Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-1-06G3A-15-0086-2018

86-GB

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	133,733.0
Muestra Auditada	38,284.3
Representatividad de la Muestra	28.6%

El universo seleccionado por 133,733.0 miles de pesos corresponde al total de recursos asignados en Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2017; la muestra auditada se integra por tres contratos para prestar los servicios de Renovación Tecnológica de Cómputo Central; Mantenimiento Preventivo, Correctivo, Evolutivo y Adaptativo del Sistema de Control de Gestión y Servicio Integral de Comunicaciones y Seguridad con pagos ejercidos por 38,284.3 miles de pesos, que representan el 28.6% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de las acciones de TIC por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros en 2017, relacionadas con el Gobierno y Administración de las TIC, Gestión de la Seguridad de la Información, Continuidad de las Operaciones y Centro de Datos, entre otras.

Antecedentes

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), tiene como finalidad promover, asesorar, proteger y defender los derechos e intereses de los usuarios frente a las instituciones financieras, arbitrar sus diferencias de manera imparcial y proveer la equidad en las relaciones entre éstos, así como supervisar y regular, de conformidad con lo previsto en las leyes financieras, y de sus instituciones, a fin de procurar la protección de los intereses de los usuarios.

Durante 2017, la CONDUSEF contó con dos proyectos estratégicos de TIC, el primero consistió en la “Ampliación del Módulo de Atención en el Exterior (MAEX) y su conexión al Sistema de Información Operativa (SIO)”, que tiene por objetivo orientar y ayudar a los connacionales en Estados Unidos, otorgando asesoría financiera y ayudando a resolver alguna queja ante

instituciones financieras en México. El segundo fue la "Fase de operación del Sistema Integral de Evaluación y Supervisión (SIES)" que tiene el objetivo de mejorar el control del proceso y reducción de tiempos para cumplir en tiempo y forma con servicios institucionales derivados como es el Buró de Entidades Financieras; ambos proyectos se encuentran alineados al Plan Nacional de Desarrollo y fueron desarrollados con recursos de la Entidad.

Entre 2013 y 2017, en la CONDUSEF se han invertido 581,240.7 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la siguiente manera:

Recursos invertidos en materia de TIC
(Miles de pesos)

PERIODO DE INVERSIÓN	2013	2014	2015	2016	2017	TOTALES
MONTO POR AÑO	86,887.7	107,746.1	124,561.7	128,312.2	133,733.00	581,240.7

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

Resultados

1. Análisis Presupuestal

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2017, se concluyó que la CONDUSEF ejerció un presupuesto de 705,809.7 miles de pesos, de los cuales 133,733.0 miles de pesos, corresponden a recursos relacionados con las TIC, lo que representan el 18.9% del total, como se muestra a continuación:

Recursos ejercidos en 2017
(Cifras en Miles de Pesos)

Capítulo	Descripción	Presupuesto	Presupuesto Pagado TIC	%
1000	Servicios personales	477,539.3	40,342.1	8.4
2000	Materiales y suministros	4,065.4	-	0.0
3000	Servicios generales	214,861.5	93,390.9	43.5
4000	Transferencias, asignaciones, subsidios y otras ayudas	9,343.5	-	0.0
	TOTAL	**705,809.7**	**133,733.0**	**18.9**

Fuente: Elaborado con la información proporcionada por la CONDUSEF.

Nota: Diferencias por redondeo.

Los recursos ejercidos en materia de TIC por 133,733.0 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2017 CONDUSEF
(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PROFESIONALES**	**40,342.1**
3000		**SERVICIOS GENERALES**	**93,390.9**
	31401	Servicio telefónico convencional	1,055.3
	31701	Servicios de conducción de señales analógicas y digitales	11,031.4
	31901	Servicios integrales de telecomunicación	32,908.9
	31904	Servicio integrales de infraestructura de computo	19,778.8
	32301	Arrendamiento de equipo y bienes informáticos	9,257.5
	32701	Patentes, Regalías y Otros	7,565.0
	33301	Servicios de Informática	3,881.1
	33304	Servicios de mantenimiento de aplicaciones informáticas	1,235.3
	33602	Otros servicios comerciales	5,381.0
	33606	Servicios de digitalización	551.8
	39801	Impuesto sobre nóminas	744.8
		TOTAL	**133,733.0**

Fuente: Elaborado con la información proporcionada por la CONDUSEF.

Nota: Diferencias por redondeo.

Las partidas específicas relacionadas con servicios personales (capítulo 1000), se corresponden con los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 40,342.1 miles de pesos durante el ejercicio fiscal 2017; considerando 84 plazas, el promedio anual por persona fue de 480.3 miles de pesos.

Por otra parte, del universo por 133,733.0 miles de pesos que corresponde al total de recursos asignados en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal 2017, se erogaron recursos por 38,284.3 miles de pesos en tres contratos que representan el 28.6% del universo, el cual se integra de la siguiente manera:

Muestra de Contratos Ejercidos durante 2017 por la CONDUSEF

(Miles de Pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2017
				Del	Al	Mínimo	Máximo	
Licitación Pública Nacional Mixta	CONDUSEF/053/2013	S&C CONSTRUCTORES DE SISTEMAS, S.A. DE C.V.	Servicio de Renovación Tecnológica de Cómputo Central	11/11/2013	31/12/2016	26,058.2	65,145.6	8,566.5
	Convenio modificatorio CONDUSEF/053/2013-1		Modificación de precio e inicio del servicio		31/05/2017	3,619.5	9,048.7	
	Convenio modificatorio CONDUSEF/053/2013-2		Modificación de precio y vigencia		31/07/2017	979.0	2,447.6	
				Subtotal		30,656.7	76,641.9	8,566.5
Adjudicación directa	CONDUSEF/047/2015	OPERBES, S.A. DE C.V. y BESTPHONE, S.A. DE C.V.	Servicio Integral de Comunicaciones y Seguridad	20/08/2015	20/10/2018	46,480.1	92,960.3	27,875.2
Adjudicación directa	CONDUSEF/027/2017	ASESORIA Y CONSULTORIA EN SOFTWARE, S.A. DE C.V.	Servicio de Mantenimiento Preventivo, Correctivo, Evolutivo y Adaptativo del Sistema de Control de Gestión	01/03/2017	31/12/2017	-	1,842.6	1,842.6
				Total		**77,136.8**	**171,444.8**	**38,284.3**

Fuente: Información proporcionada por la CONDUSEF.

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

2. Contrato CONDUSEF 053/2013 “Servicio de Renovación Tecnológica de Cómputo Central”

Se analizó el contrato abierto plurianual 053/2013 y sus convenios modificatorios CONDUSEF/053/2013-1 y CONDUSEF/053/2013-2, celebrados con la empresa S&C Constructores de Sistemas S.A. de C.V., mediante el procedimiento de licitación pública mixta número LA-006G3A001-N122-2013 con fundamento en los artículos 26 fracción I, 26 bis fracción III, 27, 28 fracción I, 29, 30, 32 segundo párrafo y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con vigencia del 11 de noviembre de 2013 al 31 de julio de 2017, por un monto mínimo de 30,656.7 miles de pesos y un monto máximo de 76,641.9 miles de pesos, para la prestación del “Servicio de Renovación Tecnológica de Cómputo Central ”, de los cuales durante el ejercicio 2017 se pagaron 8,566.5 miles de pesos.

Alcance

El alcance de los trabajos se integró por los servicios administrados de licenciamiento, infraestructura y servicios profesionales, para operar toda la infraestructura de cómputo central, los sistemas, aplicaciones y las bases de datos, con la finalidad de mantener niveles de servicio que aseguren su continua operación desde la instalación inicial y durante los incrementos futuros dentro de la vigencia del contrato.

Proceso de Contratación

En relación con la Investigación de Mercado, se carece de los elementos siguientes:

- Como mínimo dos fuentes documentales para su elaboración
- Condiciones similares en cuanto a plazos y lugares de entrega de los bienes y servicios
- Moneda a cotizar
- Forma y términos de pago
- Características técnicas de los bienes o servicios.

Sobre el Estudio de Factibilidad no se incluyeron los costos de mantenimiento, soporte y operación vinculados con el factor de temporalidad más adecuado para determinar la conveniencia de contratar servicios.

Respecto de la contratación plurianual, no se identificó la justificación de las ventajas económicas o que sus términos o condiciones son más favorables, así como que no afectará negativamente la competencia económica en el sector.

Obligaciones del Prestador de Servicios

En cuanto a los esquemas de alta disponibilidad, la CONDUSEF comentó que se validaba diariamente que ésta se encontrara activa en las bases de datos, pero no dejaba evidencia de ello, ni validaba la redundancia de los elementos de hardware; en cuanto a los equipos de comunicaciones, no se identificó un análisis para sustentar que la configuración de los mismos es adecuada para evitar riesgos a la entidad; asimismo, durante 2017 no fueron aplicados los parches y actualizaciones liberados por los fabricantes de los manejadores de bases de datos y software de virtualización.

En relación con el mantenimiento correctivo, se identificó un caso en el que se reemplazó un disco y no se aplicó el borrado seguro, por lo que los datos contenidos podrían ser recuperados y quedar expuestos; asimismo, para dar soporte el proveedor utilizaba cuentas del personal de la entidad, por lo que no habría sido posible establecer las responsabilidades de las acciones ejecutadas en caso de haber sido necesario; además, en 2017 no se ejecutó una validación de las competencias y habilidades del personal asignado por el proveedor.

Se carece de evidencias de revisión por la CONDUSEF respecto de la documentación proporcionada por el proveedor, incluyendo el Procedimiento de Atención en la Mesa de Ayuda y la Matriz de Escalamiento, la cual tampoco señalaba el personal con quien podía ser escalado un reporte fuera de los horarios de oficina, en virtud que se trataba de un servicio de 24 horas.

La CONDUSEF no recibía ni elaboraba reportes de monitoreo de los niveles de servicio, en consecuencia, no podía determinar los tiempos en que los servicios no estaban disponibles, a pesar de esto, documentó que el proveedor cumplía al 100.0% con los niveles pactados, los cuales estaban acordados con base en la severidad de la falla, la cual no quedaba documentada en los reportes de atención. El tiempo máximo de atención para las fallas de menor severidad era de 24 horas; sin embargo, se identificó un caso que rebasó el tiempo por más de 12 horas, sin quedar registro del incumplimiento ni aplicación de penalizaciones.

Especificaciones Técnicas Mínimas Requeridas

El proveedor provisionó los servidores; sin embargo, se identificó que en las Memorias Técnicas no se registraron algunos de ellos, tampoco hay evidencia de que sus características fueran acordes a lo requerido. Asimismo, para el software de virtualización, servidores web y respaldos, no se identificó que se hiciera referencia al licenciamiento de la base de datos.

En relación con la confidencialidad de la información, la entidad confirmó que después de revisar el expediente del contrato, no se identificó que se cuente con Carta de Confidencialidad o algún documento similar firmado con el proveedor.

En cuanto a las memorias técnicas, no se identificó que la entidad las haya revisado para comprobar la adecuada implementación de los componentes de hardware, software y servicios profesionales que integran la solución.

El contrato y su anexo técnico señalan las características que deben cumplir los equipos de hardware, el software, los entregables y requerimientos citados en los puntos anteriores; sin embargo, la documentación no indica que se deba aplicar penalización o deducción alguna en caso de incumplimiento; se observó que las Memorias Técnicas se encuentran fechadas entre el 5 de septiembre de 2014 y el 27 de enero de 2015, es decir, hasta 391 días después de la entrada en operación del servicio, cuando el máximo establecido eran 70 días.

Transferencia de Conocimientos y Capacitación Certificada

El proveedor capacitó al personal del Departamento de Redes y Telecomunicaciones de la CONDUSEF en relación con los equipos de hardware instalados, así como en los servicios de virtualización, migración de aplicativos y bases de datos, almacenamiento de información, directorio activo y correo electrónico. A pesar de esto, la capacitación del proveedor no acreditó lo estipulado en el Anexo I, que estableció 16 cursos para 54 personas, de los cuales sólo se identificaron 10 certificados. Sin embargo, ni el contrato, ni su anexo técnico indican que se deba aplicar penalización o deducción alguna en caso de incumplimiento, tampoco se cuenta con un desglose del costo de los servicios.

Penas Convencionales y Deductivas

En la revisión del cumplimiento de los servicios, se detectó el caso número 2006973675 que fue atendido con dos incidentes diferentes, el primero inicia cuando la herramienta Netapp detecta la falla en un disco del servidor y envía el alertamiento al proveedor, el segundo reporte fue generado para la colocación del disco nuevo; el primero tiene un retraso de 12 horas y 53 minutos adicionales a las 24 horas establecidas para solucionar este tipo de incidentes, mientras que el segundo reporte es atendido dentro del tiempo establecido contractualmente, dado lo anterior, las deductivas no aplicadas son las siguientes:

Cálculo de deducciones no aplicadas en el contrato CONDUSEF 053/2013
(Miles de Pesos)

		A	B	C	D=A*B*C
Descripción	**Nivel de servicio**	**Horas excedidas**	**Costo mensual del servicio**	**Deducción**	**Monto**
Falla de nivel de Severidad 4	Solución en un tiempo máximo de 24 horas en sitio	12	1,223.8	0.005	73.4
				Total	73.4

Fuente: Información proporcionada por la CONDUSEF.

Para cumplir con su visión de ser un organismo efectivo para la protección y defensa de los intereses y derechos de los usuarios ante las instituciones financieras, la CONDUSEF requiere de una plataforma de cómputo institucional que opere las aplicaciones e infraestructura con óptima calidad que asegure su continua operación, es por ello que la carencia de controles para el monitoreo y medición de los niveles de servicio, pone en riesgo que sus servicios siempre se encuentren disponibles.

2017-1-06G3A-15-0086-01-001 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros instrumente los mecanismos de control que le permitan llevar a cabo de manera periódica el monitoreo, verificación y registro oportuno del cumplimiento de los Acuerdos de Niveles de Servicio (SLA), así como de las obligaciones del proveedor estipuladas en los contratos y anexos técnicos en materia de TIC; asimismo, implementar procedimientos de revisión, análisis, autorización y monitoreo periódico de los entregables provistos por los prestadores de servicios, con la finalidad de asegurar el cumplimiento de los compromisos contractuales, así como la entrega eficaz, eficiente y oportuna de los bienes y servicios objeto de los contratos.

2017-1-06G3A-15-0086-01-002 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros establezca penas convencionales y deductivas por cada una de las responsabilidades principales del proveedor en los contratos en materia de TIC, de manera que en todos los casos sea posible asegurar el cumplimiento de éstas y en caso contrario, aplicar las sanciones correspondientes. Adicionalmente, se incluya dentro de los contratos las políticas de entrega de servicios, seguridad de la información y operación de la entidad, con la finalidad de garantizar el Gobierno efectivo de las Tecnologías de Información por parte de la Comisión.

2017-1-06G3A-15-0086-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 73,428.00 pesos (setenta y tres mil cuatrocientos veintiocho pesos 00/100 m.n.), por la falta de aplicación de deducciones por incumplimiento de los niveles de servicio en el caso número 2006973675, debido a que no se diseñaron ni implementaron controles para llevar a

cabo mediciones de los niveles de servicio y asegurar su cumplimiento conforme a lo establecido contractualmente; en contravención a lo establecido en el Contrato No. CONDUSEF/053/2013 con objeto de la prestación del Servicio de Renovación Tecnológica de Cómputo Central.

3. Contrato CONDUSEF/047/2015 "Servicio Integral de Comunicaciones y Seguridad"

Se analizó el contrato núm. CONDUSEF/047/2015 celebrado con las empresas Operbes, S.A. de C.V. y Bestphone, S.A. de C.V., mediante el procedimiento de adjudicación directa, la cual se fundamentó en los artículos 22, fracción II, 25 y 26, fracción III, 40 y 41 fracción III y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con lo cual se adhirió al contrato marco no. LPNE-26-31701-481/2013 firmado entre la Secretaría de Hacienda y Crédito Público (SHCP) y las mismas empresas; el contrato CONDUSEF/047/2015 tiene vigencia del 20 de agosto de 2015 al 20 de octubre de 2018, por un monto mínimo de 46,480.1 miles de pesos y monto máximo de 92,960.3 miles de pesos, con objeto de la prestación del "Servicio Integral de Comunicaciones y Seguridad" para la CONDUSEF, durante el ejercicio 2017 se realizaron pagos por 27,875.2 miles de pesos; se determinó lo siguiente:

Alcance

Es un servicio administrado integral para abastecer toda la infraestructura de MPLS (enlaces de red de conmutación de etiquetas multiprotocolo), Internet y seguridad perimetral, así como los servicios profesionales para asegurar su continua operación en todas sus oficinas a nivel nacional. El servicio incluyó el abastecimiento de equipo y el uso de licencias para la prestación del servicio, considerando el soporte técnico, mantenimiento preventivo y correctivo, así como los servicios administrados para su instalación, configuración, migración, puesta a punto y continua operación, aunado a la trasferencia de conocimientos para el adecuado uso de la plataforma tecnológica.

Proceso de Contratación

En relación con la Investigación de Mercado, no se cuenta con un documento formal de la evaluación realizada por la entidad que considere un análisis de los apartados siguientes:

- Condiciones equivalentes en cuanto a los plazos y lugares de entrega de los servicios
- Moneda a cotizar
- Forma y términos de pago
- Características técnicas de los bienes o servicios
- Circunstancias para la comparación objetiva entre servicios de la misma naturaleza

Servicios de Red Privada Virtual y de Seguridad de la Red Institucional

La Comisión no tiene consolidados la totalidad de los servicios, tal como lo manifestó en su justificación para dictaminar la excepción a la licitación pública, por lo que no se puede asegurar que son atendidas completamente sus necesidades operativas, entre las cuales se encuentran el garantizar una adecuada navegación en Internet mediante la administración del ancho de banda y su monitoreo, así como la integridad, confidencialidad y disponibilidad de la información mediante diversas herramientas de seguridad que protejan el perímetro de

la red institucional, evitando entre otros, código malicioso, intrusos, robo de información y correo basura.

Aprovechamiento del Ancho de Banda

Respecto del uso del Ancho de Banda, se observaron promedios de entrada y salida a nivel nacional del 31.0% y del 15.0% respectivamente, salvo el caso del nodo del edificio sede en donde se observó un nivel de uso del 88.0% y del 52.0% para entrada y salida, respectivamente.

El uso de memoria promedio fue del 31.8%, mientras que para la Unidad Central de Procesamiento de los dispositivos de red se registró una media del 1.2%. Cabe señalar que la entidad sólo tiene disponibles las estadísticas de los consumos del último mes, por lo que no cuenta con un análisis histórico del uso de los servicios; dichos promedios de uso a la fecha de la auditoría (mayo 2018) son los siguientes:

Promedio de uso de los servicios por nodo del contrato CONDUSEF/047/2015 del mes de abril 2018

Tipo de Nivel	Máximo	Mínimo	Promedio
Uso de Ancho de Banda (Entrada)	88.0%	18.0%	**31.0%**
Uso de Ancho de Banda (Salida)	59.0%	4.0%	**15.0%**
Consumo de Memoria	33.9%	19.3%	**31.8%**
Consumo de CPU	2.0%	1.0%	**1.2%**

Fuente: Elaborado por la ASF con información proporcionada por la CONDUSEF.

De lo anterior, se concluyó que el promedio de uso corresponde a la tercera parte de los niveles de servicio contratados, lo que impacta al criterio de eficiencia de las adquisiciones, debido a que entre otros factores; la entidad no realizó un plan de capacidades de infraestructura tecnológica previa a la contratación, ni durante el tiempo de la prestación de los servicios, aunado a que las condiciones de operación de la contratación mediante la adhesión a un contrato marco no fueron la mejor opción para la entidad.

Equipos de Videoconferencia

La entidad no cuenta con mecanismos para validar el nivel de disponibilidad del 99.85% pactado en el contrato, respaldo de datos y almacenamiento, así como el cifrado para videoconferencia en sala y escritorio.

Centros de Operación de Red y de Seguridad (NOC/SOC)

Respecto de la verificación del cumplimiento de los requisitos de los centros de operación de red y de seguridad, la entidad informó que no ha realizado una validación para asegurar que la prestación de los servicios sea conforme a lo establecido en el anexo técnico del contrato.

Firewall para Aplicaciones Web (WAF)

La entidad mencionó que han realizado pruebas de análisis de vulnerabilidades dinámicos desde internet y han creado excepciones en las políticas del Firewall para Aplicaciones Web (WAF), para poder realizar las evaluaciones de las cuales se han generado los reportes pertinentes; no obstante, no se ha validado la aplicación de las medidas para disminuir los

riesgos de los hallazgos; asimismo, en el reporte se menciona que el 56.0% de los incidentes están relacionados con aplicativos, por lo que para su correcta mitigación se tendrá que trabajar con las áreas de Desarrollo de Sistemas, lo que eleva la calificación del riesgo dada la falta de control de autenticación al solicitar recursos del aplicativo.

Niveles de Servicio

La entidad únicamente ha establecido controles para verificar el cumplimiento de los niveles de servicio que se encuentran relacionados con la disponibilidad de los enlaces, aun cuando el proveedor entrega reportes relacionados con actividades sospechosas e incidentes de seguridad, pérdida de paquetes, latencia, consumo de ancho de banda, consumo de memoria y procesador por nodo y cambios en la infraestructura; sin embargo, la entidad no ejecuta actividades para validar la exactitud de la información contenida en dichos reportes. Asimismo, para los servicios de la Unidad de Control Multipunto (MCU) que gestiona el servicio de videoconferencias y disponibilidad de Internet, no se cuenta con elementos de medición que le permitan establecer esquemas de monitoreo de niveles de servicio y el proveedor no está obligado a entregar reportes al respecto.

Pruebas del Servicio Integral de Comunicaciones y Seguridad

Se llevaron a cabo una serie de pruebas con el objetivo de verificar que los servicios relacionados con la prestación del servicio integral de comunicaciones y seguridad, hayan sido entregados de acuerdo con lo estipulado en el contrato, los resultados son los siguientes:

Pruebas del Servicio Integral de Comunicaciones y Seguridad del contrato CONDUSEF/047/2015

Servicio	Prueba	Observación
Balanceo de cargas y redundancia en medio, CPE y nodo.	Verificación de la evidencia de la configuración del balanceo de cargas.	El balanceo de cargas únicamente está considerado en el nodo de la oficina central, contrario a lo establecido en el anexo técnico, el cual indica que debe estar implementado en los nodos de alta criticidad. Esto se debe a que los nodos están subutilizados y por lo tanto el balanceo de cargas no es necesario.
	Verificación de los niveles de carga en los enlaces primarios y secundarios.	Los niveles de carga en los enlaces primarios son mínimos por lo que no se aplica el balanceo de cargas. En delegaciones no se tiene balanceo.
Servicio de Firewall/IPS/WAF	Validar el porcentaje de uso del procesador en los Firewalls e IPS (Prevención de intrusos)	Se observó que el uso de Firewall de uno de los nodos fue del 75%, mientras que el otro registró un uso del 26%; sin embargo, la CONDUSEF no cuenta con información histórica de este monitoreo.
	Revisar el estado de atención a las observaciones derivadas del análisis dinámico (WAF), relacionadas con autenticaciones, códigos maliciosos y exposición de metadatos.	La entidad no ha validado si las mejoras recomendadas han sido aplicadas por el proveedor.

Fuente: Elaborado por la ASF con información proporcionada por la CONDUSEF y el resultado de las pruebas

Mantenimiento

El mantenimiento preventivo se ejecuta a discreción del proveedor, dado que no se estableció un calendario para tal efecto. Cuando el proveedor ejecuta las actividades preventivas o correctivas, se identificó que la entidad no valida la correcta aplicación de éstas, únicamente verifica al día siguiente la disponibilidad de los enlaces, aunado a que la entidad no supervisa las actividades ejecutadas por el proveedor, lo que pone en riesgo las operaciones e información bajo su resguardo.

Calidad de Servicio

Atendiendo a lo establecido en el contrato, la entidad tenía la facultad de verificar directa, indirecta por medio de un tercero, si el prestador del servicio se encontraba desarrollando correctamente el objeto del contrato de acuerdo con las especificaciones contenidas en el mismo, lo cual no se ejecutó adecuadamente debido a que:

- No fueron programadas revisiones ni actualizaciones al programa de continuidad de las operaciones durante 2017
- Se observaron capacidades subutilizadas en lo que se refiere al uso de banda ancha, procesadores y memoria de los servidores
- No fueron validadas las características de los servicios de videoconferencia, acceso a Internet, Firewall para aplicaciones Web (WAF) ni los Centros de Control de las Redes
- La entidad no validó que se mitigaran los riesgos detectados en el análisis de vulnerabilidades
- Se incumplió con el objetivo de la adhesión del contrato para contar con servicios consolidados, debido a que la CONDUSEF no solicitó servicios tales como análisis de tráfico de voz y datos, optimización de ancho de banda y aceleración de información, contención de ataques en el perímetro de internet, sistema de nombres de dominio, prevención de fuga de información, filtrado de correo electrónico, monitoreo administrado y soporte activo, entre otros

Por lo anterior, se concluye que existen deficiencias en la validación del desempeño de los servicios que conforman el contrato, debido a que la CONDUSEF no implementó controles que le permitieran dar un adecuado seguimiento al cumplimiento de las obligaciones del proveedor.

2017-1-06G3A-15-0086-01-003 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros fortalezca los procedimientos y controles para realizar investigaciones de mercado que permitan verificar la oferta de bienes, arrendamientos o servicios de TIC de manera pormenorizada, así como actualizar los precios de referencia de los requerimientos específicos, con la finalidad de cumplir con las necesidades de la contratación y obtener las mejores condiciones para la entidad, debido a que el servicio de ancho de banda obtenido mediante la adhesión a un contrato marco, es varias veces superior a las necesidades de la Comisión.

2017-1-06G3A-15-0086-01-004 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implemente un programa de capacidad de la infraestructura tecnológica que garantice que todos los servicios de TI cuenten con un correcto dimensionamiento para el procesamiento, almacenamiento y transmisión de datos, con la finalidad de que los recursos sean aprovechados adecuadamente y se aseguren los niveles de servicio requeridos para una óptima operación de la entidad, evitando la subutilización de la infraestructura, como fue el caso del consumo del procesamiento y memoria de los servidores en el servicio integral de comunicaciones y seguridad; lo anterior, para que las contrataciones en materia de TIC cumplan con los criterios de economía y eficiencia que deriven en mejores condiciones para la Comisión.

2017-1-06G3A-15-0086-01-005 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros diseñe y ejecute un plan para el análisis de vulnerabilidades a los aplicativos que soportan los procesos sustantivos de la entidad, con la finalidad de identificar todos los riesgos para las operaciones y aplicar acciones de remediación que disminuyan de forma expedita todas las posibilidades de riesgo alto, así como buscar una solución a corto plazo para todas aquellas vulnerabilidades de riesgo medio y bajo.

2017-9-06G3A-15-0086-08-001 **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 la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión del contrato número CONDUSEF/047/2015 para la prestación del Servicio Integral de Comunicaciones y Seguridad, se detectaron irregularidades vinculadas con las responsabilidades de los titulares de la Dirección General de Desarrollo Financiero, Estadístico y de Tecnologías de Información, Subdirección de Informática y Telecomunicación, Departamento de Redes y Telecomunicaciones, Departamento de Desarrollo y Mantenimiento de Sistemas, debido a las deficiencias en los controles que le permitan asegurar que los servicios contratados se otorguen adecuadamente, poniendo en riesgo el acceso a los servicios tecnológicos como internet, correo electrónico, directorio activo, multifuncionales, biométricos, servicios de trasferencia de video para sesiones remotas, optimización de la navegación en internet mediante la administración del ancho de banda, protección de los portales Web institucionales para su operación continua, mantenimientos preventivos ejecutados oportunamente y la utilización de las redes con protocolos seguros para la transmisión de información.

4. Contrato CONDUSEF/027/2017 “Servicio de Mantenimiento Preventivo, Correctivo, Evolutivo y Adaptativo del Sistema de Control de Gestión”

Se analizó el Contrato No. CONDUSEF/027/2017 celebrado con la empresa Asesoría y Consultoría en Software, S.A. de C.V., mediante el procedimiento de adjudicación directa con

fundamento en los artículos 25, 26, fracción III, 40 y 42; segundo párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con vigencia del 1º de marzo al 31 de diciembre de 2017, por un monto de 1,842.6 miles de pesos, para la prestación del "Servicio de Mantenimiento Preventivo, Correctivo, Evolutivo y Adaptativo del Sistema de Control de Gestión", de los cuales se pagó la totalidad del monto durante el ejercicio 2017; se determinó lo siguiente:

Alcance

Los servicios podían aplicarse en los módulos siguientes:

Descripción de los módulos del Sistema de Control de Gestión

MÓDULO	DESCRIPCIÓN
Memorándum electrónico inicial	Contiene las acciones para el registro y seguimiento de los memorándums electrónicos, que sirven de comunicación entre las distintas áreas de la institución.
Memorándum electrónico de respuesta	Este módulo sirve para dar seguimiento a una solicitud de memorándum y formular la respuesta, ya sea turnando el asunto a otra instancia o bien redactando directamente el memorándum de respuesta.
Módulo de préstamo de expedientes	En este módulo se encuentran las opciones para dar de alta las solicitudes de préstamos de expedientes, dar el seguimiento adecuado, ver el reporte de expedientes prestados con uso de semáforos para identificar los que están en tiempo y los préstamos ya vencidos, además de contar con un reporte general de las solicitudes de préstamos de expedientes con la posibilidad de exportarlo a Excel.
Módulo de correspondencia de entrada	Este módulo cuenta con las opciones para registrar la mensajería que llega en la oficialía de partes y para darle seguimiento tiene su tablero de respuestas y diversos reportes.
Módulo de correspondencia de salida	Aquí se tienen las opciones para registrar la mensajería que será enviada fuera de CONDUSEF, tanto a una delegación o institución local o foránea. Cuenta con diversos reportes y un control de administración de guías foráneas.
Módulo de registro de expedientes(Antes ARCON)	Esta opción sirve para dar de alta las portadas de expedientes.
Módulo de inventario de uso múltiple (Transferencias)	Este módulo cuenta con las opciones para registrar y dar seguimiento a las transferencias documentales.
Módulo de ficha de valoración	Aquí se administran los elementos que componen el cuadro de clasificación archivística. Alta, baja y modificación de los rubros temáticos, la normatividad, secciones, series y subseries.
Enlace Sistema de expedientes digitalizados EDI	En este módulo se realizan búsquedas de expedientes utilizando distintos criterios, al momento de enlazarse con el sistema de digitalización, se pueden adjuntar imágenes digitalizadas a los expedientes.
Módulo mesa de ayuda	Segmento donde se registran y se atienden las incidencias del Sistema de Control de Gestión.
Módulo Acuses, etiquetas, formatos, instructivos y manuales	Formatos e información de apoyo para el correcto uso del sistema de control de gestión.

Fuente: Información proporcionada por la CONDUSEF

Mantenimientos Cancelados o No realizados

- Consulta Externa: con la finalidad de optimizar sus recursos, la entidad decidió que este requerimiento fuera atendido por el proveedor del Software de Administración, mediante un convenio modificatorio del contrato CONDUSEF/026/2017 "Software de Administración"; sin embargo, a la fecha de la auditoría (mayo 2018) no se tiene evidencia de la terminación y aceptación de este requerimiento.
- Administración de Formatos: la CONDUSEF señaló que como resultado de sus prioridades canceló el requerimiento de Administración de Formatos, sin proporcionar evidencia sobre cuáles eran dichas prioridades.
- Reporte de Productividad: la entidad determinó como no prioritario llevar a cabo la modificación relativa al "Reporte de Productividad", el administrador del contrato decidió dejar fuera los elementos "Exportar Memorándum", "Administración de Formatos", "Rol de Consulta Externa" y "Rediseño de Reportes".

El proveedor ocupó 42 horas (el 4.8% del total contratado) en levantar los requerimientos, analizar y diseñar los mantenimientos que fueron cancelados o no realizados (a un costo por hora de 1.3 miles de pesos), al considerarse no prioritarios, sin tener evidencia de la terminación de las fases de desarrollo, pruebas e implementación para las solicitudes, lo que derivó en la falta de integración de los componentes para su entrega e impidió el aprovechamiento de los recursos de TIC; por lo tanto, los pagos ejercidos por servicios no devengados son los siguientes:

Pagos no aprovechados del contrato CONDUSEF/027/2017

(Miles de Pesos)

	A	B	C	D=A+B+C	E	G= D*E
Requerimiento	**Definición de Requerimiento (horas)**	**Análisis y diseño (horas)**	**Construcción y Pruebas**	**Total de Horas**	**Costo por hora**	**Pagos no aprovechados**
Administración de Formatos	3	11	0	14	1.3	17.8
Consulta Externa	3	11	0	14	1.3	17.8
Reporte de Productividad	3	11	0	14	1.3	17.8
Total	**9**	**33**	**0**	**42**	**Total**	**53.4**

Fuente: Elaborado por la ASF con información proporcionada por la CONDUSEF

Diferencias por Redondeo

Responsabilidades y obligaciones del cumplimiento del contrato

En el análisis del servicio de mantenimiento preventivo, correctivo, evolutivo y adaptativo del Sistema de Información de Control de Gestión (SCG), se identificaron las inconsistencias siguientes:

- La Dirección de Gestión y Control Documental, no efectúa una validación para corroborar que el esfuerzo de los recursos, costos y tiempos de los mantenimientos del SCG sean los calculados y entregados por el proveedor
- El área de tecnología de la entidad no cuenta con herramientas que detecten y en su caso, eviten la instalación en el ambiente productivo de código malicioso o con fallas que pudiera afectar la operación de los aplicativos, tampoco gestiona el control de versiones, la administración de configuración, ni cuenta con procedimientos para desarrollar componentes de seguridad en los sistemas
- El SCG no es revisado mediante un análisis de vulnerabilidades de forma periódica, ni se tienen controles para la segregación de funciones en los ambientes de pruebas y producción a los que tiene acceso el proveedor, incluyendo modificaciones a las bases de datos
- La entidad carece de una herramienta para el monitoreo de las bitácoras de acceso a los sistemas y bases de datos, con la finalidad de detectar y evitar el acceso no autorizado de terceros
- No se cuenta con un procedimiento formalizado para la gestión de los cambios a los sistemas, inclusive el proveedor puede actualizar directamente el ambiente productivo, lo que pone en riesgo la integridad de los aplicativos que soportan la operación de la entidad

Desarrollo de Soluciones Tecnológicas

Se revisó el Sistema de Información Operativa Institucional (SIO) de la CONDUSEF, cuyo objetivo principal es brindar a las áreas de atención a usuarios, herramientas para registrar y dar seguimiento a las asesorías y controversias que presentan los usuarios de servicios financieros; respecto del cumplimiento de la metodología de desarrollo de software se determinó lo siguiente:

- Administración de Solicitudes de desarrollo de Software: para la gestión de las solicitudes no se utiliza un cronograma que muestre el control de la duración del proyecto, las fechas de inicio y fin de cada solicitud, e incluya hitos de control, desviaciones y riesgos potenciales ni se implementan indicadores para verificar el nivel de cumplimiento que tuvo la entidad de acuerdo con los cronogramas de trabajo.
- Planificación de solicitudes de desarrollo de software: el procedimiento para la aprobación de las solicitudes de desarrollo para SIO de las áreas usuarias se realiza de forma manual y no se utiliza una metodología para determinar la duración de las actividades solicitadas ni el número de recursos asignados por cada solicitud de desarrollo.

- Arquitectura Orientada a Servicios: el SIO no está implementado con esta Arquitectura, por lo que aún no genera funcionalidades reutilizables e interoperables entre diversas áreas de la Institución o entre otras instituciones.
- Aseguramiento de la Calidad: la entidad no tiene implementado un procedimiento formalizado de revisión a la calidad del código, componentes y productos de los desarrollos de software.
- Gestión de Cambios: en la metodología de desarrollo de software implementada por la entidad, no se consideran estándares de documentación, gestión de cambios, requerimientos de calidad y aprobación de las áreas involucradas, a fin de garantizar el cumplimiento con los requerimientos definidos. La Dirección de Informática; no tiene implementados controles para asegurar que las peticiones de cambio mantienen la integridad de la configuración de los componentes de la solución, ni solicita por parte del área usuaria, la evaluación del impacto en los módulos de la aplicación, sistemas existentes y seguridad basada en los resultados del análisis de riesgos.
- Plan de Riesgos: al planear el desarrollo de una solicitud al SIO, no se evalúan los riesgos que pueden afectar a la entidad ni al mismo desarrollo, tampoco se tienen implementados mecanismos para identificar y documentar los riesgos asociados a los requerimientos de las propuestas de desarrollo para SIO, a fin de determinar sus impactos y tratamientos; se carece de una metodología para la identificación, análisis, gestión, monitoreo y evaluación del proceso de riesgos.
- Plan de Pruebas: se carece de un plan de pruebas en la fase de diseño en donde se especifique la participación de determinados perfiles para la ejecución de las mismas; no se generan datos de prueba para el ambiente no productivo; se carece de un procedimiento mediante el cual se generen los datos de prueba para dicho ambiente; se carece de políticas para la planeación y ejecución de pruebas de desarrollo (Unitarias, Integrales y Funcionales), No funcionales (stress y seguridad), Funcionales (pruebas de aceptación del usuario) y Regresivas (en aquellos casos en que se integran o adicionan componentes de software a un módulo ya existente del SIO, para comprobar que la funcionalidad del aplicativo se mantenga inalterada y que la relativa al componente integrado o adicionado es consistente), finalmente, no se tiene un método para resguardar la documentación de las pruebas ejecutadas a las solicitudes de desarrollo y cambios a los sistemas.
- Cierre de Proyectos: se tiene implementado un formato de cierre con la firma de la Dirección General de Desarrollo Financiero, Estadístico y de Tecnologías de Información; sin embargo, se carece de la firma del usuario solicitante; asimismo, se carece de un repositorio único de información en donde se preserve y mantenga disponible la información del desarrollo de cada solicitud.
- Pase a Producción y Gestión de Código Fuente: no se tiene una herramienta de apoyo a la metodología de Desarrollo para el control de versiones, establecimiento de líneas base, y repositorio consolidado y organizado de todos los documentos generados durante el proyecto, la entidad carece de mecanismos formales que aseguren que las

bibliotecas de los desarrollos se encuentren actualizadas con la versión del componente de la solución que está siendo transferido a Producción, que se archive la versión existente y su documentación de soporte.

- Controles de Seguridad: la CONDUSEF no cuenta con controles implementados que protejan al código del SIO, sus componentes, productos y demás elementos relacionados con fines distintos a su desarrollo; no se tiene habilitada la bitácora de accesos de usuarios del sistema operativo; se carece de Políticas y Normas Generales de Seguridad de la Información, mediante las cuales se comuniquen los planes, medidas y acciones relativas al ámbito de sistemas para el tratamiento, protección y seguridad de los datos y medios informáticos; no se realizan análisis de vulnerabilidades previo al inicio de la puesta en operación de una solicitud de desarrollo de sistemas.

Como consecuencia de la revisión de la metodología de Desarrollo de Sistemas implementada por la CONDUSEF, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la entidad son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS	
Factor crítico	**Riesgo**
Análisis de Vulnerabilidades	La falta de ejecución de un análisis de vulnerabilidades a las solicitudes de desarrollo de sistemas antes de su puesta a producción, representa un riesgo en la disponibilidad de las funcionalidades de la aplicación, debido a que no se están protegiendo los recursos que forman parte del sistema a nivel hardware, software, telecomunicaciones y datos.
Segregación de los ambientes de Desarrollo y Producción	Debido a que se carece de controles para la segregación de los ambientes de desarrollo y producción, se identifica un riesgo para el código de los sistemas, sus componentes y productos, y demás elementos relacionados, pues no se tienen procedimientos que impidan que se copien, envíen, transmitan o difundan los programas con las debidas autorizaciones y pruebas de calidad para su correcto funcionamiento.
Análisis de Riesgos	El equipo de análisis de riesgos de desarrollo de software no tiene evidencia para identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos que da atención los módulos de los sistemas, de manera que se obtengan planes de remediación y mitigación para definir los controles a implantar de acuerdo con las capacidades y recursos de las áreas, para mantener aceptable el nivel de riesgos y evitar la materialización de las amenazas.
Plan de pruebas	Las pruebas son cruciales para determinar que se hayan validado los requerimientos del usuario, al no realizarse, se tiene el riesgo latente de que el sistema no esté funcionando de acuerdo con su diseño y que los controles internos no trabajen de acuerdo a las políticas de la entidad.
Producto para pruebas	Al no generarse datos de prueba, se identifica un riesgo en la información al poder caer en manos no autorizadas que pongan en riesgo su privacidad, además las pruebas pueden ser no representativas de la población a la que se prestan los servicios.
Administración de Problemas	La falta de gestión de los problemas; impide la identificación de las fallas que se presentan con mayor frecuencia, aunado a que no se puede definir el impacto que puede ocasionar un incidente. Lo que provoca deficiencias en la prevención e identificación de riesgos, así como en los mecanismos de respuesta para controlarlos, mitigarlos y erradicarlos.
Administración de Cambios	Los cambios a los programas deben ser probados y, eventualmente certificados para asegurar que realicen las funciones que se pretenden. Además de esto, si el análisis de riesgo determina que es necesario, se podrían requerir pruebas adicionales para asegurar que la funcionalidad existente, el desempeño del sistema y la seguridad del aplicativo, no se ve afectada por el cambio.

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS	
Factor crítico	**Riesgo**
Plan de Calidad	El aseguramiento de la calidad se enfoca en aspectos formales del desarrollo de software, tales como adherirse a estándares de codificación y a la metodología de desarrollo de la entidad, la cual al no tener un procedimiento para la revisión de los resultados y productos que se deben entregar en cada etapa, así como la confirmación del cumplimiento de los requerimientos, no está asegurando la calidad del sistema debido a que no mide el grado de alineación a la metodología, con la finalidad de proponer mejoras a los procedimientos de desarrollo de sistemas.
Gestión de Código Fuente	Se carece de procedimientos para el control de versiones en el código fuente de los programas, para poder revertirlos en caso necesario, lo que impide realizar cambios sobre los elementos almacenados de código fuente; asimismo, se carece de un registro histórico de las acciones realizadas con cada versión de código fuente, lo que puede causar afectaciones a la funcionalidad de aplicaciones e impactos a los activos de información.
Manual de Mantenimiento	Debido a la carencia de un manual de mantenimiento, no están establecidas las normas, organización y procedimientos que se utilizan en los sistemas para efectuar la función de mantenimiento en todos y cada uno de sus módulos. Lo anterior, genera un riesgo a los procesos porque no se encuentran ordenados, ni desarrollados de una manera satisfactoria, además se desconocen los posibles impactos por la falta de atención.
Manual Técnico	Al carecer de un manual técnico del sistema, no se identifica la estructura de datos que utiliza cada función, variable, metodologías de programación e interrelaciones con otros aplicativos. Al no tener esta documentación, se complica la realización de futuras modificaciones, ya que es difícil identificar la lógica de programación, por lo que representa un riesgo de cometer errores al retomar un proyecto o darle mantenimiento al sistema.
Administración de Proyectos	Debido a la carencia de una administración de proyectos, no se está asegurando que todas las iniciativas cuenten al menos, con su documento de planeación del proyecto, así como los planes subsidiarios, desde su inicio hasta su cierre, con la actualización en tiempo y forma de acuerdo con los avances de los mismos. Adicionalmente, se carece de controles para dar seguimiento al alcance, tiempo, riesgos y costos que pueden impactar de manera negativa al beneficio esperado por la entidad.

Por lo anterior, se reflejan deficiencias para la administración y desarrollo de soluciones tecnológicas, así como para contribuir en alcanzar una mayor eficiencia en los procesos institucionales.

2017-1-06G3A-15-0086-01-006 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros fortalezca los mecanismos de control para establecer procedimientos en el desarrollo de soluciones tecnológicas que le permitan: validar que el esfuerzo de los recursos, costos y tiempos estén debidamente calculados; detectar y evitar la instalación en el ambiente productivo de código malicioso o con fallas; establecer controles para la segregación de funciones en los ambientes de pruebas y producción; monitorear las bitácoras de acceso a los sistemas y bases de datos; así como instrumentar un procedimiento para la gestión de cambios a los sistemas.

2017-1-06G3A-15-0086-01-007 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implemente los mecanismos y controles para la elaboración de políticas, normas y procedimientos para el Desarrollo de Soluciones Tecnológicas, que le permitan estandarizar la entrega de productos de software, con la finalidad de garantizar un adecuado funcionamiento y mantenimiento de los mismos, considerando las mejores prácticas para

contar con elementos tales como: Gestión de Requerimientos; Plan de Riesgos; Plan de Pruebas; Gestión de Problemas; Plan de Calidad; Gestión del Código Fuente; Lineamientos para el Producto para Pruebas; Manual de Mantenimiento; Manual Técnico y Acta de Cierre del Proyecto, entre otros.

2017-9-06G3A-15-0086-08-002 **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 la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión del Sistema de Información Operativa Institucional (SIO), propiciaron irregularidades vinculadas con las responsabilidades de los titulares de la Dirección de Desarrollo y Evaluación del Proceso Operativo, Departamento de Desarrollo y Administración de Sistemas, Departamento de Redes y Telecomunicaciones, debido a las deficiencias en los controles para el cumplimiento de las directrices para la formulación, desarrollo y actualización de los sistemas informáticos; la administración y planificación de solicitudes de desarrollo de software; la ejecución del análisis de vulnerabilidades; la configuración de la arquitectura orientada a servicios; el aseguramiento de la calidad; la gestión de cambios; el plan de riesgos; el plan de pruebas; los controles de seguridad en los aplicativos; la segregación de ambientes de desarrollo y producción; así como la gestión del código fuente y gestión de problemas.

2017-1-06G3A-15-0086-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 53,456.11 pesos (cincuenta y tres mil cuatrocientos cincuenta y seis pesos 11/100 m.n.), por la carencia de evidencias de la terminación de las fases de desarrollo, pruebas e implementación para las solicitudes correspondientes a la "Administración de Formatos", "Consulta Externa" y "Reporte de Productividad", debido a que se invirtieron 42 horas en su definición de requerimientos, análisis y diseño, los cuales finalmente fueron cancelados, lo que originó la falta de integración de los componentes necesarios para su entrega, impidiendo el aprovechamiento de los recursos de TIC, lo que se constituyó en pagos ejercidos por servicios no devengados; en contravención a lo establecido en el Contrato No. CONDUSEF/027/2017 para la prestación del Servicio de Mantenimiento Preventivo, Correctivo, Evolutivo y Adaptativo del Sistema de Control de Gestión.

5. Gobierno y Administración de las TIC

Para evaluar los procesos de gobernabilidad y administración de las TIC, se analizó la información respecto de los Procesos de Planeación Estratégica, Administración de Proyectos y Administración de la Operación del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI); se identificó lo siguiente:

Establecer la gobernabilidad de las operaciones

- Se carece de un procedimiento formalizado para la elaboración del plan para la gestión de los Proyectos Estratégicos de TIC (PETIC).

- En 2017 no se contó con un procedimiento que alineara el PETIC con el Plan Nacional de Desarrollo y Programas Sectoriales, así como con las iniciativas orientadas a la mejora de los procesos sustantivos de la CONDUSEF.
- No se cuenta con un procedimiento para la toma de decisiones para la dirección y control de las TIC; tampoco, no se tienen planes alternativos para evitar que los proyectos se desfasen o tengan incumplimientos.
- No se tiene un procedimiento que defina los criterios para analizar las tendencias tecnológicas que sirvan como insumo para el diseño de la dirección tecnológica apropiada para cumplir con los objetivos y estrategias de TIC, acordes a las necesidades de la entidad.
- Se carece de una matriz de responsabilidades en donde se asegure que durante la gestión de proyectos se relacionen las actividades con los recursos (individuos o equipos de trabajo), logrando que cada uno de los componentes del alcance del proyecto esté asignado a una persona o a un equipo, en consecuencia, no se tiene una adecuada segregación de funciones.
- No se tiene implementado un procedimiento formalizado para determinar las fortalezas, oportunidades, debilidades y amenazas (FODA) del ámbito de las TIC. Por otro lado, la metodología de administración de riesgos se fundamenta en el FODA, el cual carece de una metodología que facilite el descubrimiento de conocimientos confiables, para solucionar los problemas, por lo anterior, se carece de un tablero de control de la situación actual que permita obtener un diagnóstico adecuado para la toma de decisiones en búsqueda del cumplimiento de los objetivos institucionales.
- No se cuenta con un procedimiento para evaluar el cumplimiento de los niveles de servicio establecidos para las contrataciones de TIC, en consecuencia, la entidad no conoce el desempeño de los servicios para identificar y proponer mejoras; también, carece de indicadores para determinar el rendimiento de las TIC.
- Se carece de una metodología para las actividades establecidas en la gestión de riesgos, en consecuencia, no se identifican, clasifican ni priorizan los riesgos para evaluar su impacto sobre las TIC, para generar planes de remediación, y así mantener aceptable el nivel de riesgo y evitar la materialización de las amenazas.
- No se generan estadísticas ni encuestas de niveles de satisfacción de los usuarios de TIC, con la finalidad de canalizar los recursos o mejoras a las iniciativas que dan los mayores beneficios.

Gestión de la Cartera de Proyectos de TIC

- No se tiene evidencia de la revisión, validación y autorización del grupo de trabajo en relación con el PETIC 2017.
- No se realiza la difusión del PETIC a la entidad.
- Se carece de procedimientos para el monitoreo del cronograma, gestión de desviaciones, medición de objetivos y cuadro de mando integral, en consecuencia, no se identifican los niveles críticos para apoyar la definición de acciones correctivas en

la estrategia del programa de proyectos, por lo que se carece de información del avance de la cartera operativa de proyectos y de los riesgos que deben ser tratados.

- No se cuenta con un procedimiento para la elaboración del anteproyecto anual de presupuesto de la Institución en lo relativo a TIC, tomando como criterios principales recursos financieros, materiales y humanos.
- Se carece de un procedimiento para la elaboración de los anexos técnicos y documentación en la contratación de bienes y servicios que contenga los requisitos funcionales y no funcionales.
- No se tiene designado un responsable para la gestión del portafolio de contratos de servicios, por lo que se tiene el riesgo del incumplimiento de los proveedores por la falta de seguimiento de los compromisos contractuales.

Monitorear la infraestructura de TIC en operación.

- No se cuenta con evidencia de la supervisión de incidentes por parte de la CONDUSEF; tampoco se tiene documentación para asegurar que los problemas fueron atendidos y resueltos a entera satisfacción de los usuarios.

Como resultado de la revisión de los procesos de gobernabilidad y administración de TIC, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la CONDUSEF son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL GOBIERNO Y ADMINISTRACIÓN DE LAS TIC	
Factor crítico	**Riesgo**
Metodología para la elaboración del PETIC	Al carecer de un procedimiento formal para alinear el PETIC con los objetivos institucionales, Plan Nacional de Desarrollo y programas sectoriales, existe el riesgo de que los proyectos estratégicos de la CONDUSEF, no estén acorde a las prioridades institucionales y a la cartera ejecutiva de proyectos de TIC, lo que puede propiciar que aporten un bajo valor a la entidad.
Metodología para FODA	El FODA permite identificar las principales fortalezas y debilidades de la entidad para el cumplimiento de sus objetivos y funciones, al no tener una metodología para su implementación; existe el riesgo de no llevar a cabo las acciones para la mejora y disponibilidad de recursos tecnológicos, así como para incrementar la calidad de los aplicativos sustantivos e infraestructura tecnológica; asimismo, la identificación de las debilidades permite crear planes de acción para su tratamiento y eliminación.
Niveles de Servicio	No se tiene implementado un mecanismo para verificar el cumplimiento de los niveles de servicio establecidos para los servicios de TIC, al no monitorear los niveles de servicio, la entidad carece de las actividades para informar el desempeño de las contrataciones de TI a la CONDUSEF, y no desarrolla controles que permitan identificar las mejoras necesarias. Aunado a lo anterior, no se crean indicadores para la toma de decisiones con la finalidad de obtener un mejor rendimiento de los proyectos.
Análisis de Riesgos	Se carece de un procedimiento para el descubrimiento de riesgos en las iniciativas de TIC, en consecuencia, la entidad no tiene asegurado que los riesgos (financieros, seguridad de la información, regulatorios, entre otros), sean evaluados y tratados en términos del impacto que pueden ocasionar a los procesos y servicios de la entidad.
Tablero de control de proyectos	Al no tener un tablero de control de proyectos, no se identifican los niveles críticos para definir las acciones correctivas a la estrategia del programa de proyectos; tampoco se verifica ni evalúa de manera continua el estado de cada uno de los proyectos de TIC, de acuerdo con sus hitos y puntos de control, para determinar su contribución a los objetivos de TIC; aunado a lo anterior, no se informa al grupo de trabajo para la dirección de TIC, por lo que carecen de información del avance de la cartera operativa de proyectos y de los riesgos que pueden presentarse.

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL GOBIERNO Y ADMINISTRACIÓN DE LAS TIC	
Factor crítico	**Riesgo**
Gestión de Compromisos Contractuales	Se carece de seguimiento en conjunto con el administrador del contrato, para corroborar que el proveedor de cada contrato, cumpla con las obligaciones estipuladas en el mismo, en consecuencia, no se controla el cumplimiento de obligaciones para comunicar cualquier incidente o desviación que se detecte al administrador de proyecto o a los responsables de los procesos involucrados para corregir las desviaciones.

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

De acuerdo a la CONDUSEF, en el período de enero a diciembre de 2017, recibió 1,343 reclamaciones en materia de consumos no reconocidos vía internet y 3,264,105 reclamaciones presentadas ante los bancos en materia de comercio por internet, por esta razón, es fundamental contar con los mecanismos para la adecuada gestión de los Proyectos Estratégicos de TIC y de una metodología para la Gestión de Riesgos Institucionales, con la finalidad de garantizar que las reclamaciones de los usuarios de servicios financieros sean atendidas y que el impacto de los riesgos sobre la tecnología para prestar dichos servicios este controlado.

2017-1-06G3A-15-0086-01-008 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implemente una metodología que permita asegurar la alineación de los Proyectos Estratégicos de Tecnologías de la Información y Comunicaciones (PETIC), con los objetivos Institucionales; la elaboración de la Planeación Estratégica; la creación de criterios de clasificación y priorización de las iniciativas; la definición de los parámetros para la conformación y seguimiento de la cartera de proyectos de las TIC; la identificación y tratamiento de las fortalezas, oportunidades, debilidades y amenazas del ámbito de las TIC, así como la gestión de proveedores que regule el cumplimiento de las obligaciones establecidas en los contratos.

2017-1-06G3A-15-0086-01-009 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros instrumente los procedimientos para la gestión de riesgos, que permita identificarlos, clasificarlos y priorizarlos para evaluar su impacto sobre los procesos y los servicios de la Institución; la elaboración de una matriz de segregación de funciones; la medición de los niveles de servicio de los proyectos; la gestión de incidentes para la resolución de todo tipo de problemas; así como la generación de estadísticas de niveles de satisfacción de los servicios de TI, con la finalidad de identificar los proyectos estratégicos para mejorar su gestión y resultados.

6. Gestión de la Seguridad de Información

En la revisión y análisis de la información relacionada con los Procesos de Administración de la Seguridad de la Información (ASI) y Operación de Controles de Seguridad de la Información y del ERISC (OPEC) del MAAGTICSI, así como las políticas y lineamientos proporcionados por la entidad, se detectaron las observaciones siguientes:

Políticas y Manejo de Contraseñas

- En las Políticas de Contraseñas no se tomaron en cuenta las mejores prácticas para determinar las reglas en la composición y tiempo de vida de las mismas, esto aplica en los distintos ambientes de sistemas operativos.
- Las contraseñas de los aplicativos sustantivos no son almacenadas de manera segura, en algunos de ellos se almacenan en claro, mientras que para otros se aplican algoritmos de cifrado débil, por lo que las credenciales de autenticación podrían estar en riesgo.
- Las credenciales de los aplicativos sustantivos también están expuestas cuando son transmitidas hacia los servidores para su autenticación, esto se debe a que no utilizan Certificados Digitales que brinden protección y confianza sobre el sitio de la aplicación, además otros son accedidos mediante el Protocolo de Transferencia de Hipertexto (HTTP) que es inseguro. Cabe señalar que algunos aplicativos utilizan el Protocolo Seguro de Transferencia de Hipertexto (HTTPS).

Altas, Bajas y Cambios en la Asignación de Privilegios de Usuarios

- Los procedimientos de administración de usuarios no se encuentran documentados, autorizados ni formalizados. La administración de usuarios dentro de la entidad es una función que se encuentra desagregada, el responsable de ejecutar las altas, bajas y cambios, varía dependiendo de la aplicación, lo cual propicia que los procedimientos de administración de usuarios sean diferentes para cada sistema.
- La ejecución de las Altas, Bajas y Cambios está a cargo del personal de desarrollo de sistemas, propiciando el incumplimiento en la segregación de funciones de las mejores prácticas, debido a que los programadores podrían otorgarse accesos no autorizados, lo que puede resultar en una mayor posibilidad de fraude, errores, irregularidades en los procesos, en el procesamiento de transacciones y en los reportes financieros.

Recertificación de Usuarios y Protección de Cuentas Privilegiadas

- Los aplicativos no cuentan con un esquema de recertificación de usuarios y privilegios, por lo que es posible que existan usuarios que ya no deban contar con acceso a las aplicaciones, o usuarios que cuenten con privilegios superiores a los que necesitan para llevar a cabo sus actividades; tampoco hay un mecanismo de bajas y cambios de privilegios basado en la información de Recursos Humanos, por lo que las áreas a cargo de la administración de usuarios no son informadas cuando un empleado causa baja o cambia de puesto.
- El Departamento de Redes y Telecomunicaciones trabaja directamente con cuentas privilegiadas, ya que no ha generado perfiles de usuario con privilegios específicos para la ejecución de sus actividades. Además, las cuentas privilegiadas no son resguardadas en una bóveda de contraseñas para requerir autorización para su uso, tampoco se han implementado procesos de monitoreo sobre las cuentas con privilegios especiales, para validar que todas las actividades ejecutadas se encuentren justificadas.

Borrado Seguro

- Durante 2017, la política de borrado seguro no se había desarrollado y a la fecha de la auditoría (mayo 2018), no se encuentra autorizada ni formalizada. Lo anterior ocasionó que el proveedor de servicios asociado al contrato de Cómputo Institucional retiró sus equipos debido a la finalización del contrato y no aplicó ningún procedimiento de borrado seguro, por lo que los datos almacenados en los equipos de cómputo central retirados podrían ser recuperados y quedar expuestos.

Clasificación de Activos Informáticos

- Los resultados plasmados dentro del catálogo de infraestructuras críticas 2017 no fueron obtenidos mediante la aplicación de una metodología formal. Debido a esto, no es posible asegurar que las infraestructuras de los aplicativos calificadas como críticas, sean las únicas que debieran aparecer con esta clasificación, sobre todo si se toma en cuenta que no hay documentación en la que se encuentre el análisis para la clasificación de la infraestructura asociada al resto de las aplicaciones.

Análisis de Vulnerabilidades

- La entidad atendió las vulnerabilidades clasificadas como críticas en tres aplicativos sustantivos y elaboró un plan de trabajo para los rangos menores; sin embargo, en los reportes de vulnerabilidades para el resto de los aplicativos e infraestructura tecnológica, se identificaron 404 vulnerabilidades que no se encuentran dentro del plan de trabajo, incluyendo 95 críticas y 13 de riesgo alto.

Comunicaciones Seguras

- Los servidores en los que se alojan los aplicativos sustantivos fueron escaneados durante las pruebas de auditoria y se identificaron vulnerabilidades de riesgo crítico, riesgo alto y medio, por lo que se incrementa el riesgo de que atacantes remotos logren hacerse de información sensitiva en texto claro.
- En cuanto a los túneles de Redes Privadas Virtuales (VPN) establecidos entre la entidad y terceros para el intercambio de información, se utilizan algoritmos de cifrado y validación de integridad de datos que son considerados inseguros, además se observó una conexión que solamente se utilizó para pruebas de concepto y no ha sido deshabilitada.

Antivirus

- En relación con los servidores que usan el sistema operativo Solaris, la entidad señaló que no se cuenta con software antivirus, por lo que se incrementa el riesgo de afectación a la operación de la Comisión sin que se identifiquen y ejecuten acciones para su contención o eliminación de forma oportuna.

Líneas Base de Configuración

- El Departamento de Redes y Telecomunicaciones señaló que los proveedores son responsables de la aplicación de las líneas base de configuraciones de seguridad (Hardening), en los equipos que están bajo su administración; sin embargo, la Entidad refiere no haber validado la aplicación ni la definición de reglas de Hardening para

sistemas operativos, manejadores de bases de datos, middleware, máquinas virtuales, equipos de comunicaciones y de seguridad.

- No se tiene el método ni las políticas para el tratamiento de aquellos casos en que se adicionen componentes de software a un aplicativo de cómputo o a un servicio de TIC ya existente, para aplicar las pruebas de seguridad que sean pertinentes.
- No se verifica que en la estructura de datos del repositorio de configuraciones, se consideren al menos los atributos de los elementos de configuración y de sus componentes, así como el estado en que se encuentran; en caso de la presencia de un evento o problema, no se tiene un método formalizado para verificar el riesgo e impacto en los activos de TIC con respecto a los atributos relacionados.

Grupos de Trabajo para la Seguridad de la Información

- El equipo de trabajo para la identificación de infraestructuras críticas y las áreas involucradas no analizó los procesos existentes para determinar cuáles son críticos, ni se tienen políticas para efectuar una alineación de TIC con la Institución respecto de la seguridad de la información; tampoco se asegura que la entrega de servicios de TIC genere el valor que necesita la entidad.
- El Responsable del Proceso de la Seguridad de la Información en la Institución (RSII) no ha dado a conocer el Sistema de Gestión de Seguridad de la Información (SGSI) y su programa de implementación, a los servidores públicos involucrados con el mismo. Tampoco ha asignado al servidor público que será el encargado de supervisar a los responsables de implementar controles de seguridad del SGSI y controles para el manejo de riesgos, con la finalidad de que lleven a cabo su tarea en tiempo y forma.
- El Equipo de Respuesta a Incidentes de Seguridad en TIC en la Institución (ERISC), con base a la directriz rectora de los incidentes de seguridad, no tiene formalmente gestionados los incidentes; asimismo, se carece de la documentación de las lecciones aprendidas y el repositorio para la administración del conocimiento entre otros, el Responsable de TIC manifestó que se tiene planeado implementar una mesa institucional de servicios con la herramienta de gestión de incidentes.
- El equipo de trabajo para realizar el análisis de riesgos, en coordinación con las áreas y unidades administrativas de la Institución involucradas, requiere robustecer el SGSI e integrar el documento de resultados del análisis de riesgos y el programa de implementación para el manejo de riesgos, el cual deberá incluir la asignación de responsables de la ejecución de cada control.

Roles Funcionales con Actividades en Materia de Seguridad de la Información

- De acuerdo con las evidencias presentadas por la entidad, el personal que forma parte del Grupo Estratégico de Seguridad, así como el que desarrolla actividades no formalizadas en esta materia, no cuenta con una formación especializada, ni se capacita de manera continua en seguridad de la información.

Como resultado de la revisión de los procedimientos para la Gestión de la Seguridad de la Información, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la CONDUSEF, son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	
Factor	**Riesgo**
Clasificación de Infraestructuras y Activos de Información críticos	Se carece del análisis de los procesos existentes para determinar cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos; en consecuencia, se presenta una brecha entre las expectativas de la Comisión y las capacidades de TIC, al no considerar los activos de información críticos, ni los indicadores de evaluación del desempeño que son relevantes para la Institución, ocasionando políticas de seguridad mal diseñadas, incumplimientos regulatorios, pérdidas financieras por proyectos mal definidos, entre otros.
Administración de usuarios	Debido a que no se tienen procedimientos formalizados para la gestión de claves de usuarios, éstos podrían tener permisos para acceder a información que no le corresponde de acuerdo con sus funciones y responsabilidades; en consecuencia, se pierde la confidencialidad en la información y se pueden ejecutar transacciones no autorizadas que ponen en riesgo la integridad de los activos de la institución; asimismo, existen cuentas de usuarios que ya no se encuentran en la Institución y pueden seguir activas.
Privacidad de la Información	No se asegura el cifrado de datos, ni redes con protocolos seguros para la transferencia de información; tampoco se consideran pruebas de seguridad en los aplicativos; en consecuencia, se podrían tener alteraciones en la información, borrado o mal uso de los datos, así como operaciones no autorizadas al no asegurar que los nuevos desarrollos integren funciones de seguridad.
Monitoreo de las pistas de auditoría y bitácoras de los aplicativos y bases de datos	No se realiza una revisión periódica de las pistas de auditoría y las bitácoras de los aplicativos sustantivos, a fin de 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.
Gestión de configuraciones	En la estructura de datos del repositorio de configuraciones no se verifica que se consideren los atributos básicos relacionados con los elementos de configuración y sus componentes, así como el estado en que se encuentran, con el riesgo de que en caso de la presencia de un evento o problema, no se tenga un repositorio que permita verificar el impacto en los activos de TIC respecto de sus características esenciales.
Sistema de Gestión de Seguridad de la Información (SGSI)	Se carece de un Sistema de Gestión de Seguridad de la Información (SGSI), así como de su programa de implementación y operación, en consecuencia, se tienen diversos riesgos, 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 pueden ser alterados, provocando pérdidas económicas y fraudes; afectación a la disponibilidad de los servicios que impide que los usuarios accedan a las aplicaciones cuando lo requieran; asimismo, los mecanismos de seguridad de la información se mantienen estáticos, en un entorno dinámico que requiere de la aplicación de acciones preventivas y correctivas generadas por las revisiones que se efectúen al SGSI.

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

La CONDUSEF reportó de enero a diciembre 2017, que el monto de los fraudes cibernéticos ascendió a 6,201 millones de pesos, de los cuales 3,264,105 reclamaciones corresponden al Comercio por Internet; 119,654 son de Operaciones por Internet; 57,430 relacionadas con la Banca Móvil y 1,289 por pagos de celular. Por lo anterior, resulta prioritario: fortalecer los controles sobre las deficiencias en las Políticas de Contraseñas; el borrado seguro de los dispositivos; el cifrado de datos con protocolos seguros para la transferencia de información, todo ello para contar con un sistema de gestión de seguridad de la información que asegure la privacidad de los datos de los usuarios de servicios financieros.

2017-1-06G3A-15-0086-01-010 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implemente un Sistema de Gestión de Seguridad de la Información, que permita salvaguardar los activos de información e instrumentar políticas para la protección de información sensible, así como acciones que aseguren una adecuada gestión de los procedimientos relacionados con la privacidad de la información, atención de incidentes, administración de usuarios, monitoreo de las bitácoras de los aplicativos, bases de datos y sistemas operativos; con la finalidad de disminuir los riesgos que pudieran impactar en la operación y manejo de la información de la entidad, dada la relevancia de la información financiera que maneja la Comisión al ser uno de los actores reguladores del sistema bancario mexicano.

2017-1-06G3A-15-0086-01-011 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros instrumente procedimientos de control para validar periódicamente las configuraciones de línea base en la infraestructura tecnológica para prevenir que las vulnerabilidades sean explotadas; asegurar que todos los sistemas operativos cuenten con antivirus y soporte por parte del fabricante; ejecutar las acciones para remediar las vulnerabilidades identificadas en los servidores de las aplicaciones sustantivas; implementar credenciales de autenticación cifradas con algoritmos robustos durante su almacenamiento y transmisión; así como aplicar el borrado seguro a todos los dispositivos con capacidades de almacenamiento que contengan información que no sea de carácter público; con la finalidad de fortalecer los controles para asegurar la privacidad de la información de los interesados en los servicios de la Comisión, como son las instituciones bancarias y los usuarios de servicios financieros.

2017-1-06G3A-15-0086-01-012 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros en razón de las debilidades identificadas en la administración de los usuarios que operan los sistemas de la entidad, tal es el caso del Sistema de Información Operativa Institucional (SIO), fortalezca los procedimientos para regular: el acceso a recursos compartidos; los privilegios de los usuarios; la adecuada segregación de funciones; las recertificaciones de usuarios; el manejo de cuentas con privilegios especiales; la bóveda de contraseñas de acceso restringido; así como la composición y tiempo de vida de las contraseñas para los sistemas operativos.

2017-9-06G3A-15-0086-08-003 **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 la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión respecto a las políticas, procedimientos y normativas para la Gestión de la Seguridad de la Información, propiciaron irregularidades vinculadas con las responsabilidades de los titulares de la Dirección General

de Desarrollo Financiero, Estadístico y de Tecnologías de Información, Subdirección de Informática y Telecomunicación, Departamento de Redes y Telecomunicaciones, debido a las deficiencias en los controles para el establecimiento de un modelo de gobierno de seguridad de la información; diseño y operación del Sistema de Gestión de Seguridad de la Información; identificación y protección de las infraestructuras de información críticas, así como los activos clave; elaboración del análisis de riesgos enfocado en la seguridad de la información; operación del equipo de respuesta a Incidentes para su detección y atención; implementación de los controles para la asignación, revocación o modificación de los privilegios de acceso a la información; así como la aplicación de los procedimientos de borrado seguro de la información en los dispositivos.

7. Continuidad de las Operaciones y Centro de Datos

En la revisión y análisis de la información relacionada con los Procesos de Administración de Servicios (ADS), Administración de la Operación (AOP) y Administración de la Seguridad de la Información (ASI) del MAAGTICSI, así como las políticas y lineamientos proporcionados por la entidad, se detectaron las observaciones siguientes:

Continuidad de las Operaciones

- La entidad carece de un procedimiento para la definición, análisis, planificación, medición y mejoramiento de la disponibilidad de servicios de TIC.
- El catálogo de servicios de TIC está incompleto, debido a que no contempla la información relativa a la descripción, responsable técnico y usuario, detalle de sus componentes (procesos, aplicaciones e infraestructura tecnológica), disponibilidad (comprometida y real), métricas, indicadores y costo de operación.
- No se cuenta con un análisis de impacto al negocio (BIA), se carece de: la identificación de los procesos y actividades en función a la contribución de valor que aportan a la organización; evaluación de impactos operacionales; configuración de los RTO/RPO (Tiempo Objetivo de Recuperación/Punto Objetivo de Recuperación).
- Se carece de un Programa de Capacidad de la Infraestructura Tecnológica, no se cuenta con: el monitoreo del rendimiento y capacidad utilizada en la infraestructura; identificación y análisis de los incidentes por falta de capacidad; actualización de activos especificando los que requieren actualización, mejoras o sustitución; clasificación de los componentes de la infraestructura que son necesarios para cumplir con los requerimientos de desempeño y disponibilidad de los servicios de TIC.
- No se tiene elaborado un Programa de Continuidad de las Operaciones, la entidad no realiza: priorización de situaciones de recuperación; pruebas de recuperación, al menos semestralmente, para confirmar que los servicios de TIC puedan ser reestablecidos de forma efectiva; revisión de las actividades con los involucrados en la ejecución del plan de continuidad, para validar que cubren con los aspectos técnicos y funcionales deseados.
- Se carece de políticas formalizadas para las actividades de respaldos de información, aunado a que no se tienen procedimientos institucionales para la clasificación y resguardo de la información, en consecuencia, la entidad no tiene forma de acreditar

que la información a recuperarse garantiza la correcta operación de los procesos críticos.

- No se cuenta con un Plan de Recuperación de Desastres (DRP), se carece de: mecanismos de atención ante contingencias y tareas diseñadas para la recuperación de las operaciones; creación de planes para la recuperación de todos los recursos de los activos de información críticos y los medios que los contienen; generación del plan de concientización y capacitación a las áreas involucradas sobre la creación y ejecución del DRP en la entidad.

Centro de Datos

- No se ha realizado ningún análisis para evaluar la viabilidad de certificar el centro de datos, aun cuando la Comisión manifiesta que administra datos de carácter confidencial.
- El Centro de Cómputo tiene las debilidades siguientes: no cuenta con detectores de movimiento; las videograbaciones sólo se respaldan 15 días; la salida del Centro se hace sin autenticación alguna; se carece de controles para identificar al personal de seguridad que accede al centro de datos.
- La entidad no cuenta con un centro de datos alterno, los respaldos son resguardados en los equipos de almacenamiento que están dentro del mismo Centro, aunado a que las cintas y unidades ópticas con los respaldos se almacenan en la cintoteca a menos de un kilómetro del Centro, por lo que no se tienen condiciones favorables para asegurar la recuperación de la información en caso de contingencias.

Como resultado de la revisión de los objetivos del procedimiento de Continuidad de las Operaciones y Centro de Datos, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la CONDUSEF son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD EN EL CENTRO DE DATOS Y EN EL PROGRAMA DE CONTINUIDAD DE LAS OPERACIONES	
Factor Crítico	**Riesgos**
Planeación de la capacidad	Al no contar con procedimientos para gestionar la capacidad de la infraestructura tecnológica, se incrementa el riesgo de que los servicios no se vean respaldados por una capacidad de procesamiento y almacenamiento adecuada, por lo tanto, los recursos podrían no ser aprovechados y ejecutarse acciones equivocadas en cuanto a su mantenimiento y administración, o ser insuficientes teniendo como consecuencia una probable degradación de la calidad del servicio.
Plan de Recuperación de Desastres (DRP)	Al no tener implementado un DRP se incrementa el riesgo de no contar con la capacidad de recuperar satisfactoriamente los datos, la infraestructura tecnológica y los aplicativos sustantivos, para que la entidad pueda reiniciar sus operaciones en caso de un desastre natural o provocado.
Análisis de Impacto al Negocio (BIA)	Al no tener implementado un BIA, no se tienen identificadas las funciones, actividades, unidades administrativas, así como los servicios sustantivos que podrían resultar afectados como resultado de la interrupción de los servicios de TIC, ni la estimación del impacto técnico, económico y reputacional para la entidad.

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD EN EL CENTRO DE DATOS Y EN EL PROGRAMA DE CONTINUIDAD DE LAS OPERACIONES	
Factor Crítico	**Riesgos**
Políticas de recuperación y respaldo	Debido a la carencia de un procedimiento formalizado para la ejecución de pruebas de restauración de respaldos, se incrementa el riesgo de que los medios no funcionen adecuadamente en caso de que se necesite de la información para reestablecer los servicios.
Programa de Continuidad de las Operaciones	No se cuenta con una política de continuidad, en la cual se muestren los objetivos, metas, controles, procesos y procedimientos para el restablecimiento de las operaciones, aunado a que se carece de un centro de cómputo alterno, por lo que la entidad no cuenta con los elementos necesarios para asegurar que la operación de los servicios y procesos críticos no se interrumpan.

Fuente: Elaborado por la ASF en base a la información proporcionada por la CONDUSEF.

De enero a diciembre 2017, el tiempo de respuesta de la CONDUSEF para las reclamaciones en materia de consumos no reconocidos vía internet fue de 23 días, los cuales pueden aumentar en caso de contingencia, si la institución no toma acciones para mitigar las deficiencias detectadas en el Análisis de Impacto al Negocio, la Capacidad de la Infraestructura Tecnológica y la Recuperación de la Infraestructura Tecnológica ante Desastres.

2017-1-06G3A-15-0086-01-013 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implemente las acciones necesarias para la elaboración y pruebas del Análisis de Impacto al Negocio (BIA), Plan de Continuidad del Negocio (BCP) y Plan de Recuperación ante Desastres (DRP), con la finalidad de garantizar una óptima continuidad operativa de los procesos críticos, aplicativos sustantivos e infraestructura tecnológica de la entidad, aunado a que el intercambio de información y los servicios que presta la Comisión a los participantes del sistema bancario mexicano se encuentren siempre disponibles.

2017-1-06G3A-15-0086-01-014 **Recomendación**

Para que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros fortalezca los procedimientos para la custodia y rotación de los respaldos para contar con condiciones óptimas de seguridad y ambientales que protejan adecuadamente a la información; asimismo, instrumentar políticas de respaldo y restauración de la información (considerando las plataformas históricas), con el objetivo de garantizar que los mecanismos de recuperación funcionen adecuadamente en caso de que se necesite de la información resguardada.

Recuperaciones Probables

Se determinaron recuperaciones probables por 126,884.11 pesos.

Resumen de Observaciones y Acciones

Se determinaron 6 observaciones las cuales generaron: 14 Recomendaciones, 3 Promociones de Responsabilidad Administrativa Sancionatoria y 2 Pliegos de Observaciones.

Dictamen

Con base en los resultados de la auditoría practicada a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), cuyo objetivo consistió en 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 por 38,284.3 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:

- No se tiene implementado un mecanismo para verificar el cumplimiento de los niveles de servicio establecidos para los servicios de TIC, debido a esto, no es posible determinar los tiempos en que los servicios estaban disponibles; asimismo, la Comisión no tiene consolidados la totalidad de los servicios de comunicaciones y seguridad, con lo cual justificó adherirse al contrato marco de la SHCP, por lo que no se puede asegurar que son atendidas completamente todas sus necesidades operativas, entre las cuales se encuentran la integridad, confidencialidad y disponibilidad de la información por medio de diversas herramientas de seguridad que protejan el perímetro de la red institucional, evitando entre otros, código malicioso, intrusos, robo de información y correo basura.

- Se carece de un procedimiento para gestionar la capacidad de la infraestructura tecnológica, lo que incrementa el riesgo de que los servicios no se vean respaldados por una capacidad de procesamiento y almacenamiento adecuada, en consecuencia, se observó que el promedio de uso de los servicios de comunicaciones corresponde a la tercera parte de los niveles de servicio contratados, donde las capacidades subutilizadas principalmente se refieren al uso de banda ancha, procesadores y memoria de los servidores, por lo que las condiciones de operación de la contratación mediante la adhesión al contrato marco de la SHCP no fueron la mejor opción para la Comisión.

- Se identificaron deficiencias en la administración y desarrollo de soluciones tecnológicas, lo que disminuye la capacidad de contribuir en alcanzar una mayor eficiencia en los procesos institucionales, entre los principales procesos con debilidades se encuentran la cuantificación del esfuerzo de los recursos, costos y tiempos para los desarrollos; el aseguramiento de la calidad; la gestión de cambios; el plan de riesgos; los planes de pruebas y los controles de seguridad en los aplicativos.

- En relación con el Gobierno de las Tecnologías de Información, se carece de un procedimiento formal para alinear el plan estratégico con los objetivos institucionales, Plan Nacional de Desarrollo y programas sectoriales; tampoco se cuenta con un procedimiento para el descubrimiento de riesgos en las iniciativas de

TIC, aunado a que no se da seguimiento en conjunto con el administrador del contrato, para corroborar que los proveedores cumplan con las obligaciones pactadas.

- Sobre la Seguridad de la Información, se carece del análisis de los procesos existentes para determinar cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos; no se tienen procedimientos formalizados para la gestión de claves de usuarios, por lo que éstos podrían tener permisos para acceder a información que no les corresponde de acuerdo con sus funciones y responsabilidades; tampoco se cuenta con un Sistema de Gestión de Seguridad de la Información, así como de su programa de implementación y operación, en consecuencia, se tienen diversos riesgos, principalmente la pérdida de la confidencialidad de la información que puede ser conocida y utilizada por personas que no tienen autorización.
- Respecto de la Continuidad de las Operaciones no se tienen identificadas las funciones, actividades, unidades administrativas, así como los servicios sustantivos que podrían afectarse por la interrupción de los servicios de TIC; asimismo, no se tiene implementado un plan de recuperación ante desastres, lo que incrementa el riesgo de no contar con la capacidad de recuperar satisfactoriamente los datos, la infraestructura tecnológica y los aplicativos sustantivos; se carece de un procedimiento formalizado para la ejecución de pruebas de restauración de respaldos, por lo que existe el riesgo de que los medios no funcionen adecuadamente en caso de que se necesite de la información para reestablecer los servicios.

Los procedimientos de auditoría aplicados, la evidencia objetiva analizada, así como los resultados obtenidos, fundamentan las conclusiones anteriores.

El presente dictamen se emite el 15 de junio 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
Lic. Genaro Hector Serrano Martínez	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 se corresponden con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; análisis del gasto ejercido en materia de TIC en los capítulos contables de la Cuenta Pública fiscalizada.
2. Validar que el estudio de factibilidad comprende 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 el proceso de contratación, cumplimiento de las especificaciones técnicas y económicas, así como distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los servicios arrendados 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 de 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 y entregables, así como la pertinencia de su penalización y/o deducción 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 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, deducciones y garantías); pruebas de cumplimiento y sustantivas; implementación y post-Implementación.
6. Evaluación del riesgo inherente a 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; análisis del diagnóstico de las funciones sustantivas y administrativas de las TIC que lleva a cabo la entidad fiscalizada; evaluación del 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; revisión del avance en la implementación del MAAGTICSI o, en su caso, la normativa que se aplique. Revisión del cumplimiento de las disposiciones en materia de Datos Abiertos.
8. Evaluar los mecanismos que permitan la administración de la seguridad de la información 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.
9. Evaluar los mecanismos que permitan disminuir el impacto que puede sufrir la entidad a causa de eventos adversos y/o desastres que atenten contra la continuidad de las operaciones. Evaluación de la seguridad física del Centro de Datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).

Áreas Revisadas

La Dirección General de Desarrollo Financiero, Estadístico y de Tecnologías de la Información, la Dirección de Adquisiciones y la Dirección de Programación y Finanzas de la CONDUSEF.

Disposiciones Jurídicas y Normativas Incumplidas

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

1. Constitución Política de los Estados Unidos Mexicanos: Art. 134;
2. Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 1;
3. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 48 fracción II; Art. 53; Art. 53 Bis;
4. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 30; Art. 97;
5. Otras disposiciones de carácter general, específico, estatal o municipal: Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, publicado en el D.O.F. el 08 de mayo de 2014, última reforma publicada el 04 de febrero de 2016: Art. 11 fracción II; Art. 12; Art. 17 fracción I; Art. 26; Art. 27 fracción IV y VI; Reglas Generales numerales 2, 3, 6, 17; Objetivo general del Proceso I.A Planeación Estratégica (PE);Objetivo general, Regla 7 del

Proceso I.B Administración del Presupuesto y las Contrataciones (APCT); Objetivo general, Objetivos Específicos, numeral 1, Regla 5 del Proceso II.A Administración de Servicios (ADS); Actividad ADS 3 Administrar la capacidad de la infraestructura de TIC del Proceso II.A Administración de Servicios (ADS); Actividad ACNF 2 Definir la estructura del repositorio de configuraciones, Factor Crítico 1 del Proceso II.B de Administración de la Configuración (ACFN); Objetivo general, Regla 9, 12, 13 y 14, Actividad ASI 1 Establecer un modelo de gobierno de seguridad de la información, Actividad ASI 2 Operar y mantener el modelo de gobierno de seguridad de la información, Factor Crítico 1, 2, 3, 4, 5, 7, 8, 9, Actividad ASI 3 Diseño del SGSI, Factores Críticos 5, 6, 7, 14, 15, 16, 17, 18, Actividad ASI 4 Identificar las infraestructuras de información esenciales y, en su caso, criticas, así como los activos clave, Factores Críticos 2 y 3, Actividad ASI 5 Elaborar el análisis de riesgos, Factores Críticos 1, 3, 4, 5, 6, 7, 8, 9, 11, 12, 16 y 17, Actividad ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información, Factor Crítico 1 y 2 del Proceso II.C Administración de la Seguridad de la Información (ASI); Objetivo general del Proceso III.A Administración de Proyectos (ADP); Objetivo General del Proceso III.B Administración de Proveedores (APRO); Objetivo general del Proceso III.C Administración de la Operación (AOP); Regla 1 del Proceso III.C Administración de la Operación (AOP); Objetivo general, Actividad OPEC 1 Designar un responsable de la supervisión de la implementación de los controles de seguridad definidos en el SGSI y en el análisis de riesgos, Factores Críticos 1, 2 y 3; Actividad OPEC 2 Establecer los elementos de operación del ERISC, Factor Crítico 2, 3 y 4; Actividad OPEC 3 Operación del ERISC en la atención de incidentes , Factor Crítico 1 del Proceso III.D Operación de Controles de Seguridad de la Información y del ERISC (OPEC);

Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros: Art. 14 fracciones XXXVI, XXXIX y XLI;

Manual de Organización General de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros: Art. VIII, clave 2222000, funciones 2 y 6; clave 222004 función 4; Sección 2533000, funciones 7 y 8;

Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios: Numeral VI.1.5 Cargo de los Servidores Públicos o el área responsable de realizar la investigación de mercado de conformidad con las disposiciones del Reglamento de la Ley; Numeral VI.3.6 Aspectos a considerar para la determinación de los términos, condiciones y procedimientos a efecto de aplicar las penas convencionales y deducciones, atendiendo lo dispuesto en los artículos 53 y 53 BIS de la Ley;

Contrato No. CONDUSEF/053/2013: cláusula décima primera;

Contrato CONDUSEF/047/2015: cláusula Décima Tercera;

Contrato No. CONDUSEF/027/2017: cláusula décima;

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.