

Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado**Auditoría de TIC**

Auditoría Financiera y de Cumplimiento: 15-1-19GYN-02-0295

295-DS

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios cuantitativos y cualitativos establecidos en la Normativa para la Fiscalización Superior de la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2015 considerando lo dispuesto en el Plan Estratégico de la ASF 2011-2017.

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.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	1,660,791.8
Muestra Auditada	719,942.8
Representatividad de la Muestra	43.3%

El universo seleccionado por 1,660,791.8 miles de pesos corresponde al total de recursos ejercidos en 15 contratos vigentes en el ejercicio fiscal de 2015, correspondientes a las Tecnologías de la Información y Comunicaciones (TIC); la muestra auditada se integra de cuatro contratos por un monto total de 719,942.8 miles de pesos, que representan el 43.3% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de las acciones realizadas en TIC por el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) en 2015, relacionadas con el Gobierno y Administración de las TIC, Desarrollo de Soluciones Tecnológicas, Gestión de la Seguridad de la Información y Continuidad de las Operaciones, entre otras.

Antecedentes

El ISSSTE es una entidad paraestatal, como organismo descentralizado contribuye a satisfacer niveles de bienestar integral de los trabajadores al servicio del Estado, pensionados, jubilados y familiares derechohabientes. Cuenta con 14 macroprocesos sustantivos, los de mayor impacto a los derechohabientes son: Pensiones; Préstamos personales; Servicios de atención para el desarrollo infantil; Atención médica preventiva; Atención médica curativa, maternidad

y rehabilitación; Comercialización de productos básicos y medicamentos; Servicios turísticos y Administración de cuentas individuales.

En las Cuentas Públicas 2012, 2014 y 2015, se llevaron a cabo las auditorías números 1187, 156 y 295-DS respectivamente, en donde reiteradamente se han encontrado resultados con deficiencias en materia de gobierno de TIC, seguridad de la información y gestión de los contratos de servicios; de las cuales se han emitido recomendaciones y pliegos de observaciones, no obstante en las revisiones actuales se continúan presentando las mismas situaciones, sin que se hayan implementado acciones o mecanismos de control para solventar estas deficiencias.

Entre 2011 y 2015, se han invertido más de 10,830,544.6 miles de pesos en sistemas de información e infraestructuras tecnológicas.

Recursos Invertidos en Materia de TIC

(Miles de pesos)

PERÍODO DE INVERSIÓN	2011	2012	2013	2014	2015	TOTALES
MONTO POR AÑO	3,088,400.0	2,538,700.0	2,017,500.0	1,283,800.0	1,902,144.6	10,830,544.6

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

Resultados

1. Análisis Presupuestal

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2015, se concluyó que el ISSSTE ejerció un presupuesto de 225,808,181.5 miles de pesos, de los cuales 1,902,144.6 miles de pesos corresponden a recursos relacionados con las TIC, que representan el 0.8% del total, como se muestra a continuación:

Recursos ejercidos en 2015

(Miles de pesos)

Capítulo	Concepto	Ejercido	Ejercido TIC	%
1000	Servicios personales	35,196,405.5	67,235.1	0.2
2000	Materiales y suministros	15,486,225.3	3,489.0	0.0
3000	Servicios generales	16,550,803.5	1,831,420.5	11.1
4000	Transferencias, asignación, subsidios y otras ayudas	156,056,474.3	0.0	0.0
5000	Bienes Muebles, Inmuebles e Intangibles	813,519.8	0.0	0.0
6000	Inversión Pública	1,704,753.1	0.0	0.0
Total		225,808,181.5	1,902,144.6	0.8

Fuente: Cuenta de la Hacienda Pública Federal 2015.

Los recursos ejercidos en materia de TIC por 1,902,144.6 miles de pesos, se integran de la manera siguiente:

Recursos ejercidos relacionados en materia de TIC en 2015 (Miles de pesos)			
Partida Gasto	Descripción	Importe Ejercido	%
1000	SERVICIOS PERSONALES	67,235.1	3.5
2000	MATERIALES Y SUMINISTROS	3,489.0	0.2
3000	SERVICIOS GENERALES	1,831,420.5	96.3
31101	Servicio de energía eléctrica	241.9	0.0
31401	Servicio telefónico convencional	2,865.0	0.2
31701	Servicios de conducción de señales analógicas y digitales	480,015.9	25.2
31801	Servicio postal	16.3	0.0
31904	Servicios integrales de infraestructura de cómputo	505,709.7	26.6
32301	Arrendamiento de equipo y bienes informáticos	116,829.3	6.1
32601	Arrendamiento de maquinaria y equipo	431.5	0.0
32701	Patentes, derechos de autor, regalías y otros	155,981.4	8.2
33104	Otras asesorías para la operación de programas	68,782.7	3.6
33301	Servicios de desarrollo de aplicaciones informáticas	382,897.9	20.1
33304	Servicios de mantenimiento de aplicaciones informáticas	107,925.3	5.7
33602	Otros servicios comerciales	0.5	0.0
33604	Impresión y elaboración de material informativo derivado de la operación y administración de las dependencias y entidades	19.8	0.0
33606	Servicios de digitalización	0.1	0.0
33801	Servicios de vigilancia	2,841.4	0.2
33901	Subcontratación de servicios con terceros	775.5	0.0
35201	Mantenimiento y conservación de mobiliario y equipo de administración	6.7	0.0
35501	Mantenimiento y conservación de vehículos terrestres, aéreos, marítimos, lacustres y fluviales	243.0	0.0
35801	Servicios de lavandería, limpieza e higiene	1,778.0	0.2
37101	Pasajes aéreos nacionales para labores en campo y de supervisión	110.5	0.0
37104	Pasajes aéreos nacionales para servidores públicos de mando en el desempeño de comisiones y funciones oficiales	136.1	0.0
37201	Pasajes terrestres nacionales para labores en campo y de supervisión	77.5	0.0
37204	Pasajes terrestres nacionales para servidores públicos de mando en el desempeño de comisiones y funciones oficiales	48.4	0.0
37504	Viáticos nacionales para servidores públicos en el desempeño de funciones oficiales	124.6	0.0
39202	Otros impuestos y derechos	78.9	0.0
39401	Erogaciones por resoluciones por autoridad competente	3,482.6	0.2
TOTAL		1,902,144.6	100.0

Fuente: Documentación proporcionada por el ISSSTE.

El presupuesto de TIC se destina principalmente a las partidas siguientes: 31904 "Servicios Integrales de infraestructura de cómputo" (505,709.7 miles de pesos), 31701 "Servicios de conducción de señales analógicas y digitales" (480,015.9 miles de pesos), 33301 "Servicios de

desarrollo de aplicaciones informáticas" (382,897.9), "32701 "Patentes, derechos de autor, regalías y otros" (155,981.4 miles de pesos) y 32301 "Arrendamiento de equipo y bienes informáticos" (116,829.3 miles de pesos), las cuales suman un monto total de 1,641,434.2 miles de pesos, que representan el 86.3% del total de gastos de TIC ejercidos en 2015.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC considerando 255 plazas con una percepción anual de 67,235.2 miles de pesos durante el ejercicio 2015, que representan el 3.5 % de los recursos totales en esta materia. El costo promedio por plaza es de 263.7 miles de pesos anuales.

Del total ejercido en 2015 por 1,660,791.8 miles de pesos en 15 contratos en materia de TIC, se seleccionó una muestra de cuatro contratos de prestación de servicios relacionados con las TIC, en los cuales se ejercieron 719,942.8 miles de pesos, que representan el 43.3% del universo seleccionado y se integran como sigue:

Muestra de Contratos de Prestación de Servicios ejercidos en 2015
(Miles de Pesos)

Núm.	Contrato/ Convenios Modificatorios	Proceso de Adjudicación	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2015
					Del	Al	Mínimo	Máximo	
1	AD-CS-DA-SRMS-113/2014	Adjudicación Directa	Mer Security Systems, S.A. DE C.V. (1)	Servicio de Asesoría de Seguridad Integral Informática e Implementación de Protocolos.	01/05/2014	31/05/2016	102,053.1		65,908.8
	CM-CS-DA-SRMS-029/2014			Convenio para precisiones del lugar y forma de pago	10/10/2014	31/05/2016			
	CM-CS-DA-SRMS-014/2015			Convenio para cambio de domicilio fiscal	02/06/2015	31/05/2016			
2	AD-CS-DA-SRMS-286/2014	Adjudicación Directa	Sixsigma Networks México,S.A. de C.V.	Infraestructura de Centro de Datos (Servicio de Cómputo Empresarial)	04/11/2014	17/10/2017	628,546.8	1,568,589.9	479,513.9
3	AD-CS-DA-SRMS-307/2014	Adjudicación Directa	Universidad Politécnica de Chiapas	Servicio de Administración, Desarrollo de Mantenimiento y Soporte de Aplicaciones (ADMA) (Unidad de Administración de Proyectos de Calidad UAPC)	24/11/2014	23/11/2017	74,137.9	259,482.7	83,200.4
4	AD-CS-DA-SRMS-002/2015	Adjudicación Directa	BConnect Services S.A. de C.V.	Centro de Contacto Telefónico para la Atención de Llamadas, para los Ejercicios Fiscales 2014,2015,2016 y 2017	01/01/2015	31/12/2017	201,895.1	504,737.8	91,319.6
Total							904,579.8	2,434,863.4	719,942.8

Fuente: Contratos, facturas y soporte documental proporcionados por el ISSSTE.

Nota (1): Monto de 5,885.5 miles de dólares valuados al Tipo de Cambio del 31 de diciembre de 2015 por 17.3398 pesos, publicado en el Diario Oficial de la Federación (DOF)

Nota (2): La suma de los parciales puede no coincidir debido al redondeo aplicado.

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

2. Contrato AD-CS-DA-SRMS-113/2014

Del análisis del contrato número AD-CS-DA-SRMS-113/2014 celebrado con Mer Security Systems, S.A. de C.V., mediante el procedimiento de adjudicación directa, con fundamento en el artículo 41, fracción X, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (por tratarse de información de carácter reservada respecto de servicios de consultoría, asesoría o investigaciones), con el objeto de la prestación del servicio de asesoría de “Seguridad integral informática e implementación de protocolos”, vigente del 1° de mayo de 2014 al 31 de mayo de 2016, por un monto de 5,885.5 miles de dólares que valuados al tipo de cambio de 17.3398 pesos por dólar del 31 de diciembre de 2015, publicado en el Diario Oficial de la Federación (DOF), asciende a 102,053.1 miles de pesos, de los cuales se pagaron 65,908.8 miles de pesos durante 2015, es importante señalar que el mismo fue revisado durante la auditoría de la Cuenta Pública 2014 detectándose diversas irregularidades en el proceso de adjudicación; de la revisión actual se determinó lo siguiente:

El alcance de los trabajos se integró por 10 servicios administrados los cuales consideran, entre otros aspectos, la asesoría y acompañamiento para la implementación de soluciones de TIC; con fecha 10 de octubre de 2014 se celebró el primer convenio modificatorio CM-CS-DA-SRMS-029/2014, y el 02 de junio de 2015 se celebró el segundo convenio modificatorio CM-CS-DA-SRMS-014/2015, ambos con la finalidad de hacer precisiones en relación con el lugar y forma de pago, así como la aceptación de los servicios.

Proceso de contratación

De la revisión del proceso de contratación, se solicitó el estudio de factibilidad; al respecto la entidad respondió que al ser un servicio de asesoría no está obligada a realizarlo; en contraste, las definiciones de TIC estipuladas en los “Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos” incluyen los servicios realizados a través del equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

De acuerdo con las especificaciones técnicas del contrato, para prestar los servicios el proveedor utilizó software y dispositivos para proteger la información para llevar a cabo las actividades de los módulos siguientes: pruebas de penetración y de código en al menos 14 aplicaciones principales; mapeo de la arquitectura completa de redes incluidos los equipos activos, sistemas de análisis de transacciones y de seguridad análisis de reglas de cortafuegos, y la evaluación de las políticas de privacidad en cada sistema.

Por lo tanto, se incumplió con la elaboración, presentación y autorización del estudio de factibilidad para llevar a cabo el proceso de contratación, así como una investigación de mercado.

La contratación cuando la información es clasificada como reservada o confidencial debe cumplir varios requisitos, entre otros, que los documentos clasificados como reservados o confidenciales cuenten con las carátulas o leyendas elaboradas en términos de la Ley Federal

de Transparencia y Acceso a la Información Pública Gubernamental, así como justificar fehacientemente mediante una investigación de mercado, que la selección del proveedor y el precio del servicio refleja las mejores condiciones para el Estado.

Sin embargo, la documentación presentada por la entidad respecto a la clasificación de información reservada corresponde al ejercicio de 2009, siendo que el contrato fue celebrado en el ejercicio 2014, además, se carece de una investigación de mercado.

Pagos

Para realizar los pagos al proveedor, se efectuó la conversión de dólares a pesos mexicanos, considerando el tipo de cambio publicado en el DOF del día del contra recibo de la Cuenta por Liquidar Certificada (CLC) y no al tipo de cambio del día en que se realizó el pago, de acuerdo con lo estipulado en el contrato y sus convenios modificatorios; en consecuencia, se realizaron pagos en exceso por 648.2 miles de pesos, de acuerdo con lo siguiente:

Diferencias de pago (Fecha Contra recibo de CLC VS Fecha real de pago)
(Miles de pesos)

N° de Factura	Importe en dólares	Fecha de Contra recibo CLC	A		B	C=A-B
			Importe al tipo de cambio (M.N.) DOF Fecha de contra recibo CLC	Fecha de pago real	Importe al tipo de cambio (M.N.) DOF Fecha real de pago	Diferencia
B-36	436.9	11/02/2015	6,523.5	11/02/2015	6,523.5	0.0
B-42	2,338.0	13/03/2015	36,006.4	06/04/2015	35,352.5	653.9
B-49	56.1	23/07/2015	903.3	07/08/2015	917.8	-14.5
B-50	755.9	31/07/2015	12,434.7	17/08/2015	12,370.2	64.5
B-58	164.2	22/09/2015	2,739.5	12/10/2015	2,695.4	44.1
B-59	429.1	10/12/2015	7,301.3	04/01/2016	7,401.1	-99.8
	4,180.2		65,908.7		65,260.5	648.2

Fuente: Elaborado con documentación proporcionada por el ISSSTE y consulta DOF.

Nota: Diferencias por redondeo.

Revisión de Entregables

Se detectó que algunos entregables no cumplieron técnicamente con los servicios contratados, aunado a que se proporcionaron incompletos y no fueron implementados conforme a lo estipulado en el contrato, los cuales son los siguientes:

Entregables que no cumplieron técnicamente y no fueron implementados de acuerdo al contrato AD-CS-DA-SRMS-113/2014
(Miles de pesos)

Módulo/Fase	Entregable	Observaciones	Importe (1)	Factura
A1.3 Aseguramiento de ingresos Fase I	Documento de resultado del análisis de riesgos y vulnerabilidades sobre el aseguramiento de ingresos.	El entregable no cumplió técnicamente, debido a que no contiene información relacionada a los siguientes procesos: Préstamos, Nómina institucional, Servicios Integrales y Gastos Indirectos. Asimismo, no se cuenta con evidencia de su implementación.	8,260.0	B 42
A1.3 Aseguramiento de ingresos Fase II	Bitácora de la logística y operación.	El entregable no cumplió técnicamente, debido a que no contiene información del análisis de la logística, recursos humanos, tecnología de la información y seguridad de las operaciones principales y sus procesos. En función a lo anterior no se puede garantizar que el contenido del mismo contenga todos los procesos; asimismo no se cuenta con evidencia de su implementación.	7,058.9	B 50
A1.3 Aseguramiento de ingresos Fase III	Documento con el reporte de análisis de datos.	El entregable no cumplió técnicamente, debido a que no se documenta el análisis de las operaciones principales y sus procesos, así como el análisis de la logística, recursos humanos, tecnología de la información y seguridad, las cuales forman parte de la "Fase I", en función a lo anterior, no se puede garantizar que el contenido del mismo sea íntegro; asimismo no se cuenta con evidencia de su implementación.	7,301.3	B 59
A1.4 Administración de identidades de acceso identity management/ authenticity management (IDM/IAM) Fase IV	Documentación con diseño de alternativas de solución.	El entregable no cumplió técnicamente, debido a que no se identifica información relacionada a la administración de identidades, accesos, minería de roles y políticas para asignar a los usuarios derechos en los recursos y evitar el acceso a información que no les corresponde. En consecuencia, no se tienen identificados los usuarios asignados en cada cuenta y la correlación entre ellos, asimismo se carece de un repositorio de las cuentas de usuarios internos y externos, por lo que las recomendaciones generadas por el proveedor no se encuentran soportadas; asimismo no se cuenta con evidencia de su implementación.	1,159.3	B 50
	Plano de redes		1,159.3	B 50
TOTAL (2)			24,938.9	

Fuente: Elaborado con información proporcionada por el ISSSTE.

Nota (1): Cálculos determinados con base al costo unitario por entregable.

Nota (2): La suma de los importes puede no coincidir debido al redondeo aplicado.

Con lo anterior, se determina que los pagos realizados a Mer Security Systems, S.A. de C.V., por 24,938.9 miles de pesos son injustificados, debido a que los entregables no cumplieron técnicamente con los servicios requeridos y al momento de la auditoría no habían sido implementados.

Entregables no implementados

Se solicitó a la entidad proporcionar evidencias de la implementación de las recomendaciones de la asesoría realizada por el proveedor durante 2015 y de las mejoras aplicadas en el instituto para fortalecer la seguridad de sus sistemas; al respecto, se identificaron entregables que no han cumplido con este objetivo, los cuales son los siguientes:

Entregables no implementados del contrato AD-CS-DA-SRMS-113/2014

Módulo/Fase		Entregable	Importe	Factura
A1.1 Revisión y actualización de políticas y procedimientos en seguridad informática FASE II	1	Plan de trabajo para la implementación de las políticas y procedimientos desarrollados.	187.1	B 36
	2	Documento de integración del equipo de implementación y evaluación de las políticas, normas y procedimientos aplicados.	187.1	B 36
A1.2 Campaña de Concientización Fase II	3	Documentación del portal web para la concientización.	218.2	B 36
	4	Documento con propuestas de prevención y contención existentes en el mercado	218.2	B 36
	5	Documento con los resultados de la evaluación posterior a la aplicación de los planes de concientización para la identificar las brechas existentes.	218.2	B 36
A1.3 Aseguramiento de ingresos Fase I	6	Documentos con los resultados del análisis de al menos seis procesos.	8,260.0	B 42
A1.4 Administración de identidades de acceso – Identity Management / Authenticity Management (IDM / IAM) Fase II	7	Resultados de la auditoría de la información existente en los sistemas informáticos relevantes a Recursos Humanos.	526.1	B 36
A1.4 Administración de identidades de acceso identity management / authenticity management (IDM/IAM) Fase III	8	Documento con matriz de autorización.	1,627.9	B 42
	9	Documento con comparativo tecnológico de las soluciones existentes en el mercado y su aplicabilidad a los procesos del ISSSTE.	1,627.9	B 42
A1.5 Mejora de arquitectura y seguridad de la red Fase II	10	Diseño de alternativas de solución de alto y bajo nivel	974.3	B 42
	11	Recetario de soluciones.	974.3	B 42
	12	Documentación de las políticas de control de acceso a las redes para su implementación con los proveedores.	974.3	B 42
	13	Plan de evaluación constante y de auditorías para los accesos a las redes.	974.3	B 42
A1.6 Fortalecimiento en las medidas de seguridad Fase I	14	Resultados de la evaluación de seguridad de la información dentro de las plataformas existentes.	167.6	B 36
	15	Resultados de la evaluación de las políticas de privacidad y complejidad de contraseñas en cada sistema.	167.6	B 36
A1.7 Punto Final (End-Point) y medios portátiles Fase I	16	Matriz de mapeos, incluyendo el resultado del mapeo de las políticas de acceso.	903.3	B 49

Entregables no implementados del contrato AD-CS-DA-SRMS-113/2014

Módulo/Fase	Entregable	Importe	Factura
A1.7 Punto Final (End-Point) y medios portátiles Fase II	17 Documento con hallazgos de la revisión de procedimientos, herramientas de control de la información por medio de almacenamientos externos y DLP (rastreo de la información)	936.5	B 58
A1.8 Seguridad de Aplicaciones Fase IV	18 Resultado de revisión de código de 3 aplicativos y resultado de las pruebas de penetración	1,803.0	B 58
A 1.9 Gestión de la seguridad de la información Security Information Management (SIM) centro de operaciones de seguridad Security Operation Center (SOC) Fase I	19 Documento con hallazgos del análisis de estado actual de seguridad.	1,387.3	B 36
A 1.9 Gestión de la seguridad de la información Security Information Management (SIM) centro de operaciones de seguridad Security Operation Center (SOC) FASE III	20 Resultado del análisis de las herramientas disponibles en el mercado para aseguramiento de la información en los procesos.	1,073.2	B 42
	21 Propuesta de integración del SOC e implementación del CERT	1,073.2	B 42
	22 Plan de evaluaciones periódicas y pruebas de penetración	1,073.2	B 42
	23 Constancias de transferencia de conocimiento al personal encargado de replicar en el ISSSTE, el conocimiento y buenas prácticas adquiridas durante la prestación de servicios.	1,073.2	B 42
		1,073.2	B 42
Total		27,699.2	

Fuente: Elaborado con documentación proporcionada por el ISSSTE.

De los entregables anteriores, no se cuenta con evidencias de su implementación ni de la aplicación de las mejoras para fortalecer la seguridad de los sistemas, por lo que los trabajos desarrollados no han tenido beneficio ni utilidad para el Instituto.

Adicionalmente, se identificó que durante el ejercicio 2015 se devengaron servicios que al mes de agosto de 2016 no han sido recibidos de conformidad ni pagados por el Instituto, debido a deficiencias presentadas en los entregables proporcionados por el proveedor, los cuales son los siguientes:

Estimación de Servicios devengados en 2015 no pagados ni recibidos a conformidad
(Miles de pesos)

MÓDULO	ENTREGABLES	IMPORTE (1)
A 1.3	Aseguramiento de ingresos Fase IV *Políticas de acceso y transferencia de información documentadas. *Plan de evaluación continuo. *Documento con el diseño de la propuesta tecnológica. *Constancias de transferencia de conocimiento al personal encargado de replicar en el ISSSTE el conocimiento y buenas prácticas adquiridas durante la prestación del servicio.	3,720.1
A1.7	Punto Final (End-Point) y medios portátiles Fase III *Documento con reporte de herramientas de punto final detección de DLP / EPS existentes en el ISSSTE. *Políticas documentadas para las herramientas existentes *Políticas documentadas por perfiles de usuarios.	973.1
A1.8	Seguridad de Aplicaciones Fase V *Resultado de revisión de código de 3 aplicativos y resultado de las pruebas de penetración	1,873.6
A 1.10	*Plan de Continuidad de negocio - Business Continuity Plan (BCP) Fases I y II *Documento con reporte de activos críticos dentro del ISSSTE con su análisis de riesgo. *Resultado del análisis de los planes de recuperación de desastres-(DRP). *Resultado del análisis de opciones externas para el soporte de sistemas críticos en caso de falla. *Resultado del análisis de impacto y recuperación *Plan de recuperación de desastres	5,071.0
Total		11,637.8

Fuente: Elaborado con documentación proporcionada por el ISSSTE.

Nota (1): Moneda origen: Dólares (valuados al Tipo de Cambio al 31 de diciembre de 2015 de 17.3398 pesos, publicado en el Diario Oficial de la Federación)

En relación con la estimación anterior por 11,637.8 miles de pesos, no se cuenta con evidencias de la implementación de los trabajos del proveedor ni de la aplicación de las mejoras para fortalecer la seguridad de los sistemas; por lo tanto, el Instituto deberá evaluar y determinar las acciones pertinentes por el incumplimiento en la calidad, oportunidad y eficiencia comprometida en los entregables antes citados; así como resolver si aún con el retraso de la entrega, los productos son necesarios y útiles, en virtud del alto riesgo del cambio de condiciones de vulnerabilidad detectadas, lo que implica que las recomendaciones no surtan el efecto esperado.

Debido a que el incumplimiento de las condiciones contractuales se extiende a un periodo posterior al fiscalizado, se informó a la instancia de control competente (OIC), mediante el oficio número DGATIC-281/2016 del 07 de noviembre de 2016.

15-9-19GYN-02-0295-08-001 Promoción de Responsabilidad Administrativa Sancionatoria

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no verificaron el cumplimiento de lo establecido en el contrato AD-CS-DA-SRMS-113/2014 y convenios modificatorios CM-CS-DA-SRMS-029/2014 y CM-CS-DA-SRMS-014/2015; en consecuencia, se determinaron pagos en exceso por 648.2 miles de pesos debido a que para el pago de los servicios, no se realizó la conversión de dólares a pesos

al tipo de cambio de la fecha en que se efectuaron los pagos, en contravención de lo estipulado en el contrato y convenios modificatorios.

Esta acción se deriva del(de los) Pliego(s) de Observaciones que se emite(n) en este informe con la(s) clave(s):

15-1-19GYN-02-0295-06-001

15-9-19GYN-02-0295-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no verificaron el cumplimiento de lo establecido en el contrato AD-CS-DA-SRMS-113/2014, Anexo 1 y convenios modificatorios CM-CS-DA-SRMS-029/2014 y CM-CS-DA-SRMS-014/2015; en consecuencia, los pagos realizados al prestador de servicios por un monto de 24,938.9 miles de pesos, los cuales fueron efectuados por la asesoría para la implementación de soluciones de seguridad informática resultan injustificados, debido a las deficiencias en los entregables "Documento de resultado del análisis de riesgos y vulnerabilidades sobre el aseguramiento de ingresos" (A1.3 Aseguramiento de ingresos Fase I); "Bitácora de la logística y operación" (A1.3 Aseguramiento de ingresos Fase II); "Documento con el reporte de análisis de datos" (A1.3 Aseguramiento de ingresos Fase III); "Documentación con diseño de alternativas de solución" y "Plano de Redes" (A1.4 Administración de identidades de acceso identity management/authenticity management (IDM/IAM) Fase IV), los cuales no cumplieron técnicamente con los servicios requeridos y no fueron implementados conforme a lo estipulado en el contrato y sus anexos.

Esta acción se deriva del(de los) Pliego(s) de Observaciones que se emite(n) en este informe con la(s) clave(s):

15-1-19GYN-02-0295-06-002

15-9-19GYN-02-0295-08-003 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no vigilaron el cumplimiento del contrato AD-CS-DA-SRMS-113/2014 para su implementación y aplicación de las mejoras para fortalecer la seguridad de los sistemas; en consecuencia, los entregables A1.1 Revisión y actualización de políticas y procedimientos en seguridad informática Fase II; A1.2 Campaña de Concientización Fase II; A1.3 Aseguramiento de ingresos Fase I; A1.4 Administración de identidades de acceso Identity Management / Authenticity Management (IDM / IAM) Fase II; A1.4 Administración de identidades de acceso identity management / authenticity management (IDM/IAM) Fase III; A1.5 Mejora de arquitectura y seguridad de la red Fase II; A1.6 Fortalecimiento en las medidas de seguridad Fase I; A1.7 Punto Final (End-Point) y medios portátiles Fase I; A1.7 Punto Final (End-Point) y medios portátiles Fase II; A1.8 Seguridad de Aplicaciones Fase IV; A 1.9 Gestión de la seguridad de la información Security Information Management (SIM) centro de operaciones de seguridad Security Operation Center (SOC) Fase I; A 1.9 Gestión de la seguridad de la información Security Information Management (SIM) centro de operaciones

de seguridad Security Operation Center (SOC) FASE III no han tenido beneficio ni utilidad para el Instituto, por los cuales se pagaron 27,699.2 miles de pesos.

15-1-19GYN-02-0295-06-001 Pliego de Observaciones

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 648,236.42 pesos (seiscientos cuarenta y ocho mil doscientos treinta y seis pesos 42/100 M.N.) por pagos en exceso, debido a que para el pago de los servicios por concepto de asesoría del proveedor para la implementación de soluciones de seguridad informática, no se realizó la conversión de dólares a pesos al tipo de cambio de la fecha en que se efectuó el pago de los servicios, en incumplimiento de lo estipulado en el contrato AD-CS-DA-SRMS-113/2014 y sus convenios modificatorios.

15-1-19GYN-02-0295-06-002 Pliego de Observaciones

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 24,938,900.07 pesos (veinticuatro millones novecientos treinta y ocho mil novecientos pesos 07/100 M.N.) por pagos injustificados, debido a que los entregables "Documento de resultado del análisis de riesgos y vulnerabilidades sobre el aseguramiento de ingresos" (A1.3 Aseguramiento de ingresos Fase I); "Bitácora de la logística y operación" (A1.3 Aseguramiento de ingresos Fase II); "Documento con el reporte de análisis de datos" (A1.3 Aseguramiento de ingresos Fase III); "Documentación con diseño de alternativas de solución" y "Plano de Redes" (A1.4 Administración de identidades de acceso identity management/authenticity management (IDM/IAM) Fase IV) correspondientes al contrato AD-CS-DA-SRMS-113/2014 no cumplieron técnicamente con los servicios requeridos y no fueron implementados conforme a lo estipulado en el contrato y sus anexos.

3. Contrato AD-CS-DA-SRMS-286/2014

Del análisis del contrato número AD-CS-SRMS/286/2014 celebrado con Sixsigma Networks México, S.A de C.V., mediante el procedimiento de adjudicación directa, con fundamento en los artículos 41, fracción III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (porque existen circunstancias que pudieran provocar pérdidas o costos adicionales), con objeto de prestar los servicios de "Infraestructura de Centro de Datos" (Servicio de Cómputo Empresarial), vigente del 04 de noviembre de 2014 al 17 de octubre de 2017, por un monto mínimo 628,546.8 y máximo 1,568,589.9 miles de pesos, de los cuales se pagaron 479,513.9 miles de pesos durante 2015, se determinó lo siguiente:

El alcance de los trabajos se integró por el aprovisionamiento de infraestructura para virtualización (Motor), enlaces de telecomunicaciones entre los centros de datos propuestos, sistemas de seguridad física y lógica, gestión de desempeño y continuidad del negocio, con las características siguientes:

- Aprovisionamiento tecnológico y migración de datos
- Proceso de migración y optimización de infraestructura
- Aprovisionamiento tecnológico para el Plan de Recuperación de Desastres (DRP)
- Continuidad del servicio
- Transferencia de servicios

Contratación

- De acuerdo a los procedimientos de auditoría Se revisó la investigación de mercado, propuesta y evaluación técnica, propuesta económica y la justificación de la adjudicación directa del contrato; no se detectaron observaciones relevantes.
- Se revisó la investigación de mercado, propuesta y evaluación técnica, propuesta económica y la justificación de la adjudicación directa del contrato.
- Durante el mes de marzo de 2015, se efectuaron pagos por 46,400.0 miles de pesos correspondientes a la Migración y Aprovechamiento de la Infraestructura, no obstante que de acuerdo con las actas de entrega-recepción, acta de terminación y memoria técnica de los servicios instalados y en operación en la Infraestructura del Centro de Datos la solución quedó aprobada e implementada el 3 de julio de 2015, aun cuando quedaba pendiente la migración de 32 servidores por lo que los pagos fueron efectuados de manera anticipada, debido a que los servicios no habían sido devengados en su totalidad.
- Para los entregables de “Disponibilidad del Servicio WEB” y “Equipamiento Local y Remoto” de los meses de marzo, abril, julio y octubre de 2015, se proporcionó un ejemplo de la disponibilidad de los servicios, por lo que los entregables no cumplieron técnicamente con lo requerido y no fue posible acreditar el nivel de disponibilidad de los servicios proporcionados durante el ejercicio 2015.
- Durante el mes de julio de 2015, la Jefatura de Servicios de PENSIONISSSTE solicitó siete cursos para el mes de agosto de 2015 a la Subdirección de Tecnologías de Información; el proveedor proporcionó la propuesta de Servicios Bajo Demanda del 29 de julio de 2015, mediante la cual cotizó los siete cursos por un monto de 208.7 miles de pesos, no obstante, el pago por estos servicios ascendió a 626.2 miles de pesos; por lo tanto, se determinaron pagos en exceso por 417.5 miles de pesos de acuerdo con la tabla siguiente:

Cursos proporcionados a PENSIONISSSTE (Miles de pesos)					
Concepto	Servicios que fueron requeridos y proporcionados		Servicios proporcionados y pagados		Pagos injustificados (B-A)
	Cantidad	Importe cotizado (de acuerdo a la propuesta de servicios bajo demanda) (A)	Cantidad	Importe pagado (B)	
1. Curso de administración de los switches de interconexión de la solución SAN (LOCAL).	2	59.6	2	178.9	119.3
2. Curso de administración de los Enclosures, incluyendo instalaciones de servidores blades.	2	59.6	2	178.9	119.3
3. Curso de administración de la solución del sistema de almacenamiento (REMOTO).	2	59.6	1	89.4	29.8
4. Curso de administración de la solución del sistema de respaldos de datos (REMOTO).	1	29.8	2	178.9	149.1
Total	7	208.7	7	626.2	417.5

Fuente: Elaborado con documentación proporcionado por el ISSSTE

Nota: La suma de los importes puede no coincidir debido al redondeo aplicado.

Por lo anterior, se presume que los pagos por 417.5 miles de pesos correspondientes a los cursos proporcionados por el proveedor son en exceso, debido a que el monto cobrado por los servicios no corresponde a los importes cotizados en la propuesta de Servicios Bajo Demanda del 29 de julio de 2015 y a las condiciones establecidas en el contrato. Cabe señalar que un curso fue cambiado respecto a la solicitud de servicios presentada por el ISSSTE.

15-9-19GYN-02-0295-08-004 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no verificaron las obligaciones derivadas de la celebración del contrato AD-CS-SRMS/286/2014; en consecuencia, se efectuaron pagos en exceso por 417.5 miles de pesos por siete cursos solicitados por PENSIONISSSTE para el mes de agosto de 2015, debido a que los montos cobrados por los servicios no corresponden a los precios cotizados en la propuesta de Servicios Bajo Demanda del proveedor ni a las condiciones establecidas en el contrato.

15-1-19GYN-02-0295-06-003 **Pliego de Observaciones**

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 417,498.34 pesos (cuatrocientos diecisiete mil cuatrocientos noventa y ocho pesos 34/100, M.N.) por los pagos en exceso por siete cursos solicitados por PENSIONISSSTE para el mes de agosto de 2015 derivados del contrato AD-CS-SRMS/286/2014, debido a que los montos cobrados por los servicios no corresponden a los precios cotizados en la propuesta de Servicios Bajo Demanda del proveedor ni a las condiciones establecidas en el contrato.

4. Contrato AD-CS-DA-SRMS-307/2014

Del análisis del contrato número AD-CS-DA-SRMS-307/2014 celebrado con la Universidad Politécnica de Chiapas, mediante el procedimiento de adjudicación directa con fundamento en el Artículo 1°, párrafo quinto, de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público (por los actos jurídicos que se celebren entre dependencias, o bien los que se lleven a cabo entre alguna dependencia o entidad de la Administración Pública Federal con alguna perteneciente a la administración pública de una entidad federativa), con objeto de prestar los “Servicios de Administración, Desarrollo, Mantenimiento y Soporte de Aplicaciones (Unidad de Administración de Proyectos y Calidad)”, vigente del 24 de noviembre de 2014 al 23 de noviembre de 2017, por un monto mínimo de 74,137.9 miles de pesos y un máximo de 259,482.7 miles de pesos, de los cuales se pagaron 83,200.4 miles de pesos durante 2015, se determinó lo siguiente:

El alcance de los trabajos fue medir la calidad y efectividad de las actividades y productos generados por parte de los proveedores que prestan los servicios para las unidades de desarrollo y mantenimiento de software; los servicios consisten en determinar fortalezas y debilidades para lograr una tercerización exitosa y contar con las herramientas adecuadas para gestionar correctamente la calidad de los entregables suministrados por los proveedores, los cuales fueron pagados por concepto de costos fijos y variables.

Revisión de los Pagos

El entregable “Estimación de Esfuerzo – Costo” describe el esfuerzo estimado en horas y su estimado en costo variable; con este reporte se emite la facturación mensual, sin embargo no se contó con los reportes de los meses de febrero, marzo, abril, mayo, junio, julio, octubre y noviembre por los servicios facturados durante 2015, asimismo de los que sí fueron entregados se identificaron diferencias contra lo facturado.

Asimismo, no se contó con la documentación que permita identificar la cantidad de recursos humanos, perfiles, responsabilidades y actividades realizadas que sirvieron de base para determinar el número de horas que fueron facturadas en el costo variable pagadas en 2015.

Análisis de los Entregables

Se seleccionaron los meses de febrero y octubre de 2015, por los cuales se pagaron 23,681.4 miles de pesos que representan el 28.5% del total pagado en 2015.

- En las actas de entrega recepción no se incluyeron 47 entregables acordados entre el Instituto y el proveedor mediante minuta de fecha 9 de diciembre de 2014, por lo que no se cuenta con información que acredite su desarrollo.
- En relación con los entregables del costo fijo del mes de febrero, el acta de entrega-recepción enlista un total de 285 entregables de los cuales uno de éstos no fue proporcionado y en 174 (61.1%) no se identifica la fecha de elaboración, revisión y autorización de los mismos.

Cumplimiento del Objeto del Contrato

- Para el cumplimiento de los objetivos de los servicios a realizar por el proveedor, en el Anexo Técnico del contrato se señala que se deberá contar con la implantación y operación de un modelo de “Servicio de Administración, Desarrollo, Mantenimiento y Soporte de Aplicaciones (ADMA)”, sin embargo, éste no fue aprobado ni implementado por el ISSSTE.
- No se contó con el soporte documental que acredite la definición e implementación de los planes de los acuerdos de niveles de operación, transición, acciones de mejora, riesgos, así como las estrategias para la priorización, seguimiento y administración de proyectos.
- No se dio cumplimiento a los objetivos del servicio de acuerdo con el contrato y anexos técnicos.

Administración y Medición de Proyectos.

- Se carece de la documentación que acredite las actividades realizadas por el Instituto para validar que las labores ejecutadas por parte de la Unidad de Administración de Proyectos y Calidad (UAPC) para la administración de proyectos se realizaron con base en las mejores prácticas, de acuerdo con lo establecido en el contrato y su anexo técnico.
- No fue posible visualizar la herramienta utilizada para la gestión de incidentes, la lista de incidentes registrados y el flujo de actividades desde su registro hasta su solución. Asimismo, no fue posible verificar el procedimiento para realizar la actualización de la

información contenida en la herramienta y al personal que contaba con acceso a la misma, debido a que se dio por terminada la relación contractual el 31 de julio de 2016.

- Se carece de documentación que permita acreditar las actividades realizadas por los líderes técnicos de cada sistema para validar que las iniciativas se encuentren alineadas con los objetivos y visión del Instituto y de la Dirección de Tecnología y Estrategia Digital, que permitan dar cumplimiento a los objetivos establecidos en el anexo técnico del contrato.

Aseguramiento de Calidad de Procesos y Productos

- Se identificaron retrasos hasta de 11 meses en la entrega de los reportes de Auditorías de Calidad, las cuales al no presentarse con oportunidad tuvieron un impacto en la eficacia de sus recomendaciones. Adicionalmente, no se identificó al personal que participó en la elaboración, revisión y autorización de los mismos.
- Se carece del documento de planeación de las auditorías de calidad, que permita identificar las ejecutadas durante 2015, conforme a lo establecido en el Anexo Técnico.
- Se carece del soporte que permita acreditar que los programas de aseguramiento de la calidad organizacional, plan de mejora de procesos y reporte de mediciones relacionadas a la ejecución de la mejora de procesos, se encuentran implementados en el Instituto.
- No se proporcionó documentación de los hallazgos o no conformidades identificados por el proveedor durante 2015, así como las acciones para remediarlos, conforme se estipula en el anexo técnico del contrato.

Despliegue y Capacitación

- Para la Capacitación de la Mesa de Ayuda, no se tiene evidencia documental que acredite la relación del personal que participó y las fechas en que se llevó a cabo la capacitación.

Los pagos injustificados por los entregables que incumplieron los requerimientos del contrato y anexos técnicos, se ven reflejados en la tabla siguiente:

Pagos injustificados del Contrato AD-CS-DA-SRMS-307/2014
(Miles de pesos)

Folio	Fecha	Costo	Total
07 E	14/01/2015	Costo	Fijo: 2,059.4
		3.1.2.1 Entregables de Administración y Medición de	Proyectos.
		3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	
		Costo	Variable: 2,730.4
		3.1.2.1 Entregables de Administración y Medición de Proyectos.	
06 E	12/01/2015	Costo	Variable: 2,172.0
		3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	
		Costo	Variable: 245.7
		3.1.2.3 Entregables de Arquitectura de Software.	
06 E	12/01/2015	Costo	Fijo: 514.8
		3.1.2.1 Entregables de Administración y Medición de	Proyectos.
		3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	
		Costo	Variable: 553.5
		3.1.2.1 Entregables de Administración y Medición de Proyectos.	

Pagos injustificados del Contrato AD-CS-DA-SRMS-307/2014
(Miles de pesos)

Folio	Fecha	Costo	Total
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 732.7
19 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad.	Fijo: 2,059.4 Proyectos
20 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable 1,075.7
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable 1,958.0
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable 230.3
21 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad.	Fijo: 2,059.4 Proyectos
22 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 3,300.2
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 4,587.7
		Costo 3.1.2.4 Entregables de Despliegue y capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable: 434.9
23 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4 Proyectos.
24 E	22/06/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 1,448.2
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 1,833.4
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicios de Análisis y Levantamiento de Requisitos.	Variable: 809.4
31 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4 Proyectos.
32 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 917.9
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 692.4
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable: 759.9
33 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4 Proyectos.
34 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 1,268.2
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 722.7

Pagos injustificados del Contrato AD-CS-DA-SRMS-307/2014
(Miles de pesos)

Folio	Fecha	Costo	Total
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable: 409.0
35 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4
36 E	01/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 613.0
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 471.3
		3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	405.3
38 E	02/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4
40 E	04/09/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable 560.0
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable 481.9
41 E	01/10/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo: 2,059.4
42 E	01/10/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable: 2,123.4
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable: 1,304.5
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable: 418.7
44 E	18/11/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo 2,059.4
43 E	18/11/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable 2,648.8
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable 1,873.8
		Costo 3.1.2.4 Entregables de Despliegue y Capacitación Servicio de Análisis y Levantamiento de Requisitos.	Variable 232.5
45 E	19/11/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo 2,059.4
46 E	19/11/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable 8,919.4
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable 2,320.4

Pagos injustificados del Contrato AD-CS-DA-SRMS-307/2014
(Miles de pesos)

Folio	Fecha	Costo	Total
47 E	08/12/2015	Costo 3.1.2.1 Entregables de Administración y Medición de 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Fijo 2,059.4
48 E	08/12/2015	Costo 3.1.2.1 Entregables de Administración y Medición de Proyectos.	Variable 4,226.2
		Costo 3.1.2.2 Entregables de Aseguramiento de Calidad de Procesos y Productos.	Variable 4,491.4
TOTAL			83,200.4

Fuente: Elaborado con documentación proporcionada por el ISSSTE.

El Instituto no sustentó los pagos realizados al proveedor, asimismo se detectaron deficiencias en la gestión del contrato, debido a que no fue autorizado ni implementado el modelo de servicios ADMA, así como tampoco fue posible verificar las actividades ejecutadas por el proveedor, por lo tanto, los pagos realizados a la Universidad Politécnica de Chiapas correspondientes a los servicios de: Administración y Medición de Proyectos, Servicio de Aseguramiento de Calidad de Procesos, Servicio de Arquitectura de Software y Servicio de Despliegue y Capacitación por 83,200.4 miles de pesos son injustificados.

En relación con el Desarrollo de Soluciones Tecnológicas, se carece de la documentación que acredite que el Instituto cuenta con una metodología para el desarrollo de soluciones de TIC, así como para la definición de procedimientos del proceso de desarrollo de soluciones, revisiones de calidad, cerrar iniciativas y proyectos de TIC, definir requerimientos de los nuevos servicios y diseñar los servicios de TIC; adicionalmente, se carece de documentación en donde se identifiquen los criterios para la segregación de funciones de los ambientes de desarrollo y producción.

15-1-19GYN-02-0295-01-001 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado instrumente una metodología para el desarrollo de soluciones de TIC, que considere entre otros elementos, los requerimientos de los servicios, el diseño de las soluciones, las revisiones de calidad, el cierre de las iniciativas y la evaluación de los beneficios de los proyectos; asimismo, que implemente controles para la segregación de funciones en los ambientes de desarrollo y producción de las soluciones tecnológicas.

15-9-19GYN-02-0295-08-005 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no verificaron ni cumplieron con los compromisos del contrato AD-CS-DA-SRMS-307/2014; debido a que se carece de elementos para verificar los recursos humanos asignados al proyecto así como el detalle de actividades y horas facturadas; así mismo se corrobora la falta de implementación del modelo de "Servicio de Administración,

Desarrollo, Mantenimiento y Soporte de Aplicaciones (ADMA)"; se carece de documentación que acredite el aprovechamiento e implementación de los programas de aseguramiento de la calidad, plan de mejora de procesos y reporte de mediciones a la ejecución de la mejora de procesos; por lo tanto, los servicios de Administración y Medición de Proyectos, Servicio de Aseguramiento de Calidad de Procesos, Servicio de Arquitectura de Software y Servicio de Despliegue y Capacitación del contrato AD-CS-DA-SRMS-307/2014 no han tenido utilidad ni beneficio para el instituto; en consecuencia los pagos realizados por un monto de 83,200.4 miles de pesos se presumen injustificados.

15-1-19GYN-02-0295-06-004 **Pliego de Observaciones**

Se presume un probable daño o perjuicio o ambos a la Hacienda Pública Federal por un monto de 83,200,429.96 (ochenta y tres millones doscientos mil cuatrocientos veintinueve pesos 96/100 M.N) por los pagos injustificados correspondientes a los servicios de Administración y Medición de Proyectos, Servicio de Aseguramiento de Calidad de Procesos, Servicio de Arquitectura de Software y Servicio de Despliegue y Capacitación, del contrato AD-CS-DA-SRMS-307/2014 no tuvo utilidad ni beneficio para el instituto.

5. Contrato núm. AD-CS-DA-SRMS-002/2015

Del análisis del contrato número AD-CS-DA-SRMS-002/2015, celebrado con Bconnect Services, S.A. de C.V., mediante el procedimiento de Adjudicación Directa al amparo del artículo 41, fracción XX, de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público (debido a la suscripción de contratos específicos que deriven de un contrato marco), con objeto de la Prestación de los Servicios de Centro de Contacto, con una vigencia del 01 de enero de 2015 al 31 de diciembre 2017, por un monto mínimo de 201,895.1 miles de pesos y un máximo de 504,737.8 miles de pesos, de los cuales se pagaron 91,319.6 miles de pesos durante 2015, se determinó lo siguiente:

El alcance de los trabajos fue proporcionar el servicio del Centro de Atención Telefónica (CAT), como enlace entre los derechohabientes, el ISSSTE y las diferentes áreas que requieran de los servicios que se prestan a través de sus Unidades Médicas y oficinas. El servicio consiste en la programación de citas a través del aplicativo "Sistema de Cita Médica Telefónica e Internet", el cual prestará el servicio de Campañas Telefónicas y otros a través de una Plataforma, que permita contar con el registro de todas las actividades realizadas en cada campaña telefónica, envío de mensaje SMS, correo electrónico y video chat, así como la aplicación de reconocimiento y biometría de voz.

Proceso de Contratación

- Se incumplió con el nivel de disponibilidad del 99.9% requerido en el anexo técnico del contrato para el servicio del Centro de Datos del proveedor, durante el recorrido de pruebas al Centro de Datos ubicado en Gómez Palacio, Durango, se constató que su nivel de disponibilidad era del 99.0%, acreditado mediante el certificado ICREA nivel II que así lo avala.
- Conforme a lo estipulado en el contrato, se carece de la documentación que permita acreditar que el Instituto verificó que el personal del proveedor asignado cumplió con los perfiles establecidos para la prestación de los servicios.

Análisis de los Entregables

Se seleccionaron los meses de enero, octubre y noviembre de 2015, por los cuales se pagaron 27,703.5 miles de pesos que representan el 30.3% del total pagado en 2015, identificando lo siguiente:

- La facturación mensual se valida con un archivo en Excel el cual muestra las cantidades y servicios realizados en cada mes, sin embargo, se observó que es generado por el proveedor y se carece de evidencia de las validaciones efectuadas por el ISSSTE para confirmar que las cantidades por servicios facturados fueron correctos.
- La base para el cálculo de penalizaciones se determinó de acuerdo a lo facturado, sin embargo, debido a la falta de validación de las cantidades y servicios por parte del ISSSTE, no es posible acreditar que la determinación de las penalizaciones sea imparcial y correcta.
- Respecto al proceso que garantice el cumplimiento de los niveles de servicio se entregó el documento "Proceso de Validación de Entregables vs Facturación", con el cual el ISSSTE revisa la cantidad de llamadas y su detalle; sin embargo, no fue posible identificar las actividades realizadas por el Instituto para garantizar la cantidad y detalle de cada una de las llamadas, ni la integridad de los reportes de llamadas contestadas.
- No se cuenta con un control que permita identificar el porcentaje real de abandono, el tiempo de espera máximo en las llamadas recibidas, el umbral de desborde o denegación de servicio, así como para asegurar que se reciben todas las llamadas efectuadas por los derechohabientes.

Por lo anterior, se concluye que existieron deficiencias en la gestión del contrato, en razón de que no fue posible acreditar las actividades realizadas por el Instituto para los controles siguientes: validaciones para confirmar que las cantidades de los servicios facturados por el proveedor son correctos; determinación imparcial y correcta de las penalizaciones por incumplimiento de los niveles de servicio; controles para verificar el porcentaje real de abandono, el tiempo de espera máximo en las llamadas recibidas, el umbral de desborde de llamadas o denegación de servicio, así como para asegurar que se reciben todas las llamadas efectuadas por los derechohabientes.

15-1-19GYN-02-0295-01-002 Recomendación

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado instrumente los mecanismos de control a efecto de verificar que las cantidades de los servicios facturados por el proveedor son correctos; determinar de manera imparcial las penalizaciones por incumplimiento de los niveles de servicio; así como asegurar que se reciben todas las llamadas efectuadas por los derechohabientes para la mejora continua del servicio.

15-9-19GYN-02-0295-08-006 Promoción de Responsabilidad Administrativa Sancionatoria

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no acreditaron las actividades realizadas por el Instituto para la

adecuada administración del contrato AD-CS-DA-SRMS-002/2015 debido a que no se realizan las validaciones para confirmar que las cantidades de los servicios facturados por el proveedor son correctos; no cuentan con elementos de información objetiva para que en su caso puedan aplicar correctamente las penalizaciones y no establecer controles para verificar el porcentaje real de abandono, el tiempo de espera máximo en las llamadas recibidas, el umbral de desborde de llamadas o denegación de servicio, así como para asegurar que se reciben todas las llamadas efectuadas por los derechohabientes por dichas actividades se pagaron 91,319.6 miles de pesos.

6. Gobierno y Administración de las TIC

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

- El Grupo de Trabajo para la Dirección de TIC no verificó las inversiones en materia de TIC y que éstas se encuentran alineadas a los objetivos estratégicos del Instituto.
- Se carece de un procedimiento que permita evaluar y vigilar los niveles de servicio en todas las contrataciones de TIC del Instituto.
- No se identificó el mecanismo mediante el cual el Responsable de la Seguridad de la Información comunicó al Grupo de Trabajo para la Dirección de TIC los criterios técnicos de Seguridad de la Información para gestionar los riesgos en la Institución durante el 2015.
- No existe evidencia para validar que durante el ejercicio 2015 se dio seguimiento al presupuesto autorizado de TIC a nivel Institucional, así como al presupuesto autorizado del Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC).
- No se cuenta con evidencia que permita validar que los proyectos del PETIC 2015 cuentan con una línea base y programa de trabajo.
- Se carece de indicadores de desempeño para los procesos de TIC ejecutados en 2015, que permitan identificar posibles desviaciones para mitigar los riesgos en la operación.
- Durante 2015, no se identificó la implementación de metodologías para la gestión de riesgos de TIC.
- No se tiene evidencia de la evaluación de Segregación de Funciones en las actividades operativas de TIC, que permita identificar oportunamente procedimientos que pudieran impactar en fraude, irregularidades en los procesos, duplicidad de funciones, etc.

Análisis de Datos Abiertos

En relación con el “DECRETO por el que se establece la regulación en materia de Datos Abiertos” se detectó lo siguiente:

- No se realizaron las designaciones del Enlace Institucional y del Administrador de Datos Abiertos, por lo que se incumplió con la obligación de notificarlas a la Unidad de Gobierno

Digital de la Secretaría de la Función Pública (SFP) y a la Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República.

- No se cuenta con evidencia de que se haya solicitado a la Unidad de Enlace de transparencia, el reporte del acceso a la información pública más recurrente del ISSSTE.
- No se encontraron: los conjuntos de datos solicitados anualmente mediante la Infraestructura Estratégica de Datos Abiertos; así como los considerados como Información de Interés Nacional, los de carácter público que sean publicados en los sitios, micrositios y otras plataformas institucionales; así como los datos demandados por la ciudadanía mediante las solicitudes de acceso a la información más recurrentes.
- No se cumplió con lo establecido en el Cronograma de implementación por parte de las entidades, así como los mecanismos para seguridad y privacidad de datos.

De la evaluación al avance en la implementación del MAAGTICSI, el cual fue reportado al 47.0% por el ISSSTE en todos sus procesos, de un universo de 48 subprocesos, la entidad fiscalizadora revisó una muestra de 29 (60.4%), detectando inconsistencias en ocho de ellos (27.6%), con lo cual se estima un 43% de avance en la implementación, detectándose observaciones en: seguimiento a la planeación estratégica; seguimiento del presupuesto de TIC; diseño de los servicios; diseño del sistema de gestión de seguridad de la información; elaboración del análisis de riesgos; identificación de iniciativas de TIC; así como el monitoreo al avance del desempeño de los proveedores.

Por lo anterior, se identificó falta de implementación de la segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; incumplimiento del Decreto en materia de Datos Abiertos; el seguimiento de la planeación estratégica de TIC; el seguimiento del presupuesto de TIC; el diseño del sistema de gestión de seguridad de la información; la elaboración del análisis de riesgos; la identificación de iniciativas de TIC; así como el monitoreo del avance del desempeño de los proveedores.

En la Cuenta Pública 2012 se determinó el 37.9% de cumplimiento de las disposiciones, procesos y reglas que establece el MAAGTIC-SI y en el proceso “Administración para el Desarrollo de Soluciones Tecnológicas” un nivel de implementación crítico del 10.0%; por lo tanto, el avance del ISSSTE en la implementación del marco rector de procesos para las TIC resulta deficiente.

15-1-19GYN-02-0295-01-003 **Recomendación**

Para que Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado Instrumente los mecanismos de control necesarios para implementar la segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; el cumplimiento del Decreto en materia de Datos Abiertos; el seguimiento a la planeación estratégica de TIC; el seguimiento del presupuesto de TIC; el diseño e implementación del sistema de gestión de seguridad de la información; la elaboración del análisis de riesgos; así como el monitoreo del avance del desempeño de los proveedores.

15-9-19GYN-02-0295-08-007 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y, en su caso, inicie

el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no verificaron ni cumplieron con la implementación de segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; la instrumentación del Decreto en materia de Datos Abiertos; el seguimiento de la planeación estratégica de TIC; el seguimiento del presupuesto de TIC; el diseño de los servicios; el diseño del sistema de gestión de seguridad de la información; la elaboración del análisis de riesgos; la identificación de iniciativas de TIC; así como el monitoreo al avance del desempeño de los proveedores.

7. Gestión de la Seguridad de Tecnologías de la Información y Comunicaciones (TIC) y Continuidad de los Servicios.

De la revisión y análisis de la información proporcionada por el ISSSTE relacionada con la Administración de la Seguridad de la Información (ASI) y la Operación de los controles de la Seguridad de la Información y del ERISC (OPEC), se determinó que los controles de seguridad de la información y continuidad de las operaciones no son suficientes; se observó lo siguiente:

Seguridad de la Información

- Durante el ejercicio 2015, no se contó con la designación del responsable de la Seguridad de la Información en el Instituto ni se informó al Centro de Investigación y Seguridad Nacional (CISEN). Asimismo no se contó con un enlace para mantener comunicación con el Equipo de Respuesta a Incidentes de Seguridad (ERISC) con otras Instituciones.
- No se cuenta con evidencia de las sesiones realizadas durante 2015 que acrediten la operación de los grupos de trabajo siguientes: Grupo Estratégico Multidisciplinario de TIC y Seguridad de la Información; Equipos de trabajo de Infraestructura Crítica y Análisis de Riesgos; Equipo de Respuesta a Incidentes (ERISC).
- No se acreditó la definición e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en el Instituto, así como la documentación para verificar su eficacia, eficiencia y mejora continua.
- En relación con la atención de incidentes, no se cuenta con soporte documental que permita validar que se llevaron a cabo actividades de investigación técnica de los incidentes, erradicación de los mismos, así como la recuperación de la operación.
- Se carece del soporte técnico que permita validar que dentro de los dispositivos móviles asignados a los empleados del ISSSTE, se instalan mecanismos de cifrado de información que permitan asegurar la información reservada de la Institución.
- Se carece de un análisis de riesgos del área de TIC.
- En relación con la administración de cuentas de usuarios en el Instituto, no se cuenta con evidencia de la revisión periódica de los movimientos generados por los usuarios.
- No se acreditó la implementación de pistas o bitácoras de auditoría en los aplicativos y bases de datos de la institución.
- No se cuenta con un catálogo de los dueños de los aplicativos del Instituto.
- No se cuenta con un procedimiento para el uso de herramientas de borrado seguro en los equipos de cómputo.

- Se carece de procedimientos para conectar remotamente los equipos de cómputo a la red institucional del ISSSTE.
- Se carece de políticas para determinar la viabilidad del software que se pretende adquirir e instalar en los equipos de cómputo, dispositivos electrónicos o sistemas de información.

De la revisión de los objetivos de la Seguridad de la Información y Operación de los controles de la seguridad de la información y del ERISC, se obtuvo que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos del ISSSTE son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y OPERACIÓN DEL ERISC	
Factor crítico	Riesgo
Sistema de Gestión de Seguridad de la Información (SGSI)	La carencia de implementación del SGSI ocasiona principalmente la pérdida de la confidencialidad de la información que puede ser conocida y utilizada por personas que no tienen autorización; falta de integridad ya que los datos que pueden ser alterados con facilidad, provocando pérdidas económicas y fraudes; falta de disponibilidad que impide que los usuarios accedan a las aplicaciones cuando lo requieran y falta de "no repudio" de las transacciones para evitar que los usuarios pueden negar que realizaron alguna modificación a la información, ya no existe evidencia que demuestre lo contrario.
Gestión de incidentes del ERISC	La falta de gestión de los incidentes del ERISC, impide la identificación de los problemas 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.
Análisis de Riesgos	Se carece de la identificación, clasificación y priorización de los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, de manera que se obtengan planes de remediación y mitigación para definir los controles a implantar de acuerdo a las capacidades y recursos de las áreas, proporcionales a su valor e importancia, para mantener aceptable el nivel de riesgos y evitar la materialización de las amenazas.
Administración de usuarios	Debido a que no se cumplen los procedimientos para la gestión de claves de usuarios, éstos podrían tener permisos para acceder a información que no le corresponde de acuerdo a sus funciones y responsabilidades, en consecuencia, se pierde la confidencialidad en la información y se pueden ejecutar transacciones no autorizadas que ponen en riesgo los activos de la institución.
Monitoreo de las pistas de auditoría y las 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
Carencia del Responsable de la Seguridad de la Información	No se cuenta con un responsable que permita asegurar el cumplimiento de las acciones en materia de seguridad, mecanismos de control y administración de riesgos, entre otros, para vigilar la correcta operación y aseguramiento de la información del instituto, con la finalidad de que las acciones emprendidas sean consecuentes con lo previsto en las normativas vigentes.

Continuidad de la Operación

- Se carece del análisis de impacto al negocio (BIA), en el que se identifiquen las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el impacto de las consecuencias que se generarían.
- No se cuenta con evidencia que permita validar la implementación del Plan de Continuidad del Negocio (BCP).
- Se carece de un plan de capacidad de la infraestructura tecnológica, que le permita al Instituto cumplir con los niveles de servicio acordados; el crecimiento previsto de la demanda de infraestructura; la mejora de los niveles de servicio y la incorporación de los nuevos servicios de TIC.

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

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES EN LOS PROGRAMAS DE CONTINUIDAD DE LAS OPERACIONES

Factor Crítico	Principales Riesgos por su Carencia y sus Consecuencias Potenciales para las Operaciones y Activos
Análisis de impacto al negocio	Se carece de la identificación de las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias que se generarían, por lo tanto, los puntos objetivos de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) de la información, serían mucho mayores a los requeridos para la continuidad de las operaciones.
Plan de Capacidad de la infraestructura tecnológica	No se cuenta con la evaluación y seguimiento para que todos los servicios se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada, en consecuencia, los recursos no se aprovechan adecuadamente y se realizan acciones equivocadas en mantenimiento y administración, aunado a que los recursos pueden ser insuficientes con la consecuente degradación de la calidad del servicio.

Por lo anterior, se reflejan deficiencias en la definición e implementación del Sistema de Gestión de Seguridad de la Información (SGSI); Gestión de incidentes del ERISC; Análisis de Riesgos; Administración de usuarios; Monitoreo de las pistas de auditoría y las bitácoras de los aplicativos y bases de datos; Implementación del Análisis de Impacto al Negocio y Plan de Capacidad de la infraestructura tecnológica.

En la Cuenta Pública 2012 se identificaron deficiencias en el manejo de cuentas privilegiadas, pistas de auditoría, facultades de usuarios, borrado seguro de equipos y análisis de impacto al negocio, éstas se debieron a la falta de cumplimiento en el establecimiento de un SGSI, por lo que se concluye que la Dirección de Tecnología y Desarrollo Institucional ha tenido avances precarios para fortalecer la Seguridad de la Información y la Continuidad de las Operaciones en el Instituto.

15-1-19GYN-02-0295-01-004 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado implemente los controles y las acciones para la instrumentación del Sistema de Gestión de

Seguridad de la Información (SGSI); Gestión de incidentes del ERISC; Análisis de Riesgos; Administración de usuarios; Monitoreo de las pistas de auditoría y las bitácoras de los aplicativos y bases de datos; Análisis de Impacto al Negocio y Plan de Capacidad de la infraestructura tecnológica.

15-9-19GYN-02-0295-08-008 **Promoción de Responsabilidad Administrativa Sancionatoria**

Ante el Órgano Interno de Control en el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, para que realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por los actos u omisiones de los servidores públicos que en su gestión no vigilaron ni implementaron los controles para el Sistema de Gestión de Seguridad de la Información (SGSI); Gestión de incidentes del ERISC; Análisis de Riesgos; Administración de usuarios; Monitoreo de las pistas de auditoría y las bitácoras de los aplicativos y bases de datos; Análisis de Impacto al Negocio y Plan de Capacidad de la infraestructura tecnológica.

Recuperaciones Probables

Se determinaron recuperaciones probables por 109,205.0 miles de pesos.

Resumen de Observaciones y Acciones

Se determinó(aron) 6 observación(es) la(s) cual(es) generó(aron): 4 Recomendación(es), 8 Promoción(es) de Responsabilidad Administrativa Sancionatoria y 4 Pliego(s) de Observaciones.

Adicionalmente, en el transcurso de la auditoría se emitió(eron) oficio(s) para solicitar o promover la intervención de la(s) instancia(s) de control competente con motivo de 1 irregularidad(es) detectada(s).

Dictamen

Con base en los resultados de la auditoría practicada al Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, 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 719,942.8 miles de pesos se concluye que en términos generales no cumplió con las disposiciones legales y normativas que son aplicables en la materia debido a los resultados descritos en el presente informe de auditoría, los cuales arrojaron deficiencias que son importantes, entre las que destacan las siguientes:

- El Instituto no sustentó los pagos realizados al proveedor, asimismo se detectaron deficiencias en la gestión del contrato, debido a que no fue autorizado ni implementado el modelo de servicios ADMA, así como tampoco fue posible verificar las actividades ejecutadas por el proveedor, por lo tanto, los pagos realizados a la Universidad Politécnica de Chiapas correspondientes a los servicios de: Administración y Medición de Proyectos, Servicio de Aseguramiento de Calidad de Procesos, Servicio de Arquitectura

de Software y Servicio de Despliegue y Capacitación por 83,200.4 miles de pesos son injustificados.

- Se determinaron pagos injustificados por 24,938.9 miles de pesos, debido a que los entregables para el análisis, diseño e implementación de las soluciones de seguridad informática no cumplieron técnicamente con los servicios requeridos, aunado a que no fueron implementados conforme a lo estipulado en el contrato y sus anexos.
- En el pago de servicio para la implementación de soluciones de seguridad informática, se identificó que el procedimiento de conversión de dólares a pesos fue realizado con un criterio distinto al estipulado en el contrato, por lo que se identifican pagos en exceso por 648.2 miles de pesos.
- Se presumen pagos en exceso por 417.5 miles de pesos, correspondientes a siete cursos solicitados por PENSIONISSSTE derivados del contrato de servicios de Infraestructura de Centro de Datos, debido a que los montos cobrados no corresponden a los precios cotizados por el proveedor ni a las condiciones establecidas en el contrato.
- El contrato para los Servicios de Centro de Contacto Telefónico para la Atención de Llamadas, carece de los controles: validaciones para confirmar que las cantidades de los servicios facturados por el proveedor son correctos; determinación imparcial y correcta de las penalizaciones por incumplimiento de los niveles de servicio; controles para verificar el porcentaje real de abandono, el tiempo de espera máximo en las llamadas recibidas, el umbral de desborde de llamadas o denegación de servicio, así como para asegurar que se reciben todas las llamadas efectuadas por los derechohabientes.
- Se carece de una metodología para el desarrollo de soluciones de TIC, que considere entre otros elementos, los requerimientos de los servicios, el diseño de las soluciones, las revisiones de calidad, el cierre de las iniciativas y la evaluación de los beneficios de los proyectos.
- En materia de Gobierno de las Tecnologías de la Información y Comunicaciones (TIC), se carece de la implementación de segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; la instrumentación del Decreto en materia de Datos Abiertos; el seguimiento de la planeación estratégica de TIC; el seguimiento del presupuesto de TIC; la identificación de iniciativas de TIC, así como el monitoreo al avance del desempeño de los proveedores.
- Respecto a la Seguridad de la Información y Continuidad de las Operaciones, se carece de los controles para el Sistema de Gestión de Seguridad de la Información (SGSI); Gestión de incidentes del ERISC; Análisis de Riesgos; Administración de usuarios; Monitoreo de las pistas de auditoría y las bitácoras de los aplicativos y bases de datos; Análisis de Impacto al Negocio, así como el Plan de Capacidad de la infraestructura tecnológica.
- En la Cuenta Pública 2012 se determinó el 37.9% de cumplimiento de las disposiciones, procesos y reglas que establece el MAAGTIC-SI y en el proceso “Administración para el Desarrollo de Soluciones Tecnológicas” un nivel de implementación crítico del 10.0%; por

lo tanto, el avance del ISSSTE en la implementación del marco rector de procesos para las TIC resulta deficiente.

- En la Cuenta Pública 2012 se identificaron deficiencias en el manejo de cuentas privilegiadas, pistas de auditoría, facultades de usuarios, borrado seguro de equipos y análisis de impacto al negocio, éstas se debieron a la falta de cumplimiento en el establecimiento de un SGSI, por lo que se concluye que la Dirección de Tecnología y Desarrollo Institucional ha tenido avances precarios para fortalecer la Seguridad de la Información y la Continuidad de las Operaciones en el Instituto.

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

El presente dictamen se emite el 07 de noviembre de 2016, fecha de conclusión de los trabajos de auditoría correspondientes a la Cuenta Pública 2015, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable.

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública corresponden con las registradas por la entidad fiscalizada en su Estado del Ejercicio del Presupuesto y Auxiliares Presupuestales; asimismo verificar que los registros presupuestarios y contables de los recursos asignados a las TIC cumplen con la normativa.
2. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; analizar la documentación de las contrataciones para descartar asociaciones indebidas, subcontrataciones en exceso, adjudicaciones sin fundamento, transferencia de obligaciones, suscripción de los contratos (facultades para la suscripción, cumplimiento de las obligaciones fiscales, fianzas), revisar que los contratos plurianuales se sujetan a la autorización correspondiente, entre otros.
3. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuenten con controles para su fiscalización, correspondan a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización en caso de incumplimientos.
4. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados vinculados con la infraestructura tecnológica, telecomunicaciones y aplicativos sustantivos para verificar: antecedentes; investigación de mercado; adjudicación; beneficios esperados; análisis de entregables (términos, vigencia, entrega, resguardo, operación, penalizaciones y garantías); pruebas de cumplimiento y sustantivas; implementación y post-Implementación. Evaluar el riesgo inherente en la administración de proyectos, desarrollo de soluciones tecnológicas, administración de

procesos y servicios administrados, así como el plan de mitigación para su control, manejo del riesgo residual y justificación de los riesgos aceptados por la entidad.

5. Evaluar el nivel de gestión que corresponde a los procesos relacionados con la dirección, el control y la administración de riesgos en materia de tecnologías de la información y comunicaciones; analizar el diagnóstico de las funciones sustantivas y administrativas de las TIC que lleva a cabo la entidad fiscalizada; evaluar el nivel de alineación de la estrategia de TIC con los objetivos de la Organización, así como de los mecanismos de medición, seguimiento y cumplimiento de sus metas; revisar el avance en la implementación del Manual Administrativo de Aplicación General en las Materias de Tecnologías de Información y Comunicaciones y, en la de Seguridad de la Información (MAAGTICSI) o, en su caso, la normativa que aplique y revisar el cumplimiento de las disposiciones en materia de Datos Abiertos.
6. Realizar pruebas sustantivas a los resultados relevantes del estudio de TIC en materia de Desarrollo de Sistemas; analizar el Ciclo de Vida y Soporte del aplicativo sustantivo más relevante para la operación de la entidad (evaluación del riesgo, gestión del proyecto, control de cambios, seguridad desde el diseño, pruebas selectivas de integridad lógica) y evaluar la gestión de la configuración, problemas y operaciones.
7. Evaluar los mecanismos para la administración de la seguridad de la información, así como la disminución del impacto de eventos adversos que potencialmente podrían afectar los objetivos de la institución o constituir una amenaza para la seguridad nacional; evaluar el nivel de cumplimiento en la optimización del riesgo, gestión de seguridad de la información y gestión de los programas de continuidad de las operaciones.

Áreas Revisadas

La Subdirección de Recursos Materiales y Servicios; la Subdirección de Programación y Presupuesto; la Subdirección de Tecnología de la Información; la Subdirección de Coordinación de Proyectos y la Subdirección de Innovación y Calidad.

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. Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 1;
2. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 66, fracción III;
3. Otras disposiciones de carácter general, específico, estatal o municipal: Acuerdo por el que se emiten las disposiciones en Materia de Control Interno publicado en DOF el 12 de julio de 2010 y reforma del 2 de mayo de 2014, Disposición 12, Capítulo III

Acuerdo que tiene por objeto emitir las Políticas y Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias publicado el 8 de mayo de 2014 en el Diario Oficial de la

Federación (DOF): artículos 10, fracción VII; 11, fracción II; Procesos II.A. Proceso de Administración de Servicios (ADS), Actividad ADS 3, Factor Crítico 6; Actividad ADS 5, Factores Críticos: 4 y 6; ADS 6; II.C. Proceso de Administración de la Seguridad de la Información (ASI), Actividades ASI 1, ASI 2, ASI 3, ASI 5, ASI 6 y ASI 7; III.A Proceso de Administración de Proyectos (ADP); III.B Proceso de Administración de Proveedores (APRO), Actividad APRO 2; III.C Proceso de Administración de la Operación (AOP), Actividades AOP 1 AOP 2 AOP 4 y AOP 6; III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC), Actividad OPEC 1, OPEC 2, OPEC 5; Apéndice IV.B Matriz de metodologías, normas y mejores prácticas y estándares internacionales en la materia (ISO 9001-2015, PE, COBIT, DSS06.03 "Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización");

Guía de Implementación de la Política de Datos Abiertos, publicada el 18 de junio de 2016 en el DOF: Paso "1.1 Formar un equipo de Trabajo"; Paso "1.3 Priorizar los datos de valor";

Contrato AD-CS-DA-SRMS-113/2014: cláusula tercera, séptima, novena y décima quinta.

Anexo 1 del Contrato AD-CS-DA-SRMS-113/2014: apartado: "Descripción de los servicios": A1 Soluciones para Tecnologías de la Información y Comunicaciones (TICs): A1.3 Aseguramiento de ingresos, viñeta 1, 2, 3; A1.4 Administración de identidades de acceso identity management/authenticity management (IDM/IAM) viñetas 1-8; "Alcance del servicio": Objetivo: A1.3 Aseguramiento de ingresos, Objetivo: Metodología propuesta, Entregables Fase II y III y A1.4 Administración de identidades de acceso identity management/authenticity management (IDM/IAM), Objetivo: Metodología propuesta y Entregables Fase IV.

Contrato AD-CS-DA-SRMS-286/2014: Cláusulas Cuarta; Quinta; Octava; Decima Octava;

Anexo No. 1 del Anexo Técnico del Contrato AD-CS-DA-SRMS-286/2014: Apartados Entregables del Servicio; Administración de la Capacidad y Niveles de Servicio y Nivel de Servicio Disponibilidad.

Anexo 2 Propuesta Técnica y Económica del Contrato AD-CS-DA-SRMS-286/2014: Apartado Servicios de Suministro en Demanda Centro de Datos Primario.

Contrato AD-CS-DA-SRMS-307/2014 y su Anexo Técnico.

Minuta de fecha 9 de diciembre de 2014.

Contrato AD-CS-DA-SRMS-307/2014: Cláusula Tercera "Productos Entregables".

Contrato: AD-CS-DA-SRMS-002/2015: Declaraciones II.6, Cláusulas Octava, Calidad; Décima Cuarta, Verificación de las especificaciones y aceptación de los servicios; Décima Quinta, Pena Convencional.

Contrato Marco de fecha 1º de julio de 2013, Apartados II.5.1 y II.5.3.

Fundamento Jurídico de la ASF para Promover Acciones

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

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

Artículos 6, 12, fracción IV; 13, fracciones I y II; 15, fracciones XIV, XV y XVI; 29, fracción X; 32; 39; 49, fracciones I, II, III y IV; 55; 56, y 88, fracciones VIII y XII, de la Ley de Fiscalización y Rendición de Cuentas de la Federación publicado en el Diario Oficial de la Federación el 29 de mayo de 2009, en relación con los Transitorios PRIMERO y CUARTO del Decreto por el que se expide la Ley de Fiscalización y Rendición de Cuentas de la Federación; y se reforman el artículo 49 de la Ley de Coordinación Fiscal, y el artículo 70 de la Ley General de Contabilidad Gubernamental, publicado en el Diario Oficial de la Federación el 18 de julio de 2016.

Comentarios de la Entidad Fiscalizada

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