INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-3-3891M-15-0470-2018

470-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 la operación de la entidad vinculada con 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 los ingresos, 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	758,092.3
Muestra Auditada	52,035.7
Representatividad de la Muestra	6.9%

Antecedentes

INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación pertenece a la red de Centros Públicos de Investigación del Consejo Nacional de Ciencia y Tecnología (Conacyt), cuya misión es hacer posible que las organizaciones y las personas se desarrollen mediante la apropiación de las TIC.

El INFOTEC tiene como fin realizar investigación científica e innovación y desarrollo tecnológicos en el campo de las TIC, a fin de contribuir a la apropiación y aprovechamiento estratégico de las tecnologías de la información enfocadas a Internet, así como la formación de recursos humanos de alto nivel; generar soluciones a través del uso tecnológico de las TIC enfocadas a internet, o a otros medios relacionados, con el fin de mejorar la eficiencia, transparencia y competitividad de las empresas y organizaciones del sector público, académico, social y privado, a través de las actividades de investigación, innovación, desarrollo, consultoría, difusión, formación de recursos humanos y servicios especializados, entre otros.

Entre 2013 y 2017, se han invertido 4,141,512.2 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

Recursos Invertidos en Materia de TIC
(Miles de Pesos)

Período de Inversión	2013	2014	2015	2016	2017	Total
Monto por año	664,040.4	785,812.4	1,097,789.7	835,777.4	758,092.3	4,141,512.2

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

Resultados

1. Análisis Presupuestal

Del análisis a la información presentada en la Cuenta Pública 2017, el INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación tuvo un presupuesto modificado de 1,080,966.6 miles de pesos, de los cuales se devengó 1,056,706.0 miles de pesos y pagó 939,069.1 miles de pesos que representa el 86.9% del presupuesto modificado.

Estado del Ejercicio del Presupuesto 2017 INFOTEC
(Miles de pesos)

							F=D-E	G=B-C
Capítulo	**Concepto**	**A Presupuesto Autorizado**	**B Presupuesto* Modificado**	**C Presupuesto** Devengado**	**D Presupuesto Ejercido**	**E Presupuesto ** Pagado**	**Presupuesto Devengado no pagado**	**Economías**
1000	Servicios personales	276,058.5	161,432.7	137,190.6	137,190.6	134,743.3	2,447.3	24,242.1
2000	Materiales y suministros	6,240.0	4,200.5	4,200.5	4,200.5	4,200.5	0.0	0.0
3000	Servicios generales	566,901.5	910,300.0	910,281.5	910,295.9	796,376.1	113,919.8	18.5
4000	Transferencias, asignación, subsidios y otras ayudas	800.0	5,033.4	5,033.4	5,033.4	3,749.2	1,284.2	0.0
	TOTAL	850,000.0	1,080,966.6	1,056,706.0	1,056,720.4	939,069.1	117,651.3	24,260.6

FUENTE: Elaborado con base en la información proporcionada por INFOTEC.

* Se integra del presupuesto autorizado por la Secretaría de Hacienda y Crédito Público (850,000.0 miles de pesos y 230,966,6 miles de pesos que obedecen a pasivos y pagos pendientes de ejercicios anteriores, así como los contratos plurianuales que afectan el ejercicio inmediato anterior.

** No se incluyen operaciones ajenas.

En el Informe de Auditoría Externa emitido por la empresa Portilla &. Cía. Contadores Públicos, S.C. al INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación correspondiente al ejercicio 2017, reportó impuestos federales a pagar por 284,471.1 miles de pesos, de los cuales el 31.0% corresponden a impuestos del 2017 y el 69.0% a ejercicios anteriores, lo cual además de generar actualizaciones y recargos puede ocasionar que la entidad sea acreedora a multas por omisión de impuestos.

Los gastos relacionados con Tecnologías de Información y Comunicaciones (TIC) en el ejercicio 2017 ascendieron a 758,092.3 miles de pesos que representan el 81.1% del presupuesto pagado en los capítulos afectados.

Gastos TIC 2017 INFOTEC
(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Pagado	%
1000		**SERVICIOS PERSONALES**	**32,186.0**	**4.2**
2000		**MATERIALES Y SUMINISTROS**	**2,153.1**	**0.3**
3000		**SERVICIOS GENERALES**	**723,753.2**	**95.5**
	31501	Servicio de telefonía celular	95.7	0.0
	31602	Servicios de telecomunicaciones	50.5	0.0
	31701	Servicios de conducción de señales analógicas y digitales	26,812.4	3.5
	32301	Arrendamiento de equipo y bienes informáticos	33,025.2	4.4
	32701	Patentes, derechos de autor, regalías y otros	25,960.7	3.4
	33104	Otras asesorías para la operación de programas	405,309.6	53.5
	33301	Servicios de desarrollo de aplicaciones informáticas	203,301.8	26.8
	33303	Servicios relacionados con certificación de procesos	353.5	0.0
	33603	Impresiones de documentos oficiales para la prestación de servicios públicos, identificación, formatos administrativos y fiscales, formas valoradas, certificados y títulos	8.7	0.0
	33604	Impresión y elaboración de material informativo derivado de la operación y administración de las dependencias y entidades	292.2	0.0
	33903	Servicios integrales	525.5	0.1
	35301	Mantenimiento y conservación de bienes informáticos	13,897.3	1.8
	35701	Mantenimiento y conservación de maquinaria y equipo	13,293.9	1.8
	39801	Impuesto sobre nóminas	826.1	0.1
		Total	**758,092.3**	**100.0**

FUENTE: Elaborado con base en la información proporcionada por INFOTEC.

Los costos asociados de la plantilla del personal de INFOTEC corresponden a las partidas específicas relacionadas con servicios personales (capítulo 1000 y partida 39801), con una percepción anual de 33,012.1 miles de pesos durante el ejercicio 2017. Considerando 70 plazas, el promedio anual pagado por persona fue de 471.6 miles de pesos.

Se seleccionó una muestra de tres contratos con un monto pagado en 2017 de 52,035.7 miles de pesos que representan el 6.9 % del total del universo seleccionado que corresponde a los gastos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC), los cuales se integran de la siguiente manera:

Muestra de Contratos y Convenios de Prestación de Servicios ejercidos en 2017
(Miles de pesos)

Proceso de Contratación	Contrato/ Convenio	Proveedor	Objeto del contrato	Vigencia Del	Vigencia Al	Monto Mínimo	Monto Máximo	Pagado 2017
Licitación Pública Nacional Mixta	LPN/01/09/15	Empresa 1	Proveer protección a equipos contra diferentes tipos de amenazas que pudieran intentar modificar, extraer o incluso eliminar información de los equipos del cliente.	01/09/2015	31/08/2018	0.0	638.0	194.7
	Convenio Modificatorio CM-LPN/01/09/15		Incrementar el monto del contrato 98.0 miles de pesos (15.4%).	09/02/2016	31/08/2018	0.0	98.0	
		Subtotal contrato LPN/01/09/15 (A)				0.0	736.0	194.7
Adjudicación Directa	AD/15/03/16	Empresa 2	Servicio de Transformación,	01/04/2016	31/12/2019	81,200.0	203,000.0	47,829.3

Muestra de Contratos y Convenios de Prestación de Servicios ejercidos en 2017
(Miles de pesos)

Proceso de Contratación	Contrato/ Convenio	Proveedor	Objeto del contrato	Vigencia Del	Vigencia Al	Monto Mínimo	Monto Máximo	Pagado 2017
			Almacenamiento y Aseguramiento de Información bajo demanda" (en adelante STAAI), para soportar la operación de las aplicaciones, servicios WEB y administración de bases de datos que requieren los clientes, garantizando la disponibilidad, confiabilidad y niveles de servicio.					
		Subtotal contrato AD/15/03/16 (B)				81,200.0	203,000.0	47,829.3
Licitación Pública Nacional Electrónica	LPN/53/07/17	Empresa 3	Proporcionar un servicio de infraestructura para integrar soluciones con servidores (procesamiento), almacenamiento y respaldos incluyendo la opción de utilizar tecnologías de virtualización para aprovechamiento de recursos informáticos como son memoria, disco y procesador. Además de ofrecer un servicio de contrato abierto con unidades de servicio de infraestructura que le permitirá al INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (en adelante INFOTEC) crecer en periodos de tiempo que aseguren flexibilidad para sumar y restar unidades durante el contrato.	17/07/2017	17/07/2019	0.0	34,099.0	4,011.7
		Subtotal contrato LPN/53/07/17 (C)				**0.0**	**34,099.0**	**4,011.7**
					Total (A+B+C)	**81,200.0**	**237,835.0**	**52,035.7**

FUENTE: Contratos, facturas y soporte documental proporcionado por INFOTEC.

Se identificó que el presupuesto pagado de los contratos antes citados, se registraron incorrectamente en la partida 33301 "Servicio de Desarrollo de Aplicaciones Informáticas", siendo que la naturaleza de la partida no corresponde a los servicios objeto de los contratos, debieron de aplicarse en las partidas presupuestales 31904 "Servicios Integrales de Infraestructura de Cómputo" y 35301 "Mantenimiento y Conservación de Bienes Informáticos", debido a que en dichos pagos se recibieron servicios relacionados con centros de datos principales y/o alternos incluyendo

hospedaje, así como servidores físicos y/o virtuales, esquemas y equipos de almacenamiento y respaldo de información, red local, y administración de aplicaciones, y otros servicios relacionados, así como dispositivos de seguridad.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, el INFOTEC dio inicio a las acciones para fortalecer el procedimiento de asignación de las partidas presupuestales, a fin de cumplir con las disposiciones contenidas en el Clasificador por Objeto del Gasto para la Administración Pública Federal emitido por la Secretaría de Hacienda y Crédito Público (SHCP), así como en el Clasificador único de las Contrataciones Públicas (CUCoP) emitido por la Secretaría de la Función Pública (SFP).

El análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

2017-5-06E00-15-0470-05-001 **Promoción del Ejercicio de la Facultad de Comprobación** Fiscal

Para que el Servicio de Administración Tributaria instruya a quien corresponda a fin de que se audite al INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación a fin de constatar el cumplimiento de sus obligaciones fiscales, debido a que al cierre del ejercicio del 2017 (de acuerdo al Informe de Auditoría Externa efectuada por la empresa Portilla &. Cía. Contadores Públicos, S.C. al INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación) se reportaron impuestos federales a pagar por 284,471.1 miles de pesos, de los cuales el 31.0% corresponden a impuestos del 2017 y el 69.0% a ejercicios anteriores, actualizaciones y recargos.

2. Contrato LPN/01/09/15

Se analizó el contrato número LPN/01/09/15 “Servicio de Seguridad Perimetral” celebrado con la Empresa 1, mediante el procedimiento de Licitación Pública Nacional Mixta número LA-03891 M001-N98-2015, con fundamento en los artículos 25, 26 fracción I, 26 bis, 27, 28, fracción, I, 29, 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con el objeto de proveer protección a equipos contra diferentes tipos de amenazas que pudieran intentar modificar, extraer o incluso eliminar información de los equipos del cliente, por un monto de 638.0 miles de pesos, vigente del 1° de septiembre de 2015 al 31 de agosto de 2018; el 9 de febrero de 2016, se celebró el Convenio Modificatorio CM-LPN/01/09/15 para incrementar el monto a 736.0 miles de pesos, de los cuales durante el ejercicio 2017 se pagaron 194.7 miles de pesos por los servicios devengados del 1° de diciembre de 2016 al 31 de octubre de 2017. Con el presupuesto autorizado para el 2018, se tuvieron pagos por 35.4 miles de pesos por los servicios devengados del 1° de noviembre al 31 de diciembre de 2017, se determinó lo siguiente.

Alcance

El Servicio de Seguridad Perimetral incluye las funcionalidades de Firewall, Prevención de Intrusos, Ruteo, Filtrado Web, VPN, Antivirus tipo Gateway y Traffic Shapping a través de los servicios siguientes:

SERVICIOS CONTRATO LPN/01/09/15

Solicitud	Tipo A	Tipo B	Tipo C	Tipo D	Tipo E	Tipo F
Número de interfaces requeridas	2 puertos Gigabit Ethernet (GE) Small form-factor pluggable transceptor (SFP) y 40 puertos GE cobre (RJ45)	6xGE RJ-45, 4xGE SFP	10xGE RJ-45, 8xGE SFP	2x10GE SFP+, 14xGE RJ-45, 8x shared ports pairs, 2x bypass pairs	2x10GE SFP+, 18xGE RJ-45, 16xGE SFP	8x10GE SFP+/GE SFP, 18xGE RJ45, 16xGE SFP
Throughput de Firewall	4 Gbps	8 Gbps	16 Gbps	20 Gbps	50 Gbps	80 Gbps
Throughput de Antivirus	1 Gbps	2 Gbps	3 Gbps	3 Gbps	5 Gbps	13 Gbps
Throughput de IPS	2 Gbps	2.5 Gbps	4.5 Gbps	6 Gbps	8 Gbps	11 Gbps
Túneles client-to-gateway	5,000	10,000	10,000	50,000	50,000	50,000
Túneles gateway-to-gateway	2,000	2,000	2,000	2,000	20,000	20,000
Sesiones Concurrentes	3 millones	6 millones	6 millones	7 millones	11 millones	12 millones
Dominios virtuales incluidos/soportados	10	10	10	10	10/250	10/250
Fuente de poder	Redundante	Redundante	Redundante	Redundante	Redundante	Redundante

FUENTE: Información proporcionada por el INFOTEC.

Contratación de los servicios

a) Investigación de Mercado

Para llevar a cabo la Investigación de Mercado, la Dirección General de Administración del INFOTEC utilizó el sistema CompraNet para solicitar las cotizaciones de proveedores interesados; sin embargo, no se utilizaron al menos dos fuentes de información para su integración y no se generaron los formatos FOCON-04 "Solicitud de cotización" y FOCON-05 "Resultado de Investigación", establecidos en el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público (MAAGMAASSP).

b) Convocatoria a la Licitación Pública Nacional Mixta No. 11262001-011-15 (en CompraNet No. LA-03891 M001-N98-2015)

- No se estipuló en la convocatoria si la contratación abarcaría uno o más ejercicios fiscales, ni se definió si el contrato sería abierto o cerrado.
- En el Anexo 16 "Modelo del Contrato" de la Convocatoria señala el tipo de Contrato "Arrendamiento", sin embargo, la contratación fue de Servicios.
- Después del Fallo, no se incorporó el extracto del contrato en CompraNet, por lo que se incumplió con la normativa aplicable.

c) Contrato

De la revisión al contrato y Anexo 4 Propuesta técnica, se obtuvieron las observaciones siguientes:

- No se prevé la posibilidad de que las garantías de cumplimiento o de anticipo se puedan entregar por medios electrónicos.
- No se estipuló que una vez cumplidas las obligaciones del proveedor a satisfacción de la entidad, se procederá inmediatamente a extender la constancia de cumplimiento de las

obligaciones contractuales para que se dé inicio a los trámites para la cancelación de las garantías de cumplimiento del contrato.

- En relación con los pagos, no se precisó la figura responsable que revisará y firmará los documentos de aceptación de Entregables.
- En el contrato no se estipuló el nombre del servidor público que fungirá como responsable de administrar y verificar el cumplimiento de los compromisos contractuales.
- El contrato se formalizó por un importe fijo de 638.0 miles de pesos; no obstante, no se consideraron montos mínimos y máximos, en incumplimiento de lo estipulado en el Modelo del Contrato de la Convocatoria.
- En el Anexo Único del contrato, se estipuló la contratación de los Servicios por 12, 24 o 36 meses, o a solicitud de un servicio específico por determinado tiempo (bajo demanda); no obstante, el contrato estipuló únicamente la obligación de efectuar un pago fijo por 17.7 miles de pesos y no se establecieron los servicios ni el costo unitario que integró dicho monto.

Cabe señalar que el INFOTEC prestó el Servicio de Seguridad Perimetral a través de la Empresa 1, únicamente al cliente Instituto Nacional de las Mujeres (INMUJERES) durante 2017 y no existieron servicios bajo demanda.

d) Convenio Modificatorio núm.CM-LPN/01/09/15 al contrato LPN/01/09/15

En la revisión al Convenio Modificatorio núm. CM-LPN/01/09/15 celebrado el 9 de febrero de 2016, se observaron las inconsistencias siguientes:

- El Convenio Modificatorio se incrementó por el monto de 98.0 miles de pesos sin contar con el soporte y justificación de dicho incremento.
- El documento “Propuesta de Solución, Servicio de Hospedaje de Infraestructura en Centro de Datos-Aguascalientes, Ags.” carece de firmas de aprobación por parte del Administrador del Contrato.

Por lo anterior se concluye que el INFOTEC no verificó los procesos vinculados a la contratación de los servicios, debido a las inconsistencias detectadas en la Investigación de Mercado, Convocatoria, Contrato y Convenio Modificatorio.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, el INFOTEC dio inicio a las acciones para fortalecer las deficiencias identificadas en la investigación de mercado, garantías de cumplimiento, elaboración del contrato, suscripción de los convenios modificatorios y cumplimiento de las Políticas, Bases y Lineamientos en materia de Adquisiciones y Arrendamientos de bienes muebles y la prestación de Servicios (POBALINES).

Cumplimiento técnico-funcional

a) Implementación, funcionalidad y operación de los Servicios

Los servicios contratados entre INFOTEC y su cliente INMUJERES mediante el Contrato núm. 04/2015 y sus convenios modificatorios CM/01/15 y CM/01/18 tuvieron una vigencia del 30 de enero 2015 al 31 de marzo 2018, por lo que a la fecha de la auditoría (agosto 2018) no fue posible verificar la implementación, funcionalidad y operación de los servicios, adicionalmente, el INFOTEC informó a la ASF que los equipos se mantienen desconectados desde el 30 de abril de 2018, debido a lo siguiente:

- INMUJERES decidió concluir toda relación comercial con el INFOTEC, y contratar este mismo servicio con el proveedor Teleinformática en Servicios Avanzados, S.A. de C.V. (Teleinformática), quien solicitó al INFOTEC mantener la continuidad del servicio para INMUJERES a partir del 1° de abril de 2018, durante una semana.

  Si bien, los Servicios de Seguridad perimetral fueron prestados al cliente INMUJERES hasta el mes de abril de 2018, el contrato LPN/01/09/15 tiene vigencia del 1° de septiembre de 2015 al 31 de agosto de 2018. Al respecto, el INFOTEC declaró que el contrato finalizará de acuerdo a lo estipulado contractualmente y que los Servicios de Seguridad Perimetral han sido proporcionados por la Empresa 1 durante el 2018 (enero – junio). Hasta el 2 de julio del 2018 fueron retirados los equipos de las instalaciones de INMUJERES.

  El INFOTEC informó que las capacidades de este contrato pueden utilizarse para cubrir la demanda de cualquier otro cliente que requiera el servicio de Seguridad Perimetral; no obstante a la fecha de la auditoría (agosto 2018), los servicios no han sido utilizados y el contrato vence el 31 de agosto de 2018, por lo que no se justificarían los pagos realizados de abril a agosto de 2018.

b) Entregables periódicos

Durante 2017 se generaron 12 entregables mensuales “E-10, Entregable de Servicios” de su revisión se observaron los incumplimientos siguientes:

- En ningún entregable se específica el responsable de su elaboración.
- El entregable de febrero de 2017 fue recibido el día 10 de marzo de 2017, por lo que se determinaron penalizaciones por 3 días de retraso por 0.2 miles de pesos. Al respecto, INFOTEC informó que se realizará la penalización por el incumplimiento por entrega de fecha extemporánea; no obstante a la fecha de la auditoría (agosto 2018) no se proporcionó evidencia de su aplicación.
- Se identificó que seis de las 12 “Actas de entrega de documentos” relacionadas a los Entregables del Servicio no fueron firmados por el apoderado legal; asimismo, dos actas de entrega fueron firmadas antes de finalizar el mes del servicio.

c) Niveles de Servicio

Los tickets solicitados por los clientes siempre son canalizados y registrados en primera instancia en la Mesa de Servicio del INFOTEC. Durante 2017, se identificó que 86 tickets (98.0%) fueron atendidos por la Mesa de Servicio del INFOTEC y sólo 2 (2.0%) por la Mesa de Servicios de la Empresa 1.

En relación con la Mesa de Servicios del INFOTEC, se observó que en 82 tickets existieron campos vacíos debido a deficiencias en la exportación de la información y en 4 tickets existió indisponibilidad del servicio en tiempo promedio durante 48 horas; no obstante, no fue posible determinar penalizaciones debido a que estos incidentes no fueron reportados a la Mesa de Servicios de la Empresa 1.

De los tickets atendidos en la mesa antes citada, se identificó un ticket relacionado al reporte de robo de un equipo móvil, cerrado hasta cinco meses después de su apertura sin especificar la forma en la que fue resuelto; sin embargo, ni en el contrato ni en su anexo se establecen niveles de servicio para este tipo de incidencias, por lo que no es posible determinar las penalizaciones correspondientes. Cabe señalar que estos tickets no fueron reportados en la Mesa de servicios de INFOTEC.

Adicionalmente se observó que ni el INFOTEC ni el proveedor se alinean a las mejores prácticas de cumplimiento al Sistema de Gestión del Servicio (SGS) de acuerdo con la norma ISO/IEC 20000-1:2011, por lo que incumplió con lo establecido en el Anexo Único del Contrato.

Por todo lo anterior, se concluye que existieron deficiencias en la administración, supervisión, monitoreo y seguimiento de los servicios contratados, debido a las inconsistencias encontradas en los Entregables, Servicios de Mesa de Ayuda, Disponibilidad de los servicios, así como la falta y aprovechamiento de los servicios contratados, con lo que no se acreditó el debido cumplimiento del contrato LPN/01/09/15.

2017-3-3891M-15-0470-01-001 Recomendación

Para que INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación fortalezca los mecanismos de administración, supervisión, monitoreo y seguimiento de los contratos de Tecnologías de Información y Comunicaciones, para que en la Mesa de Servicios de los proveedores se registren todos los incidentes presentados durante la vigencia de los contratos y éstos se incorporen en su totalidad a la Mesa de Servicios del INFOTEC, con la finalidad de asegurar la calidad, operación y disponibilidad de los servicios y no se ponga en riesgo la operación de los clientes de INFOTEC. Asimismo, se cuente con la justificación y documentación que soporte los cambios efectuados a los contratos, con la finalidad de transparentar el ejercicio de los recursos.

3. Contrato AD/15/03/16

Del análisis del contrato AD/15/03/16 "Servicios de Transformación, Almacenamiento y Aseguramiento de Información (STAAI)" celebrado con la Empresa 2, mediante el procedimiento de adjudicación directa, con fundamento en los artículos 41, fracción III, 47 de la LAASSP, y 72, fracción III, de su reglamento, con objeto de proveer soluciones tecnológicas con una pronta respuesta a la demanda de Servicios de Tecnologías de la Información (TI), a través del proyecto "Servicio de Transformación, Almacenamiento y Aseguramiento de Información bajo demanda" (STAAI), para soportar la operación de las aplicaciones, servicios WEB y administración de bases de datos que requieren los clientes, garantizando la disponibilidad, confiabilidad y niveles de servicio, por un monto mínimo de 81,200.0 miles de pesos y máximo de 203,000.0 miles de pesos, vigente del 1° de abril de 2016 al 31 de diciembre de 2019, de los cuales durante el ejercicio 2017 se pagaron 47,829.7 miles de pesos, se determinó lo siguiente:

Alcance

El contrato está conformado por servicios bajo demanda relacionados a Transformación, Almacenamiento y Aseguramiento de la Información, los cuales pueden ser contratados por 12, 18, 24, 36 o 48 meses, la renta mínima de cualquiera de éstos servicios es de dos meses.

1. Contratación de los servicios

a) Investigación de Mercado

- Para llevar a cabo la Investigación de Mercado, la Dirección General de Administración del INFOTEC utilizó el sistema CompraNet para solicitar las cotizaciones de proveedores interesados; sin embargo, no se utilizaron al menos dos fuentes de información para su integración. Asimismo, no se generaron los formatos FOCON-04 "Solicitud de cotización" y FOCON-05 "Resultado de Investigación", establecidos en el MAAGMAASSP.

- En relación con la calificación de los servicios, se utilizó el calificativo “superior” para evaluar la propuesta técnica presentada por un proveedor; sin embargo, no se cuenta con el parámetro utilizado para tal determinación, en la Evaluación Económica, no se integraron los servicios bajo demanda, por lo que no se tiene la certeza que todos los proveedores tuvieron las mismas condiciones para su evaluación.

b) Formalización del Contrato y Anexo Técnico

- No se prevé la posibilidad de que las garantías de cumplimiento o de anticipo se puedan entregar por medios electrónicos.
- No se estipuló que una vez cumplidas las obligaciones del proveedor a satisfacción de la entidad, se procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales para que se dé inicio a los trámites para la cancelación de las garantías de cumplimiento del contrato.
- En el contrato no se estipuló el nombre del servidor público a fungir como responsable de administrar y verificar el cumplimiento de los compromisos contractuales.
- No se proporcionó información que acredite que el Titular de la Dirección Adjunta de Desarrollo Tecnológico, envió al Órgano Interno de Control en la entidad, el informe relativo al Contrato formalizado a más tardar el último día hábil del mes, acompañando de la documentación en el que se hará constar el análisis de las proposiciones y las razones para llevar a cabo la adjudicación del contrato.
- No se proporcionó documentación que demuestre que la Subgerencia de Recursos Financieros informó a la Subgerencia de Asuntos Consultivos el presupuesto anual autorizado por el Presupuesto de Egresos de la Federación (PEF) del ejercicio 2017 y los montos máximos de adjudicación, de conformidad con los POBALINES.
- No se identificó documentación, donde se reporte la operación del contrato, así como el envío a la Subgerencia de Asuntos Consultivos de los datos para integrar los avisos e informes que deben ser enviados a la SFP dentro de los cinco días hábiles siguientes a la fecha de la formalización de la operación, de acuerdo a los POBALINES.
- No se notificó a la SFP la formalización del contrato, incumpliendo con lo estipulado en el tercer párrafo, artículo 50 de la Ley Federal de Presupuesto de Responsabilidad Hacendaria.
- En la propuesta técnica del proveedor y en el Anexo Técnico formalizado se estableció que los servicios de respaldo y recuperación de información, serían suministrados mediante el aplicativo Suite IBM Spectrum Protect, anteriormente Tivoli Storage Manager anexando ficha técnica de la solución propuesta, sin embargo se corroboró que el aplicativo utilizado corresponde a Tivoli Storage Manager v 7.1, por lo que el servicio fue provisto con una herramienta y versión inferior a lo estipulado en el Anexo Técnico del Contrato, sin que exista justificación.

c) Garantía de cumplimiento

La garantía de cumplimiento del proveedor cubre el 10.0% máximo del monto de acuerdo a lo estipulado en el contrato; sin embargo, comprende solamente el periodo del 1 de abril de 2016 al 31 de diciembre de 2018 y no hasta el 31 de diciembre de 2019, de acuerdo a la vigencia del contrato.

Por lo anterior se concluye que el INFOTEC no verificó los procesos vinculados a la contratación de los servicios, debido a las inconsistencias detectadas en la Investigación de Mercado, Adjudicación Directa, Plurianualidad, Modelo del Contrato, Garantía de cumplimiento y deficiencias en el cumplimiento las propuesta técnica presentadas por los proveedores.

2. Pagos

Durante el ejercicio 2017 se realizaron pagos por 47,829.3 miles de pesos, correspondientes a los servicios devengados de abril de 2016 a julio de 2017. Se identificaron servicios devengados de enero a diciembre de 2017 por 35,861.7 miles de pesos, pagados durante el ejercicio 2018.

De la validación de los costos y servicios que integran 61 facturas emitidas, de acuerdo a lo estipulado en el Anexo Técnico del Contrato, se detectaron las observaciones siguientes:

- 11 facturas presentan inconsistencias en el cálculo, lo que dio una diferencia por un monto total de 7.2 miles de pesos, debido a que la entidad no realizó la sumatoria correcta del desglose de servicios.
- 10 facturas consideraron los servicios con descripción "2 Networks Attached Storage (NAS) de 16 TB", por un monto total de 333.1 miles de pesos, sin embargo dicho servicio en el Contrato se estableció de 10 TB, no de 16 TB.
- 3 facturas no refieren el nombre del proyecto y/o cliente que recibió los servicios relacionados con el STAAI.
- 2 facturas corresponden al periodo del 1° al 30 de noviembre de 2017, en incumplimiento del contrato.

3. Cumplimiento Técnico y Funcional

Durante 2017, se suministraron Servicios de Transformación (Virtualización), Almacenamiento y Aseguramiento de Información (STAAI) para soportar la operación de servicios WEB y Administración de BD para 33 clientes. Al respecto, se determinó una muestra de 3 clientes (10.0%) Proyecto 1053-Financiera Nacional de Desarrollo Agropecuario, Rural y Forestal y Pesquero (FND), Proyecto 1015-Comisión Federal de Competencia Económica (COFECE) y Proyecto 417-Universidad Abierta y a Distancia de México (UnADM), para la revisión de los entregables.

a) Entregables

Por otra parte, de la revisión de los entregables de 2017 correspondientes a los Proyectos FND (CDMX y AGS), COFECE y UnADM (CDMX), se identificaron las inconsistencias siguientes:

- De la revisión de las "Actas entrega-recepción de entregables de proyecto", se detectó que no fueron suscritas por el Administrador del Contrato, por lo que no se garantiza el reconocimiento de la aceptación de los mismos, de acuerdo a lo estipulado en la Cláusula Segunda del Contrato.
- En 14 entregables no se identifica la ubicación y nombre de los servidores, en un caso, no se incluye el control de cambios relacionado, en incumplimiento a lo establecido en el Anexo Técnico.
- De la comparación de los entregables relacionados contra el Inventario de Unidades Físicas y Virtuales, se identificó que en algunos casos se reportaron incidentes, bajas y cambios que no fueron reportados en la mesa de servicios del proveedor.

- Durante 2017 no se incluyó en los entregables la bitácora de respaldos correspondientes al proyecto FND y no mostró el desempeño de los Tiers en el proyecto de COFECE.
- De los entregables “Relación de incidentes reportados, atendidos y cerrados", no es posible identificar que los incidentes reportados en la Mesa de Servicios del proveedor fueron registrados en la Mesa de Servicios del INFOTEC durante 2017, para su atención y seguimiento de inicio a fin, debido a que la herramienta del proveedor carece de un campo que permita su registro; por consiguiente, no se tiene la certeza de que todas las solicitudes de altas, bajas y cambios o incidentes de los servicios fueron previamente escalados por la Mesa de Servicios del INFOTEC.
- No se proporcionaron los entregables “Bitácora de Respaldos” de noviembre y diciembre 2017 y “Políticas de respaldos (con control de cambios)” de diciembre y enero de 2017 correspondientes al proyecto COFECE.

d) Penalización y deducciones de pago

Durante el 2017 el INFOTEC determinó una deductiva por un monto de 1.3 miles de pesos, debido a la incidencia reportada el 2 de febrero de 2017, lo cual provocó indisponibilidad del servicio durante 250 minutos con relación al proyecto “COFECE”, el cálculo de las deductivas consideró el precio mensual del servicio entre el total de minutos del mes por el número de minutos de afectación del servicio, sin embargo este se debe calcular con base a las horas de afectación. Por lo que se determinaron diferencias en el cálculo de la deductiva por 75.7 miles de pesos, las cuáles no fueron aplicadas por INFOTEC.

Al respecto, se observó que no existe un proceso que permita al INFOTEC tener la certeza de los tiempos por indisponibilidad del servicio para garantizar que el cálculo de los montos por penas convencionales y/o deductivas sea conforme a los niveles de servicios establecidos en el Anexo Técnico del Contrato.

f) Almacenamiento y aseguramiento de la información

En la revisión de los proyectos 1053- FND, 1015-COFECE y 417- UnADM, correspondientes al almacenamiento y aseguramiento de la información se detectó lo siguiente:

i. Respaldos

- Con base al entregable “Políticas de Respaldo” de diciembre de 2017, se identificaron 10 máquinas virtuales (nodos) correspondientes al proyecto COFECE, de las cuales se observó que un nodo no cuenta con la información histórica que justifique la solicitud de cambio de instalación de respaldos bajo el mismo nombre y en otro nodo se observó que a partir del mes de octubre se modificaron las políticas de respaldo; sin embargo, no existen tickets asociados que muestren las políticas configuradas a fin de verificar su cumplimiento.
- Se detectó que en 28 de 35 nodos (80.0%), correspondientes al proyecto UNaDM no se cuenta con el detalle de las solicitudes de configuración de multinodo, modificación de política de respaldo, migración, cambio de ruta, eliminación de máquinas virtuales y de Schedule, así como borrado de respaldos.
- Las incidencias detectadas en el proyecto FND se encuentran señaladas en el resultado dos correspondiente a la auditoría con número 87-GB Financiera Nacional de Desarrollo Agropecuario, Rural, Forestal y Pesquero (FND) correspondiente a la Cuenta Pública 2017.

ii. Restauración

Se verificaron mediante la herramienta Tivoli Storage Manager v 7.1. las restauraciones de información que se realizaron durante 2017, con base en la relación de los tickets de la de la Mesa de Ayuda de la Empresa 2 correspondientes a STAAI, identificando lo siguiente:

- Durante 2017 se solicitaron dos restauraciones para el proyecto UnaDM; sin embargo, se observó que debido a la configuración preestablecida en el servidor, solo se conservan de manera histórica los últimos 30 días, por lo que fue imposible confirmar si las restauraciones durante 2017 contaban con estatus (exitoso, fallido, completo, incompleto, etc.).

Las incidencias detectadas en el Proyecto FND se encuentran señaladas en el resultado 2 correspondiente a la auditoría con número 87-GB Financiera Nacional de Desarrollo Agropecuario, Rural, Forestal y Pesquero (FND), correspondiente a la Cuenta Pública 2017.

g) *Servicios de Administración, Operación, Soporte y Mantenimiento*

i. Inventario de la Infraestructura

Con base en el Inventario de Infraestructura del STTAI que estuvo vigente durante 2017 y a la visita efectuada por la ASF al Centro de Datos Primario ubicado en Aguascalientes (AGS) y Centro de Datos Alterno ubicado en la Ciudad de México, se identificaron deficiencias en 9 equipos, 2 librerías y 2 accesorios revisados debido a que las direcciones IP, series, marcas, modelos o en su caso IP no coinciden con los registrados en el inventario, lo que denota la falta de supervisión del proceso de actualización de dicho inventario.

ii. Mesa de Ayuda

De un total de 2293 tickets extraídos de la Mesa de Servicio del STAAI, se identificó que en ninguno se registran actividades de solución de cierre del ticket, el 95.0% (2178) no se asocian con un ticket de Mesa de Servicios de INFOTEC y de los que si se registran (115), el 88.8% no coinciden con los levantados en la Mesa de Servicios de INFOTEC. Por lo anterior no se garantiza que los tickets del INFOTEC referenciados a los tickets STAAI procedan de un ticket asignado y transferido por el INFOTEC.

Debido a la falta de trazabilidad entre los tickets generados en las Mesas de Ayuda STAAI e INFOTEC durante 2017, no se tiene la certeza de que el servicio de Mesa de Ayuda del proveedor garantice el cumplimiento de los niveles de servicio estipulados en el Anexo Técnico del Contrato.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, la Gerencia de Administración Integral de Infraestructura del INFOTEC giró instrucciones al interior del INFOTEC para que a partir del 31 de agosto de 2018, todos los tickets abiertos en las diferentes Mesas de Servicio de los proveedores sean registrados también en la Mesa de Servicios de INFOTEC. Asimismo, la herramienta de software que utiliza INFOTEC ha sido modificada para que cuente con un campo en el que se coloca el número de ticket del proveedor, además de estar documentando los avances del proveedor en la herramienta de INFOTEC, para contar con la trazabilidad necesaria.

h) Certificaciones

No se contó con documentación que acredite la asignación, número del personal técnico certificado (Arquitecto de Almacenamiento, Especialista en Respaldo y Recuperación, Consultor Senior en Virtualización y Especialista en Virtualización), así como la certificación del personal técnico especializado que asegure la calidad de la prestación de los servicios del “STAAI” de acuerdo a lo establecido en el contrato.

Por todo lo anterior, se concluye que el INFOTEC no verificó el cumplimiento de los compromisos contractuales, en función de las deficiencias en la facturación y pago de los servicios; entregables; indisponibilidad de los servicios, gestión de los servicios de transformación mediante procesamiento de información, almacenamiento y aseguramiento de la información y servicios de administración, operación, soporte y mantenimiento, así como a la carencia de evidencias de las certificaciones para asegurar la calidad de la prestación de los servicios, por lo cual se presume una falta de aprovechamiento de los recursos, así como una deficiente calidad en la prestación de los servicios, poniendo en riesgo la operación de los servicios que se proporcionan a INFOTEC y a sus clientes.

2017-3-3891M-15-0470-01-002 Recomendación

Para que INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación fortalezca los mecanismos de supervisión, monitoreo y seguimiento de los bienes y servicios que son contratados, así como los productos entregados de acuerdo a lo estipulado contractualmente y el cumplimiento a los niveles de servicio comprometidos, con la finalidad de asegurar la implementación, calidad, operación y disponibilidad de los servicios y que no se ponga en riesgo la operación de los clientes de INFOTEC.

4. Del análisis Contrato LPN/53/07/17 "Servicio Integral de Procesamiento para Virtualización y Almacenamiento (SIPVA)", celebrado con la Empresa 3, mediante el procedimiento de Licitación Pública Nacional Electrónica número LA-03891M001-E73-2017, con fundamento en los artículos 26 fracción I, 26 bis, 27, 28, fracción, I, 29, 47 de la LAASSP, con objeto de proporcionar un servicio de infraestructura para integrar soluciones con servidores (procesamiento), almacenamiento y respaldos incluyendo la opción de utilizar tecnologías de virtualización para aprovechamiento de recursos informáticos como son memoria, disco y procesador, por un monto de 34,099.0 miles de pesos, vigente del 17 de julio de 2017 al 17 de julio de 2019, de los cuales durante el ejercicio 2017 se pagaron 4,011.7 miles de pesos. Con el presupuesto autorizado para el 2018, se pagaron 3,991.8 miles de pesos por los servicios devengados en 2017 (incluye servicio del 1° al 15 de enero de 2018), se determinó lo siguiente.

Alcance

El contrato está conformado por Servicios Base y Servicios bajo demanda (solicitudes específicas por tiempo determinado).

Los Servicios Base consideran 8 componentes para el servicio de almacenamiento (vmax y servidor) y conectividad LAN y SAN para asegurar la disponibilidad de los servicios) por un periodo de 17 meses.

Estos mismos servicios se pueden contemplar como Servicios bajo demanda (a solicitud por tiempo determinado), 34 tipos de Unidades de procesamiento, almacenamiento, respaldos y virtualización y 3 tipos Unidades de Apoyo, Operación y Configuración Especializada (básica, media y alta).

1. Contratación de los servicios

a) Investigación de Mercado

Para llevar a cabo la Investigación de Mercado, la Dirección General de Administración del INFOTEC utilizó el sistema CompraNet para solicitar las cotizaciones de proveedores interesados; sin embargo, no se utilizaron al menos dos fuentes de información para su integración.

b) Convocatoria a la Licitación Pública Nacional Electrónica número LA-03891M001-E73-2017

- No se estipuló en la convocatoria si la contratación abarcaría uno o más ejercicios fiscales.
- La Requisición de Adquisición de Servicios no fue firmada por el Director Ejecutivo.
- El contrato no prevé la posibilidad de que las garantías de cumplimiento o de anticipo se puedan entregar por medios electrónicos.

c) Contrato

- En relación a los pagos, no se precisó la figura responsable que revisará y firmará los documentos de aceptación de entregables.
- No se estipuló que una vez cumplidas las obligaciones del proveedor a satisfacción de la entidad, se procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales para que se dé inicio a los trámites para la cancelación de las garantías de cumplimiento del contrato.
- El contrato se formalizó por un importe fijo de 34,099.0 miles de pesos; no obstante, no se consideraron montos mínimos y máximos, de acuerdo a lo estipulado en el Modelo del Contrato de la Convocatoria.
- En el contrato no se estipuló el nombre del servidor público a fungir como responsable de administrar y verificar el cumplimiento de los compromisos contractuales.

2. Cumplimiento técnico-funcional

a) Entregables

- De los entregables de Protocolos de pruebas de componentes físicos y Protocolos de pruebas de componentes lógicos de la Fase II, no se tiene evidencia de la ejecución del protocolo de pruebas descrito en los entregables.
- De los entregables correspondientes a la Fase VI. Operación del Servicio (correspondientes a los reportes de tickets, disponibilidad y atención de hardware y software con fabricantes) se identificaron las irregularidades siguientes:

– Los tickets no incluyen la hora de recepción del requerimiento, de su respuesta y término de la actividad, la cual es requerida de manera obligatoria según lo estipulado en el Anexo Propuesta Técnico; existieron tickets con estatus “atendido” sin fecha de término y se identificaron tickets con fecha de recepción o término posterior a la solicitud y respuesta, respectivamente.

– La unidad “USM UCS Prime”, a partir del mes de diciembre de 2017 se dio de baja (el servicio no fue facturado ni pagado a partir de esta fecha); no obstante, no se cuenta con un convenio modificatorio en el cual se estipule la baja del servicio, en incumplimiento a lo establecido en el contrato y no se cuenta con soporte que permita observar el análisis técnico y funcional, notificación, revisión y autorización de la baja por parte del Cliente (SHCP).

b) Servicio de Mantenimiento

- El proveedor no comunicó o notificó a INFOTEC previo a 96 horas que se llevaría a cabo la ejecución de mantenimientos preventivos, lo que incumplió con el Anexo Técnico del Contrato.

- El calendario de los servicios de mantenimiento preventivo no cuenta con número y método de mantenimiento a realizar, así como el diagnóstico de los servicios y pruebas de funcionamiento.

c) Mesa de Servicio

El proveedor realizó cambios internos para la actualización de versión de la herramienta usada para la gestión de incidentes y requerimientos para todos los clientes a los que la Empresa 3 brinda el servicio de Mesa de Servicio (Aranda Service Desk) sin emitir notificación al INFOTEC. Se menciona que la migración de la base de datos por el cambio de versiones no impactó en la entrega de servicios, sin embargo, derivado de las inconsistencias identificadas en los reportes periódicos de incidentes y requerimientos, no se garantiza la integridad y disponibilidad de la información en la base de datos del proveedor.

d) Garantías y Contratos de Soporte

Se identificó que la Empresa 3 no es una empresa autorizada para proporcionar servicios de soporte de las unidades CISCO, las cuales representan el 73.0% de la infraestructura objeto de Soporte del Anexo Técnico del contrato, el servicio fue efectuado por la empresa "Dimension Data Commerce Centre México S.A. de C.V.", la cual es un proveedor autorizado de CISCO, por lo que la Empresa 3 efectuó la subcontratación a través de esta última para proporcionar los servicios, lo que incumplió con lo establecido en la Convocatoria a la Licitación Pública Nacional Electrónica número LA-03891M001-E73-2017 y en el Contrato.

e) Personal Capacitado

Se identificó que un recurso técnico del proveedor no contó con la certificación en CISCO Certified Network Associate: Routing and Switching y F5 Certified BID-IP Administrator, en incumplimiento de lo establecido en el contrato.

Por todo lo anterior, se concluye que existieron deficiencias en la supervisión, monitoreo y seguimiento de los servicios contratados, debido a las inconsistencias encontradas en los Entregables, Mesa de Servicio, Garantías y Contratos de Soporte, así como del Personal Capacitado establecido en el contrato, por lo que no se acreditó el debido cumplimiento del contrato LPN/53/07/17.

Durante el transcurso de la auditoría y con motivo de la intervención de la ASF, el INFOTEC emitió un oficio al proveedor a efecto de notificar con anticipación la ejecución de servicios de mantenimiento, así como los cambios que se lleguen a efectuar en la Mesa de servicio del proveedor.

2017-3-3891M-15-0470-01-003 Recomendación

Para que INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación fortalezca los mecanismos de control y supervisión del Proceso de Contratación desde el origen de la necesidad del servicio. En los contratos se precisen las obligaciones y compromisos de ambas partes, que permitan garantizar las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento y oportunidad en los procesos de contrataciones relacionadas con las Tecnologías de Información y Comunicaciones.

2017-9-3891M-15-0470-08-001 **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 INFOTEC Centro de Investigación e

Innovación en Tecnologías de la Información y Comunicación 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 verificaron ni cumplieron con los compromisos del contrato LPN/53/07/17 Servicio Integral de Procesamiento para Virtualización y Almacenamiento, debido a los incumplimientos detectados en los Entregables, Mesa de Servicio y Certificaciones del personal, así como la subcontratación de servicios con un tercero para proporcionar soporte de las unidades CISCO incumpliendo con lo establecido en la Convocatoria a la Licitación Pública Nacional Electrónica número LA-03891M001-E73-2017 y en el Contrato antes citado. Adicionalmente no contaron con soporte que permita observar el análisis técnico y funcional, notificación, revisión y autorización de la baja de la unidad USM UCS Prime por parte del Cliente (Secretaría de Hacienda y Crédito Público) y al interior del INFOTEC.

5. Gestión de la Seguridad de la Información

En la revisión y análisis de la información proporcionada por el INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, relacionada con la Administración de la Seguridad de la información (ASI) y Operación de Controles de Seguridad de la información y del ERISC (OPEC), para proporcionar confidencialidad, disponibilidad e integridad de la información, se observó lo siguiente:

Administración de la Seguridad de la Información (ASI)

- Los formatos correspondientes al proceso de la Seguridad de la Información (ASI) no cuentan con fechas de elaboración, revisión y aprobación, por lo que no es posible identificar su vigencia, así como sus actualizaciones correspondientes. Asimismo, carecen de soporte documental y evidencia de las actividades y acciones definidas en estos.

Modelo de gobierno de seguridad de la información

- Durante el periodo del 1° de noviembre de 2017 al 19 de febrero de 2018 no se contó con la designación formal del responsable de la Seguridad de la Información en el INFOTEC; no obstante, a partir del 19 de febrero de 2018 se designó como responsable al Gerente de Administración Integral de Infraestructura del INFOTEC.
- Se carece de documentación que acredite que el Responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos en el INFOTEC durante 2017 llevó a cabo lo siguiente:
  - Obtener los datos necesarios para verificar la eficiencia y eficacia de los controles implementados, de acuerdo al programa de evaluaciones del SGSI.
  - Medir la efectividad de los controles de seguridad implementados.
  - Realizar la evaluación del SGSI.
  - Registrar, analizar y evaluar la información de los intentos de violaciones e incidentes de seguridad.
- No se designaron los servidores públicos que conformaron el Grupo Estratégico de Seguridad (GESI) de la Información.

Diseño del SGSI

- El Sistema de Gestión de Seguridad de la Información (SGSI), no fue implementado durante el ejercicio 2017, de acuerdo a lo establecido en el "Cronograma para la implantación" anexo en el formato ASI F4 "Documento de definición del SGSI", debió estar implementado desde el 26 de febrero de 2016. En consecuencia, el GESI durante 2017 no llevó a cabo lo siguiente:

- Elaborar, probar y mantener actualizada la directriz rectora de respuesta a incidentes.
- Ejecutar los programas de implementación para el manejo de riesgos.
- Generar el Informe de resultados de la implementación del SGSI.
- Asegurar que los controles de seguridad fueron implementados.

Por lo que el GESI, no dio seguimiento a la ejecución del programa de implementación del SGSI y no actualizó su avance.

Concienciación y Capacitación

- No se cuenta con evidencia de la propuesta de capacitación y métricas (MES-SGI-16) que el GESI elaboró para 2017, la cual debe presentarse anualmente. Tampoco se identificó soporte de que dicho Grupo la compartió al área responsable de la Capacitación en el INFOTEC.
- No se realizaron capacitaciones a recursos con responsabilidades de seguridad relevantes durante 2017.
- Si bien el personal del Centro de Operaciones de Seguridad (SOC) y el administrador de antivirus tiene conocimiento de los recursos que cuentan con privilegios y responsabilidades de seguridad relevantes, esta información no ha sido formalizada a la fecha de la auditoría (junio 2018).

Infraestructuras de información (esenciales y/o críticas, activos clave)

- No se contó con la designación formal del equipo de trabajo y de su responsable para mantener actualizado el catálogo de infraestructuras de información esenciales durante 2017.
- El "Catálogo de Infraestructuras críticas ASI F2" no cuenta con un control de cambios, por lo que no es posible determinar si el catálogo se encuentra actualizado, y no se tiene certeza de que se analicen los procesos existentes y su criticidad, considerando aquellos de los que depende el INFOTEC para alcanzar sus objetivos.

Análisis de riesgos

- No se cuenta con el soporte de la designación formal del equipo de trabajo, responsable de la Gestión de Riesgos durante 2017, tampoco fue posible verificar su experiencia y conocimientos.
- Del análisis y revisión de los documentos y/o formatos: "ASI F3 Documento de resultados del Análisis de Riesgos", "FO-UGS-05 Matriz de Análisis de Riesgos de Seguridad de la Información" y "FO-UGS-06 Matriz de Evaluación de Riesgos de la Seguridad de la Información", se detectaron las siguientes observaciones:

- No se estipuló la probabilidad de ocurrencia de las amenazas.
- No se identifica la relación de la probabilidad de ocurrencia contra el impacto de cada riesgo.
- No se realizó el análisis del costo-beneficio de los controles de seguridad.

- La Matriz de análisis de riesgos de la Seguridad de la Información no se encuentra aprobada y no se compartió a los responsables de los procesos en las diversas áreas y unidades administrativas del INFOTEC para su revisión.
- No se cuenta con el programa de implementación para el manejo de riesgos vigente durante 2017.

Por lo anterior, no es posible garantizar el seguimiento y atención de las acciones tomadas durante 2017 para minimizar la probabilidad de ocurrencia de los riesgos.

Análisis de Vulnerabilidades

Derivado del Informe Técnico de Análisis de Vulnerabilidades 2017, se identificaron vulnerabilidades de categoría alta, media y baja, resultando un nivel de amenaza Medio; sin embargo, no se cuenta con el soporte relacionado al seguimiento del Plan de remediación y su ejecución y no se identificaron las herramientas de Análisis de Vulnerabilidades que el INFOTEC utiliza.

Controles mínimos de seguridad de la información en el SGSI de acuerdo a MAAGTICSI

Borrado Seguro

- No se realizan pruebas a los procedimientos de Borrado Seguro para los sistemas de alto impacto.
- El Procedimiento para Borrado Seguro no ha sido actualizado desde su elaboración (25 de junio de 2015). Además de que no considera lo siguiente:

- Herramientas que son utilizadas para llevar a cabo el Borrado Seguro.
- Criterios para determinar que herramienta y método de borrado se utilizará de acuerdo al tipo de solicitud.
- No se definió ningún *documento involucrado* (formato, checklist, oficio, nota informativa, etc.), que permita verificar que se realizaron las actividades de verificación del borrado seguro y la validación al procedimiento realizado y certificados generados.
- El alcance del procedimiento se encuentra delimitado a los requerimientos realizados por los clientes, y no contempla los procesos y lineamientos a seguir para solicitudes realizadas por las áreas internas del INFOTEC.
- No se especifica el detalle de elaboración y generación de los informes relacionados, ni su validación y autorización.
- No se consideran pruebas a los procedimientos de Borrado Seguro.

Contraseñas

- No se encuentra habilitado el almacenamiento de contraseñas en todas las estaciones de trabajo de INFOTEC.
- No se encuentra formalizado el personal que cuenta con Privilegios y responsabilidades de Seguridad relevantes.

Protección del Sistema y Comunicaciones

- No se tienen esquemas de cifrado en los equipos portátiles del INFOTEC.

Controles de Acceso

- No se tiene configurada la función de auditoría para los accesos remotos.
- No existe una Política de Control de Accesos, para la asignación, revocación o modificación de los privilegios de acceso a la información

Gestión de la Configuración

- El INFOTEC no cuenta con herramientas de auto detección de cambios en la configuración de los activos del servicio.

Identificación y Autenticación

- No se tiene habilitada la autenticación de dos pasos en ningún sistema del INFOTEC.
- No se tienen habilitadas las políticas de auditoría a nivel Directorio Activo.
- INFOTEC no cuenta con un sistema de control de versiones de Software.

Operación de los Controles de Seguridad de la Información y del ERISC (OPEC)

Elementos de operación del ERISC

Se carece de soporte documental que permita conocer los mecanismos de coordinación del ERISC al interior de INFOTEC o con otros ERISC u organizaciones externas.

Documentos no actualizados durante 2017

- Se identificó que la siguiente documentación no fue actualizada en el INFOTEC durante 2017:

- Procedimiento de Borrado Seguro.
- ASI-F2 Catálogo de Infraestructura de Información esencial y/o críticas.
- ASI-F3 Documento de resultados del análisis de riesgos.
- FO-UGS-01 Política de Seguridad de la Información.
- FO-UGS-02 Objetivos de la Seguridad de la Información.
- FO-UGS-03 Medición de la Efectividad de los Objetivos de la Seguridad de la Información.
- FO-UGS-04 Enfoque y Criterios para la Gestión de Riesgos de Seguridad de la Información.
- FO-UGS-07 Listado de Controles de Seguridad.
- FO-UGS-10 Términos y tipificaciones de actividades sospechosas e incidentes de seguridad.
- FO-UGS-12 Código de Colores para notificaciones de Actividades Sospechosa de Incidentes de Seguridad.
- FO-UGS-16 Reporte de Incidentes de Seguridad de la Información.
- FO-UGS-17 Dictamen de actividades sospechosa.
- FO-UGS-18 Reportes de Lecciones aprendidas.

Por otra parte, para la continuidad de las operaciones no se contó con un Plan de Continuidad de Negocio (BCP), Plan de Recuperación de Desastres (DRP), Análisis de Impacto al Negocio (BIA), Gestión de Respaldos y Evaluación de Riesgos. El detalle se encuentra en el resultado siguiente.

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, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos del INFOTEC son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O DEFICIENCIAS DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y OPERACIÓN DEL ERISC

Factor crítico	Riesgo
Sistema de Gestión de Seguridad de la Información (SGSI)	La carencia de implementación del SGSI ocasiona principalmente 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 podrían ser alterados provocando pérdidas económicas y posibles 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, ya que no existe evidencia que demuestre lo contrario.
Administración de Usuarios	Los usuarios pueden tener permisos para acceder a información no autorizada de acuerdo con sus funciones y responsabilidades, en consecuencia, se podría perder la confidencialidad en la información y ejecutar transacciones no autorizadas que pueden poner en riesgo los activos del INFOTEC.
Monitoreo de las bitácoras y pistas de auditoría	Derivado de que las pistas de auditoría y las bitácoras no se encuentran activadas, no es posible detectar oportunamente movimientos irregulares o cambios no autorizados, en consecuencia, existe oportunidad para que los usuarios maliciosos puedan ejecutar transacciones no autorizadas que comprometan la integridad de los activos.
Concienciación y Capacitación	Al no existir un programa de capacitación institucional, pueden presentarse incidentes menores y mayores que impacten la seguridad de la información y operación de los servicios críticos, incumpliendo las Políticas de Seguridad relacionadas.
Análisis de Riesgos	Al existir deficiencias en la Administración de Riesgos, existe la probabilidad de que éstos se materialicen, y que puedan impactar los servicios y/o aplicaciones críticas del INFOTEC, provocando incumplimientos normativos y contractuales, lo que podría representar pérdidas financieras derivado de las interrupciones en la operación.
Cifrado de Información	La carencia de mecanismos de cifrado en los dispositivos móviles de la institución, ocasiona principalmente 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 podrían ser alterados, provocando pérdidas económicas y fraudes.
Infraestructuras Críticas y los activos clave.	Tener un Catálogo de Infraestructuras críticas que no cuente con un control de cambios y que además no contenga la fecha de elaboración, revisión y aprobación, implica riesgos como no poder determinar si el catálogo se encuentra actualizado y que no se tenga certeza de que efectivamente se analizan los procesos existentes y se determina cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos.
Borrado seguro	La carencia de pruebas a los procedimientos de borrado seguro, representa un riesgo que puede comprometer la confidencialidad de la información provocado en el uso indebido de ésta.

FUENTE: Elaboración con la información proporcionada por INFOTEC.

Cabe señalar que el INFOTEC continúa implementando el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información (MAAGTICSI) publicado en el Diario Oficial de la Federación (DOF) el 8 de mayo de 2014.

Por todo lo anterior, se reflejan deficiencias en los controles relacionados a la designación y formalización del responsable de la Seguridad de la Información y su Grupo Estratégico, implementación del Sistema de Gestión de Seguridad de la Información, actualización y seguimiento de los formatos asociados al proceso ASI, Gestión de riesgos, atención a vulnerabilidades identificadas, pruebas de Borrado Seguro, Gestión de la configuración y Bitácoras de Auditoría y bases de datos y sistemas operativos, por lo que el INFOTEC no vigiló el cumplimiento de las disposiciones normativas en materia de tecnologías de información y comunicaciones.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, el INFOTEC inició con la gestión para la corrección y actualización de todas las observaciones y documentos en comento.

2017-3-3891M-15-0470-01-004 Recomendación

Para que INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación continúe con la actualización e implementación del Sistema de Gestión de Seguridad de la Información, designación de los grupos de trabajo, que permitan salvaguardar los activos de información e instrumentar políticas para la protección de información sensible y acciones que aseguren una adecuada gestión de la administración de usuarios, monitoreo de las bitácoras de los aplicativos, bases de datos y sistemas operativos, borrado seguro de la información, cifrado de la información, identificación de infraestructuras críticas y activos clave, gestión de riesgos, planificación y ejecución de las acciones para remediar las vulnerabilidades identificadas, con la finalidad de disminuir los riesgos que pudieran impactar en la operación, manejo y privacidad de la información del INFOTEC y de sus clientes.

2017-9-3891M-15-0470-08-002 **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 INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación 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 implementaron el Sistema de Gestión de Seguridad de la Información durante el ejercicio 2017; no definieron el Grupo Estratégico de Seguridad de la Información, así como el equipo de trabajo responsable de la Gestión de Riesgos; no elaboraron la propuesta de Capacitación y métricas; no se revisaron ni actualizaron las infraestructuras de información críticas, así como los activos clave; no se contó con cifrado de información en equipos portátiles; almacenamiento de contraseñas, implementación de los controles para la asignación, revocación o modificación de los privilegios de acceso a la información; y no se actualizaron los controles existentes para el establecimiento de un modelo de gobierno de seguridad de la información. Asimismo no se contó con un Plan de Continuidad de Negocio (BCP), Plan de Recuperación de Desastres (DRP), Análisis de Impacto al Negocio (BIA), Gestión de Respaldos y Evaluación de Riesgos, con la finalidad de garantizar una óptima continuidad operativa de los procesos críticos, aplicativos sustantivos e infraestructura tecnológica del INFOTEC y de sus clientes.

6. Centro de Datos y Continuidad de la Operación

El INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (en adelante INFOTEC), cuenta con dos Centros de Datos propios, uno ubicado en Aguascalientes (Ags.), México y otro en la Ciudad de México (CDMX), México, ambos con la finalidad de garantizar la continuidad de la operación del INFOTEC y para evitar la afectación del suministro de los servicios contratados por sus Clientes.

Durante la visita a los Centros de Datos, se revisaron los procesos de Gestión, y los controles de seguridad física y lógica de la infraestructura, y se identificó lo siguiente:

VERIFICACIÓN FÍSICA EN CENTROS DE DATOS

Factor Crítico de Seguridad *	Centro de Datos	Observaciones
Prevención de Incendios	Ags.	Durante 2017 no se realizaron verificaciones a las instalaciones del Centro de Datos, por parte de Protección Civil o de algún organismo externo de INFOTEC.
	Ags.-CDMX	Durante 2017 no existieron programas de capacitación y material de apoyo para comunicar al personal clave y/o responsable, las acciones de evacuación y mitigación que deben ejecutarse en caso de presentarse un incendio en el Centro de Datos.
Control de Accesos	CDMX	No se identificó en la información proporcionada los parámetros y/o análisis para definir la distribución y/o ubicación física de las cámaras de vigilancia.

FUENTE: Elaboración con información proporcionada por el INFOTEC.

* MAAGTIC-SI, II.C. Proceso de Administración de la Seguridad de la Información (ASI), Actividad del proceso AOP 4 Implementar y verificar que se cumplan los controles de seguridad física en el centro de datos.

En el análisis de la información del Proceso de Continuidad de la Operación en el INFOTEC se observó lo siguiente:

- **Evaluación de Riesgos**

  No se tiene definida, formalizada ni difundida una directriz para la administración de riesgos.

- **Infraestructura Tecnológica**

  No se cuenta con una herramienta y/o sistema automatizado que permita controlar los elementos de configuración de la infraestructura y actualizaciones correspondientes.

- **Análisis de Impacto al Negocio (Business Impact Analysis - BIA)**

  El INFOTEC no cuenta con un BIA, por lo que no se conoce en caso de haber una interrupción parcial o total, la magnitud del impacto operacional tanto para el INFOTEC, como para los clientes a los que brinda servicio.

- **Protocolo de Recuperación de Servicios Centro de Datos CDMX**

  El Protocolo de Recuperación actualizado en junio de 2017 no se encuentra formalizado. Cabe señalar que en este documento, se hace referencia al Procedimiento para Reestablecer Suministro y Procedimiento de Emergencia en Caso de Movimiento Telúrico, sin embargo no se cuenta con este.

- **Plan de Recuperación de Desastre (Disaster Recovery Plan – DRP)**

  EL INFOTEC no cuenta con un Plan de Recuperación en Caso de Desastres (DRP), por lo que no es posible acreditar que en 2017 existió un Plan de Pruebas, su ejecución, así como el soporte de la capacitación del personal involucrado en dichas actividades y no se cuenta con un Programa de Capacidad.

- **Plan de Continuidad del Negocio (Business Continuity Plan – BCP)**

  El BCP fue elaborado en junio de 2015, sin embargo se encuentra desactualizado**.** Asimismo no se estableció el objetivo del punto de recuperación (RPO) y el objetivo del tiempo de recuperación (RTO).

  Cabe señalar que el plan no fue desarrollado con base en un Análisis de Impacto al Negocio (BIA), en virtud de que no se cuenta con éste.

No se identificó el Plan de Pruebas ni su ejecución durante el 2017, así como el soporte de la capacitación del personal involucrado en dichas actividades. Adicionalmente, no se cuenta con un Programa de Continuidad.

- **Respaldos**

  El procedimiento de respaldos carece de la definición de activos por respaldar, periodicidad, fuente, tipo, monitoreo, áreas responsables e involucradas, procedimiento de recuperación, lo cual no garantiza que la información sea resguardada y se encuentre disponible en caso de una contingencia.

  En ambos Centros de Datos, se identificó que los respaldos de información se resguardan en el mismo espacio físico donde se encuentra la infraestructura que soporta la operación del INFOTEC, y no en una ubicación alterna, aunado a que el INFOTEC no cuenta con una réplica exacta de la información que es resguardadada en los Centros de Datos de Aguascalientes y Ciudad de México. Por lo anterior, en caso de presentarse una incidencia mayor, interrupción y/o contingencia existe el riesgo de perdida total de la información e indisponbilidad de ésta.

- **Procedimientos y/o Protocolos no actualizados durante 2017**

Durante 2017 no fueron actualizados los documentos siguientes:

- Procedimiento DRP de la Energía Eléctrica para el CPD (Centro de Datos).
- Protocolo de Recuperación de Servicios Centro de Datos CDMX.
- Protocolo de Recuperación de Servicios de Bases de Datos y Plataformas Web.
- Protocolo de Emergencia en Caso de Movimiento Telúrico.
- Protocolo de Recuperación de Servicios de Publicación y Acceso a Internet.
- Protocolo de Recuperación del Servicio “CENAM”.
- Protocolo de Recuperación de Servicios redes.
- Protocolo de Recuperación de Servicios de la MCSI.
- Protocolo de Recuperación de Servicios de Plataformas tecnológicas.
- Protocolo de Recuperación del Servicio de Seguridad Perimetral.

Cabe señalar que estos documentos fueron elaborados desde 2015.

Derivado de la revisión de los controles de Continuidad de las Operaciones, los principales riesgos por la carencia o inconsistencia de estos y sus consecuencias potenciales para las operaciones y activos de INFOTEC son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES RELACIONADOS A CONTINUIDAD DE LAS OPERACIONES

Factor Crítico*	Principales Riesgos por su Carencia y sus Consecuencias Potenciales para las Operaciones y Activos
Implementación del Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)	Al carecer de la implementación de los planes de continuidad y recuperación de desastres, no es posible verificar la efectividad de las acciones definidas para realizar la recuperación de los servicios críticos, los cuales podrían resultar afectados como consecuencia de la interrupción de uno o más servicios críticos, 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.
Definición formal del Análisis de Impacto al Negocio (BIA)	Al carecer de un Análisis de Impacto al Negocio (BIA), no es posible estimar el impacto y la afectación (consecuencias) que existiría en el INFOTEC al presentarse un incidente mayor y/o desastre de cualquier tipo.
Gestión de Respaldos	Debido a que no se cuenta con las directrices y medidas precautorias para la adecuada gestión de respaldos, no es posible garantizar la recuperación de la información cuando se presente un incidente mayor y/o una interrupción en la operación que requiera poner en marcha el BCP o DRP.

FUENTE: Elaborado con información proporcionada por INFOTEC.

* MAAGTIC-SI, Proceso II.A, Actividad del Proceso ADS 1, ADS 3 y ADS 4; Proceso II.B, Actividad del Proceso ACNF 4; Proceso II.C, Actividad del Proceso ASI 5; Proceso III.C, objetivos específicos 1 y 2

Por todo lo anterior, se reflejan deficiencias en la definición y actualización formal de los procedimientos de continuidad de la operación, elaboración del plan de pruebas y su ejecución con la finalidad de garantizar la disponibilidad e integridad de la información, por lo que se concluye que el INFOTEC no vigiló el cumplimiento de las disposiciones normativas en materia de Tecnologías de Información y Comunicaciones.

2017-3-3891M-15-0470-01-005 Recomendación

Para que INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación lleve a cabo la implementación y ejecución de pruebas de un Plan de Continuidad de Negocio (BCP), Plan de Recuperación de Desastres (DRP), Análisis de Impacto al Negocio (BIA), Gestión de Respaldos y Evaluación de Riesgos, con la finalidad de garantizar una óptima continuidad operativa de los procesos críticos, aplicativos sustantivos e infraestructura tecnológica del INFOTEC y de sus clientes.

El Universo seleccionado por 758,092.3 miles de pesos corresponde a los gastos efectuados en materia de Tecnologías de la Información y Comunicaciones (TIC); la muestra auditada por 52,035.7 miles de pesos se integra por el presupuesto pagado de tres contratos relacionados con servicios de seguridad, monitoreo, almacenamiento e infraestructura, vigentes en el ejercicio fiscal 2017, que representan el 6.9% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de las acciones realizadas en TIC por el INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación en 2017, relacionadas con la Gestión de la Seguridad de la Información y Continuidad de las Operaciones.

Resumen de Observaciones y Acciones

Se determinaron 6 observaciones las cuales generaron: 5 Recomendaciones, 1 Promoción del Ejercicio de la Facultad de Comprobación Fiscal y 2 Promociones de Responsabilidad Administrativa Sancionatoria.

Dictamen

Con base en los resultados de la auditoría practicada a INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, cuyo objetivo consistió en fiscalizar la gestión financiera de la operación de la entidad vinculada con 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 los ingresos, 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 por 52,035.7 miles de pesos; se concluye que en términos generales cumplió con las disposiciones legales y normativas que son aplicables en la materia excepto por los resultados descritos en el presente informe de auditoría, que arrojaron deficiencias y debilidades que son importantes, entre las que destacan las siguientes:

Al cierre del ejercicio del 2017 INFOTEC reportó impuestos federales por pagar de 284,471.1 miles de pesos, de los cuales el 31.0% corresponden a impuestos del 2017 y el 69.0% a ejercicios anteriores, actualizaciones y recargos, lo cual podría ocasionar que la entidad sea acreedora a multas por omisión de impuestos.

En la contratación de Servicios de Transformación, Almacenamiento y Aseguramiento de Información (STAAI) se identifican deficiencias en la facturación y pago de los servicios; entregables; indisponibilidad de los servicios, calidad de los servicios y falta de personal certificado, que ponen en riesgo la operación de los servicios que se proporcionan a INFOTEC y a sus clientes.

Para la Seguridad de la Información, no se implementó un Sistema de Gestión de Seguridad de la Información, no se definió el Grupo Estratégico de Seguridad de la Información, no se cuenta con cifrado en equipos portátiles y se carece de controles para la asignación, revocación o modificación de los privilegios de acceso a la información, por lo que existen riesgos que podrían afectar la operación, manejo y privacidad de la información de INFOTEC y de sus clientes.

Respecto de la Continuidad de las Operaciones, no se tiene implementado un Plan de Recuperación de Desastres y un Análisis de Impacto al Negocio, lo que incrementa el riesgo de no contar con la capacidad de recuperar satisfactoriamente los datos, la infraestructura tecnológica y los aplicativos sustantivos de INFOTEC y de sus clientes.

El presente dictamen se emite el 15 de octubre de 2018, fecha de conclusión de los trabajos de auditoría correspondientes a la Cuenta Pública 2017, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Roberto Hernández Rojas Valderrama	Ing. 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 corresponden con las registradas por la entidad fiscalizada en su Estado del Ejercicio del Presupuesto y Auxiliares Presupuestales; asimismo verificar que los registros presupuestarios y contables de los recursos asignados a las TIC cumplen con la normativa.
2. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; 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), revisar que los contratos plurianuales se sujetan a la autorización correspondiente, entre otros.
3. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuenten con controles para su fiscalización, correspondan 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.
4. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados vinculados con 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. Evaluar el 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.
5. Evaluar los mecanismos para la administración de la seguridad de la información, así como la disminución del 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, gestión de seguridad de la información; gestión de los programas de continuidad de las operaciones y evaluación de la seguridad física del Centro de Datos principal y secundario (control de accesos, incendio, inundación, monitoreo,

enfriamiento, respaldos, replicación de datos, Plan de Recuperación ante Desastres (DRP), estándares).

Áreas Revisadas

La Dirección Adjunta de Administración (DAA), la Dirección Adjunta de Desarrollo Tecnológico (DADT), Dirección Adjunta de Administración de Proyectos, la Gerencia de Administración Integral de Infraestructura y la Gerencia de Sistemas de Información Estratégicos.

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. Código Fiscal de la Federación: Art. 81

2. Otras disposiciones de carácter general, específico, estatal o municipal: ACUERDO que tiene por objeto emitir 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 establecer el manual administrativo de aplicación general en dichas materias: Art 10, fracción VII y 27, fracción II.

   Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información (MAAGTICSI): Proceso I.A, Actividad del Proceso PE 1, Factor Crítico 7; Proceso II.A, Actividad del Proceso ADS 1, ADS 2, Factores Críticos 1, Inciso h), Fracción viii, ADS 3 y ADS 4; Actividad del Proceso ADS 3, Factores Críticos 5, Inciso d) y 6; Factor Crítico 3 y ADS 4 ; Proceso III.A., Actividad del proceso ADP 6, Relación de los productos del Proceso 3; Proceso I.B, Actividad del Proceso APCT 4, Factor crítico 6, Inciso d); Proceso II.B, Actividad del Proceso ACNF 4; Proceso II.C, Actividad del Proceso ASI 5; Proceso III.B, Actividad del proceso APRO 2; Actividades del Proceso ASI 3, ASI 4, ASI 5 y ASI 7; Proceso III.C, objetivos específicos 1 y 2, Actividad del Proceso AOP, Factor Crítico 1, Inciso b); Actividad del Proceso AOP 6, factores críticos 4, Inciso e y 5, inciso b; Proceso: III.D, Actividades del Proceso OPEC 2, OPEC 3 y OPEC 6;

   Cláusula Décima del Contrato LPN/01/09/15;

   Anexo Único del Contrato: Tabla 5;

   Manual de la Gestión del Servicio (MGS): Sección 8, procesos de resolución.

   Procedimiento para la Gestión de Incidentes y Solicitudes de Servicio: numerales 4.1, 4.2, 4.3, 4.4, 6.2

   Contrato AD/15/03/16: Cláusulas segunda, cuarta, sexta;

   Anexo Técnico del Contrato AD/15/03/16: Numerales 1.12. Penalización y Deducciones al Pago; 1.10. Entregables; 1.11. Niveles de servicio; 1.2 Consideraciones generales del servicio; 2 "Transformación mediante procesamiento de información"; 4.11 Personal para la administración del STAAI; 4 Servicios de Administración, Operación, Soporte y Mantenimiento, Quinto Punto; 4.9.5.3.2 Administración de los Estándares de Configuración, Primer Punto; 4.10 Soporte Técnico, Tercer Punto; 4.10.4.2 Apoyo Técnico Segundo y Tercer Punto; 4.13 Mesa de Ayuda; 4.15 "Altas, Bajas y Cambios", Primer Punto; 10 Niveles de Servicio.

   Norma ISO/IEC 20000-1:2011: Requisito 8.1 Gestión de Incidentes y Solicitudes de servicio;

Función de ITIL "Mesa de Servicios": Proceso Service Management;

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.