Tecnología de la Información y Comunicación

Se practicaron 3 auditorías operativas en materia de Tecnología de la Información y Comunicación, las cuales se detallan a continuación: una orientada a verificar la operatividad del Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof) y sus sistemas conexos, así como la seguridad tecnológica implementada por la Dirección General de Tecnología de Información y Comunicación (DGTIC) de la Oficina Nacional de Contabilidad Pública (Oncop) durante el ejercicio económico financiero año 2014 y el primer semestre 2015, y otras 2 dirigidas a la evaluación de la funcionalidad de los módulos del Portal iseniat de ISLR e IVA; así como la seguridad tecnológica implementada por la GGTIC del Seniat, durante el ejercicio económico financiero año 2015 y primer trimestre 2016.

Fallas y deficiencias

Como resultado de la actuación realizada por este Órgano Superior de Control, se detectó una serie de fallas y deficiencias, las cuales se describen seguidamente:

En la Dirección General de Tecnología de Información y Comunicación (DGTIC) de la Oficina Nacional de Contabilidad Pública (Oncop):

- Los manuales, planes y políticas utilizados no están formalmente aprobados por la máxima autoridad, a saber: el Manual de Normas y Procedimientos de Control de Cambios de la Plataforma Tecnológica Oficina Nacional de Contabilidad Pública (Oncop), Procedimiento de Contraseñas: plataforma tecnológica, políticas de respaldo y recuperación de servidores del Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof) en el centro de datos - Compañía Anónima Nacional Teléfonos de Venezuela (CANTV) Hatillo (Centro de Contingencia del Sistema). Tal situación trae como consecuencia discrecionalidad en la gestión de los recursos de tecnologías de información y comunicación (TIC), y afecta la continuidad del servicio o la integridad de la información procesada por la Oficina Nacional de Contabilidad Pública (Oncop).
- Se constató la prestación de servicios por parte de la Compañía Anónima Nacional Teléfonos de Venezuela (CANTV) para los servicios de red de datos *Frame Relay*, *Metro Ethernet* y

Hosting dedicado Linux en el Centro de Datos Alterno de El Hatillo sin la existencia de un documento contractual vigente que regule dicha actividad, ya que los contratos suscritos en fechas 03-04-2013 *(Frame Relay),* 13-11-2012 *(Metro Ethernet)* y 22-07-2013 (*Hosting* dedicado), que tenían vigencia de un año a partir de la fecha de su suscripción, no han sido renovados. En este sentido, la inexistencia de un documento formal a través del cual se acuerden los costos ha causado que el Ministerio del Poder Popular para la Economía y Finanzas (MPPEF) realizara pagos sobre la base de estimaciones de facturación suministradas por la empresa, lo que ha generado que este órgano se encuentre actualmente en proceso de conciliación de pagos con CANTV. Asimismo, la falta de compromisos formalmente adquiridos es un riesgo para la Oficina Nacional de Contabilidad Pública (Oncop), ya que la empresa tiene la potestad de suspender en cualquier momento el servicio que viene prestando, lo cual originaría atrasos en los registros, transacciones y procesos contables de la Oficina Nacional de Contabilidad Pública (Oncop), así como en los procesos y/o procedimientos técnicos vinculados con el Sistema de Contabilidad Pública.

- El contrato suscrito con la empresa proveedora para la reposición de partes y piezas físicas, así como para el soporte del *software* de la infraestructura tecnológica del Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof) no se encuentra vigente para el ejercicio económico financiero correspondiente al año 2015. Es importante destacar que esa empresa es la propietaria del *software* Data Protector, utilizado para generar las copias de seguridad y permitir la recuperación de archivos al Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof); sin embargo, no se evidenció un *addendum* al citado contrato que garantice su continuidad, lo que trae como consecuencia que por la inexistencia de esa figura jurídica se cause un riesgo a la administración, por cuanto la empresa proveedora tiene la facultad de suspender el servicio lo que originaría la interrupción en los procedimientos para generar las copias de seguridad y la recuperación de archivos del Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof). Igualmente, trae inconvenientes para la reposición de piezas y partes de *hardware,*

además de limitaciones técnicas en la infraestructura tecnológica de dicho sistema.

- Al respecto de las cintas de respaldo, se evidenciaron las situaciones que se mencionan a continuación: a) la caja fuerte utilizada para almacenar las cintas de respaldos con información del Sistema Integrado de Gestión y Control de las Finanzas Públicas (SIGECOF) se encuentra en un área común de la Dirección General de Tecnología de Información y Comunicación (DGTIC); b) dicha caja fuerte está ubicada en un punto ciego, fuera del alcance de las cámaras de Circuito Cerrado de Televisión (CCTV); y c) la caja fuerte posee un sistema de combinación mecánica que no puede ser modificada debido a que no existe el personal capacitado para tal fin, lo que impide su cambio periódico. Tales situaciones obedecen al uso práctico y común de las áreas de Tecnología de Información de almacenar los respaldos en sus propias instalaciones, pero con la particularidad de que la mencionada caja de seguridad se encuentra en el mismo piso y oficina, a escasos metros, del centro de datos. En consecuencia, se ve afectado el espacio físico de esta oficina, y de generarse una interrupción en los servicios de Tecnología de Información (TI) se podría comprometer la disponibilidad de los respaldos almacenados, originarse riesgo de pérdida de información y obstaculizarse el eficiente reinicio de las operaciones esenciales.

En la Gerencia General de Tecnologías de Información y Comunicación (GGTIC) del SENIAT, módulo de ISLR del Portal ISENIAT:

- Los manuales, planes, normas y políticas utilizados en la GGTIC no están formalmente aprobados por la máxima autoridad. Entre estos, se pueden mencionar: "Manual de Usuario. Sistema Impuesto Sobre la Renta (ISLR) - Versión 3.1", "Manual de Estilos. Estándares para el Diseño de la Interfaz Gráfica de Usuario - Versión 3.4", "ISENIAT Software Factory", "Manual de Estilos. Versión 3.2", "Manual de Usuario. Sistema de Retenciones de ISLR. Consulta de Retenciones - COREISLR (Contribuyente)", "Manual Técnico. Sistema Impuesto Sobre La Renta", "Manual - Plan y Políticas de Seguridad de la Información de la AR - SENIAT" y "Centro de Datos. Políticas y Normas". Al respecto, el artículo 34 de las Normas Generales de Control Interno (NGCI), Gaceta

Oficial de la República Bolivariana de Venezuela N.º 40.851 de fecha 18-02-2016, señala que la máxima autoridad jerárquica, jefes u otras autoridades administrativas de los órganos o entes son responsables de la existencia de los manuales, su divulgación y la capacitación al personal para su adecuada implementación y aplicación, en concordancia con el proceso AI4 "Facilitar la Operación y el Uso" de los Objetivos de Control para Información y Tecnologías Relacionadas, (Cobit, por sus siglas en inglés: *Control Objectives for Information and Related Technology)* en su versión 4.1, publicado por la *Information Systems Audit and Control Association* (ISACA) y el *IT Governance Institute* en el año 2007, el cual indica que se requiere la generación de documentación y manuales para usuarios y para tecnologías de información (TI), así como proporcionar entrenamiento para garantizar el uso y la correcta operación de aplicaciones e infraestructura.

- La Gerencia General de Tecnologías de Información y Comunicación no dispone de un plan de continuidad operativa que garantice el restablecimiento oportuno de las operaciones de la plataforma tecnológica o la restauración de los servicios en un tiempo razonable. Sobre este particular, se debe considerar lo establecido en el artículo 4 de las Políticas, Normas y Procedimientos de Seguridad Informática Física y Lógica, en los Bienes Informáticos de los Órganos y Entes de la Administración Pública (Gaceta Oficial de la República Bolivariana de Venezuela N.º 38.414 de fecha 06-04-2006), que prevé: "Los Órganos y Entes de la Administración Pública Nacional deben elaborar anualmente planes de continuidad operativa y de contingencia en las áreas de siniestros en sistemas informáticos, siniestros naturales y servicios básicos", en concordancia con el objetivo de control DS4.2 "Planes de Continuidad de TI" del Cobit, el cual establece: "Desarrollar planes de continuidad de TI con base en el marco de trabajo diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio…".
- En relación con la administración del *firewall,* los antivirus y otros mecanismos de seguridad, se constató que no cuentan con registros históricos de incidentes telemáticos ocurridos en el año 2015, y solo disponen de algunas trazas para el año 2016. Asimismo, no se evidenció la existencia de medios controlados

para la transmisión de datos que garanticen la comunicación segura entre los contribuyentes y el Seniat. En atención a lo descrito, cabe señalar lo dispuesto en el artículo 39, numeral 11, literal "f" de las NGCI, el cual estipula establecer procedimientos relativos a la existencia de planes de prevención, detección y corrección de *software* malicioso para proteger los sistemas de información, en concordancia con los objetivos de control del Cobit DS5.6 "Definición de Incidente de Seguridad", que señala: "Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas"; DS5.9 "Prevención, Detección y Corrección de Software Malicioso", que indica: tomar medidas preventivas y correctivas en toda la organización para proteger los sistemas de la información y a la tecnología contra *malware* (virus, gusanos, *spyware,* correo basura), y DS5.11 "Intercambio de Datos Sensitivos", que expresa: "Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen".

- En cuanto a las pruebas de control interno relacionado con el diseño de servicios del módulo de ISLR, se observó que no se ha implementado el uso de certificados y firma electrónica para los declarantes, debido a que el proyecto infraestructura de clave pública se mantiene diferido, según lo expresado por el Gerencia General de Tecnologías de Información y Comunicación mediante comunicación N.º SNAT/GGTIC/2016/00002 de fecha 04-05-2016. Al respecto, el artículo 39, numeral 6 de las NGCI señala que la máxima autoridad jerárquica de los órganos o entes deberá establecer los procedimientos para asegurar el uso eficiente, efectivo y económico de las tecnologías de información; así como los artículos 24 y 32 de la Ley de Infogobierno (LI), Gaceta Oficial de la República Bolivariana de Venezuela N.º 40.274 de fecha 17-10-2013, establecen que el Poder Público debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información a través del uso de certificados y firmas electrónicas.

- No se evidenció la existencia de un plan institucional de adaptación o migración aprobado por las autoridades competentes, de acuerdo con la Segunda Disposición Transitoria de la LI: "En caso que algún órgano o ente del Poder Público o el Poder Popular, para el momento de entrada en vigencia de la presente Ley, cuente con tecnologías de información que no cumplan con lo aquí establecido, deberán presentar ante la Comisión Nacional de las Tecnologías de Información, dentro de los doce meses siguientes, un plan institucional de adaptación o migración de las tecnologías de información para su aprobación".

En la Gerencia General de Tecnologías de Información y Comunicación (GGTIC) del Seniat, módulo de IVA del Portal iSeniat.

- Los manuales, planes, normas y políticas utilizados en la gerencia de tecnología no están formalmente aprobados por la máxima autoridad. Entre estos, se pueden mencionar: "Manual de Usuario. Sistema del Impuesto al Valor Agregado (IVA) - Versión 4.0", "Manual de Estilos. Estándares para el Diseño de la Interfaz Gráfica de Usuario - Versión 3.4", "iseniat *Software Factory",* "Manual de Estilos. Versión 3.2", "Manual - Plan y Políticas de Seguridad de la Información de la AR- seniat" y "Centro de Datos. Políticas y Normas". Al respecto, el artículo 34 de las NGCI señala que la máxima autoridad jerárquica, jefes u otras autoridades administrativas de los órganos o entes son responsables de la existencia de los manuales, su divulgación y la capacitación al personal para su adecuada implementación y aplicación, en concordancia con el proceso AI4 "Facilitar la Operación y el Uso" de los Objetivos de Control para Información y Tecnologías Relacionadas, Cobit, en su versión 4.1, publicado por ISACA y el *IT Governance Institute* en el año 2007, el cual indica que se requiere la generación de documentación y manuales para usuarios y para TI, así como proporcionar entrenamiento para garantizar el uso y la correcta operación de aplicaciones e infraestructura.
- La Gerencia General de Tecnologías de Información y Comunicación no dispone de un plan de continuidad operativa que garantice el restablecimiento oportuno de las operaciones de la plataforma tecnológica o la restauración de los servicios en un tiempo

razonable. Sobre este particular, se debe considerar lo establecido en el artículo 4 de las Políticas, Normas y Procedimientos de Seguridad Informática Física y Lógica, en los Bienes Informáticos de los Órganos y Entes de la Administración Pública, que prevé: "Los Órganos y Entes de la Administración Pública Nacional deben elaborar anualmente planes de continuidad operativa y de contingencia en las áreas de siniestros en sistemas informáticos, siniestros naturales y servicios básicos", en concordancia con el objetivo de control DS4.2 "Planes de Continuidad de TI" del Cobit, el cual establece: "Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio…".

- En relación a la administración del *firewall,* los antivirus y otros mecanismos de seguridad, se constató que no cuentan con registros históricos de incidentes telemáticos ocurridos en el año 2015, y solo disponen de algunas trazas para el año 2016. Asimismo, no se evidenció la existencia de medios controlados para la transmisión de datos que garanticen la comunicación segura entre los contribuyentes y el Seniat. En atención a lo descrito, cabe señalar lo dispuesto en el artículo 39, numeral 11, literal "f" de las NGCI, el cual estipula establecer procedimientos relativos a la existencia de planes de prevención, detección y corrección de *software* malicioso para proteger los sistemas de información, en concordancia con los objetivos de control del Cobit DS5.6 "Definición de Incidente de Seguridad", que señala: "Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas", DS5.9 "Prevención, Detección y Corrección de Software Malicioso", que indica: tomar medidas preventivas y correctivas en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura), y DS5.11 "Intercambio de Datos Sensitivos", que expresa: "Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen".

- En cuanto a las pruebas de control interno relacionado con el diseño de servicios del módulo de IVA, se observó que no se ha implementado el uso de certificados y firma electrónica para los declarantes, debido a que el proyecto infraestructura de clave pública se mantiene diferido, según lo expresado por la Gerencia General de Tecnologías de Información y Comunicación mediante comunicación N.º SNAT/GGTIC/2016/00002 de fecha 04-05-2016. Al respecto, el artículo 39, numeral 6 de las NGCI señala que la máxima autoridad jerárquica de los órganos o entes, deberá establecer los procedimientos para asegurar el uso eficiente, efectivo y económico de las tecnologías de información; así como el artículo 24 de la LI, el cual establece que el Poder Público debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información a través del uso de certificados y firmas electrónicas.
- No se evidenció la existencia de un plan institucional de adaptación o migración aprobado por las autoridades competentes, como lo establece la Segunda Disposición Transitoria de la LI: "En caso que algún órgano o ente del Poder Público o el Poder Popular, para el momento de entrada en vigencia de la presente Ley, cuente con tecnologías de información que no cumplan con lo aquí establecido, deberán presentar ante la Comisión Nacional de las Tecnologías de Información, dentro de los doce meses siguientes, un plan institucional de adaptación o migración de las tecnologías de información para su aprobación".

Recomendaciones

En virtud de la importancia de las observaciones señaladas y con la finalidad de que estas sean subsanadas en beneficio de una gestión administrativa eficiente y eficaz, este Máximo Órgano Contralor recomienda lo siguiente:

A la Dirección General de Tecnología de Información y Comunicación (DGTIC):

- Realizar las gestiones necesarias para definir e implementar los planes, políticas y manuales de normas y procedimientos utilizados, a los fines de su aprobación por parte de la máxima autoridad.

- Emprender, conjuntamente con la Dirección General de la Oficina de Gestión Administrativa del Ministerio del Poder Popular para Banca y Finanzas (MPPBF), las acciones pertinentes para la renovación de los contratos con la Compañía Anónima Nacional Teléfonos de Venezuela (CANTV), a fin de garantizar el servicio eficiente y oportuno en cuanto a la conexión de red y transmisión de datos *(Frame Relay* y *Metro Ethernet)* y el servicio hospedaje *(hosting* dedicado en el Centro de Datos Alterno).
- Definir la renovación del contrato suscrito con la empresa proveedora, con la finalidad de dar continuidad a los servicios de reposición de partes y piezas físicas, al soporte del *software* de la infraestructura tecnológica y a la generación de copias de seguridad, y permitir la recuperación de archivos al Sistema Integrado de Gestión y Control de las Finanzas Públicas (Sigecof).
- Efectuar las gestiones necesarias para resguardar las copias de respaldo fuera de las instalaciones de la Institución.

A la Gerencia General de Tecnologías de Información y Comunicación (GGTIC) del Seniat, en los módulos de ISLR e IVA del Portal iSeniat:

- Dirigir lo concerniente para dar celeridad al proceso de revisión y actualización de los planes, políticas y manuales de normas y procedimientos utilizados en la GGTIC, a los fines de su aprobación por parte de la máxima autoridad.
- Elaborar un plan de continuidad operativa que responda a los procesos de recuperación de la información del iSeniat. Dicho manual debe ser aprobado por la máxima autoridad e informado al personal involucrado.
- Implementar un sistema de control de incidentes telemáticos, que considere el registro, escalamiento, resultado, tiempo de respuesta y seguimiento de las eventualidades detectadas. Asimismo, agilizar los trámites administrativos para la implementación de medios de transmisión seguros, a los fines de garantizar la integridad y confidencialidad de los datos intercambiados entre los contribuyentes y el Seniat.
- Realizar las gestiones pertinentes para ejecutar los proyectos relacionados con la implementación de certificados y firmas electrónicas, así como los servicios de intercambio de datos

básicos del declarante con el organismo encargado de proveer esta información.

- Girar las instrucciones necesarias para la elaboración del plan institucional de migración de las tecnologías de información, de conformidad con lo establecido en la Segunda Disposición Transitoria de la Ley de Infogobierno.