento de la infraestructura tecnológica*

Objetivo de control: La organización debe contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado de manera de mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Este objetivo de control afecta, primariamente:

–la eficacia,

–la eficiencia,

y en forma secundaria:

–la integridad.

Nivel de madurez: Inicial. Si bien se reconoce que la infraestructura de la TI es importante, no hay un enfoque general uniforme. El organismo carece de políticas y procedimientos referentes a la adquisición, implementación y mantenimiento de hardware y software. Los cambios de infraestructura se introducen para cada nueva necesidad sin un plan general.

Observaciones: La organización no ha elaborado un plan de adquisición y mantenimiento de la Infraestructura tecnológica que permita asegurar que la configuración, la instalación y el mantenimiento del software de base no pongan en peligro los datos y programas que se almacenan. Por consiguiente se pudo observar que las adquisiciones en la materia no alcanzan a compensar el nivel de obsolescencia y el crecimiento vegetativo de los servicios, a prestar El inventario de la configuración no está debidamente actualizado.

No existen políticas ni procedimientos relacionados con:

– análisis de impacto de la incorporación de hardware y el software nuevos,

– análisis de integración entre distintas plataformas,

– análisis de tercerización con aprovechamiento de infraestructura interna o externa,

– el manejo de casos en los que se depende de un proveedor de única fuente,

– el mantenimiento preventivo del hardware.

La contratación de infraestructura de TI, se realiza a través del ente cooperador.

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

4.2.4. *Desarrollo y mantenimiento de procedimientos*

Objetivo de control: Se debe aplicar un enfoque estructurado para el desarrollo de procedimientos del usuario y de operaciones, requerimientos de servicios y materiales de capacitación. La metodología del Ciclo de vida de desarrollo de sistemas del organismo debe garantizar la definición oportuna de los requerimientos operativos y niveles de servicio, la preparación de manuales del usuario y de operaciones y el desarrollo de materiales de capacitación.

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la integridad,

– el cumplimiento,

– la confiabilidad.

Nivel de madurez: Inicial. La organización ha tomado conciencia de la necesidad de generar un marco estándar, definido y monitoreado, para el desarrollo de la documentación y los procedimientos. Ocasionalmente se produce documentación, pero está dispersa, es inconsistente y sólo está disponible para grupos limitados. Gran parte de la documentación y los procedimientos son incompletos, están desactualizados y prácticamente no hay integración de éstos entre distintos sistemas y unidades sustantivas. Los materiales de capacitación son aislados y de calidad variable.

Observaciones: No existe un marco estándar, definido y monitoreado, para el desarrollo de la documentación y los procedimientos. No se evalúan los requerimientos operativos tomando como base los datos históricos. No se definen ni planifican los requerimientos operativos, ni los niveles de servicio ni las expectativas de desempeño.

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

4.2.5. *Instalación y acreditación de aplicativos*

Objetivo de control: Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere ensayos adecuados en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación, la transición al ambiente de producción y revisar la posimplantación. Esto garantiza que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados esperados.

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la integridad,

– la disponibilidad.

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

Observaciones: Se carece de procesos estándares para la instalación y acreditación de aplicaciones. No se han separado los entornos de desarrollo, pruebas y producción. Los usuarios realizan las pruebas en entorno de desarrollo y los desarrolladores, junto con el administrador de la base de datos, pasan el software al entorno de producción. No hay mecanismos de aprobación formal de las pruebas por parte de los usuarios involucrados, previo al pasaje a producción. No se hace gestión de aseguramiento de la calidad de las aplicaciones a instalar.

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

4.2.6. *Administración de cambios.*

Objetivo de control: Todos los cambios, incluyendo el mantenimiento de emergencia y soluciones transitorias, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. Las modificaciones (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación; y revisar contra los resultados planeados. Esto garantiza la reducción de riesgos que impactan negativamente en la estabilidad o integridad del ambiente de producción.

Este objetivo de control afecta, primariamente:

–la eficacia,

–la eficiencia,

–la integridad,

–la disponibilidad,

y en forma secundaria:

–la confiabilidad.

Nivel de madurez: Inicial. Se reconoce que los cambios deberían ser administrados y controlados, pero no hay un proceso uniforme que pueda seguirse. Las prácticas varían y es probable que ocurran cambios no autorizados. La documentación de los cambios es escasa o nula y la documentación de la configuración es incompleta y poco confiable. Esto podría dar lugar a deficiencias e interrupciones en el ambiente de producción.

Observaciones: No se han establecido procedimientos similares para administrar cambios de manera estándar para todas las solicitudes realizadas.

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

En lo relativo al punto 4.3. “Entrega y soporte” señala lo siguiente:

4.3.1. *Definición y administración de los niveles de servicio*.

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

Este objetivo de control afecta, primariamente:

–la eficacia,

–la eficiencia,

y en forma secundaria:

–la confidencialidad,

–la integridad,

–la disponibilidad,

–el cumplimiento,

–la confiabilidad.

Nivel de madurez: Repetible. Los niveles de servicio están acordados pero son informales y no son revisados. Los reportes de los niveles de servicio están incompletos y pueden ser irrelevantes o engañosos para los clientes y dependen, en forma individual, de las habilidades y la iniciativa de los administradores. Está designado un coordinador de niveles de servicio con responsabilidades definidas, pero con autoridad limitada. Si existe un proceso para el cumplimiento de los acuerdos de niveles de servicio es voluntario y no está implementado.

Observaciones: No existe una política formalmente definida que promueva la definición de acuerdos de nivel de servicios, ni existen acciones que promuevan la participación de los usuarios en su definición. La responsabilidad de los usuarios se formaliza mediante un documento donde se establecen las condiciones para el uso de los sistemas pero no existe control del cumplimiento del mismo. La responsabilidad de los proveedores está definida caso por caso, sin una política general en los contratos. Los registros seccionales reciben una circular con recomendaciones sobre la infraestructura informática que deben poseer pero el documento que lo formaliza es una circular de la Coordinación de Sistemas y no una resolución de la DNRPA. Su cumplimiento no es obligatorio. La Coordinación de Sistemas evalúa el estado de los recursos informáticos de los registros seccionales de acuerdo a un procedimiento estándar y el resultado es informado a cada registro con el fin de señalarle los errores y faltas para que sean corregidas; pero el registro no tiene obligación formal de cumplir estas recomendaciones.

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

4.3.2. *Administración de servicios prestados por terceros*

Objetivo de control: El directorio debe implementar medidas de control orientadas a la revisión y al monitoreo de los contratos y procedimientos existentes para

garantizar su eficacia y el cumplimiento de la política del organismo.

Este objetivo de control afecta, primariamente:

–la eficacia,

– a eficiencia,

y en forma secundaria:

– la confidencialidad,

– la integridad,

– la disponibilidad,

– el cumplimiento,

– la confiabilidad.

Nivel de madurez: Repetible. El proceso de supervisión de los proveedores de servicios y de sus prestaciones es informal. Se usa un contrato firmado con términos y condiciones estándares para los proveedores y una descripción de los servicios a prestar.

Observaciones: No existen políticas formalmente definidas referidas a las relaciones con terceros. El organismo realiza las adquisiciones a través de un convenio suscrito en el año 1986 entre la Secretaria de Justicia y la Asociación de Concesionarios de la República Argentina, por él se establece un acuerdo de cooperación entre ambas organizaciones que tiene por finalidad mejorar el funcionamiento y modernizar los métodos operativos de la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios.

Por medio de este convenio la DNRPA le solicita al ente cooperador la provisión de distintos suministros que necesita, desde servidores y PC hasta insumos menores. Estas compras no siguen la normativa ni los procedimientos para compras del estado.

De la documentación recibida del organismo se observa que en las órdenes de compras de provisión de servicio de Internet y de transmisión de datos no adoptan los estándares mínimos sugeridos por la ONTI para este tipo de servicios.

Se analizó documentación sobre la compra de un software antivirus del año 2005 que por distintos motivos administrativos recién se terminó de adquirir en el año 2006. Actualmente la dirección está en una situación similar, la licencia del software antivirus se encuentra vencida desde hace más de dos meses y el mismo no se actualiza con el riesgo que esto implica.

De la documentación recibida se observó que los procedimientos de compras son excesivamente lentos, si bien el sistema fue ideado para que las mismas se realizaran en forma más dinámica al no tener que cumplir con las exigencias y controles que tiene el Estado. Actualmente existen demoras que impiden obtener en tiempo y forma los elementos indispensables para un buen funcionamiento del área de sistemas.

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

4.3.3. *Administración de la capacidad y el desempeño.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la disponibilidad.

Nivel de madurez: Repetible. Los responsables del organismo y la gerencia de TI están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general en base a evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas 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 de los usuarios.

Observaciones: No se realizan tareas de evaluación sobre la capacidad y desempeño en forma sistemática. No existen niveles de servicio definidos para los servicios prestados por el área de sistemas. La Coordinación de Sistemas emitió una circular con los requerimientos mínimos de equipamiento informático, para su redacción se tuvo en cuenta la opinión de los registros seccionales, pero el promedio de los mismos poseen un equipamiento obsoleto que desean seguir utilizando. Esta circular no es de cumplimiento obligatorio solo es una recomendación de un estándar mínimo para infraestructura informática.

No se utilizan herramientas específicas para monitorear el desempeño. No se pide información a los usuarios para establecer plazos o definiciones de servicios No se realizan informes sobre este tema, y los controles son informales.

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

4.3.4. *Garantía de un servicio continuo.*

Objetivo de control: Verificar si se ha implementado un plan probado y operativo de continuidad de TI que concuerde con el plan de continuidad general del organismo y los requerimientos de actividad relacionados.

Este objetivo de control afecta, primariamente:

–la eficacia,

–la disponibilidad,

y en forma secundaria:

–la eficiencia.

Nivel de madurez: Repetible. Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en los objetivos del organismo. No hay un plan documentado de continuidad de TI, aunque se hacen esfuerzos para mantener disponible el servicio. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.

Observaciones: No se encontró un plan formal de continuidad de los servicios de información del organismo ni planes de contingencia que analicen posibles causas, escenarios y riesgos asociados. Tampoco se encontraron procedimientos para resolver los problemas que pudieran presentarse. En la documentación entregada como plan de contingencia solo figura el procedimiento a seguir en el caso de corte de energía. No está definido un sitio de procesamiento alternativo para el caso de que el centro de cómputos dejara de funcionar. No existen políticas, planes o procedimientos que incluyan capacitación o concientización de los roles individuales o grupales para asegurar la continuidad.

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

4.3.5. *Garantía de la seguridad de los sistemas.*

Objetivo de control: La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de los roles y responsabilidades, las políticas, estándares y procedimientos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes identificados.

Este objetivo de control afecta, primariamente:

–la confidencialidad,

–la integridad,

y en forma secundaria:

–la disponibilidad,

–el cumplimiento,

–la confiabilidad.

Nivel de madurez: Inicial. El organismo reconoce la necesidad de la seguridad de TI pero la concientización depende de cada persona. La seguridad se encara en forma reactiva y no se realizan mediciones. Las violaciones a la seguridad invocan respuestas de señalar a los culpables si son detectadas, porque las responsabilidades no son claras. Las respuestas a las violaciones de la seguridad son impredecibles.

Observaciones: No se encontró evidencia de la existencia un plan estratégico formalmente aprobado de seguridad. Solamente hay un borrador del plan de seguridad informática que no esta aprobado por la dirección.

El área de seguridad no está centralizada, ni es independiente. De la seguridad informática se ocupa el responsable de redes.

No hay un esquema de clasificación de datos formalmente definido. El sector de normativa define solamente qué información puede ser de acceso al público a través de la página web del organismo y cual es de uso interno.

No hay autenticación de usuarios para conectarse a la red. Las PC se identifican en los servidores mediante sus direcciones internas (IP), esto permite que cualquier persona que utilice una máquina pueda hacer uso de los permisos de su titular independientemente de quien sea el usuario, dado que no necesita identificarse. No existen perfiles de seguridad definidos. Cada jefe de sector solicita al área de sistemas el alta de un usuario a las distintas aplicaciones que a su juicio cree que el empleado necesitará (esto también contempla la navegación por Internet, el uso de mensajería instantánea, etcétera). El usuario se identifica solamente al utilizar los aplicativos. Existe un único mecanismo de autenticación, que no está basado en políticas formales. Las autenticaciones no tienen límite de tiempo, ni se bloquean las aplicaciones por inactividad prolongada. No existen políticas de contraseñas, por lo que éstas pueden mantenerse indefinidamente, ni hay una extensión mínima para garantizar su inviolabilidad No existe la verificación de contraseñas por diccionario.

El organismo tenía un antivirus pero su licencia expiró hace meses, por lo tanto no hay protección actualizada contra ataques de virus.

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

4.3.6. *Identificación e imputación de costos*.

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

Este objetivo de control afecta, primariamente:

– la eficiencia,

– la confiabilidad.

Nivel de madurez: Repetible. Hay conciencia general de la necesidad de identificar y asignar costos. La asignación de costos esta basada en suposiciones informales o rudimentarias, por ejemplo los costos de hardware. No hay capacitación o comunicación formal sobre la identificación de costos estándar y sobre los procedimientos de asignación. No está delimitada la

responsabilidad sobre la recopilación o la adjudicación de los costos.

Observaciones: El organismo se financia con fondos provistos por un ente cooperador. Se presenta un presupuesto anual ante el Ministerio de Justicia que es aprobado y remitido al ente para su ejecución. Todas las compras las realiza el ente y entrega los bienes y servicios solicitados al organismo. La DNRPA realiza informes periódicos sobre los gastos globales realizados con estos fondos, sin realizar su imputación.

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

4.3.7. *Educación y capacitación de los usuarios.*

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

Este objetivo de control afecta, primariamente:

–la eficacia,

y en forma secundaria:

–la eficiencia.

Nivel de madurez: Inicial. Hay evidencia de que el organismo reconoció la necesidad de un programa de educación y capacitación, pero no hay procesos estandarizados. En ausencia de un programa organizado, los empleados identifican y asisten a cursos de capacitación por cuenta propia. El enfoque global de la dirección carece de cohesión y la comunicación de los temas y abordajes de la educación y capacitación es solo esporádica y poco coherente.

Observaciones: No existen políticas y procedimientos referentes a la concientización permanente en seguridad de la información. La capacitación se basa en la oferta de cursos que realiza el INAP (Instituto Nacional de la Administración Pública) en su mayoría (sobre gobierno electrónico y uso de software de oficina). No hay cursos internos sobre seguridad informática. No hay políticas ni procedimientos que incentiven la capacitación y actualización permanente del personal de sistemas.

Para el proyecto SURA (Sistema Único de Registro Automotor) se realizó un relevamiento para determinar sus necesidades de capacitación. Y se procedió a buscar en el mercado las ofertas más adecuadas para cada uno de los temas, pero sin una metodología que permita una correcta evaluación de las distintas posibilidades.

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

4.3.8. *Asistencia y asesoramiento a los usuarios de tecnología de la información.*

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

Este objetivo de control afecta, primariamente:

–la eficacia.

Nivel de madurez: Repetible. Existe una conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal para la tarea y la responsabilidad sobre la misma es delegada al individuo.

Observaciones: El proceso de asistencia y asesoramiento a usuarios no está definido formalmente. Los registros se comunican a la mesa de ayuda por medio de números telefónicos directos del sector, estas llamadas son atendidas por una operadora que las deriva a la persona encargada de resolverlo. La persona que recibe la consulta, anota en un cuaderno el llamado entrante y resuelve el problema o consulta preferentemente en el acto, en caso de no poder hacerlo, toma los datos para entregar la solución cuando esté disponible y eleva el pedido a una instancia superior. Una vez finalizada la llamada se la carga en un sistema denominado "Incidentes" incluyendo los datos del registro, una breve descripción del problema y su solución.

El equipamiento del sector de mesa de ayuda no es el adecuado, la central telefónica no dispone de las características necesarias para esta tarea y los aparatos telefónicos no disponen de cabezales para que los operadores puedan atender la llamada y utilizar la PC al mismo tiempo.

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

4.3.9. *Administración de la configuración.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la disponibilidad,

– la confiabilidad.

Nivel de madurez: Repetible. La gerencia está consciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico.

Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.

Observaciones: No se encontró evidencia de la existencia de procedimientos de administración de la configuración ni procedimientos de mantenimiento de inventarios de hardware y software. Se entregó un inventario completo de los servidores y equipos del

organismo que muestra un parque adecuado de computadoras de escritorio pero con servidores en el límite de su capacidad y vida útil.

El organismo dispone de un inventario completo y parcialmente actualizado de equipamiento informático de sus oficinas, en el mismo se encuentran perfectamente detallados los equipos pero la ubicación física de los mismos no está actualizada.

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

4.3.10. *Administración de problemas e incidentes.*

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

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la disponibilidad.

Nivel de madurez: Repetible. Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro del organismo como en la función de servicios de información. El proceso de resolución ha evolucionado al punto en el que algunos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.

Observaciones: No existen procedimientos formalmente definidos de administración de problemas. Los eventos se registran pero no existen procedimientos formales para registrar eventos no estándar.

Si bien se llevan estadísticas que permiten tener una idea sobre la tendencia de los problemas, no existe un procedimiento formal para realizar el seguimiento de las mismas.

Existe escalamiento de problemas, pero no existe un procedimiento formal que obligue a la notificación del mismo al nivel correspondiente.

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

4.3.11. *Administración de datos*.

Objetivo de control: La máxima autoridad debe establecer y mantener una combinación eficaz de controles generales y de aplicación sobre las operaciones de Tecnología de la Información para asegurar que los datos permanezcan durante su entrada, actualización y almacenamiento completos, precisos y válidos.

Este objetivo de control afecta, primariamente:

–la integridad,

–la confiabilidad.

Nivel de madurez: Repetible. En la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.

Observaciones: Los registros seccionales hacen el cierre del día y envían las operaciones realizadas a la DRNPA. Los datos se remiten utilizando un correo electrónico, en el cual como adjunto va un archivo plano, comprimido y encriptado. Se utiliza para ello un esquema de clave pública y privada con el software de licencia libre PGP.

El correo se recibe, se descomprime y desencripta el archivo adjunto, se verifica que los formatos de los datos sean correctos y después se controla que todos los campos de los registros estén completos.

Si el archivo cumple con los controles realizados se agregan los registros a la base central en un motor de base de datos SQL Server. En el caso de no cumplirlos se le informa al Registro Seccional que lo envió para que lo corrija. Este registro no podrá enviar nuevos archivos hasta tanto no corrija el que le fuera devuelto.

Los archivos son almacenados en su versión original (comprimidos y encriptados) y en su versión final (la anterior a ser agregados a la base de datos) y de ellos se hacen backup diarios en DVD y semanales en cinta. Finalmente, los datos almacenados en la primera etapa, son replicados en una segunda base con un motor PostgreSQL (gratuito de fuente abierta), y partir de ella se generan bases parciales según las necesidades de los usuarios externos que son accedidas desde Internet.

En cada archivo están identificados el Registro Seccional que lo envía y el operador que realizó la transferencia de datos. En cada uno de los registros de la base de datos está identificado el empleado que realizó la operación.

En cuanto a la calidad de los datos almacenados en la base de datos del organismo se detectaron inconsistencias debidas a:

–Un incorrecto diseño de la arquitectura de la información, de la base de datos y de los aplicativos,

–Tecnología obsoleta en los Registros Seccionales.

–Una inadecuada organización de la forma de trabajo.

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

4.3.12. *Administración de instalaciones.*

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

Este objetivo de control afecta, primariamente:

– la integridad

– la disponibilidad

Nivel de madurez: Inicial. El organismo reconoce la necesidad de brindar un entorno físico adecuado que proteja a los recursos y al personal contra los peligros generados por la naturaleza y el hombre. No existen procedimientos estándares y la administración de las instalaciones y los equipos dependen de la idoneidad y capacidad de ciertas personas clave. No se revisan las actividades de maestranza en las instalaciones y la gente se desplaza sin restricciones. La dirección no monitorea los controles ambientales de las instalaciones ni el movimiento del personal.

Observaciones: No existen procesos formalmente definidos de revisión periódica de perfiles, ni de análisis de violaciones de seguridad, ni registros de visitas ni pases temporarios. No hay procedimientos para el control de parámetros climáticos. No se aborda el tema de la seguridad física en el plan de contingencia general.

No se cumplen los requerimientos de protección de equipos de computación mencionados en la norma NFPA 75 (traducida y editada por IRAM) / ISO 27001.

El centro de cómputos, los locales linderos y los ubicados en el piso inferior no poseen protección contra incendios. La puerta de ingreso al centro de cómputos y el cerramiento del local no son resistentes al fuego. Los tabiques actuales son de vidrio. No posee un sistema automático de extinción de incendios.

No se recibió la siguiente información, solicitada oportunamente:

– Capacitación del personal del centro de cómputos en el manejo de los matafuegos.

– Cumplimiento de los controles trimestrales obligatorios a los matafuegos según lo establecido en la norma IRAM 3517-Parte 2.

– Ejecución de los simulacros de evacuación

– Plan de mantenimiento de las luces de emergencia.

– Plan de mantenimiento de las instalaciones eléctricas.

– Puesta a tierra del centro de cómputos, y las mediciones realizadas.

– Mantenimiento predictivo, preventivo y correctivo de los equipos de aire acondicionado.

– Mantenimiento predictivo, preventivo y correctivo de las UPS.

–Procedimiento indicando qué se debe realizar con las cintas, los cartuchos usados de las impresoras y con los equipos informáticos obsoletos.

No se han instalado en la puerta principal controles de emergencia de las instalaciones eléctricas y equipo de aire acondicionado (llaves de corte de los servicios usadas en casos de emergencia). No se han efectuado las mediciones de los niveles de iluminación. El centro de cómputos no posee piso técnico. Los racks no tienen puertas.

Los cables de datos y de alimentación eléctrica no poseen la debida canalización.

La disposición del equipamiento dificulta los trabajos de mantenimiento.

Las UPS se encuentran dentro del centro de cómputos y en el piso, rodeadas de cables de alimentación eléctrica y comunicaciones.

No existe un procedimiento para realizar la limpieza del centro de cómputos. Los recipientes de residuos y las bolsas de residuos son de color negro.

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

4.3.13. *Administración de operaciones*.

Objetivo de control: Un procesamiento completo y apropiado de la información requiere de una efectiva administración de su tratamiento y del mantenimiento del hardware. Éste incluye la definición de políticas y procedimientos de operación para una gestión efectiva de la protección de datos de salida sensitivos, monitoreo de la infraestructura y mantenimiento preventivo del hardware.

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la integridad,

– la disponibilidad.

Nivel de madurez: Inicial. La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándares y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos.

Observaciones: No existen procedimientos definidos para operaciones de TI. No hay una programación de tareas que permita mejorar la utilización de los recursos informáticos.

No hay normas de desempeño, acuerdos de nivel de servicio del usuario ni procedimientos formales de mantenimiento de equipos.

No existe un software de administración de red que permita la implementación y el control de las políticas de usuarios.

No existe un plan de capacitación permanente para mantener sus competencias.

No existe una política formal de backup, se utiliza un procedimiento adecuado y estándar para el resguardo

de los datos pero no está aprobado ni está incluido en un plan de continuidad de operaciones.

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

En lo que respecta al punto 4.4. "Monitoreo", señala:

4.4.1. *Monitoreo de los procesos*.

Objetivo de control: La máxima autoridad debe impulsar la definición de indicadores del desempeño relevantes, el informe sistemático y oportuno y la acción inmediata en caso de desviaciones.

Este objetivo de control afecta, primariamente:

– la eficacia,

y en forma secundaria:

– la eficiencia,

– la confidencialidad,

– la integridad,

– la disponibilidad,

– el cumplimiento,

– la confiabilidad.

Nivel de madurez: Inicial. La dirección reconoce la necesidad de recopilar y evaluar información sobre los procesos de monitoreo. No se identificaron procesos estándares de recopilación y evaluación. El monitoreo se implementa y las métricas se eligen caso por caso, según las necesidades de procesos y proyectos de TI específicos. El monitoreo en general se implementa en forma reactiva a un incidente que causó una pérdida o problema de imagen al organismo. El monitoreo es implementado por la función de servicios de información para beneficio de otros departamentos, pero no para los procesos de TI.

Observaciones: No existen informes internos referentes a la utilización de los recursos de la función servicios de información (personal, instalaciones, sistemas de aplicación, tecnología y datos). No existe un plan formal de mejora del desempeño con políticas y procedimientos documentados. No se cuenta con un análisis formal de la satisfacción del usuario.

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

4.4.2. *Evaluación de la idoneidad del control interno*.

Objetivo de control: Debe existir el compromiso del funcionario principal de servicios de información de monitorear los controles internos, evaluar su eficacia y realizar informes en forma periódica.

Este objetivo de control afecta, primariamente:

– la eficacia,

– la eficiencia,

y en forma secundaria:

– la confidencialidad,

– la integridad,

– la disponibilidad,

– el cumplimiento,

– la confiabilidad.

Nivel de madurez: Inicial: El organismo carece de un compromiso gerencial con la seguridad operativa regular y la garantía del control interno. Cada uno aplica sus propios conocimientos para evaluar la idoneidad del control interno, en forma ad hoc. La gestión de TI no tiene asignada formalmente la responsabilidad de monitorear la eficacia de los controles internos. Las evaluaciones de controles internos de TI se realizan como parte de auditorías financieras tradicionales, con metodologías y conjuntos de habilidades que no reflejan las necesidades de la función de servicios de información.

Observaciones: Dada la inexistencia de controles internos formales no existen procedimientos para su evaluación.

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

Asimismo, la AGN informa que el proyecto de informe de auditoría fue enviado al organismo auditado, para que formule las observaciones y/o comentarios que estime pertinentes. Los mismos fueron remitidos por la Dirección Nacional de los Registros Nacionales de la Propiedad del Automotor y de Créditos Prendarios, con fecha 16 de julio de 2010, a través de su nota DN 2.935. Señala la AGN que en dicha respuesta, se aceptan las observaciones oportunamente formuladas por lo cual las mismas quedan ratificadas.

Consecuentemente, en su apartado 6 efectúa las siguientes recomendaciones:

6.1. Planificación y organización

6.1.1. *Definición de un plan estratégico de TI:* El departamento de TI debe implementar planes a corto y largo plazo que sean compatibles con la misión y las metas de la organización aprobadas por la presidencia. En este aspecto, debe garantizar que:

– la tecnología de información forme parte del plan de la organización a corto y largo plazo,

– se elabore un plan de TI a largo plazo,

– se actualice el enfoque y la estructura de la planificación de TI a largo plazo,

– se realicen los cambios del plan de TI a largo plazo,

– se elabore la planificación a corto plazo de la función de servicios de información,

– se comuniquen los planes de TI,

– se controlen y evalúen los planes de TI,

– se evalúen los sistemas existentes.

6.1.2. *Definición de la arquitectura de la información:* La máxima autoridad debe impulsar la creación y el mantenimiento de un modelo que contemple lo siguiente:

– un modelo de arquitectura de la información,

– el diccionario de datos del organismo y reglas de sintaxis de los datos,

– un esquema de clasificación de los datos,

– los niveles de seguridad.

6.1.3. *Determinación de la dirección tecnológica:* Se debe crear y actualizar periódicamente un plan de infraestructura tecnológica que incluya la arquitectura de los sistemas, la dirección tecnológica y las estrategias de información.

6.1.4. *Definición de la organización y las relaciones de TI:* Al ubicar la función de servicios de información dentro de la estructura del organismo, la presidencia debe garantizar autoridad, masa crítica e independencia de las áreas de usuarios en la medida necesaria para lograr soluciones de tecnología de información eficientes. En este aspecto se debe asegurar:

– la designación de un comité permanente de planificación de TI,

– la ubicación adecuada de la función de servicios de información en la estructura del organismo,

– la revisión de los logros organizacionales,

– la definición de los roles y responsabilidades,

– la responsabilidad sobre el aseguramiento de calidad,

– la responsabilidad sobre la seguridad lógica y física,

– la propiedad y custodia de los datos,

– la supervisión de las actividades de TI,

– la separación de funciones,

– la competencia del personal de TI,

– las descripciones de los puestos del personal de TI,

– las políticas y procedimientos relativos al personal contratado,

– las relaciones de coordinación, comunicación y enlace.

6.1.5. *Administración de la Inversión en TI:* Debe implementarse un proceso de formulación presupuestaria que contemple lo siguiente:

– un presupuesto operativo anual de TI por centro de costos,

– el monitoreo de costos y beneficios,

– la justificación de costos y beneficios.

6.1.6. *Comunicación de los Objetivos y Directivas de la Gerencia:* Se debe implementar un marco y un programa de concientización que propicien un ambiente de control positivo en todo el organismo. Este marco debe abordar la integridad, los valores éticos y la competencia de las personas, la filosofía de gestión, el estilo operativo y la rendición de cuentas. En este aspecto, la máxima autoridad y el departamento de TI deben garantizar:

– las responsabilidades sobre la formulación de las políticas,

– la comunicación de las políticas del organismo,

– la disponibilidad de los recursos para la implementación de políticas,

– el mantenimiento de políticas,

– el cumplimiento de las políticas, los procedimientos y las normas,

– el compromiso con la calidad,

– la política marco de seguridad y control interno,

– la observancia de los derechos de propiedad intelectual,

– la comunicación de la concientización en materia de seguridad.

6.1.7. *Administración de los Recursos Humanos:* El organismo debe contar con una fuerza laboral que tenga las habilidades necesarias para lograr sus metas. La máxima autoridad y el departamento de TI deben garantizar:

– el cumplimiento de los períodos de vacaciones,

– la selección y promoción del personal,

– la formación y experiencia del personal,

– la definición de roles y responsabilidades,

– la capacitación del personal,

– la capacitación cruzada o personal de reemplazo,

– los procedimientos de verificación de antecedentes del personal,

– la evaluación del desempeño laboral,

– el cambio de puestos y la seguridad en la extinción de la relación laboral.

6.1.8. *Garantía del cumplimiento de los requerimientos externos:* La máxima autoridad y la jefatura de TI deben establecer y mantener procedimientos para la revisión de los requerimientos externos que permitan identificar los relacionados con las prácticas y controles de la TI. Además, se debe determinar en qué medida es preciso que las estrategias respalden los requerimientos de cualquier tercero relacionado. En este aspecto, la máxima autoridad y la jefatura de TI deben garantizar:

– la revisión de los requerimientos externos,

– las prácticas y procedimientos para garantizar el cumplimiento de los requerimientos externos,

– el cumplimiento de la normativa en materia de seguridad y ergonomía,

– la privacidad de datos y la propiedad intelectual,

– el cumplimiento de la legislación en las actividades de comercio/gobierno electrónico,

– el cumplimiento de los contratos de seguro.

6.1.9. *Evaluación de Riesgos:* Se debe establecer un marco de evaluación sistemática de riesgos. Dicho marco debe incorporar una evaluación periódica de los riesgos de información relacionados con la consecución de los objetivos del organismo, que constituya una base para determinar cómo deben administrarse los riegos a un nivel aceptable. El departamento de TI debe garantizar que se realice:

– una evaluación de riesgos de la actividad,

– la identificación de riesgos,

– la medición de riesgos,

– un plan de acción de reducción de riesgos,

– la aceptación de riesgos.

6.1.10. *Administración de proyectos:* Se debe establecer un marco de administración de proyectos que debe contemplar, como mínimo, la asignación de responsabilidades, división de tareas, presupuestación del tiempo y los recursos, plazos, puntos de verificación y aprobaciones. La presidencia y el departamento de TI deben garantizar que:

– se aplique un marco de administración de proyectos,

– se contemple la participación del departamento de usuarios en el inicio del proyecto,

– se asignen miembros y responsabilidades del equipo del proyecto,

– exista una definición del proyecto,

– se aprueben las fases del proyecto,

– exista un plan maestro del proyecto,

– se defina un plan de garantía de calidad del sistema,

– se implemente la administración formal de riesgos del proyecto,

– se elabore un plan de pruebas,

– se elabore un plan de capacitación,

– se desarrolle un plan de revisión posterior a la implementación.

6.1.11. *Administración de la calidad:* Debe desarrollarse y mantenerse periódicamente un plan general de calidad basado en los planes del organismo y de tecnología de información a largo plazo. La presidencia y el departamento de TI deben garantizar que exista:

– un plan general de calidad,

– un enfoque de garantía de calidad,

– una planificación de garantía de calidad,

– la revisión de garantía de calidad en cuanto al cumplimiento de las normas y procedimientos de TI,

– una metodología del ciclo de vida del desarrollo de sistemas,

– una metodología para la introducción de cambios importantes en la tecnología existente,

– la actualización de la metodología del ciclo de vida del desarrollo de sistemas,

– la coordinación y comunicación entre los usuarios y el personal de TI,

– un marco de adquisición y mantenimiento de la infraestructura tecnológica,

– un marco para las relaciones con terceros a cargo de la implementación,

– la observación de las normas de documentación de programas, verificando que:

– se cumplan las normas de prueba de programas;

– se cumplan las normas de prueba de sistemas;

– se utilicen pruebas en paralelo/piloto;

– la documentación de pruebas de sistemas.

6.2. *Administración e implementación.*

6.2.1. *Identificación de soluciones automatizadas:* Se deben definir prácticas que contemplen la solidez del diseño, la robustez de la funcionalidad y también la operabilidad (que incluye desempeño, escalabilidad e integración), la aceptabilidad (que cubre administración, mantenimiento y soporte) y la sustentabilidad (que considera costo, productividad y aspecto).

– Se deben definir los criterios para evaluar las opciones de desarrollo interno, soluciones compradas y tercerización.

– Definir formalmente un método general de adquisición e implementación o metodología de ciclo de vida de desarrollo de sistemas.

– Definir formalmente un proceso para la planificación, iniciación y aprobación de soluciones.

– Implementar un proceso estructurado de análisis de requerimientos.

– Considerar los requerimientos de seguridad y control desde el principio.

6.2.2. *Adquisición y mantenimiento del software de aplicación:* Definir una metodología de adquisición e implementación formal.

– Implementar herramientas de soporte automatizadas.

– Establecer una metodología para fijar qué requerimientos clave son prioritarios.

– Monitorear el cumplimiento con la arquitectura de TI del organismo, incluyendo un proceso formal de aprobación de las desviaciones.

6.2.3. *Adquisición y mantenimiento de la infraestructura tecnológica:* Definir una metodología de adquisición e implementación.

– Realizar un inventario pormenorizado de la infraestructura de TI (hardware y software).

– Definir una metodología de ciclo de vida para seleccionar, adquirir, mantener y quitar componentes de la infraestructura de TI.

6.2.4. *Desarrollo y mantenimiento de procedimientos*: Definir acuerdos de nivel de servicio.

– Diseñar la infraestructura y estructura organizativa para promover y compartir la documentación del usuario, los procedimientos técnicos y el material de capacitación entre los instructores, la mesa de ayuda y los grupos de usuarios.

– Definir los planes de capacitación del organismo y de TI.

– Mantener el inventario de aplicativos, los procedimientos del organismo y de TI utilizando herramientas automatizadas.

– Definir el proceso de desarrollo asegurando el uso de procedimientos operativos estándares y una apariencia estándar.

– Definir un marco estándar para la documentación y los procedimientos.

6.2.5. *Instalación y acreditación de sistemas de aplicación:* Definir una metodología de adquisición e implementación que garantice la aplicación de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– capacitación de los usuarios y personal de servicios de información,

– evaluación del desempeño del software de aplicación,

– desarrollo del plan de implementación,

– conversión de sistemas de aplicación,

– conversión de datos,

– definición de la estrategia y los planes de prueba,

– realización de la prueba de cambios,

– aplicación de criterios de ejecución de pruebas paralelas/piloto,

– realización de la prueba de aceptación final,

– realización de las pruebas de acreditación de seguridad,

– realización de la prueba de funcionamiento,

– transición a producción,

– evaluación del cumplimiento de los requerimientos del usuario,

– revisión de la gerencia posterior a la implementación.

6.2.6. *Administración de cambios:* Definir e implementar políticas y procedimientos de administración de cambios.

– Integrar la administración de cambios con la administración de las versiones de software y de la administración de la configuración.

– Definir un proceso de planificación, aprobación e iniciación que cubra la identificación, categorización, evaluación de impacto y fijación de prioridades para los cambios.

– Definir un proceso formal para la transición desde el ambiente de desarrollo al de producción.

– Establecer un procedimiento de emergencias que permita llevar la solución de un problema en el menor tiempo posible alterando o agilizando alguno de los pasos del procedimiento estándar.

– Todos estos procedimientos de administración de cambios deben contemplar, por último, una etapa de cierre que incluya la documentación de usuario y un proceso de revisión para garantizar la implantación completa de los cambios. Pueden también ser revisados los costos ejecutados.

6.3. *Entrega y Soporte.*

6.3.1. *Definición y administración de los niveles de servicio:* Garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– establecer un marco de acuerdos de nivel de servicio,

– procedimientos de ejecución,

– monitoreo e informes,

– revisión de los contratos y acuerdos de nivel de servicio,

– establecer un programa de mejora del servicio.

6.3.2. *Administración de servicios prestados por terceros:* Se debe verificar que los servicios prestados por terceros se identifiquen de modo adecuado y que la interrelación técnica y funcional con los proveedores esté documentada. La conducción del organismo debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– interrelación con proveedores de TI,

– asignar la responsabilidad por tales relaciones,

– formalización de contratos con terceros,

– evaluación del conocimiento y la experiencia de terceros,

– formalización de contratos de tercerización,

– asegurar la continuidad de los servicios,

– acordar las relaciones de seguridad,

– monitoreo de la prestación del servicio.

6.3.3. *Administración de la capacidad y el desempeño:* La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– identificación de requerimientos de disponibilidad y desempeño,

– establecer un plan de disponibilidad,

– monitoreo e informes del desempeño de los recursos de TI,

– utilización de herramientas para la creación de modelos,

– administración proactiva del desempeño,

– la realización de pronósticos de la carga de trabajo,

– administración de la capacidad de los recursos,

– establecer la disponibilidad de recursos,

– planificación de recursos.

6.3.4. *Garantía de un servicio continuo:* Se debe crear un marco de continuidad que defina los roles, las responsabilidades, el enfoque y las normas y estructuras para documentar un plan de contingencia que garantice el servicio continuo La presidencia y el departamento de TI deben garantizar la eficacia de las

políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– un marco de continuidad de TI,

– definir estrategias y filosofía del plan de continuidad de TI,

– establecer contenido del plan de continuidad de TI,

– reducción de los requerimientos de continuidad de TI,

– mantenimiento del plan de continuidad de TI,

– realizar la prueba del plan de continuidad de TI,

– capacitación en el plan de continuidad de TI,

– distribución del plan de continuidad de TI,

– resguardo de la posibilidad de procesamiento alternativo para el usuario,

– identificar recursos críticos de TI,

– definir el sitio y equipamiento alternativos,

– almacenamiento de resguardo en sitio alternativo,

– reevaluación periódica del plan.

6.3.5. *Garantía de la seguridad de los sistemas:* La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– administración de las medidas de seguridad,

– identificación, autenticación y acceso,

– la seguridad del acceso en línea a los datos,

– administración de cuentas de usuarios,

– revisión de la gerencia de cuentas de usuarios,

– el control ejercido por el usuario en sus propias cuentas,

– la supervisión de la seguridad,

– clasificación de los datos,

– administración centralizada de identificaciones y derechos de acceso,

– realizar informes de violación y actividades de seguridad,

– manejo de incidentes,

– acreditación de soluciones,

– normar la confianza en la contraparte,

– autorización de transacciones,

– establecer la imposibilidad de rechazo,

– definir ruta de acceso confiable,

– protección de las funciones de seguridad,

– administración de claves criptográficas,

– prevención, detección y corrección de software malicioso,

– establecer arquitectura de firewalls y conexiones con redes públicas,

– protección del valor electrónico.

6.3.6. *Identificación e implementación de costos:* La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– identificar ítems imputables,

– definir procedimientos de determinación de costos,

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

6.3.7. *Educación y capacitación de los usuarios:* La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– identificación de necesidades de capacitación,

– organización de sesiones de capacitación,

– capacitación y concientización en los principios de seguridad.

6.3.8. *Asistencia y asesoramiento a los usuarios de TI:* El departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– registro completo de consultas de usuarios,

– escalamiento de consultas de usuarios,

– monitoreo de soluciones,

– análisis e informe de tendencias.

Es recomendable contar con una central telefónica que permita el reconocimiento inteligente de voz, y disponga de software para análisis del flujo de llamadas.

6.3.9. *Administración de la configuración:* Se deben implementar procedimientos de control para identificar y registrar todos los bienes de TI y su ubicación física, y una rutina de verificación regular que confirme su existencia. El departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– registro de la configuración,

– establecer el nivel básico de configuración,

– registro del estado de la configuración,

– control de la configuración,

– detectar el software no autorizado,

– almacenamiento del software,

– administración de configuración,

– seguimiento y control de versiones de software.

6.3.10. *Administración de problemas e incidentes:* El departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– sistema de administración de problemas,

– escalamiento de problemas,

– seguimiento de problemas y pistas de auditoría,

– autorizaciones de emergencia y acceso temporario,

– establecer las prioridades de procesamiento de emergencia.

6.3.11. *Administración de datos:* La jefatura de TI, los responsables de programas y actividades y el jefe de operaciones deben garantizar la eficacia de los procedimientos y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– preparación de datos,

– autorización de documentos fuente,

– recopilación de datos de documentos fuente,

– manejo de errores de documentos fuente,

– conservación de documentos fuente,

– autorización de entrada de datos,

– verificación de exactitud, integridad y autorización,

– manejo de errores de entrada de datos,

– asegurar la integridad del procesamiento de datos,

– validación y edición del procesamiento de datos,

– manejo de errores del procesamiento de datos,

– manejo y conservación de salidas,

– distribución de salidas de datos,

– balanceo y conciliación de salidas de datos,

– revisión y manejo de errores de salidas de datos,

– seguridad de los informes de salida,

– protección de información crítica durante la transmisión y el transporte,

– protección de información crítica eliminada,

– administración del almacenamiento,

– establecer períodos de conservación y condiciones de almacenamiento,

– establecer un sistema de administración de biblioteca de medios,

– definir las responsabilidades de administración de la biblioteca de medios,

– resguardo y restauración,

– tareas de resguardo,

– almacenamiento de resguardos,

– administración de archivos,

– protección de mensajes críticos,

– autenticación e integridad.

6.3.12. *Administración de instalaciones:* La presidencia y el departamento de TI deben garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– seguridad física,

– asegurar la discreción del sitio de tecnología de información,

– acompañamiento de visitas,

– salud y seguridad del personal,

– protección contra factores ambientales.

6.3.13. *Administración de operaciones:* El departamento de TI debe garantizar la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– desarrollo de manuales de instrucciones y procedimientos de las operaciones de procesamiento,

– documentación del proceso de puesta en marcha y otras operaciones,

– fijación de programas de trabajo,

– control de las desviaciones de los programas estándares de trabajo,

– asegurar la continuidad del procesamiento,

– registración de operaciones,

– salvaguardia de formularios especiales y dispositivos de salida,

– realización de operaciones remotas.

Se debe establecer y documentar los procedimientos estándares para las operaciones que garanticen la eficacia de las políticas y prácticas establecidas para las siguientes tareas y/o actividades de TI:

– manuales de instrucciones y procedimientos de las operaciones de procesamiento,

– documentación del proceso de puesta en marcha y otras operaciones,

– programas de trabajo,

– desviaciones de los programas estándares de trabajo,

– continuidad del procesamiento,

– registro de operaciones,

– salvaguardia de formularios especiales y dispositivos de salida,

– operaciones remotas.

6.4. *Monitoreo*

6.4.1. *Monitoreo de los procesos:* La presidencia y el departamento de TI son responsables de que se definan los indicadores de desempeño pertinentes y se recopilen datos para la elaboración de informes de gestión e informes de excepción con respecto a estos indicadores. La evaluación de la función servicios de información se debe llevar a cabo en forma continua. En este aspecto, la alta gerencia es responsable de garantizar:

– que se recopilan los datos de monitoreo,

– que se evalúa el desempeño en forma continua,

– que se evalúa la satisfacción del usuario,

– que se elaboran informes de gestión.

6.4.2. *Evaluación de la idoneidad del control interno*: La presidencia y el departamento de TI son responsables de monitorear la eficacia de los controles internos en el curso normal de las operaciones. Además, las desviaciones graves deben informarse a la máxima autoridad del organismo. La alta gerencia y el funcionario principal de servicios de información son responsables de garantizar:

– el monitoreo del control interno,

– la operación oportuna del control interno,

– los informes del nivel de control interno.

El órgano de control externo finaliza su informe con las siguientes conclusiones:

La DNRPA es un organismo creado en 1958. La estructura orgánica interna y las misiones y funciones correspondientes a TI no han sido aprobadas a la fecha de los trabajos de campo.

Por otra parte existe un Ente Cooperador (ACARA) que es responsable de realizar las contrataciones del personal de TI y de gestionar las compras de equipamiento por fuera de la órbita de la ONTI, lo que hace posible que no siempre se satisfagan sus requisitos.

La falta de una estructura formal genera entre otros inconvenientes:

a) la inexistencia de una auditoría interna en TI, dentro del organismo, que garantice el funcionamiento de los controles necesarios para su correcto desempeño;

b) la inexistencia formal de las áreas internas de sistemas, impidiendo el nombramiento de sus responsables y de los subordinados con las descripciones de puesto correspondientes;

c) el 100 % del personal de TI está contratado por el ente cooperador;

d) falta de autoridad del sector informático para imponer las normas de seguridad necesarias tanto a nivel interno de la dirección, como en los registros seccionales.

El organismo no define ni hace cumplir políticas informáticas acordes con las buenas prácticas. Esto se refleja en una serie de situaciones que dificultan eficacia y eficiencia, como por ejemplo:

a) La seguridad interna está limitada al reconocimiento automático de las máquinas en la red, sin necesidad de introducir la identificación del usuario y su palabra clave. Por lo tanto cualquier persona que encienda la máquina tendrá acceso a los recursos y contenidos de la misma. Es fundamental solucionar este grave problema con una política adecuada de administración de usuarios.

b) Existen funcionarios que tienen habilitado el servicio de mensajería instantánea, lo que abre una puerta de acceso vía Internet a personas mal intencionadas que podrían provocar inconvenientes o hacerse de información reservada.

c) Existe duplicación de información instalada en distintos motores de base de datos (FoxPro, en los Registros Seccionales y SQLServer y PostgresSQL en la Dirección Nacional). La consecuencia directa de esta situación es la falta de integridad de información sensible, aparte de los problemas técnicos y administrativos que genera.

d) Falta claridad en la definición sobre la propiedad de los datos. Si bien los registros seccionales son los responsables de los datos que generan, es aconsejable disponer de un sistema que trabaje con una única base de datos centralizada y completa, teniendo cada registro sus propios datos, replicados localmente para una eventual pérdida de comunicación que permita la sincronización automática en el momento en que ésta se recupere.

e) No hay autoridad del organismo sobre los registros seccionales en materia de TI. Para ellos existen sólo recomendaciones de baja exigencia en materia de configuración y esto provoca que cualquier solución que quiera implementarse desde la DNRPA deba ajustarse para satisfacer la realidad de cada uno de los distintos registros.

En síntesis, los riesgos de ineficiencia e ineficacia en el cumplimiento de la misión del organismo son altos y en general, la información está sometida a riesgos que superan los valores aceptables.

Para superar el actual estado de situación, es necesario darle prioridad a:

– la definición de la estructura de Tecnología de Información, de sus misiones y funciones, de las políticas y procedimientos a cumplir y el nombramiento del personal idóneo, responsable de cumplirlas satisfactoriamente,

– deberá ponerse fuerte énfasis en resolver las inconsistencias en los datos en el desarrollo de la nueva versión del aplicativo y previo a la puesta en producción, realizar la depuración de la base,

– tender a que la madurez de la calidad de la gestión se aproxime, cuanto menos, al nivel de "Procesos definidos",

– superar a la brevedad las limitaciones de los procesos ponderados en niveles "No conforma" e "Inicial", particularmente en los casos en que la estimación del riesgo es alta.

La evaluación realizada con el modelo genérico de madurez indica que más del 60 % de los objetivos de control se encuentran en el nivel "Inicial", y ninguno alcanza el valor mínimo recomendable de "Proceso Definido".

Para corregir las falencias detectadas es imprescindible un fuerte compromiso de las máximas autoridades de la DNRPA para organizar los servicios de TI y de las autoridades del ministerio para proveer los recursos necesarios y una urgente formalización de la estructura.

Heriberto A. Martínez Oddone. – Nicolás A. Fernández. – Luis A. Juez. – Gerardo R. Morales. – Ernesto R. Sanz. – Juan C. Morán. – Gerónimo Vargas Aignasse. – José M. Díaz Bancalari. – Walter A. Agosto.

ANTECEDENTES

Ver expedientes 1.681-D.-2011 y 310-O.V.-2010.