

**Secretaría de Relaciones Exteriores****Aprovechamiento de Infraestructura y Servicios de las TICs**

Auditoría Financiera y de Cumplimiento: 12-0-05100-02-1176

GB-036

***Criterios de Selección***

Esta auditoría se seleccionó con base en los criterios cuantitativos y cualitativos establecidos en la Normativa Institucional de la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2012, considerando lo dispuesto en el Plan Estratégico de la ASF 2011-2017.

***Objetivo***

Fiscalizar la gestión financiera de las erogaciones, comprobar la eficacia y eficiencia en la utilización de los recursos asignados, así como la adecuada administración de riesgos en la gestión de los proyectos y la operación de las TICs. Asimismo, verificar que los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

***Alcance***

	<b>EGRESOS</b>
	Miles de Pesos
Universo Seleccionado	429,360.2
Muestra Auditada	253,626.0
Representatividad de la Muestra	59.1%

El universo seleccionado está integrado por 429,360.2 miles de pesos que corresponden al total ejercido en contratos relacionados con TICs, de los cuales se revisaron 2 contratos por un importe de 253,626.0 miles de pesos, lo que representa el 59.1%, se integran por 193,320.9 miles de pesos registrados en la partida 38301 "Congresos y Convenciones" con cargo al presupuesto de la Dirección General de Tecnologías de Información e Innovación y 60,305.1 miles de pesos registrados en la partida 33603 "Impresiones de documentos oficiales para la prestación de servicios públicos" con cargo al presupuesto de la Dirección General de Delegaciones.

***Antecedentes***

Las organizaciones en su proceso de administración y gestión deben buscar la eficiencia en el manejo de la información y esto sólo será posible utilizando adecuadamente las TICs. Estas se conforman por un conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento e intercambio de información, para su uso eficiente debe asegurarse:

- Mantener la información con un alto nivel de calidad para soportar las decisiones.
- Generar valor a la organización a través de las inversiones en las TICs.
- Lograr la excelencia operativa aplicando la tecnología de manera confiable y eficiente.

- Mantener los riesgos relacionados con las TICs en un nivel aceptable.
- Optimizar el costo de la tecnología y los servicios de las TICs.
- Cumplir con las regulaciones, leyes, acuerdos contractuales y políticas relevantes.

La Secretaría de Relaciones Exteriores (SRE) tiene como misión ampliar y profundizar las relaciones políticas, económicas, culturales y de cooperación con las distintas regiones del mundo a favor del desarrollo integral de todos los mexicanos.

Para dar cumplimiento a sus metas y objetivos la SRE por medio de la Dirección General de Tecnologías de Información e Innovación (DGTII) proporciona diferentes servicios sustantivos como la expedición de pasaportes, visas, cartillas, documentos relativos al registro civil, entre otros, en México y en el extranjero; por lo que requiere de la automatización de sus procesos así como de una sólida infraestructura tecnológica que permita soportar los sistemas informáticos que apoyan estas funciones sustantivas. Entre 2007 y 2012 la SRE ejerció recursos por 1,081.7 millones de pesos en esta materia.

## **Resultados**

### **1. Normatividad Interna**

Se revisó la normatividad interna y se comprobó que la estructura orgánica y la estructura funcional vigentes para 2012 son diferentes, por otro lado las funciones, niveles de autoridad y responsabilidades de la DGTII, no corresponden con la información proporcionada en el “Manual de Organización de la Dirección General de Comunicaciones e Informática” vigente autorizado en julio de 2006.

Del análisis de la información se comprobó que los documentos “Políticas de Seguridad y Auditoría de Bases de Datos (Ambientes No Productivos)”, “Procedimiento relacionado con el Control de Versiones en el Proceso de Desarrollo”, “Procedimiento de Desarrollo de Sistemas” no se encuentran formalizados y no cuentan con firmas de autorización.

Por lo anterior, se concluye que la DGTII, en coordinación con la Dirección General de Programación, Organización y Presupuesto (DGPOP) no actualizó el Manual de Organización de la DGTII.

La DGTII a diciembre de 2013 tiene en proceso de actualización las estructuras orgánicas y funcionales, las cédulas de descripción y perfiles de puestos, con la finalidad de iniciar las gestiones para su autorización; respecto de las funciones, niveles de autoridad y responsabilidades de la DGTII, presentó un proyecto de mejora de la Gestión de TICs, en el que se incluirá y actualizará el Manual de Organización correspondiente, así como los documentos de Políticas de Seguridad y Auditoría de Bases de Datos, procedimientos relacionados con el control de versiones en el proceso de ejecución y desarrollo de sistemas.

#### **12-0-05100-02-1176-01-001 Recomendación**

Para que la Secretaría de Relaciones Exteriores actualice el Manual de Organización Específico de la Dirección General de Tecnologías de Información e Innovación, así como su normatividad de conformidad con lo establecido en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, debido a que no se encuentran formalizados ni autorizados.

## 2. Asignación Presupuestal

Del análisis de la información de la Cuenta de la Hacienda Pública Federal del ejercicio 2012, el gasto programable total de la SRE fue por un monto total de 9,784,370.3 miles de pesos, de los cuales se ejercieron recursos en contratos relacionados con TICs por 429,360.2 miles de pesos equivalentes al 4.4% del presupuesto total, se integran de la siguiente forma:

Recursos ejercidos en 2012 por la SRE (Miles de pesos)	
Gasto Programable	Importe
Servicios Personales	3,307,377.9
Gasto de Operación	4,130,687.3
Otros gastos corriente	2,216,022.4
Gasto de inversión	<u>130,282.7</u>
<b>Total</b>	<b>9,784,370.3</b>

Fuente: Cuenta de la Hacienda Pública Federal de 2012.

Los recursos ejercidos en contratos relacionados con TICs se integran de la siguiente forma:

Recursos ejercidos en 2012 (Miles de Pesos)		
Partida Gasto	Descripción	Importe
3100	Servicios básicos (telefonía, conducción de señales)	20,799.7
3200	Servicios de arrendamientos (patentes)	1,880.4
3300	Servicios profesionales, científicos, técnicos y otros servicios	155,284.5
3500	Servicios de instalación, reparación y mantenimiento	19,094.6
3700	Servicios de traslados y viáticos	1,344.2
3800	Servicios oficiales	230,956.8
	<b>Total</b>	<b>429,360.2</b>

Fuente: Integración de la Cuenta de la Hacienda Pública Federal de 2012 capítulo 3000.

Del total ejercido en 2012, se seleccionó una muestra de dos contratos de prestación de servicios relacionados con las TICs, de los cuales se ejercieron 253,626.0 miles de pesos en 2012.

Muestra de Contratos de Prestación de Servicios Cuenta Pública 2012 (Miles de Pesos)				
Unidad responsable	Partida	Descripción partida	Contrato	Importe Ejercido
Dirección General de Tecnologías de Información e Innovación	38301	Congresos y Convenciones	SRE-DRM-AD-72-12	193,320.9
Dirección General de Delegación	33603	Impresiones de documentos oficiales para la prestación de servicios públicos	SRE-DRM-LP-66-12	<u>60,305.1</u>
				253,626.0

Fuente: Contratos, facturas y soporte documental.

Se verificó que los pagos respectivos fueran reconocidos en las partidas presupuestarias correspondientes y el análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

### 3. Gobierno y Administración de TICs

Para la evaluación de gobierno y administración de las TICs, se tomaron como base los siguientes objetivos específicos: “Proporcionar a las instituciones procesos simplificados y homologados en materia de TICs y de Seguridad de la Información” y “Contribuir a alcanzar una mayor eficiencia en las actividades y procesos institucionales, mediante la aplicación del Marco Rector de Procesos”, contenidos en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTIC-SI).

Se solicitó a la DGTII la información y documentación relacionada con la implementación del MAAGTIC-SI, la respuesta recibida refleja 34.9% de implementación.

Asimismo se solicitó el reporte y la documentación del cumplimiento al MAAGTIC-SI al Órgano Interno de Control (OIC) en la SRE, de la respuesta recibida se detectó que el nivel de implementación determinado por el OIC alcanza un 41.4%.

Del análisis de la información y documentación relacionada con la implementación del MAAGTIC-SI se determinó lo siguiente:

- No se cuenta con un procedimiento documentado que establezca la forma de administrar los proyectos de tecnología acordes con los procesos, que garantice el aprovechamiento de los recursos, mediante la priorización de las iniciativas tecnológicas, considerando el alcance, el tiempo, los recursos, las comunicaciones y los riesgos.
- La DGTII, no ha integrado los Grupos de trabajo para la dirección y desarrollo de actividades estratégicas de TICs.
- No existen métricas definidas para evaluar el cumplimiento de los proyectos en su totalidad.
- Se constató que en lo referente al portafolio de proyectos, no se cuenta con una estrategia y con un informe de rendimiento, donde se definan las directrices para la aplicación y uso eficiente de los recursos de las TICs, como se señala en el MAAGTIC-SI.

Los principales riesgos y consecuencias potenciales que se determinaron debido a la carencia o inconsistencia de las evidencias son los siguientes:

**Porcentaje de Cumplimiento de los Procesos del MAAGTIC-SI**

Grupo de Procesos	Factores Críticos	% Cumplimiento verificado por ASF	Riesgos por la carencia de las evidencias y las consecuencias potenciales
Dirección y Control de TICs	151	0.0	No se encuentran formalmente documentados los elementos regulatorios, normativos y tecnológicos que aplican en la ejecución de las actividades y servicios que brinda la Unidad de Tecnologías de la Información y Comunicaciones (UTIC) en apoyo a las funciones sustantivas de la SRE. En consecuencia, las actividades y servicios que brinda la UTIC no se encuentran alineados a las normativas y necesidades tecnológicas para el funcionamiento de las actividades sustantivas lo que impide identificar los principales hechos o eventos del ambiente externo que podrían representar alguna amenaza u oportunidad para la institución.
Dirección y Control de la Seguridad de la Información	131	27.5	No se encuentra documentado el plan y el programa de implantación del Sistema de Gestión de la Información, en consecuencia, no se cuenta con una estrategia de Seguridad de la Información lo que impide tener un diagnóstico de los requerimientos de seguridad considerando la participación de las unidades usuarias.
Administración de Proyectos	101	11.9	No se evalúa que los casos de negocio se mantengan actualizados con respecto a los cambios en la planeación estratégica del entorno, costos, riesgos y beneficios esperados, al menos semestralmente durante todo el ciclo de vida de las iniciativas de TICs, en consecuencia, la falta de evaluación impide que los proyectos estén alineados a la planeación y necesidades que les dieron origen, además la carencia de medición en los controles de cambios de las variables del ambiente de ejecución dificulta que se tomen con oportunidad las contramedidas en las condiciones para el éxito de los proyectos.
Administración de Procesos	44	0.0	No se elabora el documento de planeación de evaluación y conducción al menos una vez por año, con respecto a la forma como están operando los procesos y si se cumple con el desempeño previsto, en consecuencia, la falta de evaluación impide identificar los procesos que tienen oportunidades de mejora y no permite medir el desarrollo de las actividades de los procesos.
Administración de Recursos	42	73.0	No se realiza la identificación y consolidación de los requerimientos de recursos financieros de los proyectos y servicios de TICs existentes en los portafolios correspondientes. No se hace la priorización de proyectos de TICs y programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica, a fin de lograr la optimización en el manejo del presupuesto destinado a las TICs.
Administración de Servicios	95	17.9	No se cuenta con un Programa de continuidad ni uno de disponibilidad que permitan reducir, a niveles aceptables, el impacto causado por las interrupciones derivadas de incidentes de seguridad, desastres naturales, accidentes o fallas

			en los equipos y se pueda garantizar la restauración de los procesos críticos del negocio de la SRE en los plazos requeridos.
Administración para el Desarrollo de Soluciones Tecnológicas	179	77.7	No se realiza un registro de trazabilidad de los requerimientos de las soluciones tecnológicas, así como de sus componentes y productos, durante el ciclo de vida del proyecto de desarrollo, así como identificar y elaborar alternativas para las soluciones tecnológicas, definiendo los criterios técnicos, siempre manteniendo un adecuado equilibrio en términos de costo, tiempo y rendimiento.
Transición y Entrega	110	78.2	No se tiene establecido la forma en que se debe llevar a cabo el registro, evaluación y atención de los cambios solicitados a uno o más elementos del ambiente operativo de la UTIC. Es necesario elaborar el plan de proyecto de transición a la operación y soporte, así como y establecer los controles que permitan identificar si la solución tecnológica o el servicio de TICs, nuevo o modificado, provee el valor que la Institución requiere.
Operación de Servicios	54	57.4	No se comunica a los responsables de los procesos de Diseño de los servicios de TICs y Administración de los dominios tecnológicos, los acuerdos de nivel de servicios y operación en consecuencia, la falta de comunicación de éstos, implica que la evaluación de los tiempos de servicio y actividades de monitoreo de la mesa de servicios sean deficientes, aunado a que las métricas para la elaboración de un Programa de continuidad que permita tomar acciones ante la contingencia no sean los requeridos.
Administración de Activos	40	0.0	No se han determinado las agrupaciones lógicas de tecnologías, denominadas dominios, que conformen la arquitectura tecnológica de la Institución integrando el documento de Arquitectura de los dominios tecnológicos, estableciendo el proceso de evaluación periódica para obtener la aprobación a dichos estándares por parte del Grupo de trabajo de arquitectura tecnológica y difundirlos al Recurso humano en la UTIC. Así como Establecer y administrar un Repositorio de conocimiento de los dominios tecnológicos.
Operaciones	40	40.0	No se han establecido las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación de TICs que permitan desarrollar, implementar y mantener un Mecanismo de operación de TICs que contemple las actividades rutinarias que se deben ejecutar en cada Activo de TICs por medio de la elaboración de programas de ejecución de tareas para la operación de TICs, conforme a las necesidades de operación de la infraestructura y servicios de TICs que incluya los tiempos máximos permitidos para que un Activo de TICs permanezca fuera de operación, por incidentes en la ejecución de tareas de la operación de TICs.
Totales	987	34.9	Totales

Por lo anterior, el nivel de implantación de los controles definidos en MAAGTIC-SI únicamente alcanza el 34.9% que refleja deficiencias en los controles implementados en las actividades y procesos institucionales de TICs, se determinó que la DGTII no instrumentó los planes para el cumplimiento de la implantación del MAAGTIC-SI en todos sus procesos.

Derivado de los trabajos realizados en esta revisión, la DGTII en diciembre de 2013 inició el proceso de implementar el “Plan de Trabajo MAAGTIC-SI, proyecto para la mejora de la Gestión de TICs”, en el que se describen las acciones y periodos (comprendidos entre el 2 de diciembre de 2013 hasta el 11 de junio de 2014) en los que se llevará a cabo la alineación de los procesos de la DGTII.

#### 12-9-05514-02-1176-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no instrumentaron los planes para el cumplimiento del Manual Administrativo de Aplicación General de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, debido a la carencia en los controles implementados para contribuir en alcanzar una mayor eficiencia en las actividades establecidas en el manual.

#### **4. Incumplimiento de proyecto estratégico “Sitio Espejo”**

Del análisis de la información de los Planes, Programas y Estrategias del 2012, que sirvieron de base para las actividades de la DGTII, se identificó que un proyecto consistió en aumentar la capacidad de almacenamiento e incrementar la infraestructura del “Sitio Espejo” en Atlanta, con los mismos requerimientos arquitectónicos y de capacidad tecnológica con la que cuenta el “Sitio Central” de la SRE en México, con la finalidad de que en caso de falla o desastre se pueda continuar con las operaciones del Sistema Integral de Administración Consular (SIAC), sin embargo, la implementación del proyecto del “Sitio Espejo” fue reprogramada para su instalación y puesta en marcha en noviembre de 2012. Se determinó que no está implementado debido a que se encuentra en proceso de configuración.

El sistema que soporta los procesos sustantivos de la SRE es el SIAC, que es un sistema de información que tiene como finalidad apoyar a la Dirección General de Servicios Consulares (DGSC) y a las Representaciones de México en el Exterior (RME) con los módulos de pasaportes, visas, cartillas, recaudación consular, registro civil, el sistema estadístico de registro consular y aplicaciones satélite; este sistema se encuentra operando en el “Sitio Central” de la SRE, es crítico por las características de la información que es clasificada como de seguridad nacional.

Adicionalmente se constató que la DGTII no cuenta con un programa de continuidad de servicios de TICs, que permita restablecer y tener disponibilidad de las aplicaciones y servicios ante cualquier eventualidad o desastre, por lo que existe un riesgo en pérdida de información que puede comprometer la Seguridad Nacional.

La DGTII no instrumentó los planes estratégicos correspondientes a 2012 y a la fecha no cuenta con el proyecto “Sitio Espejo” que debió implementarse, para que en caso de una contingencia, el servicio continúe disponible.

Derivado de los trabajos realizados en esta revisión, la DGTII en diciembre de 2013 inició con un plan de trabajo para la puesta en marcha del sitio alterno para el primer semestre de

2014, de la misma manera se contempla que la continuidad de los servicios informáticos generales, que incluye al SIAC, por lo anterior se concluye que la DGTII está en proceso para poner en marcha el proyecto "Sitio Espejo", con lo que se atiende parcialmente la observación.

#### 12-9-05514-02-1176-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no cumplieron con el plan estratégico de implementar el proyecto "Sitio Espejo" en Atlanta para el Sistema Integral de Administración Consular, y no cuentan con un programa que garantice la continuidad de los servicios informáticos que proporciona la Dirección General de Tecnologías de Información e Innovación.

### **5. Evento de la Cumbre del G20**

Mediante contrato número SRE-DRM-AD72/12, que tuvo como objeto prestar los servicios de aprovisionamiento de tecnologías de información y comunicaciones para el evento de la Cumbre G-20 por un monto total de 240,000.0 miles de pesos realizado el 18 y 19 de junio de 2012, la DGTII de la SRE no garantizó las mejores condiciones de contratación para el Estado, en cuanto al precio pagado por los servicios y no existe evidencia documental del análisis que justifique la conveniencia de contratar los servicios de aprovisionamiento objeto del contrato en vez de adquirir los equipos tecnológicos que fueron utilizados en la Cumbre.

Cabe señalar que este contrato para la Cumbre fue un evento para atender la participación de 10,000 personas, al cual se le dio tratamiento de banquete y se estableció una comisión (que puede considerarse propina) del 15.0% pagada al proveedor por 24,998.0 miles de pesos, que representó un costo adicional a los servicios prestados; por otro lado al no establecer las condiciones que debieron cumplirse al término del evento, los equipos que sirvieron de base para proporcionar los servicios de aprovisionamiento de infraestructura tecnológica, pasaron a ser propiedad del proveedor. No es factible que equipos nuevos se amorticen totalmente en los 40 días que duró el contrato.

La SRE justificó la contratación realizada conforme a los artículos 40 y 41 fracción XX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASP), que establece que "Las dependencias y entidades, bajo su responsabilidad, podrán contratar adquisiciones, arrendamientos y servicios, sin sujetarse al procedimiento de licitación pública, a través de los procedimientos de invitación a cuando menos tres personas o de adjudicación directa, cuando "...Se trate de la suscripción de contratos específicos que deriven de un contrato marco".

La Secretaría de la Función Pública (SFP) conforme a sus facultades el día 21 de Julio de 2011 emitió un Contrato Marco con el objeto de "establecer las características técnicas y de calidad para prestación de servicios integrales para la organización de eventos"; la SFP clasificó a los proveedores de acuerdo a su nivel de capacidad y experiencia por niveles, siendo el 1 el nivel más alto (permite la realización de eventos a nivel Estado, Gobierno e Institucional), el contrato marco, obliga al contratante a pagar una comisión del 15.0% al proveedor por cualquier tipo de servicio prestado, que puede ser un banquete o la instalación de equipo de cómputo o telecomunicaciones. En el esquema anterior no se hace distinción en el tipo de servicio a recibir en un evento y en casos de que se provean servicios



de cómputo o algún otro como plantas de energía eléctrica, cableado, etcétera no tiene razón de ser, esta comisión es asimilable a la propina que se otorga en el caso de servicios de alimentación en banquetes.

La empresa contratada fue creada en el año 2003 y contaba con el objeto social para “la compra venta de todo tipo de arte, tales como pinturas, esculturas, arquitectura, música y literatura; así como cualquier tipo de diseño”; “la explotación y operación de restaurantes, bares, fuentes de sodas, cafeterías, merenderos, loncherías, centros nocturnos, discoteques, cantinas, tabernas, hosterías, paraderos y negociaciones similares y conexas, en los que se presten los servicios de elaboración, manufacturas, procesos industriales, y comercialización de toda clase de productos alimenticios elaborados, semielaborados y materias primas para su consumo en el local o fuera de él y de otros productos de consumo necesario o convenientes, así como toda clase de bebidas incluyendo alcohólicas”; cabe mencionar que no estaba dentro de su objeto social la “dirección, contratación, producción y operación de eventos nacionales e internacionales” actividades que se incluyeron mediante modificación a su objeto social a partir del día 14 de enero de 2011.

El proveedor de este contrato fue clasificado como nivel 1 para lo cual tuvo que acreditar mediante documentación la experiencia mínima de realización de 10 eventos de servicios integrales en los últimos cinco años; de los cuales cuatro eventos fueran por un monto mínimo de 6,200.0 miles de pesos; el proveedor tuvo un corto periodo de seis meses para cumplir con lo requerido en el nivel 1 de dicho contrato marco, se le dio el visto bueno por parte de la SFP para ser incluido como proveedor de esta categoría.

El proveedor firmó un contrato inicial el 4 de mayo de 2012, por un monto máximo de 200,000.0 miles de pesos. Posteriormente el 12 de junio de 2012 se realizó un convenio modificatorio por un monto adicional al contrato original por 40,000.0 miles de pesos. La entidad justificó esta ampliación por servicios adicionales de suministro, colocación, conexión y pruebas de plantas de energía eléctrica de diferentes capacidades requeridas en el evento, que no habían sido previstas en el requerimiento original.

Durante el evento del G20, el proveedor facturó como se muestra a continuación:

Servicios por el Evento del G20		
Miles de pesos		
Descripción		Importe
Costo Servicio		144,918.3
Comisión del 15.0% sobre el servicio		<u>21,737.7</u>
	SUBTOTAL	166,656.0
IVA 16.0%		<u>26,664.9</u>
	TOTAL	<u>193,320.9</u>

Fuente: Facturas del proveedor.

Del análisis comparativo realizado a un contrato de servicios con el Instituto Federal de Acceso y Protección de Datos (IFAI) que operó durante 2012, mediante un contrato de servicios de arrendamiento de equipos tecnológicos con características similares o superiores a las utilizadas para el G20, se seleccionaron los precios unitarios de tres partidas contempladas en ambos contratos con la misma cantidad de unidades que se proporcionaron durante el evento de la Cumbre G20, como se muestra a continuación:

COMPARATIVO ENTRE UN CONTRATO DE SERVICIOS DE APROVISIONAMIENTO DE TECNOLOGÍAS CON UN CONTRATO DE ARRENDAMIENTO DE TECNOLOGÍAS  
Miles de pesos

Contrato	Descripción partida	Unidades	Precio Unitario con IVA incluido por los 40 días del evento	Total por partida	Total por las tres partidas
Cumbre G20/SRE (aprovisionamiento de tecnologías de información)	Equipo de cómputo de escritorio	845	16.2	13,689.0	
	Equipo de cómputo Laptop	47	23.7	1,113.9	
	Servidores en los centros de datos.	10	145.0	<u>1,450.0</u>	<b>16,252.9</b>
				<b>Comisión del 15.0%</b>	<b>2,437.9</b>
			<b>Total G20</b>		<b>18,690.8</b>
Contrato de Arrendamiento de Tecnologías. (IFAI)	Equipo de cómputo de escritorio	845	2.3	1,943.5	
	Equipo de cómputo Laptop	47	3.1	145.7	
	Servidores en los centros de datos.	10	12.1	<u>121.0</u>	
				<b>Total IFAI</b>	<b>2,210.2</b>
			<b>Costo mayor para G20</b>		<b>16,480.6</b>

El costo diferencial del servicio pagado al proveedor en estos tres conceptos contra un contrato de arrendamiento de equipos es mayor en 16,480.6 miles de pesos.

La DGTII mencionó que se requirió para la Cumbre G20 un servicio integral “llave en mano”, que considerara el aprovisionamiento, transporte, almacenaje, desempaque, colocación, reconfiguración, administración de insumos, memoria fotográfica, control de entregas, licenciamiento de software, garantías, seguro, desinstalación y retiro de equipos, así como el resarcimiento de cualquier daño ocasionado en cualesquiera de los recintos producto de maniobras con éstos.

#### 12-0-05100-02-1176-03-001 Solicitud de Aclaración

Para que la Secretaría de Relaciones Exteriores aclare y proporcione la documentación justificativa y comprobatoria que soporte la contratación y los pagos por 193,320.9 miles de pesos, correspondientes al contrato para el Evento G20 establecido durante 2012, con la finalidad de validar la utilidad y entrega de los servicios incluidos. En caso de no lograr su justificación o respaldo documental, la entidad fiscalizada o instancia competente procederá, en el plazo establecido, a la recuperación del monto observado.

#### 6. Planeación Estratégica de las TICs

Del análisis de la información a la Planeación Estratégica de las Tecnologías de Información y Comunicaciones (PETIC) para el 2012, reportada a la SFP, se constató que la DGTII sólo incluyó un proyecto de tecnología de información denominado “SIPAC27”, en el cual se ejerció un presupuesto por 121.7 miles de pesos; no reportó los siguientes proyectos:

- El proyecto coordinado con la Dirección General de Servicios Consulares (DGSC) relacionado con el SIAC

- El relacionado de manera conjunta con la DGD vinculado con el Sistema de Emisión de Pasaportes en México (SEPM)
- Los servicios de aprovisionamiento de tecnología para el evento de la Cumbre G20
- El de Digitalización de Expedientes

Durante 2012 estos cuatro proyectos en conjunto ejercieron 371,399.2 miles de pesos.

Por lo anterior, resultan insuficientes los controles para seguimiento y priorización de los proyectos estratégicos de TICs que permitan una mejor toma de decisiones, la DGTII no cuenta con un Plan Estratégico autorizado.

Derivado de los trabajos realizados en esta revisión, la DGTII a diciembre de 2013 inició el proceso de implementar el “Plan de Trabajo MAAGTIC-SI, proyecto para la mejora de la Gestión de TICs”, en el que se describen las acciones y periodos (comprendidos entre el 2 de diciembre de 2013 hasta el 11 de junio de 2014) en los que se llevará a cabo la alineación de los procesos de la DGTII.

#### 12-0-05100-02-1176-01-002 **Recomendación**

Para que la Secretaría de Relaciones Exteriores instruya a la Dirección General de Tecnologías de Información e Innovación implementar medidas de control para dar seguimiento y priorizar los proyectos estratégicos de Tecnologías de Información y Comunicaciones, debido a que no cuenta con un plan documentado y autorizado.

### **7. Centros de Datos**

La SRE cuenta con tres centros de datos, dos están ubicados en instalaciones de la SRE y uno en las instalaciones de un proveedor de servicios. En los dos primeros operan los sistemas de Recursos Humanos, de Presupuesto, de Recursos Materiales, de Protección a Mexicanos, los sitios y servicios WEB de la SRE y el SIAC. El Sistema de Emisión de Pasaportes en México (SEPM) opera en el centro de datos del proveedor según el contrato de servicios SRE-DRM-LP-66-12.

Los centros de datos no cuentan con las medidas de seguridad y de procesos suficientes para salvaguardar la confidencialidad, integridad y disponibilidad de la información que garanticen la continuidad de los servicios, acorde con la importancia de los sistemas que se procesan en éstos.

La SRE tiene bajo su responsabilidad el manejo de información clasificada como de Seguridad Nacional, la cual se procesa y resguarda en los tres centros de datos.

Con base en la revisión de los controles definidos por MAAGTIC-SI relacionados con la seguridad física y lógica de los centros de datos se determinó lo siguiente:

- A. De la visita al primer centro de datos, en el que se proporcionan los servicios SIAC, Sistemas RRHH, de Presupuesto, de Recursos Materiales, de Protección a Mexicanos, se observaron los siguientes puntos:

Instalación eléctrica.

- Existe un riesgo de pérdida de energía en el centro de datos, las baterías de dos UPS finalizaron con su tiempo de vida útil, según indica el manual de operación de los equipos.

Medidas de seguridad.

- Las instalaciones físicas donde se encuentra el centro de datos, presentan condiciones que pueden poner en riesgo un nivel adecuado de temperatura. Se destaca que se tienen ventanas que lo mantienen expuesto al exterior y a altas temperaturas, podría ocasionar un sobrecalentamiento de los equipos en caso de que fallara el sistema de aire acondicionado.
  - A pesar de que se utilizan tarjetas de proximidad, no existe un control adecuado de acceso al centro de datos ya que se prestan de manera discrecional a las personas que requieren el acceso.
  - No están formalizadas las políticas y los procedimientos de respaldo y recuperación de datos para los diferentes sistemas que se manejan en la SRE.
- B. De la visita al segundo centro de datos, donde se encuentran los servidores de desarrollo y pruebas se observó lo siguiente:
- Las puertas de salida de emergencia, se encuentran dañadas.
  - El cableado del centro de datos presenta riesgos de seguridad ya que éste no está plenamente identificado y se encuentra disperso en el piso.
- C. De la visita realizada al centro de datos en las oficinas del proveedor de servicios, donde se encuentra alojado el SEPM, se revisaron las condiciones físicas conforme a las especificaciones de la norma International Computer Room Experts Association (ICREA1 por sus siglas en inglés), se detectaron las siguientes inconsistencias:
- La SRE a través del contrato SRE-DRM-LP-66-12 solicitó el 98.0% de disponibilidad de los servicios del Centro de Datos; dicho contrato en su Anexo A precisa que requiere como mínimo la norma ICREA1 que ofrece un 95.0% de disponibilidad, cuando esto no garantiza la disponibilidad estipulada en el contrato.

Medidas de seguridad:

- Las instalaciones de las plantas de energía y los cuartos de los Uninterruptible Power Supply (UPS por sus siglas en inglés), no cuentan con un sistema de extinción de incendios ni cámaras de seguridad.
- No se actualizan las bitácoras de accesos al centro de datos.
- Se comprobó que los respaldos de datos del aplicativo SEPM se encuentran en la bóveda personal del Presidente de la empresa, dentro de gavetas, no se tienen bitácoras de accesos, ni cámaras de seguridad. El protocolo de acceso no está definido, la información ahí resguardada es de carácter reservado (clasificada como de Seguridad Nacional), comprometiendo la confidencialidad de la información.
- Las instalaciones del centro de datos no cuentan con las condiciones de seguridad física que permitan un ambiente adecuado para la infraestructura que aloja, ya que son ventanales de piso a techo, a menos de metro y medio del cristal se encuentra laborando personal del proveedor de distintas áreas.

Comunicaciones:

- El cableado no está totalmente etiquetado ni estructurado.

Se determinó que la administración del SEPM al manejar información de seguridad nacional y ser un proceso sustantivo de la SRE, se encuentra indebidamente en instalaciones de un tercero que no cumple con las medidas de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información, ya que la SRE no estipuló en el contrato SRE-DRM-LP-66-12 los controles de seguridad mínimos requeridos, como consecuencia se pone en riesgo la información contenida en las bases de datos.

Adicionalmente, la DGTII no supervisó el cumplimiento del MAAGTIC-SI en los niveles de gestión: 5.11 OP – Operaciones; 5.2 DCSI – Dirección y Control de la Seguridad de la Información y 5.6 AS – Administración de Servicios.

Derivado de la revisión, la DGTII informó lo siguiente:

- Para disminuir la carga térmica del primer centro de datos se realizaron trabajos y adecuaciones, sin embargo, existen áreas de oportunidad que requieren inversiones mayores.
- Las baterías de los UPS que alimentan el centro de datos fueron reemplazadas en 2011, teniendo 2 años de uso.
- Se han iniciado mejoras en el segundo centro de datos conforme a su plan de trabajo.
- El tercer centro de datos cuenta con certificación ICREA1, que garantiza el cumplimiento de los estándares para cableado estructurado, adicionalmente se han tomado medidas para mejorar el cableado dentro de las oficinas del proveedor.

La infraestructura de cómputo del centro de datos es propiedad del prestador de servicios del contrato, su responsabilidad y obligación es el aprovisionamiento, operación, administración y monitoreo; la información y aplicativos es propiedad de la SRE, en la cláusula décima novena, la confidencialidad la debe mantener el proveedor para la ejecución de los servicios.

- Dentro del ámbito de responsabilidades de cada área y conforme a la reorganización de la DGTII, se planea alinear al MAAGTIC-SI las guías y procedimientos en la materia para su posterior viabilidad operativa en el 2014.

Por lo anterior, se concluye que la DGTII aún se encuentra en proceso de mejora en los centros de datos, así como la implementación del MAAGTIC-SI.

#### 12-9-05514-02-1176-08-003 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos de la Dirección de Proyectos de Telecomunicaciones y la Dirección General de Tecnologías de Información e Innovación que en su gestión no supervisaron el cumplimiento del Manual Administrativo de Aplicación General de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información en el proceso de Dirección y Control de Seguridad de la Información y además no estipularon en el contrato SRE-DRM-LP-66-12 los controles de seguridad mínimos requeridos, que ponen en riesgo la confidencialidad, disponibilidad e integridad de la información de seguridad nacional contenida en las bases de datos.

## 8. Seguridad de la Información y Continuidad de Servicios

Del análisis de la documentación proporcionada e información publicada en el portal de la SRE ([www.sre.gob.mx](http://www.sre.gob.mx)) se pudo constatar que:

- El documento que hace referencia a la seguridad lógica denominado “Normas de la Dirección General de Comunicaciones e Informática” se encuentra desactualizado, fue emitido en agosto 2005 y no corresponde a la operación actual.
- La documentación recibida como Políticas y Procedimientos para el Respaldo y la Recuperación de Datos, no tiene control documental ni firmas de autorización y no se tiene evidencia de su difusión de manera oficial.
- El documento recibido como evidencia del Análisis de Riesgos, no está formalmente autorizado y no cuenta con un control documental que indique la fecha en que fue realizado, el responsable de la revisión y los responsables de las áreas de negocio involucrados.

De la revisión de la documentación y de la reunión donde se trataron temas relacionados con la Seguridad de la Información, se determinó que:

- No está implementado un Sistema de Gestión de Seguridad de la Información (SGSI), por lo que no se garantiza la protección de los activos de la información de la Institución poniendo en riesgo su confidencialidad, disponibilidad e integridad.
- No se tiene una Política de Seguridad de la Información que proporcione una guía y apoyo de la Dirección para gestionarla de acuerdo a los objetivos del negocio y con las leyes y regulaciones vigentes por medio de la cual, minimizar los riesgos y hacer frente a eventos inesperados como pueden ser accesos no autorizados, modificación, destrucción de la información o divulgación.
- No se tiene una directriz rectora para la administración de riesgos, ni un programa para su manejo que contemple la identificación de los activos informáticos, la evaluación de vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto que se produciría en caso de su materialización.
- No se tiene un Análisis de Impacto al Negocio que permita evaluar los procesos críticos y determinar los tiempos, prioridades y recursos necesarios en caso de una interrupción de servicios, a partir del cual, se pueda desarrollar e implantar un programa de continuidad que permita reducir a niveles aceptables, el impacto causado por las interrupciones derivadas de incidentes de seguridad, desastres naturales, accidentes o fallas en los equipos.
- En relación con el “Reporte de pruebas de penetración realizado en 2012” del primer centro de datos, se entregó el documento “Acciones de remediación de las pruebas de penetración 2012”, que no solventa los hallazgos que se obtuvieron en los sitios consultados, comprometiendo su seguridad.
- En lo que respecta a la asignación de cuentas y uso de los privilegios, no se cuenta con un mecanismo por medio del cual se controlen y revisen periódicamente los permisos, de acuerdo con los roles y responsabilidades que los usuarios deben tener

en los sistemas bajo el principio de privilegios mínimos, lo que puede provocar el abuso de las facultades para realizar transacciones sin la autorización correspondiente. No se lleva a cabo un proceso de validación de privilegios de las cuentas asignadas al personal por cambios en el nivel de responsabilidad o término de la relación laboral.

- No se realiza un monitoreo preventivo de los servicios relacionados con el SIAC, lo que podría ocasionar que en caso de alguna falla, se incremente el tiempo de restablecimiento del servicio, dejando sin operación a todas las cancillerías que operan con este sistema. Los eventos de seguridad se atienden de forma reactiva y no preventiva, debido a que las estadísticas generadas por la herramienta “correlacionador de eventos” se revisan una vez al día.
- No se cuenta con un procedimiento de administración de incidentes formalizado que permita gestionar de manera adecuada y oportuna los incidentes de seguridad que pudieran presentarse y garantizar que la totalidad de los servicios brindados se encuentre operando de manera regular.
- La información contenida en los equipos de cómputo no se encuentra protegida con ningún tipo de cifrado y no cuenta con los mecanismos que impidan el copiado a dispositivos externos (USB, discos duros, teléfonos, entre otros), que eviten el daño, pérdida, copia, acceso no autorizado y robo de la información de carácter reservada que pueda poner en riesgo la seguridad nacional.
- No se efectúa un monitoreo de las bitácoras de acceso y modificaciones a las bases de datos de producción de la aplicación SIAC, por lo que no es posible una detección oportuna sobre movimientos o accesos no autorizados que pongan en riesgo la confidencialidad, disponibilidad e integridad de la información.

Se concluye que la DGTII no supervisó el cumplimiento de los procesos de MAAGTIC-SI, ya que resultan insuficientes los controles requeridos para la administración de la seguridad de la información. Si bien la DGTII proporcionó información de acciones que se están llevando a cabo derivadas de los hallazgos en la revisión, al cierre de la auditoría subsisten algunas.

#### 12-9-05514-02-1176-08-004 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no supervisaron el cumplimiento de factores críticos para la Secretaría de Relaciones Exteriores, como es la administración de la información de seguridad nacional, por ser insuficientes los controles existentes.

### **9. Gestión de la Infraestructura Tecnológica y Seguridad de la Información relacionados con el contrato “SRE-DRM-LP-66-12”**

Del análisis de la información del contrato plurianual número SRE-DRM-LP-66-12, se obtuvo que se pagaron 60,305.1 miles de pesos en 2012, su objeto fue proporcionar los servicios para la emisión del pasaporte mexicano que a continuación se indican:

- Operación de Pasaportes en la Delegación Cuauhtémoc
- Mejora Continua y Soporte del Sistema de Expedición de Pasaportes en México

- Aprovisionamiento de Cómputo a Delegaciones y/u Oficinas
- Solución de Personalización
- Suministro de Láminas de Seguridad
- Infraestructura Centro de Datos
- Infraestructura-Almacenamiento
- Mesa de Servicios

Durante la revisión de los servicios relacionados con los procesos del MAAGTIC-SI correspondientes a “Establecimiento del Modelo de Gobierno de TICs”, “Administración de la Seguridad de la Información”, “Diseño de Servicios de TICs”, “Administración de Niveles de Servicio”, “Administración de la Operación” y “Administración del Ambiente Físico”, se constató lo siguiente:

- No se han ejecutado las pruebas de vulnerabilidad a los equipos ubicados en el centro de datos del proveedor contratado, que soporta el SEPM.
- Del análisis a las bitácoras de rotación se detectó que las cintas de respaldo de la información en poder del proveedor no son resguardadas en otras localidades distintas al centro de cómputo lo que potencializa el riesgo de pérdida de datos.

Se determinó que los principales riesgos por la carencia o inconsistencia de los controles de seguridad de la información y sus consecuencias potenciales para las operaciones y activos de la SRE son las siguientes:

Principales riesgos en los controles de Seguridad de la Información	
Objetivo de Control de Seguridad	Riesgos por la carencia de las evidencias y las consecuencias potenciales
No existe un Plan de Recuperación de Desastres	La ausencia de las características de disponibilidad, capacidad y rendimiento de cada componente de la infraestructura de TICs, evita que éstos se fortalezcan en lo individual, impidiendo efectuar pruebas de recuperación, para confirmar que los servicios de TICs puedan ser recuperados de forma efectiva, que las deficiencias serán atendidas y comprobar su vigencia, con la finalidad de asegurar a la Institución el mínimo impacto en caso de alguna interrupción en los servicios de TICs.
No se tiene el estudio de Vulnerabilidad de la Infraestructura Tecnológica	Se carece de la identificación, clasificación y priorización de los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, de manera que se obtengan los planes de mitigación de riesgos que permitan fortalecer los mecanismos de seguridad para los aplicativos sustantivos y la infraestructura tecnológica.
Ausencia de un procedimiento de resguardo para respaldos en un sitio alternativo	Los respaldos están en el mismo predio que los servidores de misión crítica, en consecuencia, en caso de una catástrofe en el centro de datos, el punto objetivo de recuperación (RPO) de información sería mucho mayor al estimado en los anexos técnicos relacionados al contrato de prestación de servicios.

Fuente: Elaborada por la ASF con base en el análisis de la información proporcionada por la SER.



En el contrato se establece un enlace tipo “A” entre las oficinas centrales y el sitio del contrato. Se verificó su funcionamiento en modo espejo y como respaldo de las bases de datos, se detectó que hubo agotamiento de la capacidad en infraestructura del sitio de la SRE.

Se concluye que la DGTII no supervisó el cumplimiento de los procesos de seguridad de la información y continuidad de la operación, ya que resultan insuficientes los controles requeridos para la administración de la información de seguridad nacional. Si bien se proporcionó información de acciones que se están llevando a cabo derivadas de los hallazgos en la revisión al cierre de la auditoría, subsisten algunas.

**12-0-05100-02-1176-01-003 Recomendación**

Para que la Secretaría de Relaciones Exteriores fortalezca los mecanismos de control y validación y realice una planeación objetiva y, por las características de la información de seguridad nacional que maneja, evalúe la alternativa de retornar la operación del Sistema de Emisión de Pasaporte Mexicano a la infraestructura de la Secretaría de Relaciones Exteriores, y respecto al sitio espejo reconsidere ubicarlo en instalaciones de la propia Secretaría.

**10. Gestión del Sistema de Emisión de Pasaportes en México y Seguridad de la Información relacionados con el contrato “SRE-DRM-LP-66-12”**

Durante la revisión de los servicios relacionados con los procesos de “Administración de la Seguridad de la Información”, “Diseño de Servicios de TICs”, “Administración de Niveles de Servicio”, “Desarrollo de Soluciones Tecnológicas”, “Calidad de Soluciones Tecnológicas” y “Liberación-Entrega”, se constató que los principales riesgos por la carencia o inconsistencia de los controles de seguridad de la información y sus consecuencias potenciales para las operaciones y activos de la SRE son las siguientes:

Principales riesgos en los controles de Seguridad de la Información	
Objetivo de Control de Seguridad	Riesgos por la carencia de las evidencias y las consecuencias potenciales
Manejo de facultades no autorizadas por los usuarios	Un usuario puede tener permisos para acceder a información que no le corresponde de acuerdo a sus funciones y responsabilidades, en consecuencia, se pierde la confidencialidad en la información y se pueden ejecutar transacciones no autorizadas que ponen en riesgo los activos y procesos de la institución.
Manejo de contraseñas privilegiadas por los proveedores	Los proveedores tienen acceso funcional y operativo con claves de acceso ilimitado a las bases de datos principales de la institución, en consecuencia, pueden ejecutar transacciones no autorizadas sin dejar rastros que ponen en riesgo los activos y procesos de la SER.
No está implementado el Sistema de Gestión de Seguridad de la Información	La falta de prácticas para la operación, mantenimiento, seguimiento y control del modelo de gobierno de seguridad de la información a través del sistema de gestión de seguridad de la información, tiene entre otras consecuencias, que no se pueda garantizar la protección de las Infraestructuras críticas, que se carezca de un adecuado análisis de riesgos y que la atención de la operación se lleve a cabo sin una directriz rectora de respuesta a incidentes, lo que impide garantizar la disponibilidad, confiabilidad y continuidad de las operaciones.
Falta de capacitación al personal de TI respecto al sistema de seguridad de la información	La SRE deberá asegurarse de que se presente a la unidad administrativa responsable de la capacitación, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, de lo contrario, el personal competente en los temas de seguridad estará limitado para manejar la estructura, alcances y operaciones que requiere el Sistema de Gestión de Seguridad de la Información.
No existe retroalimentación en la solución de los tickets registrados en tercer nivel, por parte de la mesa de ayuda	Los equipos responsables de atender y solucionar las solicitudes de servicio, deben tener definida una responsabilidad para la solución de requerimientos, incidentes y problemas, de lo contrario, no podrán agilizar el diagnóstico de la solicitud de servicio y la investigación técnica requerida, lo que repercutirá en una deficiente atención de la solicitud de servicio.
El procedimiento de cierre de los tickets en la mesa de servicios está bajo el control del proveedor	La evaluación y cierre de las solicitudes de servicio requiere la intervención de la SRE para constatar que las mismas se hayan resuelto con la solución entregada, así como modificar su estado a concluidas, con el propósito de que el usuario solicitante tenga garantías de su cierre y finalice el ciclo de vida de la solicitud.
La aplicación del sistema de emisión de pasaportes permite duplicarlos y cambiar el estatus del documento	Los responsables del desarrollo de soluciones tecnológicas de TICs con apoyo del representante de la unidad administrativa solicitante, deberán definir e integrar en el documento de especificación de requerimientos de soluciones tecnológicas, los controles de seguridad que se requieran para la protección y trazabilidad de las transacciones y los datos, en caso contrario, la información que se genere puede perder sus características de integridad y confidencialidad, lo que compromete la eficiencia y confiabilidad de los sistemas de información.
La determinación de los costos en el desarrollo de aplicaciones y servicios no aplica la metodología de "Estructura del Desglose del Trabajo"	El Administrador del proyecto deberá elaborar la estructura de desglose del trabajo, representando en ésta el alcance total del proyecto, incluyendo la definición de paquetes de trabajo, consistentes en subdividir los entregables en componentes más pequeños, fáciles de dirigir y supervisar, de lo contrario, la cuantificación de los costos puede caer en excesos por la falta de seguimiento de las tareas que comprenden las actividades, además de tener desviaciones en los alcances y tiempos para el cumplimiento de los calendarios de trabajo.

Fuente: Elaborada por la ASF con base en el análisis de la información proporcionada por la SER.

Por lo anterior, la falta de prácticas para la operación, mantenimiento, seguimiento y control del modelo de gobierno de seguridad de la información ponen en riesgo la disponibilidad y confiabilidad de las operaciones, por lo que se concluye que la Dirección General Adjunta de Comunicaciones e Informática no formuló ni realizó los planes, programas, estrategias, políticas y normas necesarias para encauzar la actividad y desarrollo

de la informática y las telecomunicaciones, dentro de un margen de seguridad en el manejo de la información.

Asimismo, los responsables del desarrollo de soluciones tecnológicas de TICs no tomaron en cuenta los controles de seguridad requeridos para la protección y trazabilidad de las transacciones y los datos, lo que permite que el sistema de emisión de pasaportes los duplique y presente cambios en los estatus del documento, por lo que se concluye que la Dirección de Reingeniería de Sistemas no promovió ni instrumentó los planes, programas, estrategias, políticas y normas necesarias para el correcto desarrollo de los sistemas de información.

Se concluye que la DGTII no supervisó el cumplimiento del contrato SRE-DRM-LP-66-12, ya que resultan insuficientes los controles requeridos para la administración de la información de seguridad nacional que se opera con el mismo. Si bien la DGTII proporcionó información de acciones que se están llevando a cabo derivadas de los hallazgos en la revisión, al cierre de la auditoría subsisten algunas.

#### 12-9-05514-02-1176-08-005 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no supervisaron el cumplimiento del contrato SRE-DRM-LP-66-12, ya que resultan insuficientes los controles requeridos para la administración de la información de seguridad nacional que se opera con el mismo.

#### **11. Estudio de la Calidad de los Datos de Pasaportes**

Del análisis de la información realizado con una herramienta de análisis de calidad de datos se tomó una muestra de la información contenida en el SEPM, SIAC, SAIU y de expedientes solicitados para validar el soporte documental de los pasaportes emitidos, se encontró lo siguiente:

##### *Sistema de Emisión de Pasaportes en México*

En el estudio de la información se validó la consistencia de los datos de pasaportes emitidos en México; para medir la calidad fue necesario descomponer los datos en sus características observables de las cuales se evaluó que los datos fueran completos y válidos. Las direcciones fueron comparadas con los catálogos del Servicio Postal Mexicano y los teléfonos con las definiciones de la Comisión Federal de Telecomunicaciones. La muestra revisada incluyó los datos de los titulares de los pasaportes, dirección, tutor y entre otras fuentes de información proporcionadas por la SRE. Para medir la calidad fue necesario verificar los datos observables de una muestra que incluyó 525,200 registros de titulares, 558,000 registros de solicitudes y 230,000 registros de tutor, los resultados de la validación de los registros son los siguientes:

- No contienen información en el dato de :
  - ✓ CURP 268,274;
  - ✓ Código Postal 121,887;
  - ✓ 111,062 Dirección y

- 1,000 con fecha de nacimiento que son menores o iguales al año 1900.

#### *Sistema Integral de Administración Consular*

En el estudio de la información se validó la consistencia de los datos de pasaportes emitidos en el exterior; para medir la calidad fue necesario descomponer los datos en sus características observables de las cuales se evaluó que los datos fueran completos y válidos. La muestra revisada incluyó los datos de los titulares de los pasaportes y dirección, entre otras fuentes de información proporcionadas por la SRE. Para medir la calidad fue necesario verificar los datos observables de una muestra que incluyó 821,577 registros de pasaportes emitidos en el exterior, los resultados de la validación de los registros son los siguientes:

- No contienen información en el dato de
  - ✓ Código postal de nacimiento 60,327;
  - ✓ Código postal actual 24,331;
  - ✓ Estado actual 17,965;
  - ✓ Estado de nacimiento 4,466 y
- 2 con fecha de nacimiento menores o iguales al año 1900.

#### *Sistema de Administración de Identidad Única*

En el análisis de la información de la muestra de la base de datos del SAIU, se validó la consistencia entre los datos correspondientes a las tablas de datos "Temporal Auditoría" que contienen 1,865,005 registros de pasaportes, para medir la calidad fue necesario descomponer los datos en sus características observables de las cuales se evaluó que los datos fueran completos y válidos, los resultados de la validación de los registros son los siguientes:

- que contienen dato erróneo en el dato "CURP" 1,463,053;
- que contienen valor nulo en el dato "NOMBRE" 447,601;
- 208 con fecha de nacimiento mayor al año 2013 y
- 54 con fecha de nacimiento menores al año 1900.

Del análisis anterior se concluye que existe riesgo de duplicidades en los registros y posibilidad de captura y generación de pasaportes con datos incorrectos.

Reconociendo que el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública Federal implica recabar datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental para promover el uso responsable de las nuevas tecnologías de la información, atendiendo a los principios de protección de datos personales de licitud, calidad, de información al titular sobre el uso y destino de la información, de seguridad, custodia y consentimiento para su transmisión; principios que no limitan la utilización de la informática en el ámbito público.

Para verificar la consistencia de los datos en el proceso de emisión de documentos se realizó un análisis de calidad de datos y se identificaron registros activos con fecha de nacimiento

entre 1897 y 1916; por lo que se solicitó una muestra de 37 expedientes de trámites donde se identificaron dos registros que tenían un “problema de biométricos” y el proceso fue interrumpido sin concluirse el trámite y de 3 se identificaron que fueron eliminados antes de capturar los biométricos, sin que se nos haya proporcionado la documentación o evidencia que justifique la cancelación o el nuevo registro que ampare un nuevo proceso para dicho solicitante. Por lo anterior se concluye que no existen los controles suficientes para asegurar que la información registrada durante el proceso de emisión sea igual a la impresa en el documento final.

Por lo anterior, resultan deficientes los controles requeridos para la consistencia y conformidad de las operaciones y los datos, considerando la sensibilidad y nivel crítico de éstos, se concluye que la Dirección General Adjunta de Comunicaciones e Informática no garantizó que las aplicaciones sustantivas para administrar y procesar información de seguridad nacional funcionen correctamente.

#### **12-9-05514-02-1176-08-006 Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en la Secretaría de Relaciones Exteriores, para que realice las investigaciones pertinentes y, en su caso inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no garantizaron que las aplicaciones sustantivas funcionen correctamente, debido a que resultaron deficientes los controles requeridos para la consistencia y validación de las operaciones y los datos, de 37 expedientes sólo entregaron 21 por lo que la falta de evidencia documental que permitiera identificar en qué etapa finalizó el trámite del documento no permite garantizar que la información que se imprime corresponda a la capturada en el sistema.

#### ***Recuperaciones Probables***

*Se determinaron recuperaciones probables por 193,320.9 miles de pesos.*

#### ***Resumen de Observaciones y Acciones***

Se determinó(aron) 10 observación(es) la(s) cual(es) generó(aron): 3 Recomendación(es), 1 Solicitud(es) de Aclaración y 6 Promoción(es) de Responsabilidad Administrativa Sancionatoria.

#### ***Dictamen: negativo***

La auditoría se practicó sobre la información proporcionada por la entidad fiscalizada, de cuya veracidad es responsable; fue planeada y desarrollada de acuerdo con el objetivo y alcance establecidos; y se aplicaron los procedimientos de auditoría y las pruebas selectivas que se estimaron necesarios. En consecuencia, existe una base razonable para sustentar el presente dictamen, que se refiere sólo a las operaciones revisadas.

La Auditoría Superior de la Federación considera que la entidad no cumplió con las disposiciones normativas aplicables, como se precisan en los resultados que se presentan en el apartado correspondiente de este informe, donde destacan los siguientes: no se garantizaron las mejores condiciones de contratación para el Estado por los servicios pagados durante el evento de la Cumbre G20 por 193,320.9 miles de pesos (76.2% de la muestra); el nivel de cumplimiento del MAAGTIC-SI, reportado por la Secretaría de Relaciones Exteriores y el Órgano Interno de Control fue 41.4%; la evaluación determinó

34.9%; se carece de un plan de continuidad que garantice la operación del proceso de pasaportes en caso de una contingencia.

## **Apéndices**

### *Procedimientos de Auditoría Aplicados*

1. Evaluar el nivel de gestión que corresponde a los procesos relacionados con la dirección, el control y la administración de riesgos en materia de tecnologías de la información y comunicaciones (TICs), así como el análisis de la estructura orgánica y el manual de organización, con el propósito de identificar las áreas y funciones relacionadas con las TICs.
2. Revisar la gestión de los procesos relacionados con la administración de proyectos, administración de procesos, administración de recursos y administración de servicios, para identificar las actividades que permiten la óptima gestión de recursos, su correcta aplicación y verificación, así como de la mejora de los procesos en la Unidad de Tecnologías de la Información y Comunicaciones (UTIC).
3. Verificar la gestión relacionada con la operación de soluciones o servicios tecnológicos de la UTIC, así como los procesos relacionados con el control, mantenimiento y continuidad de la operación.
4. Analizar los contratos de servicios, anexos y convenios modificatorios para confirmar la utilidad de las contrataciones, así como evaluar las adquisiciones de bienes y servicios de TICs para dictaminar su eficiencia, eficacia, economía y competencia en el mercado.
5. Verificar que en los procedimientos de adjudicación y los contratos formalizados, se hayan presentado las mejores condiciones para el Estado conforme lo establecen las leyes y reglamentos en materia de adquisiciones, así como el análisis de las escrituras públicas de los licitantes para descartar una probable asociación indebida.
6. Comprobar que los pagos realizados por los trabajos contratados, estén debidamente soportados, cuenten con controles que permitan su fiscalización y correspondan a trabajos efectivamente devengados que justifiquen las facturas pagadas, así como la verificación de la autenticidad de los comprobantes fiscales proporcionados a la entidad por parte de los proveedores.

### *Áreas Revisadas*

La Dirección General de Tecnologías de Información e Innovación (DGTII), la Dirección General de Delegaciones (DGD), la Dirección General de Programación, Organización y Presupuesto (DGPOP).

### *Disposiciones Jurídicas y Normativas Incumplidas*

Durante el desarrollo de la auditoría practicada, se determinaron incumplimientos de las leyes, reglamentos y disposiciones normativas que a continuación se mencionan:

1. Constitución Política de los Estados Unidos Mexicanos: Artículo 134;
2. Otras disposiciones de carácter general, específico, estatal o municipal: Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, artículo 8, fracción I;

Reglamento Interior de la Secretaría de Relaciones Exteriores artículos 14, fracción I, VIII, 32, fracción XVIII, 36 fracción II, III;

Acuerdo por el que se reforma y adiciona el diverso por el que se establecen las disposiciones administrativas en materia de tecnologías de la información y comunicaciones y de seguridad de la información, y se expide el Manual Administrativo de Aplicación General en esas materias (MAAGTIC-SI), artículos tercero, cuarto, quinto y noveno; procesos 5.3 PR, 5.3.1. APP, 5.3.2. APTI, 5.6 AS, 5.6.1. APS, APS-4, EMG; PE-5 , PE-6 , OPEC-4, DSTI-5, 5.1.2 , EMG-3, PE-5, PE-6, 5.2 DCSI, 5.6 AS, 5.2.1, 5.2.2 OPEC, 5.7.2, 5.7.3, ASI7;

Contrato número SRE-DRM-LP-66-12;

Decreto que establece las medidas de austeridad y disciplina del gasto de la Administración Pública Federal artículo vigésimo primero;

Lineamientos Específicos para la Aplicación y Seguimiento de las Medidas de Austeridad y Disciplina del Gasto de la Administración Pública Federal numeral 23;

#### *Fundamento Jurídico de la ASF para Promover Acciones*

Las facultades de la Auditoría Superior de la Federación para promover las acciones derivadas de la auditoría practicada, encuentran su sustento jurídico en las disposiciones siguientes:

Artículo 79, fracción II, párrafos tercero y quinto y fracción IV, párrafos primero y penúltimo, de la Constitución Política de los Estados Unidos Mexicanos.

Artículos 6, 12, fracción IV; 13, fracciones I y II; 15, fracciones XIV, XV y XVI; 29, fracción X; 32; 39; 49, fracciones I, II, III y IV; 55; 56, y 88, fracciones VIII y XII, de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### *Comentarios de la Entidad Fiscalizada*

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinadas por la Auditoría Superior de la Federación, y que se presentó a esta entidad fiscalizadora para los efectos de la elaboración definitiva del Informe del Resultado.