Aeropuerto Internacional de la Ciudad de México, S.A. de C.V.

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-2-09KDN-15-0395-2018

395-DE

Criterios de Selección

Durante la primera fase de selección, a fin de establecer un primer universo, se ponderaron los siguientes criterios:

Para el Poder Ejecutivo, Legislativo y Judicial, así como Organismos Autónomos:

Contratos reflejados en CompraNet (Monto)	20%
Gastos de TIC en 2017	20%
Propuestas coincidentes con la Dirección de Programación y Planeación	15%
Proveedores relevantes	15%
Proveedores de riesgo	15%
Notas de prensa	5%
Control Interno	5%
Gasto de TIC en relación con el equipamiento de las entidades	5%

De esta primera evaluación se seleccionaron 38 entidades a las que se les solicitó información relacionada con las TIC.

En el caso de los Estados de la República:

Contratos reflejados en CompraNet (monto)	25%
Gastos de TIC en 2017	25%
Participaciones Federales asignadas	50%

De esta primera evaluación se seleccionaron 5 Estados de la República a los que se les solicitó información relacionada con las TIC.

Objetivo

Fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe individual de auditoría se comunicarán a la entidad fiscalizada, en términos de los artículos 79 de la Constitución Política de los Estados Unidos Mexicanos y 39 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, para que en un plazo de 30 días hábiles presente la información y realice las consideraciones que estime pertinentes.

En tal virtud, las recomendaciones y acciones que se presentan en este informe individual de auditoría se encuentran sujetas al proceso de seguimiento, por lo que en razón de la información y consideraciones que en su caso proporcione la entidad fiscalizada, podrán confirmarse, solventarse, aclararse o modificarse.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	89,158.7
Muestra Auditada	42,272.8
Representatividad de la Muestra	47.4%

El universo seleccionado por 89,158.7 miles de pesos corresponde al total de recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2017; la muestra auditada se integra de dos contratos relacionados con servicios para mejorar los procesos administrativos, financieros y comerciales de AICM, la implementación del eBusiness Suite Oracle R12, su soporte y mantenimiento por 5 años; y del servicio integral de tecnologías de la información para el nuevo edificio administrado por el estado mayor presidencial en AICM; con pagos ejercidos por 42,272.8 miles de pesos, que representan el 47.4% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de las acciones realizadas en materia de TIC por la Subdirección de Sistemas del Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. en 2017, relacionadas con el Gobierno y Administración de las TIC, Gestión de la Seguridad de la Información y Continuidad de las Operaciones.

Antecedentes

El Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM) es el primer aeropuerto civil de México y el más importante de toda América Latina, debido al número de pasajeros y operaciones áreas que se llevan a cabo; transportando más de 47 millones de pasajeros por año, opera con 27 aerolíneas para pasajeros nacionales e internacionales y 13 de carga; ha tenido diferentes denominaciones en el transcurso de sus más de 50 años oficiales de operación, identificándosele como Puerto Aéreo Central de la Ciudad de México, Aeropuerto Central de la Ciudad de México, Aeropuerto de México, Aeropuerto Benito Juárez y el actual, Aeropuerto Internacional Benito Juárez Ciudad de México. Durante 2006, todos

los empleados de carácter administrativo y de apoyo quedaron adscritos a la razón social Servicios Aeroportuarios de la ciudad de México, S.A. de C.V. (SACM), mientras que todo el personal operativo se mantiene adscrito a AICM.

Entre el 2013 al 2017, se han invertido 332,910.9 miles de pesos en Tecnologías de la Información y Comunicaciones (TIC), relacionados con los capítulos 1000 "Servicios Personales", 2000 "Materiales y Suministros" y 3000 "Servicios Generales".

Recursos Invertidos en Materia de TIC

(Miles de Pesos)

PERIODO DE INVERSIÓN	2013	2014	2015	2016	2017	TOTALES
MONTO POR AÑO	68,325.2	48,108.7	46,838.0	80,480.3	89,158.7	**332,910.9**

Fuente: Elaborado con base en la información definitiva proporcionada por AICM.

Resultados

1. Normativa Interna

El Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM), cuenta con un Manual General de Organización, publicado en el Diario Oficial de la Federación (DOF) el 15 de mayo de 2015 y no fue actualizado en 2017, el Manual contempla a las unidades administrativas de Servicios Aeroportuarios de la Ciudad de México (SACM) y a las del AICM, éstas se diferencian en que AICM es la empresa concesionaria y responsable de operar el aeródromo y SACM la encargada de proporcionar servicios administrativos a las dos entidades.

Se observó que la Subdirección de Sistemas no cuenta con un manual de organización específico para el desarrollo de sus funciones; no obstante, su operación se ajusta a lo estipulado en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI).

Análisis Presupuestal

En el análisis de información de la Cuenta de la Hacienda Pública Federal del ejercicio 2017, se identificó que el AICM tuvo un presupuesto modificado de 7,117,748.0 miles de pesos, de los cuales se ejercieron 5,995,399.1 miles de pesos, que representan el 84.2% respecto del presupuesto modificado, reportando economías por un monto de 1,122,348.9 miles de pesos. El AICM no realizó reintegros a la Secretaría de Hacienda y Crédito Público (SHCP), debido a que los recursos del Aeropuerto corresponden a ingresos propios y no contemplan Adeudos de Ejercicios Fiscales Anteriores (ADEFAS), sino que el presupuesto devengado no pagado lo clasifica como economías para ser utilizado en el siguiente ejercicio fiscal, dicho monto se integra como sigue:

CUENTA PÚBLICA 2017
(Miles de pesos)

		A	B	C	D	E	F=B-C
Capítulo	Descripción	Presupuesto Autorizado	Presupuesto Modificado	Presupuesto Devengado	Presupuesto Pagado	Presupuesto Ejercido	Economías
1000	Servicios personales	466,606.6	471,057.9	468,608.6	468,004.0	468,608.6	2,449.2
2000	Materiales y suministros	155,330.3	167,060.9	78,308.2	96,379.7	78,308.2	88,752.8
3000	Servicios generales	7,122,055.9	6,299,456.9	5,336,179.1	5,123,402.3	5,336,179.1	963,277.9
4000	Transferencias, asignaciones, subsidios y otras ayudas	17,350.8	17,850.9	17,370.8	17,370.8	17,370.8	480.0
6000	Inversión pública	0.0	162,321.4	94,932.4	96,418.0	94,932.4	67,389.0
	TOTAL	**7,761,343.6**	**7,117,748.0**	**5,995,399.1**	**5,801,574.8**	**5,995,399.1**	**1,122,348.9**

Fuente: Elaborado con base en la información definitiva proporcionada por AICM.
Nota: Diferencias por redondeo

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC), por 89,158.7 miles de pesos, se integran de la manera siguiente:

Recursos ejercidos en materia de TIC en 2017
(Miles de pesos)

Capítulo/ P. Presupuestaria		Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**12,836.9**
2000		**MATERIALES Y SUMINISTROS**	**11,258.0**
3000		**SERVICIOS GENERALES**	**65,063.8**
	31603	Servicios de internet	276.5
	31701	Servicios de conducción de señales analógicas y digitales	35.6
	31901	Servicios integrales de telecomunicación	28,510.3
	32301	Arrendamiento de equipo y bienes informáticos	8,261.8
	32701	Patentes, derechos de autor, regalías y otros	6,285.2
	33301	Servicios de desarrollo de aplicaciones informáticas	17,528.2
	33903	Servicios integrales	202.4
	35301	Mantenimiento y conservación de bienes informáticos	3,963.8
		TOTAL	**89,158.7**

Fuente: Elaborado con información definitiva proporcionada por AICM.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC, con una percepción anual de 12,836.9 miles de pesos durante el ejercicio fiscal 2017, considerando 38 plazas del AICM, el promedio anual por plaza fue de 337.8 miles de pesos.

Del total ejercido en 2017 por 89,158.7 miles de pesos de recursos federales asignados en materia de TIC, se erogaron 42,272.8 miles de pesos en dos contratos que representan el 47.4% del total del universo, los cuales se integran de la manera siguiente:

Muestra de los Contratos de Prestación de Servicios Ejercidos en 2017
(Miles de Pesos)

ID	Proceso Contratación	Contrato	Proveedor	Descripción	Vigencia Del	Vigencia Al	Monto	Pagado 2017
1	Adjudicación directa por Art. 41 fracción IV de la LAASSP	073-O15-AICM-3S	Latin ID, S.A. de C.V.	Prestación del servicio integral de tecnologías de la información para el nuevo edificio administrado por el estado mayor presidencial en AICM.	01/12/2015	30/11/2018	98,322.5	32,774.1
						SUBTOTAL	**98,322.5**	**32,774.1**
2	Licitación pública nacional núm. LA-009KDN001-N18-2011	021-O11-AICM-SRP-1S	Mancera, S.C., STO Systems, S.A. de C.V. y Servicios, Tecnología y Organización, S.A. de C.V.	Prestación del servicio para mejorar los procesos administrativos, financieros y comerciales de AICM, la implementación del eBusiness Suite Oracle R12 y su soporte y mantenimiento por 5 años.	01/06/2011	31/05/2017	87,841.6	9,498.7
		Convenio modificatorio No. 021-A11-AICM-SRP-1S		Modificación en los servicios para atender los requerimientos adicionales que durante el año 2012 ha estado emitiendo el Consejo Nacional de Armonización Contable, acortar los tiempos en la generación de los cierres contables-presupuestales mensuales de 2012, y atender en tiempo y forma las especificaciones propias de la entidad.	31/08/2012	31/05/2017	8,410.0	
		Convenio modificatorio No. 021-B11-AICM-SRP-1S		Servicio de aplicación para la contabilidad en medios electrónicos de acuerdo a la segunda resolución de modificaciones a la Resolución Miscelánea Fiscal para el 2014, publicadas en el Diario Oficial de la Federación el viernes 4 de julio de 2014, así como los ajustes al plan de cuentas contables de la aplicación eBusiness Suite de Oracle R12, de acuerdo a los lineamientos requeridos por el Consejo Nacional de Armonización Contable.	22/10/2014	31/05/2017	1,721.4	
		Convenio modificatorio No. 021-C11-AICM-SRP-1S		Servicio de capacitación para el personal del AICM que opera el eBusiness Suite Oracle R12 del AICM, que es el sistema en el cual se manejan todos los procesos financieros, administrativos y comerciales en AICM.	25/11/2016	31/05/2017	1,751.8	
		Convenio modificatorio No. 021-D11-AICM-SRP-1S		Servicio para dar continuidad a la operación de soporte y mantenimiento al sistema eBusiness Suite Oracle R12 que opera actualmente en AICM, por siete meses a partir del 1 de junio de 2017 y hasta el 31 de diciembre de 2017.	14/03/2017	31/12/2017	5,544.8	
						SUBTOTAL	**105,269.6**	**9,498.7**
						TOTAL	**203,592.1**	**42,272.8**

Fuente: Contratos, facturas y soporte documental proporcionados por AICM.
Nota: Diferencias por redondeo.

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

2. Contrato 073-O15-AICM-3S, "Servicio Integral de Tecnologías de la Información, para el nuevo edificio Administrado por el Estado Mayor Presidencial en el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V."

Con el análisis del contrato número 073-O15-AICM-3S celebrado con la empresa Latin ID, S.A. de C.V. mediante el procedimiento de adjudicación directa por excepción a la licitación pública, con fundamento en el artículo 41, fracción IV, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); con objeto de prestar el "servicio integral de tecnologías de la información para el nuevo edificio administrado por el Estado Mayor Presidencial (EMP) en AICM", vigente del 1 de diciembre de 2015 al 30 de noviembre de 2018; por un monto de 98,322.5 miles de pesos, se identificó lo siguiente:

El alcance de los trabajos se integró por los servicios siguientes:

1. Instalación y configuración de equipos de procesamiento; equipos de telecomunicaciones centrales, de distribución y puntos de acceso; seguridad perimetral y correlacionador de eventos; enlaces de internet y cableado estructurado

para el nuevo edificio administrado por el Estado Mayor Presidencial (EMP) para la operación del avión presidencial.

2. Reemplazo de equipo, partes y/o refracciones relacionadas con la infraestructura proporcionada para la prestación del servicio.

3. Servicios de mantenimiento correctivo y pólizas de soporte.

Proceso de contratación

Se proporcionó el dictamen con la justificación para llevar a cabo la contratación por excepción a la licitación pública, bajo el amparo del artículo 41, fracción IV, de la LAASSP, en el cual se explican los motivos en los que se sustenta el procedimiento de contratación realizado.

Pagos

Se realizaron pagos por los servicios prestados durante el año 2017 por un monto de 32,774.1 miles de pesos.

Cumplimiento técnico y funcional

- **Recursos del proveedor**
  De la estructura organizacional asignada al proyecto, no fue posible identificar las actividades ejecutadas por 5 de los 6 integrantes que conformaron la plantilla del proveedor para la prestación de los servicios. Sin embargo, se detectaron diferencias entre la cantidad de personas referidas en la estructura organizacional y los curriculums vitae (CV) proporcionados por el proveedor, debido a que se identificaron 16 CV, de los cuales 12 no contienen información referente a la experiencia relacionada con el proyecto contratado.

  Se carece de la documentación que acredite la validación que llevó a cabo el AICM y/o el EMP, del personal que desarrolló las actividades de diseño, implementación, configuración y puesta a punto de cada uno de los componentes de la solución, a fin de acreditar que éstos contaran con las capacidades técnicas y certificaciones requeridas, en incumplimiento de lo establecido en la sección “Requisitos para los Licitantes” del Anexo Técnico 1 del contrato.
- **Plan de trabajo**
  Se carece del Plan de trabajo detallado que refleje el desarrollo real del proyecto e incluya las desviaciones, hitos y demás actividades que hayan garantizado que el mismo fue ejecutado en los plazos establecidos.

- **Procedimientos e instructivos**
  Se identificó que los procedimientos de soporte técnico en sitio y remoto, así como para los casos de escalamiento con el fabricante, no especifican las herramientas de apoyo a utilizar para el registro, atención y seguimiento de incidentes; el Plan de contingencia carece de un análisis detallado del proyecto, de tiempos mínimos para el establecimiento de operaciones, de actores involucrados, así como la interacción de los equipos de trabajo encargados de dicho proceso.

- **Acuerdos del Nivel de Operación (OLA´s)**
  Se carece de la definición de Acuerdos de operación de servicio (OLA's) entre el proveedor y el AICM/EMP, en los que se definieran las relaciones técnicas internas específicas que den soporte a los acuerdos de niveles de servicio (SLA's) pactados; en incumplimiento a lo establecido en el Anexo Técnico 1 del contrato.

- **Gestión de incidentes**
  No se cuenta con herramientas para el registro, atención y seguimiento de incidentes, así como el establecimiento y operación de la mesa de servicios del proveedor; en incumplimiento a lo establecido en el apartado "Plan de Aseguramiento de la Calidad" del Anexo Técnico 1.

- **Conectividad a Internet**
  Se carece de la documentación que acredite que el servicio de conectividad a internet cumplió con las características solicitadas de pérdida de información que se transmite a través de la red (paquetes) y las demoras (latencia) máximas. Asimismo, no se cuenta con documentación que acredite que el proveedor llevó a cabo el monitoreo del comportamiento del tráfico de entrada y salida diario y su acumulado correspondiente según lo solicitado en el Anexo Técnico 1.

- **Seguridad del enlace**
  En la verificación en sitio se identificó que el proceso de análisis, control y limpieza de tráfico inusual en la red es ejecutado por el proveedor del enlace de internet; sin embargo, se carece del soporte que acredite que el proveedor proporcionó el servicio para proteger la red contra amenazas de seguridad externas e internas, al tiempo que se mantiene la continuidad del servicio, conforme a lo estipulado en el apartado "Seguridad del enlace" del Anexo Técnico 1.

- **Memorias Técnicas**
  Se verificó en sitio por medio de la consola de administración de infraestructura la licencia asignada al correlacionador de eventos; no obstante, se identificaron diferencias entre dicha licencia y lo plasmado en la memoria técnica, debido a que en el documento se hizo referencia a otro cliente; por lo anterior, el personal del EMP indicó que solicitaría la actualización del documento a fin de contar con información precisa y confiable.

- **Configuración de los equipos de telecomunicaciones.**
  En la verificación en sitio se identificó que no se llevó a cabo la optimización de las configuraciones de red por parte del prestador de servicios, debido a que éstas fueron realizadas por un tercero y por el personal de TIC del EMP, en los equipos de telecomunicaciones.

- **Bitácoras**
  Durante la verificación en sitio, se solicitó visualizar en pantalla la información correspondiente a las bitácoras generadas por el avión presidencial los días 23 de julio de 2018 y 4 de octubre de 2018, fechas en las cuales se reportaron fallas mecánicas; sin embargo, el personal de la Unidad de TIC del EMP indicó que los registros son analizados directamente por los mecánicos del EMP, quienes se encargan de hacer los cambios correspondientes. Con respecto a las alertas detectadas el 4 de octubre de 2018, a la fecha de la visita (23 de octubre de 2018) no habían sido descargadas.

  Por lo anterior, no fue posible identificar si las fallas reportadas fueron solucionadas en tiempo y forma, a fin de mitigar los riesgos en el funcionamiento del avión presidencial.

Se concluye que existieron deficiencias en la gestión del proyecto, en razón de que no fue posible identificar elementos que comprueben que el AICM y el EMP validaron que los recursos del proveedor contaran con las capacidades técnicas y certificaciones que demostraran su experiencia en proyectos similares; no se cuenta con los elementos para garantizar que el proyecto se desarrolló en tiempo y forma; no se tienen definidos los Acuerdos de operación de servicio (OLA's); no se cuenta con evidencia de que el servicio de conectividad a internet cumplió con las características solicitadas; así como con lo estipulado en el Anexo Técnico 1 del contrato referente a la administración y ejecución de las actividades requeridas por el Aeropuerto y el Estado Mayor Presidencial; y lo establecido en el III.B. Proceso de Administración de Proveedores (APRO), actividades APRO 1 y APRO 2 del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014 y sus reformas al 4 de febrero de 2016.

2017-2-09KDN-15-0395-01-001 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., en futuras contrataciones verifique los perfiles, experiencia y certificaciones de los recursos que el proveedor designe para la prestación del servicio contratado y defina planes de trabajo que permitan identificar la operación real e incluya las desviaciones, hitos y demás actividades que garanticen que el proyecto se desarrollará en tiempo y forma.

3. Contrato 021-O11-AICM-SRP-1S, "Servicio para mejorar los procesos administrativos, financieros y comerciales de AICM, la implementación del eBusiness Suite Oracle R12 y su soporte y mantenimiento por 5 años".

Se analizó el contrato número 021-O11-AICM-SRP-1S celebrado en propuesta conjunta por las empresas Mancera, S.C., STO Systems, S.A. de C.V. y Servicios, Tecnología y Organización, S.A. de C.V. mediante el procedimiento de licitación pública nacional núm. LA-009KDN001-N18-2011, con objeto de prestar el "Servicio para mejorar los procesos administrativos, financieros y comerciales de AICM, la implementación del EBusiness Suite Oracle R12 y su soporte y mantenimiento por 5 años", vigente del 1 de junio de 2011 al 31 de mayo de 2017; por un monto de 105,269.6 miles de pesos; con fecha 31 de agosto de 2012 se celebró el

primer convenio modificatorio núm. 021-A11-AICM-SRP-1S, con la finalidad de modificar los servicios para atender los requerimientos adicionales emitidos por el Consejo Nacional de Armonización Contable (CONAC) el año 2012; con fecha 22 de octubre de 2014 se celebró el segundo convenio modificatorio núm. 021-B11-AICM-SRP-1S, con la finalidad de incluir el servicio de aplicación para la contabilidad en medios electrónicos de acuerdo con la segunda resolución de modificaciones a la Resolución Miscelánea Fiscal para el 2014, publicadas en el Diario Oficial de la Federación el viernes 4 de julio de 2014, de acuerdo con los lineamientos requeridos por el CONAC; con fecha 25 de noviembre de 2016 se celebró el tercer convenio modificatorio núm. 021-C11-AICM-SRP-1S, con la finalidad de incluir el servicio de capacitación para el personal del AICM que opera el sistema de administración financiera, que maneja los procesos financieros, administrativos y comerciales en AICM; con fecha 14 de marzo de 2017 se celebró el cuarto convenio modificatorio núm. 021-D11-AICM-SRP-1S, con la finalidad de incluir servicio de continuidad operativa al sistema por siete meses a partir del 1 de Junio de 2017 y hasta el 31 de diciembre de 2017; se identificó lo siguiente:

El alcance de los trabajos se integró por:

1. Fase 1: definición de la solución, que contempló el análisis, diagnóstico de la situación actual y discusión de dicho diagnóstico.

2. Fase 2: construcción, implantación, entrega y puesta en operación del sistema de administración financiera.

3. Fase 3: operación, mantenimiento y soporte de la solución implementada.

Proceso de contratación

La convocatoria de Licitación Pública Nacional Electrónica número LA-009KDN001-N18-2011 fue publicada en el Sistema Compranet el 14 de abril de 2011, mientras que las juntas de aclaraciones se llevaron a cabo del 26 de abril de 2011, donde participaron diversos prestadores de servicios; sin embargo, el 2 de mayo de 2011 en la junta de presentación y apertura de proposiciones, únicamente se presentó la propuesta conjunta de las empresas Mancera, S.C., STO Systems, S.A. de C.V. y Servicios, Tecnología y Organización, S.A. de C.V. Antes de la convocatoria de la licitación número LA-009KDN001-N18-2011, existió una licitación de número LA-009KDN001-N1-2011 con el mismo objeto, la cual fue declarada desierta el 2 de febrero de 2011.

El Acto de Fallo se llevó a cabo el 6 de mayo de 2011, el cual fue presidido por el Subgerente de Adquisiciones, mediante el cual declara que la adjudicación a las empresas Mancera, S.C., STO Systems, S.A. de C.V. y Servicios, Tecnología y Organización, S.A. de C.V. se efectuó con base en el resultado de la evaluación integral realizada por la Gerencia de Desarrollo e Informática.

En la revisión al proceso de investigación de mercado, se identificó que:

- El Aeropuerto no especificó la moneda en la que las cotizaciones debían enviarse, por lo que una se presenta en dólares, mientras que las demás son presentadas en pesos, en incumplimiento al artículo 30 del Reglamento de la Ley de Adquisiciones,

Arrendamientos y Servicios del Sector Público. Durante el desarrollo de los trabajos de auditoría, el AICM presentó los formatos utilizados para la petición de cotizaciones en donde se especifica el tipo de moneda en la que se cotizará.

- El AICM no elaboró el Resultado de la Investigación de Mercado, sólo se cuenta con la documentación relativa a las cotizaciones, excepto el análisis realizado a partir de las mismas, en contravención del artículo 30 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como a lo dispuesto en las Políticas Bases y Lineamientos en Materia de Adquisiciones Arrendamientos y Servicios de AICM, S.A. de C.V. y SACM, S.A. de C.V. numeral 6.1.5 "de la investigación de mercado".

Pagos

Se reportaron pagos realizados durante el año 2017 por un monto de 9,498.7 miles de pesos, correspondientes a los servicios adquiridos mediante el tercer y cuarto convenio modificatorio.

Cumplimiento técnico y funcional

- **Migración y Calidad de datos**
  Se verificó que el Aeropuerto definió una estrategia para la migración de datos; sin embargo, se carece de la documentación que acredite los mecanismos mediante los cuales implementó la metodología, definición, limpieza y gestión de datos, la construcción de las interfaces que permitirán comunicar los módulos que sean migrados o creados y el resultado de su migración.

  El AICM no proporcionó la documentación y esquemas de la arquitectura de aplicaciones que permitió evaluar la interrelación del sistema con otros que no forman parte del alcance del proyecto (Sistema ASA y Meta 4), pero que son proveedores y receptores de la información generada por el sistema.

- **Pruebas**
  Se carece de la documentación que acredite el resultado de la ejecución de las pruebas integrales, funcionales y de aceptación, así como de las acciones correctivas implementadas. No se cuenta con la evidencia que refleje la planeación, ejecución y el resultado de los escenarios de las pruebas de seguridad, de volumen, de integración de los módulos y del comportamiento del sistema para ninguno de los módulos del sistema de administración financiera.

- **Administración de la Calidad**
  Se carece de la documentación relacionada con las revisiones de calidad y nivel de satisfacción del AICM ejecutadas por el proveedor, para cada fase del proyecto, así como la planeación y documentación de los estándares de calidad de la solución.

- **Administración de riesgos**
  Se identificó que los documentos relacionados con las bitácoras de riesgos se encuentran incompletos en varios campos, incluidos los siguientes: dueño del riesgo,

detalle del riesgo y efecto. De igual forma, carecen de un seguimiento hasta su atención y formalización correspondiente.

- **Gestión de usuarios.**
  La Gerencia de Desarrollo e Informática realiza actividades relacionadas con la gestión de usuarios; se carece de un procedimiento formalizado para llevar a cabo dicha administración, por lo que existe el riesgo de que, en caso de ausencia del personal encargado de ésta tarea, podrían verse afectadas las actividades que permitan la continuidad y gestión de las operaciones.

- **Respaldos y restauraciones**
  Se identificó que la política de respaldos carece de los términos bajo los cuáles serán probados, sus periodos de conservación y rotación de cintas, así como los procedimientos que se emplearían para la destrucción o eliminación de la información almacenada en los medios físicos.

  Se carece de la documentación relacionada con la validación y registro de los procedimientos de restauraciones llevados a cabo en 2017.

  La bitácora de respaldos carece de información que permita identificar que éstos se realizaron con la periodicidad solicitada y que fueron o no exitosos, a fin de validar si presentaron o no fallas que pudieran repercutir en la integridad de la información.

- **Administración de la Seguridad**
  Se carece de una matriz de segregación de funciones a nivel transaccional en el sistema de administración financiera, la cual debe definirse en conjunto con las áreas de negocio.

  No se identificó la documentación del tercero contratado por el AICM para auditar la seguridad del sistema de administración financiera y su apego a las políticas, procedimientos y estándares de seguridad definidos por AICM; la seguridad de los datos durante la transmisión a las instalaciones de AICM, así como las capacidades y herramientas utilizadas para la protección de la infraestructura tecnológica, incluyendo la documentación de cambios a las configuraciones de dicha infraestructura.

- **Pruebas realizadas al Sistema en operación.**

  Se verificó en sitio las funcionalidades requeridas para el macro procesos de Finanzas, submódulos Contabilidad General, Control Presupuestal General, Tesorería, Control de Ingresos; y para el macro proceso Comercial, submódulos Control de Facturación y Cobranza de Servicios Aeroportuarios, comerciales y complementarios (Cuentas por Cobrar); así como a las interfaces del actual Sistema Aeroportuario (ASA) y para el Sistema de nómina (Meta 4); se identificó lo siguiente:

- El sistema no maneja información estadística, gráfica o comparativa; sin embargo, la funcionalidad fue requerida.
- No fue posible validar la implementación de la interfaz con el Sistema Aeroportuario (SITA), debido a que SITA nunca se desarrolló, solo fue un proyecto y en su lugar se encuentra el sistema ASA.
- No fue posible generar el reporte de presupuesto maestro/detalle, debido a que el usuario no identificó a que reporte pertenece, por lo que no se pudo verificar que dicha funcionalidad haya sido implantada.
- No se validó el proceso de carga de datos del sistema "Meta 4" al sistema de administración financiera por medio de la interfaz creada para tal fin; debido a que durante la prueba no funcionó el acceso a la consulta de la información y el sistema generó cuadros de diálogo con pantallas de error de ejecución de instrucciones.

Los usuarios indicaron que la Subdirección de Sistemas actualizó recientemente la versión del sistema Oracle, lo que generó contratiempos en la operación del sistema. Adicionalmente, se encuentran migrando sus equipos de cómputo, situación que ha disminuido el desempeño del sistema de administración financiera, ya que las versiones que manejan los nuevos equipos tienen problemas de compatibilidad con las versiones bajo las cuales se implementó. Este hecho ha impactado las tareas de los usuarios, mayormente a los que utilizan el sistema Meta 4, donde a la fecha de la visita (noviembre 2018), los usuarios tenían problemas para ingresar al sistema.

Se concluye que existieron deficiencias relacionadas con la administración del contrato, en razón de que se identificaron carencias relacionadas con la migración de datos, la planeación y ejecución de pruebas, administración de calidad y riesgos, la gestión de usuarios en el sistema implantado, ejecución de respaldos y restauraciones, administración de la seguridad del sistema y actualizaciones a los equipos de cómputo mismos que pudiesen repercutir en la operación integral y eficiente de los principales procesos administrativos, financieros y comerciales del AICM que dan cumplimiento a lo establecido en la Ley General de Contabilidad Gubernamental y las disposiciones de la CONAC aplicables al AICM; así como a lo estipulado en el Contrato número 021-O11-AICM-SRP-1S, numerales IV.3.4; IV.3.5; Secciones "Administración de Calidad", "Administración de Riesgos", "Administración de la operación, respaldos y recuperación", "Seguridad" y "Administración de la seguridad" del Anexo Técnico T1.

Asimismo, se identificó que la mayoría de las actividades ejecutadas por la Gerencia de Desarrollo e Informática relacionadas con la administración y operación del sistema de administración financiera no se encuentran formalizadas, por lo que, en caso de existir rotación del personal de la Gerencia, no existirían los lineamientos para continuar con las tareas de atención y soporte llevadas a cabo.

2017-2-09KDN-15-0395-01-002 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., defina una matriz de perfiles con el objetivo de incluir por puesto las transacciones que debe tener el usuario para desempeñar su función en el sistema de administración financiera, con el objetivo de

identificar posibles conflictos de segregación de funciones y brindar un seguimiento adecuado. Asimismo, defina y formalice las actividades ejecutadas por la Gerencia de Desarrollo e Informática relacionadas con la gestión y operación del sistema de administración financiera.

2017-2-09KDN-15-0395-01-003 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., lleve a cabo las acciones pertinentes, a fin de adoptar una metodología para el desarrollo de soluciones tecnológicas, que contemple la ejecución y documentación de pruebas unitarias, integrales, funcionales, de aceptación, entre otras; así como las acciones correctivas implementadas en el aeropuerto, que garanticen la operación de sus sistemas.

4. Gobierno y Administración de Tecnologías de la Información y Comunicaciones (TIC)

Para evaluar los procesos de gobernabilidad y administración de TIC, se analizó la información relacionada con el cumplimiento del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), con lo cual se obtuvo lo siguiente:

- Se identificó en el documento "Informe de la Implementación del MAAGTICSI 2017", de febrero de 2018, un porcentaje de implementación del 93%; sin embargo, se carece de la documentación que acredite dicho avance. El informe de implementación presentado no cuenta con fechas de elaboración y autorización, así como del personal que participó en la revisión y análisis de los procesos y subprocesos del MAAGTICSI.

Porcentaje de avance de implementación del MAAGTICSI en 2017

Procesos / Subprocesos MAAGTICSI	Porcentaje de avance
GOBERNANZA	
I.A. Planeación estratégica (PE)	85%
I.B. Administración del Presupuesto y las Contrataciones (APCT)	92%
ORGANIZACIÓN	
II.A. Administración de servicios (ADS).	96%
II.B. Administración de la configuración (ACNF)	91%
II.C. Administración de la seguridad de la información (ASI)	97%
ENTREGA	
III.A. Administración de proyectos (ADP)	85%
III.B. Administración de proveedores (APRO)	96%
III.C. Administración de la operación (AOP).	95%
III.D. Operación de los controles de seguridad de la información y del ERISC (OPEC).	96%
Avance total	**93%**

Fuente: Información proporcionada por AICM.

A la fecha de la auditoría (enero 2019) el aeropuerto reportó en la herramienta "Gestión de Política TIC" la implementación del 100% del Manual; no obstante, no se cuenta con la documentación que garantice lo anterior.

Adicionalmente, no se presentó documentación que permita acreditar que el Órgano Interno de Control en el AICM verificó el cumplimiento de lo dispuesto en el *Acuerdo que tiene por objeto emitir las políticas y disposiciones de Gobierno Digital, en materia de tecnologías de la información y comunicaciones, así como establecer el manual administrativo de aplicación general en dichas materias y el MAAGTICSI*, conforme a lo estipulado en su artículo 32.

- Se identificó que la siguiente documentación no se encuentra formalizada: Matriz de Asignación de Responsabilidades (RACI) para Contratación de Bienes y Servicios Informáticos, Integración y Operación del Grupo de Trabajo para la Dirección de TIC, Documento Estratégico de TIC, Portafolio de Iniciativas y Proyectos 2017, Directriz de administración de riesgos, Documento de Resultados del Análisis de Riesgos ASI F3 Servidores, así como las matrices de perfiles de puestos y segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; por lo que no fue posible validar que dichos documentos reflejaran la operación actual del AICM, así como al personal que participó en su elaboración.

- No se cuenta con un procedimiento para determinar la priorización de las iniciativas y proyectos de TIC, en incumplimiento del proceso I.A de Planeación Estratégica, actividad "PE 1 Establecer la gobernabilidad de las operaciones de la UTIC" del MAAGTICSI.

- Se carece de evidencia relacionada con la coordinación del Grupo de Trabajo para la Dirección de TIC y el responsable de la Seguridad de la Información para armonizar el gobierno de TIC, la administración de riesgos y el Sistema de Gestión de Seguridad de la Información (SGSI) del AICM, en contravención de lo definido en el proceso I.A de Planeación Estratégica, actividad "PE 1 Establecer la gobernabilidad de las operaciones de la UTIC", del MAAGTICSI.

- No se establecieron escenarios para el adecuado ejercicio del presupuesto destinado a las TIC, donde se indiquen los gastos indispensables para garantizar la continuidad de la operación contra los riesgos operativos y los correspondientes a las iniciativas comprometidas; en incumplimiento del proceso II.A de Administración del Presupuesto y las Contrataciones, Planeación Estratégica, actividad "APCT 1 Participar en el establecimiento de prioridades del presupuesto de TIC" del MAAGTICSI.

- No se cuenta con un análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de las actividades relacionadas a TIC del Aeropuerto.

- Se carece del procedimiento y documentación relacionada con los procesos para identificar, registrar y administrar las acciones correctivas en caso de desviación en el avance real del Plan Estratégico de TIC (PETIC), a fin de verificar el cumplimiento de sus indicadores.

- El aeropuerto no tiene definido un mecanismo para evaluar los programas de iniciativas de proyectos de TIC, conforme a lo definido en el proceso III.A de Administración de Proyectos, actividad "ADP 6 Cerrar iniciativas y proyectos de TIC" del MAAGTICISI.

- En 2017 no se estableció una metodología para la administración de proyectos; no obstante, como resultado de los trabajos de auditoría, el Encargado de la Subdirección de Sistemas realizó la definición y difusión, el 18 de enero de 2019, de los formatos siguientes:

    1. Acta de proyecto o nacimiento
    2. Plan de comunicaciones
    3. Plan de Pruebas
        - Casos de Prueba
        - Pruebas de Software
        - Informe de ejecución de pruebas de software
        - Solicitud de cambios
    4. Plan de Gestión
    5. Minuta

    Los formatos serán implementados por el personal de la subdirección en futuras contrataciones para la gestión de los proyectos, a fin de contar con mecanismos de control y supervisión para verificar el cumplimiento de las obligaciones contractuales.

Por lo anterior, se reflejan deficiencias en los controles existentes para formalizar los documentos en materia de gobernabilidad y administración de TIC, la definición de un análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de las actividades relacionadas a TIC, la implementación del MAAGTICSI y su validación. Se concluye que el AICM no vigiló el cumplimiento de las disposiciones normativas en materia de Tecnologías de Información y Comunicaciones, en contravención del Artículo 32 del *Acuerdo que tiene por objeto emitir las políticas y disposiciones de Gobierno Digital, en materia de tecnologías de la información y comunicaciones, así como establecer el manual administrativo de aplicación general en dichas materias*; así como de lo estipulado en los procesos: I.A de Planeación Estratégica, actividad PE 1; II.A Administración del Presupuesto y las Contrataciones Planeación Estratégica, actividad APCT 1; III.A Administración de Proyectos, actividades ADP 1 y ADP 6; del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI), publicado el 4 de febrero de 2016, en el Diario Oficial de la Federación (DOF).

2017-0-27100-15-0395-01-001 **Recomendación**

Para que la Secretaría de la Función Pública instruya al Órgano Interno de Control en el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., a llevar a cabo las acciones pertinentes para verificar y documentar el cumplimiento en el aeropuerto de lo dispuesto en el Acuerdo que tiene por objeto emitir las políticas y disposiciones de Gobierno Digital, en materia de tecnologías de la información y comunicaciones, así como establecer el manual administrativo de aplicación general en dichas materias y el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, conforme a lo estipulado en su artículo 32.

2017-2-09KDN-15-0395-01-004 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., lleve a cabo la definición y formalización de los procedimientos, políticas o lineamientos en materia de gobernabilidad y administración de TIC; defina un análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de las actividades relacionadas a TIC que sean acordes a la operación del Aeropuerto; identifique a los responsables de cada proceso crítico, usuarios y actores que intervienen en la ejecución de éstos, a fin de garantizar que al momento de presentarse una contingencia se pueda notificar al personal correspondiente y así garantizar la continuidad de la operación del AICM.

5. Gestión de la Seguridad de la Información y Continuidad de TIC.

En la revisión y análisis de la información, relacionada con la Administración de la Seguridad de la información (ASI) y Operación de Controles de Seguridad de la información y del ERISC (OPEC) definidos en el Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones de la Seguridad de Información (MAAGTICSI), se observó lo siguiente:

- Se identificó que la última designación del Responsable de la Seguridad de la Información Institucional (RSII) notificada al Centro de Investigación y Seguridad Nacional (CISEN) fue el 4 de junio de 2014. Al cierre de la auditoría (enero 2019) se carece de la actualización del RSII, debido a que éste causo baja del aeropuerto el 08 de marzo de 2018; así como de los enlaces responsables de mantener comunicación con los equipos de respuesta a incidentes de seguridad en TIC, para efectos de su registro en el CISEN.
- No se cuenta con la definición de los activos de información que soportan la generación, procesamiento, trasmisión y almacenamiento de la información, así como de los procesos críticos del Aeropuerto.

- No se identificó el establecimiento del Equipo de Respuesta a Incidentes de Seguridad en TIC (ERISC), así como los mecanismos de coordinación del ERISC al interior de la Institución o con otros ERISC u organizaciones externas, a fin de estar en concordancia con la directriz rectora de respuesta a incidentes.

- Se carece del establecimiento del Equipo de trabajo de Infraestructuras de Información Esenciales y/o Críticas (ETIIEC) y de la definición del catálogo de infraestructuras críticas. Asimismo, no se identificó la existencia de mecanismos para

garantizar la protección de las infraestructuras críticas bajo la administración de terceros.

- El análisis de riesgos presentado carece de la fecha de elaboración y demás elementos que complementen su contenido, tales como los programas de mitigación de riesgos, el programa de contingencia, los responsables, el análisis del costo-beneficio y la frecuencia de análisis.

- Se identificó que la Directriz de Administración de Riesgos del AICM carece del análisis y definición de estrategias, metodologías y herramientas que administren los riesgos, su integración en el marco normativo que resulte aplicable, el establecimiento de reglas para medir la efectividad de los controles y la interacción de los grupos, equipos de trabajo, áreas y unidades administrativas del Aeropuerto y externos que darán atención y seguimiento sobre los riesgos a los que se encuentran expuestos los procesos.

- Se carece de la documentación relacionada con la Directriz Rectora de Respuesta a Incidentes que contenga la guía técnica de atención a incidentes de acuerdo a la criticidad de los activos de TIC afectados.
  Se identificó que el Sistema de Gestión de la Seguridad de la Información (SGSI) carece de un diseño coordinado con las diferentes áreas y unidades administrativas del Aeropuerto y su apego a alguna estrategia de seguridad de la información, estructura y alcances.

- El SGSI carece del diagnóstico de los requerimientos de seguridad de la información del Aeropuerto y en su alcance no se establecen los límites de protección desde la perspectiva institucional para proporcionar la seguridad requerida a los activos de información.

- No se identificaron estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos del Aeropuerto, reglas técnicas para los controles y las acciones, métricas para evaluar el grado de cumplimiento, el programa de implementación del SGSI y el informe de resultados de implementación del mismo.

- Adicionalmente, no se cuenta con la documentación mediante la cual se notificó al Titular del Aeropuerto el documento de definición del SGSI, que incluya el programa de implantación desarrollado y los incumplimientos al SGSI reportados al Órgano Interno de Control.

- Se carece de un programa de capacitación de personal en temas relacionados con la Seguridad de la Información.

- Se identificó que el Aeropuerto carece de las siguientes políticas o procedimientos institucionales:

- Control para el ingreso y salida de activos de información.
- Control para el borrado seguro de dispositivos de almacenamiento.
- Para el intercambio seguro de la información.
- Clasificación de la información.
- Contraseñas.
- Respaldo y restauración de la información.
- Configuración de las herramientas de protección en las redes Institucionales y en los servidores.
- Administración de usuarios.
- Conexiones a redes públicas.
- Dispositivo móvil.
- Eliminación o modificación de los privilegios de acceso a información.
- Registro de auditorías o bitácoras de seguridad.

Asimismo, las siguientes políticas y procedimientos no se encuentran formalizados y carecen de fechas de elaboración y aprobación que permitan acreditar que se encuentran apegadas a la operación actual del AICM:

- Para evitar el daño, pérdida, robo, copia y acceso no autorizados a los activos de información.
- Uso del servicio de Internet en la Institución y herramientas de filtrado de contenido.
- Uso de controles criptográficos.
- Control de accesos a los aplicativos sustantivos e infraestructura tecnológica.
- Validación periódica de usuarios (internos, externos y privilegiados) con acceso a sistemas críticos y servidores de producción.

- Se carece de una bitácora de las actividades ejecutadas sobre las bases de datos que permita monitorear los movimientos o extracciones no autorizados y se brinde un seguimiento oportuno de los mismos; asimismo, no se cuenta con un procedimiento definido para la revisión periódica de las bitácoras, se realiza por solicitud expresa del área interesada.

- No se ejecutó un análisis de vulnerabilidades y amenazas a los activos de información del AICM; así como pruebas de hackeo ético a su infraestructura de TIC.

- No se cuenta con la documentación referente al monitoreo periódico de los servidores físicos y virtuales del AICM, y la periodicidad con la que se ejecutan.

Por lo anterior, derivado de la revisión de los objetivos de la Seguridad de la Información y Operación de los controles de la Seguridad de la Información y del ERISC, se concluyó que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos del AICM son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y OPERACIÓN DEL ERISC	
Factor crítico	**Riesgo**
Responsable de la Seguridad de la Información Institucional (RSII)	La falta de designación del responsable de la seguridad de la información puede impactar en que el Aeropuerto carezca de una visión estratégica respecto a la implementación y adopción del modelo de gobierno de seguridad de la información en el AICM.
Procesos críticos y activos de información	La falta de la identificación de los procesos críticos y activos de información representa un riesgo de que la Institución no implante de manera adecuada los controles que aseguren la disponibilidad, confidencialidad e integridad de los activos de información crítica.
Análisis de vulnerabilidades y amenazas de los activos de información	La falta de un análisis de vulnerabilidades representa un riesgo de que el Aeropuerto no implemente controles preventivos y correctivos que permitan identificar y mitigar posibles amenazas que pudieran ocasionar una afectación a la confidencialidad, disponibilidad e integridad de la información de la entidad, las cuales en caso de materializarse, tendrían efectos negativos sobre la operación en uno o varios de los activos de información definidos por el AICM.
Sistema de Gestión de Seguridad de la Información (SGSI)	La carencia de implementación del SGSI puede ocasionar la pérdida de la confidencialidad de la información que puede ser conocida y utilizada por personas que no tienen autorización; falta de integridad ya que los datos que podrían ser alterados, provocando pérdidas económicas y fraudes; falta de disponibilidad que impide que los usuarios accedan a las aplicaciones cuando lo requieran y falta de “no repudio” de las transacciones para evitar que los usuarios pueden negar que realizaron alguna modificación a la información.
Equipos de Trabajo ERISC, ETAR y ETIEC	La carencia del establecimiento de los Equipos de trabajo mencionados, podría ocasionar que la visión para la identificación de infraestructuras esenciales y/o críticas, riesgos e incidentes, no cubran el alcance de seguridad que el Aeropuerto requiere, lo cual puede generar la exposición de los activos de TIC a riesgos innecesarios, impactando la disponibilidad, confidencialidad e integridad de la información del AICM.
Estrategia de la seguridad de la información	La carencia de una Estrategia de seguridad de la información en el Aeropuerto, es la base para el establecimiento del SGSI. Al no contar con estrategias específicas de seguridad de la información que permitan cumplir con la misión, visión y objetivos del Aeropuerto puede incurrir en riesgos a la integridad, confidencialidad y disponibilidad de la información.
Directriz Rectora de respuesta a incidentes	La Directriz establece las reglas de operación y los mecanismos de coordinación del ERISC, incluyendo los canales de comunicación que deberán ser seguros. De no contar con dicha Directriz, la entidad puede incurrir en fallas en los mecanismos de notificación, escalamiento y atención de incidentes, en su funcionamiento interno y de interacción con otras entidades.
Políticas y procedimientos institucionales	La carencia de políticas y procedimientos institucionales da pauta a confusiones y mal uso de los activos de TIC por parte de los usuarios finales y administradores de tecnologías, ya que al no contar con procedimientos oficializados, se desconoce cómo actuar ante situaciones de riesgo.

Monitoreo de las pistas de auditoría y las bitácoras de bases de datos	Al no revisar periódicamente las pistas de auditoría y las bitácoras de las bases de datos, se tiene el riesgo de no detectar oportunamente las transacciones irregulares o cambios no autorizados de los sistemas. En consecuencia, existe oportunidad para que los usuarios maliciosos puedan realizar acciones no autorizadas que comprometan la integridad, confidencialidad y disponibilidad de los activos, sin que sean detectados
Programa de capacitación institucional	Al no contar con un programa de capacitación que contenga temas relacionados con la difusión de los conceptos e importancia de la seguridad de la información, se pueden materializar riesgos ocasionados por usuarios que desconocen las mecánicas mediante las cuales puede ejecutarse acciones maliciosas cometidas mediante phishing, pharming y spam, por citar algunos.
Histórico y documentación del monitoreo de servidores.	El no contar con la documentación del monitoreo de los servidores, limita visualizar la evolución de las tecnologías en la entidad, que le permitan identificar las diversas tecnologías a fin de desarrollar estrategias para su evolución.

Fuente: Elaborado por la ASF con base en la información proporcionada por el AICM

Por todo lo anterior, se reflejan deficiencias en los controles existentes para la designación del responsable de la seguridad de la información institucional; identificación de infraestructuras esenciales y/o críticas; los procesos críticos y activos de información que soportan su generación; la integración y operación de los Equipos de Respuesta a Incidentes de Seguridad en TIC (ERISC), ETIIEC, ETAR; la Estrategia de la Seguridad de la Información Institucional; definición, implantación y mejora continua del SGSI a las necesidades del Aeropuerto; el establecimiento de la Directriz de Administración de Riesgos y ejecución de un análisis de vulnerabilidades y amenazas de los activos de información; el programa de capacitación institucional; políticas y procedimientos en materia de seguridad de la información; la revisión periódica de bitácoras; y la documentación del monitoreo de los servidores físicos y virtuales.

Se presume un incumplimiento de lo señalado en los artículos 21, 22, 23, 24, 25, 26 y 27 del ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias; procesos: II.C. Proceso de Administración de la Seguridad de la información (ASI), Actividades ASI 1, ASI 2, ASI 3, ASI 4, ASI 5, ASI 6; III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC), Actividad OPEC 1, y III.C. Proceso de Administración de la Operación (AOP), Actividad AOP 3, AOP 4; del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.

Centro de Datos

En la revisión de los Centros principal y alterno del AICM ubicados en las Terminales 1 y 2 del Aeropuerto, se identificó lo siguiente:

Centro de datos principal

- Se observó que 4 de 10 indicadores de presión de los extintores cuentan con un bajo nivel de presión, por lo que podría verse afectada la efectividad para el control de incendios en caso de un evento. No fue posible validar en la bitácora de mantenimiento de extintores que los equipos del centro de datos en las terminales T1 y T2 hayan sido contemplados dentro del mantenimiento efectuado durante 2017.

- El centro de datos opera con porcentajes de humedad del 52.3 al 58.7% y representan un riesgo para el funcionamiento de los equipos alojados en el mismo, debido a que lo recomendado por mejores prácticas internacionales es mantener el límite de humedad en los umbrales del 40.0% y 55.0% como máximo, a fin de minimizar el riesgo de que se presenten descargas electroestáticas y corrosión de los equipos del Centro de Datos.

- Los tanques de diésel de las plantas eléctricas de respaldo se encuentran ubicados justo debajo del centro de datos. Lo anterior representa un riesgo de seguridad, debido a que cualquier incidente relacionado con dicha planta, puede ocasionar problemas de operación y disponibilidad de los recursos de TIC alojados en dicha ubicación.

- Se verificó que el sitio destinado para el resguardo de cintas magnéticas, carece de mecanismos de control de acceso, la puerta no cuenta con llave para su ingreso; existe equipo de oficina almacenado, cajas de cartón, documentos y el gabinete donde residen las cintas no cuenta con cerradura. Por lo tanto, existe el riesgo de que pueda verse afectada la integridad de la información almacena, así como el daño o pérdida de la misma.

Centro de datos alterno

- Se identificó que cuenta con cableado estructurado y etiquetado en forma deficiente, humedad en el techo del centro de datos y existen en su interior materiales flamables (cajas de cartón y documentos).

- La clave de acceso es de uso general para los usuarios autorizados, por lo que no se tiene un listado específico que contenga el nombre, ID de empleado y/o referencia que permita identificar quiénes ingresan al sitio.

- No se cuenta con un sistema de video vigilancia para la entrada principal del centro y sus interiores, lo cual representa un riesgo en la operación de los sistemas alojados, debido a que no existe forma de verificar y dar seguimiento a las actividades que

realiza el personal que cuenta con acceso al centro de datos (limpieza, proveedores, AICM, entre otros).

- Ambos centros carecen de mecanismos de mitigación de daños en caso de inundación.

Se concluye que existen deficiencias en el centro de datos principal relacionadas con la disponibilidad de los mecanismos de control de incendios; la operación de los equipos dentro de los umbrales de humedad establecidos en las mejores prácticas internacionales; mecanismos de mitigación de daños contra inundación en ambos centros de datos y se carecen de controles de acceso para el sitio donde se resguardan las cintas. Para el centro de datos alterno se identificaron deficiencias relacionadas con sus controles de acceso, la calidad del cableado estructurado y etiquetado, y carencia de un sistema de video vigilancia. Lo anterior contraviene lo establecido en el artículo 13 y III.C. Proceso de Administración de la Operación (AOP), Actividad AOP 4, del Manual de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.

Continuidad de la Operación

- Se carece de un Análisis de impacto al negocio (BIA), en el que se identifiquen los procesos críticos del AICM, funciones, actividades, áreas o unidades administrativas, los servicios que podrían resultar afectados como consecuencia de la interrupción de uno o más de los servicios de TIC y su impacto en la operación del Aeropuerto.

- El Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación de Desastres (DRP) no contemplan la totalidad de los activos críticos del Aeropuerto y los servicios relacionados, únicamente consideran lo referente al sistema de administración financiera.

  El Plan presentado no establece las acciones a seguir para la programación, ejecución y seguimiento de tareas para la operación de todos los sistemas, aplicaciones y servicios críticos de TIC que deban habilitarse en caso de desastres; no se identificó que dicho documento contemple el sistema ASA, aplicativo crítico utilizado para controlar la operación, administración, facturación y cobro de los servicios aeroportuarios y complementarios proporcionados a las aerolíneas que operan en el AICM, el cual se encuentra obsoleto tecnológicamente y no puede ser actualizado debido a que no cuentan con su código fuente, por lo que existe el riesgo de que en caso de una falla podrían verse afectados algunos servicios que se brindan al Aeropuerto.

Por lo anterior, se reflejan deficiencias en el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación de Desastres (DRP), debido a que no contemplan la totalidad de los servicios y aplicativos críticos del aeropuerto; y se carece de un Análisis de Impacto al Negocio (BIA). Se concluye que el AICM no vigiló el cumplimiento de las disposiciones normativas en materia de tecnologías de información y comunicaciones, lo que contraviene los procesos: II.A. Proceso de Administración de Servicios (ADS), Actividades ADS 3 y ADS 4; así como a lo establecido en el apartado III.C. Proceso de Administración de la Operación (AOP), objetivos

específicos 1 y 2; del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.

De la revisión de los controles de planes de Continuidad de las Operaciones de TIC, los principales riesgos por la carencia o inconsistencia de éstos y sus consecuencias potenciales para las operaciones y activos del AICM son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE CONTINUIDAD DE LAS OPERACIONES	
Factor crítico	**Riesgo**
Definición del Análisis de Impacto al Negocio (BIA), Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)	Al carecer de la implementación de un Análisis de Impacto al Negocio (BIA) y los planes de continuidad y recuperación de desastres, no es posible verificar la efectividad de las acciones definidas para realizar la recuperación de todos los servicios y aplicativos críticos del AICM, los cuales podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC. Asimismo, no es posible validar si los puntos objetivos de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) de la información, serían mucho mayores a los requeridos para la continuidad de las operaciones.

Fuente: Elaborado por la ASF con base en la información proporcionada por el AICM.

2017-2-09KDN-15-0395-01-005 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., implemente las acciones pertinentes para realizar un análisis de vulnerabilidades a los activos de información del aeropuerto; así como evalúe la posibilidad de ejecutar una revisión de hackeo ético a toda la infraestructura crítica del mismo, a fin de identificar y remediar posibles amenazas que pudieran ocasionar una afectación a la confidencialidad, la disponibilidad e integridad de la información de la entidad.

2017-2-09KDN-15-0395-01-006 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., defina, autorice, implemente y divulgue al interior de la Subdirección de Sistemas las políticas y procedimientos correspondientes a la Seguridad de la Información, a fin de robustecer las actividades relacionadas con esta materia.

2017-2-09KDN-15-0395-01-007 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., defina e implemente un Plan de Continuidad de Negocio (BCP), Análisis de Impacto al Negocio (BIA) y el Plan de Recuperación en caso de Desastres (DRP), que contemple los servicios y aplicativos críticos del aeropuerto, a fin de garantizar la continuidad de la operación, o mínimo impacto de la infraestructura y servicios de TIC. Asimismo, para que evalúe la pertinencia de actualizar, mejorar o sustituir plataformas tecnológicas obsoletas, a fin de mitigar el riesgo de lentitud de procesamiento, vulnerabilidades de seguridad, falta de soporte y garantía por parte de fabricante, incremento en la probabilidad de fallas y pérdida de información.

2017-2-09KDN-15-0395-01-008 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., evalúe la implementación de mecanismos para la prevención, detección y corrección de daños por inundación en los Centros de Datos; verifique que los espacios asignados al equipamiento de telecomunicaciones y cintas sean de uso exclusivo; efectúe mantenimientos preventivos y correctivos a los mecanismos de control de incendios y de humedad correspondientes; y lleve a cabo el monitoreo de la capacidad de infraestructura alojada en los Centros de Datos.

2017-2-09KDN-15-0395-01-009 **Recomendación**

Para que el Aeropuerto Internacional de la Ciudad de México, S.A. de C.V., defina la Estrategia de Seguridad de la Información; realice un diagnóstico que permita definir, actualizar o modificar los controles y acciones establecidos en el Sistema de Gestión de la Seguridad de la Información (SGSI); defina métricas para evaluar el grado de cumplimiento del SGSI y realice las acciones correctivas correspondientes; determine el Plan de Capacitación de Seguridad de la Información; establezca el catálogo de infraestructuras críticas y mecanismos que garanticen la protección de las mismas; y realice el monitoreo periódico de las bitácoras de los aplicativos y bases de datos.

2017-9-09KDH-15-0395-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en el Grupo Aeroportuario de la Ciudad de México, S.A. de C.V., o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión no definieron los procesos críticos, activos de información y una estrategia de Seguridad de la Información del Aeropuerto, omitieron la evaluación del grado de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI), así como la definición de su programa de implementación, alineado con los objetivos y necesidades operativas del negocio, no definieron las estrategias, metodologías y herramientas para la gestión de riesgos ni los equipos de trabajo relacionados con la Seguridad de la Información, con la finalidad de dar seguimiento a la implementación de la estrategia de seguridad. Asimismo, no determinaron un Análisis de Impacto al Negocio (BIA) ni garantizaron que los Planes de Continuidad de Negocio (BCP) y de Recuperación de Desastres (DRP) contemplaran la totalidad de los activos críticos del Aeropuerto y los servicios relacionados.

Resumen de Observaciones y Acciones

Se determinaron 4 observaciones las cuales generaron: 10 Recomendaciones y 1 Promoción de Responsabilidad Administrativa Sancionatoria.

Dictamen

El presente se emite el 28 de enero de 2019, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, el Aeropuerto Internacional de la Ciudad de México S.A. de C.V. cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- Del contrato número 073-O15-AICM-3S para prestar el servicio Integral de Tecnologías de la Información para el Nuevo Edificio Administrado por el Estado Mayor Presidencial en el AICM, celebrado con la empresa Latin ID, S.A. de C.V. se determinó lo siguiente:
    - El proveedor proporcionó la infraestructura de cómputo y de conectividad de internet requeridos para la operación del avión Presidencial; no obstante, no fue posible validar que el prestador de servicios contara con las capacidades técnicas y certificaciones requeridas.
    - Se carece de los elementos para garantizar que el proyecto se desarrolló en tiempo y forma.
    - Una vez concluida la vigencia del contrato (30 de noviembre de 2018) el prestador de servicios retiró la infraestructura implementada para la operación del avión Presidencial.
- Del contrato 021-O11-AICM-SRP-1S, respecto al servicio para mejorar los procesos administrativos, financieros y comerciales de AICM y la implementación del sistema de administración financiera, celebrado de forma mancomunada por las empresas Mancera, S.C., STO Systems, S.A. de C.V. y Servicios, Tecnología y Organización, S.A. de C.V., se identificó lo siguiente:
    - Se carece de políticas, lineamientos y procedimientos definidos para la gestión de usuarios, administración de riesgos y respaldos; así como para la planeación y ejecución de pruebas del sistema. No se cuenta con matriz de segregación de funciones de las transacciones utilizadas por los roles del sistema de administración financiera.
- Se carece de la formalización de los documentos en materia de gobernabilidad y administración de Tecnologías de la Información y Comunicaciones (TIC), determinación del análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) de las actividades de TIC, definición de los procesos críticos del Aeropuerto, acreditación del porcentaje de implementación del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI), no se cuenta con estrategias, metodologías y herramientas para la gestión de riesgos tecnológicos.

- Se identificaron deficiencias en el proceso de Seguridad de la Información; debido a que no se cuenta con la definición de una estrategia de Seguridad de la Información, activos de información, infraestructuras críticas y los mecanismos para su protección; el Sistema de Gestión de Seguridad de la Información (SGSI) no se encuentra alineado con los objetivos y necesidades operativas del negocio y no se cuenta con los Equipos de Trabajo relacionados con la Seguridad de la Información.

- Se carece del Análisis de Impacto al Negocio (BIA); el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación en caso de Desastres (DRP) no contemplan la totalidad de los servicios y aplicativos críticos; no consideran el sistema ASA, aplicativo crítico utilizado para controlar la operación, administración, facturación y cobro de los servicios aeroportuarios y complementarios proporcionados a las aerolíneas que operan en el AICM, el cual se encuentra obsoleto tecnológicamente y no puede ser actualizado debido a que no cuentan con su código fuente, por lo que existe el riesgo de que en caso de una falla podrían verse afectados algunos servicios de operación en el Aeropuerto.

- Existen deficiencias en el centro de datos principal relacionadas con la disponibilidad de los mecanismos de control de incendios; la operación de los equipos dentro de los umbrales de humedad establecidos en las mejores prácticas internacionales y el resguardo de cintas de respaldos.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Roberto Hernández Rojas Valderrama	Alejandro Carlos Villanueva Zamacona

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 determinados por la Auditoría Superior de la Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; analizar el gasto ejercido en materia de TIC en los capítulos contables de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprenda el análisis de las contrataciones vigentes; la determinación de la procedencia de su renovación; la pertinencia de realizar contrataciones consolidadas; los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como el estudio de mercado.

3. Verificar que el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio se realizó de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; analizar la documentación de las contrataciones para descartar asociaciones indebidas, subcontrataciones en exceso, adjudicaciones sin fundamento, transferencia de obligaciones, suscripción de los contratos (facultades para la suscripción, cumplimiento de las obligaciones fiscales, fianzas), entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permitan su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados vinculados a la infraestructura tecnológica, telecomunicaciones y aplicativos sustantivos para verificar: antecedentes; investigación de mercado; adjudicación; beneficios esperados; análisis de entregables (términos, vigencia, entrega, resguardo, operación, penalizaciones y garantías); pruebas de cumplimiento y sustantivas; implementación y post-Implementación.

6. Evaluar del riesgo inherente en la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados, así como el plan de mitigación para su control, manejo del riesgo residual y justificación de los riesgos aceptados por la entidad.

7. 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; analizar el diagnóstico de las funciones sustantivas y administrativas de las TIC que lleva a cabo la entidad fiscalizada; evaluar el nivel de alineación de la estrategia de TIC con los objetivos de la Organización; así como de los mecanismos de medición, seguimiento y cumplimiento de sus metas; revisar el avance en la implementación

del MAAGTIC-SI o en su caso, la normativa que aplique; revisar el cumplimiento de las disposiciones en materia de Datos Abiertos.

8. Evaluar los mecanismos que permitan la administración de la seguridad de la información, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar los objetivos de la institución o constituir una amenaza para la seguridad nacional; evaluar el nivel de cumplimiento en la optimización del riesgo; verificar la gestión de seguridad de la información y gestión de los programas de continuidad de las operaciones; revisar el control de accesos y privilegios, segregación de funciones, controles de las cuentas funcionales y privilegiadas en los aplicativos y bases de datos sustantivos; verificar los mecanismos implementados para la transferencia de datos sobre canales seguros, así como los estándares aplicados para el cifrado de datos en operación. Evaluar la seguridad física del Centro de Datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).

Áreas Revisadas

La Subdirección de Sistemas del Aeropuerto Internacional de la Ciudad de México, S.A. de C.V. (AICM).

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. Otras disposiciones de carácter general, específico, estatal o municipal: Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, Art. 10 Frac. II y IX; Art. 13 Frac. I y VII; Art. 21; Art. 22; Art. 23; Art. 24; Art. 25; Art. 27, Art. 32;

Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, I.A. Proceso de Planeación Estratégica, Actividad PE 1; III.B. Proceso de Administración de Proveedores (APRO), Actividades APRO 1, APRO 2 y APRO 3; III.A. Proceso de Administración de Proyectos (ADP), Actividades ADP1, ADP 4 y ADP 6; I.B. Proceso de Administración del Presupuesto y las Contrataciones (APCT), APCT 1; Reglas del proceso número 7; I.A. Proceso de Planeación Estratégica (PE), Actividad PE 1; II.C. Proceso de Administración de la Seguridad de la información (ASI), Actividades ASI, ASI 2, ASI 3, ASI 4, ASI 5, ASI 6; III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC), Actividad OPEC 1; III.C. Proceso de Administración de la Operación (AOP), Actividades AOP 2, AOP 3 y AOP 4; II.A. Proceso de Administración de Servicios (ADS), Actividades ADS 3 y ADS 4; Regla General número 6; Apéndice IV.B Matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC;

Contrato número 073-O15-AICM-3S y su Anexo Técnico 1 (T1), numerales "Requisitos para los licitantes" y "Recursos Humanos";

Contrato número 021-O11-AICM-SRP-1S y su Anexo T1, numerales IV.3.4; IV.3.5; Secciones "Administración de Calidad", "Administración de Riesgos", "Administración de la operación, respaldos y recuperación", "Seguridad" y "Administración de la seguridad";

Fundamento Jurídico de la ASF para Promover Acciones

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

Artículo 79, fracciones II, párrafo tercero, y IV, de la Constitución Política de los Estados Unidos Mexicanos.

Artículos 10, fracción I, 14, fracción III, 15, 17, fracción XV, 36, fracción V, 39, 40, de la Ley de Fiscalización y Rendición de Cuentas de la Federación.