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

**Auditoría de TIC**

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2019-1-19GYN-20-0215-2020

215-DS

***Criterios de Selección***

Esta auditoría se seleccionó con base en los criterios establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2019 considerando lo dispuesto en el Plan Estratégico de la ASF.

***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 | 2,704,221.7 |
| Muestra Auditada | 751,627.7 |
| Representatividad de la Muestra | 27.8% |

El universo seleccionado por 2,704,221.7 miles de pesos corresponde al total ejercido en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2019; la muestra auditada está integrada de cuatro contratos relacionados con la prestación de los Servicios Administrados de Equipo de Cómputo Personal; de Ambientes de Prueba y Calidad para Aplicativos Institucionales; y el de Infraestructura de Seguridad en el Centro de Datos, con pagos ejercidos por 751,627.7 miles de pesos, que representan el 27.8% del universo seleccionado.

***Antecedentes***

El Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) es un organismo descentralizado de la Administración Pública Federal, con personalidad jurídica y patrimonio propio. Tiene por objeto garantizar el derecho a la seguridad social que consagra la Constitución Política de los Estados Unidos Mexicanos y contribuir al bienestar de los trabajadores, pensionados y familiares derechohabientes, a través de la administración de los seguros, prestaciones y servicios.

El ISSSTE contribuye a satisfacer los niveles de bienestar integral de los trabajadores al servicio del estado, pensionados, jubilados y familiares derechohabientes, con el otorgamiento eficaz y eficiente de los seguros, prestaciones y servicios, con atención esmerada, respeto, calidad y cumpliendo siempre con los valores institucionales de honestidad, legalidad y transparencia.

Las instituciones de salud es decir los hospitales, las clínicas y los laboratorios, como la mayoría de las organizaciones modernas dependen cada vez más de sistemas de información para una gran variedad de funciones, por lo que se han convertido en un blanco atractivo para los cibercriminales, dado que manejan información personal, financiera y médica de sus pacientes, pero el malware[1] y los ataques dirigidos no son los únicos riesgos que enfrentan, ya que los empleados (actuales o antiguos) también pueden ser causantes de incidentes de seguridad, debido al desconocimiento o uso irresponsable de la tecnología en el trabajo.

En el contexto que actualmente nos encontramos (2020) al hacer frente a la pandemia ocasionada por el virus SARS-COV2 (COVID-19), un ataque informático a un hospital puede tener consecuencias importantes, los ataques dirigidos al sector de la salud se han incrementado gradualmente.

[1] Cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

- En abril del 2020 la INTERPOL (Organización Internacional de Policía Criminal por sus siglas en inglés) emitió un comunicado de alerta sobre un crecimiento significativo de ataques de ransomware[2] hacia los hospitales en distintos países del mundo.

- En los Estados Unidos de Norte América, el FBI (Buró Federal de Investigaciones, por sus siglas en inglés) en el año 2020 emitió una alerta como consecuencia del incremento de engaños dirigidos a organizaciones de la salud y entidades gubernamentales. En abril del 2020, se lanzó una nueva advertencia en la que hacía referencia a correos de phishing [3] dirigidos a proveedores del sector de la salud en aquel país.

- La principal agencia de ciberseguridad de República Checa publicó en abril del 2020 una advertencia donde manifiesta su preocupación ante un posible ataque a gran escala especialmente dirigido a hospitales y al sector de la salud en general.

- Por otra parte, el 13 de marzo del 2020, el Hospital Universitario de Brno, en República Checa, donde funciona uno de los 18 centros de pruebas sobre el COVID-19, fue víctima de un ciberataque, al tiempo que en la noche del 15 de marzo del mismo año, el sitio web del Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) recibió un ataque de Denegación de Servicio Distribuido (DDoS) que aparentemente tenía como objetivo afectar la información y debilitar la respuesta en el marco de la pandemia.

Entre 2015 y 2019, el ISSSTE invirtió 11,628,826.5 miles de pesos en Tecnologías de la Información y Comunicaciones (TIC), integrados de la manera siguiente:

**Recursos invertidos en materia de TIC**
**(Miles de pesos)**

| Periodo de inversión | 2015 | 2016 | 2017 | 2018 | 2109 | Total |
|---|---|---|---|---|---|---|
| **Monto por año** | 1,876,906.9 | 2,607,955.0 | 2,201,183.4 | 2,238,559.5 | 2,704,221.7 | **11,628,826.5** |

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

## *Resultados*

### 1. Análisis Presupuestal

El Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019, publicado en el Diario Oficial de la Federación el 28 de diciembre de 2018, menciona que el presupuesto aprobado para el ISSSTE sería de 323,322,195.1 miles de pesos, de acuerdo con

[2] Programa de software malicioso que infecta computadoras y muestra mensajes a los usuarios que exigen el pago de dinero para restablecer el funcionamiento del sistema.

[3] Una forma de ingeniería social que utiliza correos electrónicos de apariencia auténtica, pero falsos, para solicitar información a los usuarios o dirigirlos a un sitio web falso.

lo reportado en la Cuenta de la Hacienda Pública Federal 2019, se tuvo un presupuesto modificado por 341,042,446.7 miles de pesos, lo que superó en 17,720,251.6 miles de pesos el presupuesto autorizado, cifra mayor en 5.5% con relación al presupuesto original, como se muestra a continuación:

**ESTADO ANALÍTICO DEL EJERCICIO DEL PRESUPUESTO DE EGRESOS 2019**

**(Miles de pesos)**

| | | A | B | C= A-B |
|---|---|---|---|---|
| **Capítulo** | **Descripción** | **Presupuesto Autorizado** | **Presupuesto Modificado** | **Diferencia** |
| 1000 | Servicios Personales | 42,607,111.7 | 44,015,885.0 | 1,408,773.3 |
| 2000 | Materiales y Suministros | 17,050,324.9 | 17,688,719.2 | 638,394.3 |
| 3000 | Servicios Generales | 35,381,838.5 | 48,706,624.9 | 13,324,786.4 |
| 4000 | Transferencias, Asignaciones, Subsidios y Otras Ayudas | 533,120.0 | 504,977.8 | -28,142.2 |
| 4500 | Pensiones y Jubilaciones | 226,143,000.0 | 229,026,082.7 | 2,883,082.7 |
| 5000 | Bienes muebles, inmuebles e intangibles | 964,080.0 | 811,013.9 | -153,066.1 |
| 6000 | Inversión pública | 642,720.0 | 289,143.1 | -353,576.9 |
| | **TOTAL** | **323,322,195.1** | **341,042,446.7** | **17,720,251.6** |

**Fuente:** Elaborado con base en la información proporcionada por el ISSSTE
**Nota:** Diferencias por redondeo

**Diferencias Cuenta Pública/Estado Analítico del Ejercicio del Presupuesto de Egresos ISSSTE 2019**

**(Miles de pesos)**

| | | A | B | C=A+B | D | E | F=C-D |
|---|---|---|---|---|---|---|---|
| **Capítulo** | **Descripción** | **Presupuesto Original** | **Ampliaciones/ Reducciones** | **Presupuesto Modificado Autorizado** | **Devengado** | **Pagado** | **Economías** |
| 1000 | Servicios Personales | 0.0 | 0.0 | 0.0 | 3,135,954.4 | 0.0 | -3,135,954.4 |
| 2000 | Materiales y Suministros | 0.0 | 0.0 | 0.0 | 600,151.8 | 0.0 | 600,151.8 |
| 3000 | Servicios Generales | 0.0 | 327,351.3 | 327,351.3 | 3,912,997.1 | 327,351.3 | - 3,585,645.8 |
| 4000 | Trasferencias, Asignaciones, Subsidios y Otras Ayudas | 0.0 | 56,284.4 | 0.0 | - 103,217.2 | 0.0 | 103,218.0 |
| 4500 | Pensiones y Jubilaciones | 0.0 | - 8,426.0 | - 8,426.0 | - 497,739.7 | - 8,426.0 | 489,313.7 |
| 5000 | Bienes Muebles e Inmuebles Intangibles | 0.0 | 306,132.2 | 0.0 | 18,442.0 | 0.0 | -18,442.0 |
| 6000 | Inversión Pública | 0.0 | 707,153.8 | 0.0 | - 16,576.9 | 0.0 | 16,576.9 |
| | **TOTAL** | **0.0** | **318,925.3** | **318,925.3** | **7,050,011.5** | **318,925.3** | **-6,731,086.3** |

**Fuente:** Elaborada con base en la información proporcionada por el ISSSTE y la consulta realizada en la página https://www.cuentapublica.hacienda.gob.mx
**Nota:** Diferencias por redondeo

Se identificaron diferencias al comparar las cifras de la Cuenta Pública con el Estado Analítico del Ejercicio del Presupuesto de Egresos 2019 proporcionado por el ISSSTE, en los Capítulos 3000, 4000, 4500, 5000 y 6000 por 318,925.3 miles de pesos por concepto del presupuesto modificado y del presupuesto devengado por 7,050,011.5 miles de pesos.

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC), correspondieron a 2,704,221.7 miles de pesos, como se muestra a continuación:

**GASTOS TIC 2019 ISSSTE**
**(Miles de pesos)**

| Capítulo | Partida | Descripción | Presupuesto Ejercido |
|---|---|---|---|
| **1000** | | **SERVICIOS PERSONALES** | **94,277.5** |
| **2000** | | **MATERIALES Y SUMINISTROS** | **422.2** |
| | 21401 | Materiales y Útiles Consumibles para el procesamiento en Equipos y Bienes Informáticos | 31.7 |
| | 29401 | Refacciones y Accesorios para Equipo de Cómputo y Telecomunicaciones | 390.5 |
| **3000** | | **SERVICIOS GENERALES** | **2,609,522.0** |
| | 31401 | Servicio Telefónico Convencional | 11.1 |
| | 31701 | Servicios de Conducción de Señales Analógicas y Digitales | 480,421.9 |
| | 31904 | Servicios Integrales de Infraestructura de Cómputo | 677,358.3 |
| | 32301 | Arrendamiento de Equipo y Bienes Informáticos | 927,097.4 |
| | 32701 | Servicios de Conducción de Señales Analógicas y Digitales | 111,923.4 |
| | 33104 | Otras asesorías para la operación de programas | 2,842.0 |
| | 33301 | Servicios de Desarrollo de Aplicaciones Informáticas | 157,204.0 |
| | 33304 | Servicios de Mantenimiento de Aplicaciones informáticas | 240,088.8 |
| | 35301 | Mantenimiento y Conservación de Bienes Informáticos | 12,575.1 |
| | | **TOTAL** | **2,704.221.7** |

**Fuente:** Elaborado por la ASF con base en la información proporcionada por el ISSSTE.
**Nota:** Diferencias por redondeo

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC, con una percepción anual de 94,277.5 miles de pesos durante el ejercicio fiscal 2019; considerando 52 plazas, el promedio anual percibido por persona fue de 1,813.0 miles de pesos.

Del total ejercido en TIC por 2,704,221.7 miles de pesos, se seleccionó una muestra de cuatro contratos por los que se realizaron pagos de 751,627.7 miles de pesos que representan el 27.8% del universo seleccionado, los cuales se integran de la manera siguiente:

**Muestra de Contratos Ejercidos durante 2019 por el ISSSTE**
**(Miles de pesos)**

| Procedimiento de Contratación | Contrato | Proveedor | Objeto del Contrato | Vigencia | | Monto | | Pagado 2019 |
|---|---|---|---|---|---|---|---|---|
| | | | | Del | Al | Mínimo | Máximo | |
| Adjudicación Directa Art. 41, Fracción III de la LAASSP | AD-CS-DA-SRMS-257/2016 | Axtel, S.A.B. de C.V., Alestra Comunicación, S. de R.L. de C.V. y Avantel, S. de R.L. de C.V. | Servicio Administrado de Ambientes de Prueba y Calidad para Aplicativos Institucionales | 01/09/2016 | 31/12/2019 | 393,618.9 | 393,618.9 | 87,470.9 |
| Adjudicación Directa Art. 41, Fracción III de la LAASSP | AD-CS-DA-SRMS-311/2016 CM-CS-DA-SRMS-002/2017 | Axtel, S.A.B. de C.V. en Participación Conjunta con Ultrasist, S.A. de C.V. | Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos | 01/11/2016 | 31/12/2019 | 165,366.0 | 165,366.0 | 65,003.4 |
| Adjudicación Directa Art. 41, Fracción III de la LAASSP | AD-CS-DA-SRMS-141/2015 Primer Convenio Modificatorio CM-CS-DA-SRMS-004/2016 Segundo Convenio Modificatorio CM-CS-DA-SRMS-015/2018 | Tecnoprogramación Humana Especializada en Sistemas Operativos S.A. de C.V., Servicios de Integración y Garantías S.A. de C.V. y Tecnología en Service Desk, S.A. de C.V., en participación conjunta. | Servicio Administrado de Equipo de Cómputo Personal (SAECP), para los ejercicios Fiscales 2015, 2016, 2017 y 2018 (40 meses) | 01/04/2015 | 31/08/2019 | 1,274,091.6 | 2,753,539.1 | 599,153.4 |
| Adjudicación Directa Art. 41, Fracción V de la LAASSP | AD-CS-DNAF-SRMS-434/2019 | Tecnoprogramación Humana Especializada en Sistemas Operativos S.A. de C.V., Servicios de Integración y Garantías S.A. de C.V. y Tecnología en Service Desk, S.A. de C.V., en participación conjunta. | Servicio Administrado de Equipo de Cómputo Personal (SAECP) | 01/09/2019 | 31/12/2019 | 159,345.2 | 180,000.0 | 0.0 |
| | | | | | **Total** | **1,992,421.7** | **3,492,524.0** | **751,627.7** |

**Fuente:** Elaborado por la ASF con base en la información proporcionada por el ISSSTE.
**Nota:** Diferencias por redondeo

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

**Manual de Organización**

La última fecha de actualización del Manual de Organización General del ISSSTE fue el 12 de octubre de 2018, el cual no se encuentra alineado a las modificaciones del Estatuto Orgánico del ISSSTE, publicado el 1 de febrero de 2019 en el Diario Oficial de la Federación (DOF), ya que en éste aún se menciona a la Dirección de Tecnología y Estrategia Digital, la que a raíz de la publicación del Estatus Orgánico se convirtió en la Subdirección de Tecnología de Información adscrita a la Dirección Normativa de Administración y Finanzas, por lo que las atribuciones de dicha subdirección así como de las áreas que la conforman se encuentran desactualizadas.

2019-1-19GYN-20-0215-01-001 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado actualice su Manual de Organización General de acuerdo con las modificaciones realizadas en su Estatuto Orgánico publicado el 1 de febrero de 2019 en el Diario Oficial de la Federación. Se fortalezcan los controles en los que instrumente y sea obligatoria la revisión y actualización periódica del Manual de Organización.

2019-1-19GYN-20-0215-01-002 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado implemente procedimientos y mecanismos de control para validar que sus cifras reportadas en el Estado Analítico del Ejercicio del Presupuesto de Egresos se concilien con las presentadas por la Secretaría de Hacienda y Crédito Público en la Cuenta Pública en los Capítulos 3000, 4000, 4500, 5000 y 6000, con la finalidad de cumplir con la rendición de cuentas y contribuir a la transparencia del gasto público.

**2. Contrato Número AD-CS-DA-SRMS-257/2016 Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales**

Se revisó el Contrato Plurianual número AD-CS-DA-SRMS-257/2016 celebrado con Axtel, S.A.B., de C.V., Alestra Comunicación, S. de R.L. de C.V., y Avantel, S. de R.L. de C.V., mediante el procedimiento de contratación por adjudicación directa con fundamento en los artículos 22, fracción ll, 26, fracción III, 40 y 41, fracción III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), 71 y 72, fracción III, de su Reglamento (RLAASSP), con el objeto de prestar el "Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales", con vigencia del 01 de septiembre de 2016 al 31 de diciembre de 2019, por un monto total de 393,618.9 miles de pesos, con pagos realizados en 2019 por 87,470.9 miles de pesos, de los cuales 32,801.6 miles de pesos correspondieron a los servicios devengados en los meses de octubre noviembre y diciembre de 2018, así como 54,669.3 miles de pesos por servicios de enero a mayo de 2019, el cual se

dio por concluido como resultado de un proceso de terminación anticipada el 01 de junio de 2019, y se determinó lo siguiente:

**Antecedente**

En el anexo técnico del contrato se hace la siguiente referencia: “el ISSSTE actualmente (2016) cuenta con servicios de ambientes aplicativos, los cuales son objeto de servicios en demanda de un contrato existente y fueron habilitados conforme a las necesidades del ISSSTE, dichos servicios requirieren ser modernizados, actualizados e implementados bajo las mejores prácticas de la industria, así como apegados a estándares internacionales y nacionales de seguridad como ISO 27001 y MAAGTIC-SI por mencionar algunos”.

**Objeto**

Reducir los riesgos en el proceso de despliegue de los aplicativos institucionales, mediante un "Servicio Administrado de Ambientes de Prueba y Calidad para Aplicativos Institucionales", orientados a asegurar su correcto funcionamiento antes de ser liberados para uso de la derechohabiencia del Instituto, así como las áreas y organismos que lo conforman, con niveles de servicio, que permitan garantizar los tiempos de entrega o en su caso penalizar o aplicar deductivas, obteniendo como resultado un mayor control y respuesta.

**Alcance**

Provisionar un servicio administrado de infraestructura en demanda para satisfacer las necesidades tecnológicas, de personal, capacidad de procesamiento, procesos, servicios y componentes tecnológicos de hardware y software para aplicativos institucionales durante un periodo de treinta y seis meses a partir de la conclusión del periodo de implementación.

**Investigación de Mercado**

En el resultado de la investigación de mercado, elaborada por la Subdirección de Coordinación de Proyectos, adscrita a la Dirección de Tecnología y Estrategia Digital (DTED), se observa lo siguiente:

- Al momento de realizar la investigación, el ISSSTE contaba con el servicio de “Infraestructura de Centro de Datos” formalizado a través del contrato AD-CS-DA-SRMS-286/2014 con el proveedor Sixsigma Networks México, S.A. de C.V. (KIO), cuya vigencia era del 04 de noviembre de 2014 al 17 de octubre de 2017, y su alcance consistía en proporcionar la infraestructura integral de servicios que, entre otras cosas, incluía servicios de administración, sistema de monitoreo, recursos humanos para la administración de los ambientes propuestos, consolidación y virtualización de ambientes y todo lo necesario para proporcionar el Servicio de infraestructura de Centro de Datos; dada la naturaleza de los servicios

proporcionados, este proveedor podía cubrir el requerimiento solicitado por el ISSSTE, sin embargo, no fue considerado en la investigación de mercado.

- La investigación de mercado fue acotada a 4 proveedores (Axtel, S.A.B. de C.V., Orben Comunicaciones, S.A.P.I. de C.V., Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V. y Nuga SYS, S.A. de C.V.) de los cuales el ISSSTE no presentó los criterios por los que fueron seleccionados; cabe señalar que estos proveedores fueron los mismos que se escogieron en el contrato número AD-CS-DA-SRMS-311/2016 "Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos" (resultado 3).

- El ISSSTE contrató a Axtel, S.A.B de C.V., Alestra Comunicación, S. de R.L. de C.V., y Avantel, S. de R.L de C.V., con el argumento de que contaba con un contrato vigente adjudicado mediante la Licitación Pública Nacional Electrónica No LA-019GYN905-N42-2014, con el Fondo de la Vivienda del ISSSTE (FOVISSSTE), para la contratación de "Servicios Administrados para el Plan de Recuperación ante desastres", y aceptaba otorgar el servicio en iguales condiciones en cuanto a precio, características y calidad, sin embargo, la naturaleza de los servicios prestados en la licitación son distintos a las necesidades requeridas por el Instituto.

- No se elaboró un análisis de necesidades en el que se indique las razones prioritarias de llevar de forma independiente la gestión de sus ambientes de preproducción mediante un contrato específico y con un proveedor distinto al de su centro de datos principal. A la fecha de la auditoría (agosto 2020) el Instituto cuenta con el ambiente de preproducción en la misma infraestructura del centro de datos principal, en contradicción con la justificación proporcionada en el estudio de factibilidad, en la que se mencionó que de acuerdo con las mejores prácticas este ambiente debía estar separado de la infraestructura de producción, sin embargo, no proporcionó la referencia o evidencia de la mejor práctica señalada. No obstante, la separación de ambientes se puede realizar mediante la segregación de segmentos de red separados por actividad sin que convivan entre sí o mediante la aplicación de redes virtuales, cumpliendo con las mejores prácticas, como lo señalado en Integración de Modelo de Madurez de Capacidades (CMMI, por sus siglas en inglés) e ISO 27001 anexo 12.1.4 (estándar para la seguridad de la información), lo cual también reduce el riesgo de continuidad en caso de falla o contingencia y no necesariamente se tiene que realizar una contratación de otro centro de datos para esta actividad.

La Subdirección de Coordinación de Proyectos no comparó los servicios ofertados en la Licitación Pública Nacional Electrónica No LA-019GYN905-N42-2014 con las necesidades requeridas para demostrar que eran equiparables y que se prestarían en igualdad de condiciones y precio dado que tampoco incluyó el desglose de los servicios ofertados por el proveedor.

**Justificación de excepción a la licitación pública**

- La Subdirección de Coordinación de Proyectos tomó como base la Licitación Pública Nacional No. LA-019GYN905-N42-2014, en donde se apreciaban servicios que en conjunto hacían las veces del servicio de ambientes de prueba y calidad, cuyas características son similares o equiparables a las requeridas por el ISSSTE.

- En el análisis realizado por la ASF, se identificó que los servicios solicitados en el contrato número AD-CS-DA-SRMS-257/2016 y los contenidos en la Licitación Pública Nacional No. LA-019GYN905-N42-2014 del FOVISSSTE no eran similares dado que el alcance de dicha licitación correspondía a la Infraestructura para la implementación de un Centro de Datos Principal y uno Alterno, los cuales tenían un objetivo distinto al que buscaba el ISSSTE (gestión de ambientes de preproducción).

- Entre los servicios solicitados por el ISSSTE y que no eran parte del objeto del contrato, se encuentran los siguientes: firewall perimetral de siguiente generación, borrado seguro, análisis de vulnerabilidades, pruebas de penetración, AntiDDOS (Denegación de servicio, por sus siglas en ingles), SOC (Centros de Operaciones de Seguridad, por sus siglas en ingles), correlación de eventos de seguridad y análisis de riesgos.

- En el contrato pactado con el ISSSTE fueron requeridos servicios que no fueron utilizados y son los siguientes: Acceso remoto a instancias de prueba, Soporte técnico a migración de plataformas físicas o virtuales, Servicio consultivo para la ejecución y aplicación de mejores prácticas, Servicio consultivo de tendencias y actualizaciones, de plataformas tecnológicas, Servicio consultivo de identificación de riesgos, escenarios para migración tecnológica; así como los servicios de seguridad administrados conformados por el Servicio de Análisis de Vulnerabilidades, Servicio de Pruebas de Penetración, Servicio AntiDDoS, Servicio de SOC, Servicio de Correlación de Eventos de Seguridad y Servicio de Análisis de Riesgos, los cuales no estaban asociados a las necesidades requeridas por el Instituto para la gestión de software en su ciclo de vida, motivo primordial de la contratación.

**Pagos**

El ISSSTE no proporcionó la información bancaria mediante la cual se pudiera corroborar que la cuenta de destino pertenecía al proveedor.

En la documentación relacionada con los pagos mensuales fijos, no se desglosa el costo unitario de cada servicio pactado en el contrato. Como parte del servicio integral se incluyeron servicios bajo demanda, los cuales no estaban asociados al objeto de la contratación mismos que no fueron utilizados, y si se forman parte del pago mensual del servicio.

**Supervisión**

- Se identificó que las actas de entrega-recepción y cédulas de supervisión a los entregables del contrato fueron firmadas y autorizadas por personal distinto al que se estipula en el contrato.

**Análisis de los servicios contratados**

- El ISSSTE carece de la evidencian que se hayan prestado los servicios siguientes: proceso de instalación de aplicativos en el ambiente de desarrollo, carga de datos de prueba, administración de accesos en ambientes de prueba y el proceso de creación de sistemas en el ambiente de desarrollo, servicios que se encuentran incluidos en el pago mensual y no fueron proporcionados equivalentes a 87,470.9 miles de pesos.

- Se carece de la documentación que demuestre que el proveedor realizó las actividades de gestión de solicitudes de soporte, configuración de aplicaciones, base de datos, así como de sistemas operativos/técnicos.

- El ISSSTE no proporcionó evidencia que permita validar que se contaba con personal en sitio para la gestión de solicitudes.

- No se demostró que el proveedor alineará el servicio a normas internacionales y nacionales de acuerdo con lo especificado en el contrato y tampoco proporcionó los entregables solicitados para los servicios de Análisis de Vulnerabilidades y de Pruebas de Penetración.

- De los 31 servicios del anexo técnico, en 10 de ellos (32.3%) el ISSSTE no demostró que se prestaran durante la vigencia del contrato, para 8 servicios (25.8%) el Instituto indicó que no fueron utilizados aun cuando en el anexo técnico se enlistaban como servicios que debían ser cubiertos como parte integral del servicio; sólo 13 (41.9%) de los 31 servicios tienen un entregable o reporte que justifique su ejecución. De estos 13 servicios, de 8 de ellos no se demostró que fueran efectuados por el proveedor y 5 eran relacionados al monitoreo de la infraestructura de ambientes de pruebas, los cuales fueron ajenos a la naturaleza de la contratación.

- La DTED no realizó un análisis de necesidades en el que se demostrará y se justificará que se requería contar con servicios de seguridad y con un centro de datos exclusivo para la gestión del ambiente de preproducción, dado que el ambiente puede estar separado del de producción sin que sea necesario contar con un centro de datos específico.

- No se cuenta con la información que permita validar que el ISSSTE llevó a cabo el proceso de gestión de las solicitudes tales como tickets, correos electrónicos de seguimiento y notificación del cierre de la solicitud.

- El ISSSTE no demostró que el centro de datos cumplió con las siguientes características solicitadas en el contrato:

    - Capacidad de espacios para habilitación del servicio.
    - Suministro eléctrico que soporte el consumo de la plataforma.
    - Tecnológica implementada.
    - Sistema de aire acondicionado.
    - Sistema de refrigeración y control de humedad.
    - Seguridad física en un esquema 7x24x355.
    - Sistema de video vigilancia.
    - Dos acometidas eléctricas.
    - Planta de emergencia.
    - Sistemas de energía interrumpida (UPS).
    - Bancos de baterías.
    - Sistema de distribución de energía (PDU).
    - Sistema de tierras.

**Operación de la Mesa de Servicio**

- El ISSSTE no cuenta con entregables que permitan verificar que estuvo en operación la Mesa de Servicio y que se cumpliera con los procedimientos definidos en el anexo técnico.

**Terminación Anticipada**

El 20 de mayo de 2019, la Subdirección de Tecnología de la Información inició el trámite de la terminación anticipada del contrato número AD-CS-DA-SRMS-257/2016 para que se

procediera a realizar las acciones correspondientes que tendrían efecto a partir del 01 de junio de 2019, argumentado las razones siguientes:

- Representaría un beneficio reestructurar un nuevo contrato del Servicio Administrado de Ambiente de Pruebas y Calidad para Aplicativos Institucionales, bajo un esquema más flexible y eficiente del ejercicio del presupuesto o para reorientar el ejercicio del presupuesto a otras necesidades más prioritarias.

- Las condiciones en que se encontraba el contrato resultaban inoperables e impedía asegurar los objetivos que perseguía el Instituto, ya que se tenían 73 ambientes disponibles que no se utilizaban en su totalidad, lo que ocasionaba un gasto oneroso para el Instituto.

- La reorientación de los recursos de este contrato permitiría al Instituto destinarlos a otros proyectos en beneficio de sus derechohabientes.

Dichas causas no se justificaron ni se sustentaron con la documentación requerida por la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En análisis de la información proporcionada para el sustento del proceso de la terminación anticipada se observó lo siguiente:

- La Subdirección de Tecnología de la Información no realizó el dictamen técnico legal que soportara la justificación de la terminación anticipada del contrato.

- El 06 de agosto de 2019, la apoderada legal del proveedor Axtel, S.A.B. de C.V., así como de la participación conjunta, presentó un escrito en alcance al comunicado de fecha 31 de julio de 2019, donde indicó que el proveedor había convenido internamente renunciar al requerimiento realizado y donde solicitaban gastos por inversiones no recuperables por 2,659.3 miles de dólares, de lo anterior el ISSSTE no proporcionó el detalle de cómo el proveedor determinó dicha cantidad.

- En el anexo técnico del contrato y en los entregables mensuales solicitados, no se hace referencia a los 73 ambientes que se mencionan en las causas de la terminación anticipada.

- La Subdirección de Recursos Materiales y Servicios Generales no cuenta con el expediente, ni con la documentación soporte que sustente el proceso de terminación anticipada.

- El 30 de diciembre de 2019, la Jefatura de Servicios de Convenios y Contratos del ISSSTE emitió el dictamen final que dio por concluida la contratación.

**Conclusiones**

La contratación se basó en la Licitación Pública Nacional No. LA-019GYN905-N42-2014, cuyos servicios no eran similares en su mayoría a los requeridos por el ISSSTE. Como parte del servicio el Instituto agregó nuevos requerimientos que no formaban parte del objeto de la contratación. Adicionalmente se identificó que los servicios siguientes no fueron prestados y formaban parte del pago mensual: proceso de instalación de aplicativos en el ambiente de desarrollo, carga de datos de prueba, administración de cuentas en ambientes de pruebas y el proceso de creación de sistemas en el ambiente de desarrollo, por lo cual se presumen pagos injustificados por 87,470.9 miles de pesos en incumplimiento del artículo 9, inciso IV; 10 inciso I del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como del Manual de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 04 de febrero de 2016; de la Regla 5 del proceso I.B. Proceso de Administración del Presupuesto y las Contrataciones (APCT); Actividad 4 de proceso APCT 3 Estudios de Factibilidad del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información publicado en el Diario Oficial de la Federación el 04 de febrero de 2016; de las funciones 1, 6, 7 y 12 del numeral 8 Dirección de Tecnología y Estrategia Digital, funciones 1, 3 y 5 del numeral 8.1 Subdirección de Tecnología de la Información del Manual de Organización General del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado publicado en el Diario Oficial de la Federación el 11 de julio de 2018; y de los artículos 41 fracción III, y 54 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con última reforma publicada en el Diario Oficial de la Federación el 10 de noviembre de 2014.

El Instituto no demostró que la contratación del Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales resultaba crítica y esencial para sus actividades y operaciones, ya que conforme a lo indicado en el dictamen de terminación anticipada, el ISSSTE finalizó el contrato en razón de que "*si bien se tienen 73 ambientes disponibles, no se utilizan en su totalidad, lo que ocasiona un gasto oneroso para el instituto"*, lo que se contrapone a la señalado en la justificación para realizar el proceso de contratación AD-CS-DA-SRMS-257/2016. Se observó que la causa de justificación para la terminación anticipada no cumple con los elementos requeridos por la LAASSP; tampoco se cuenta con el expediente de la terminación anticipada de conformidad con el artículo 54 bis de la LAASSP, artículo 102 de su respectivo RLAASSP y el numeral 5.1.5 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del ISSSTE.

Al respecto, se procederá en los términos del Artículo 22 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2019-1-19GYN-20-0215-01-003 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado en subsecuentes procesos de terminación anticipada relacionados a contratos de TIC, documente a través de un dictamen técnico-legal, la justificación pormenorizada y con evidencia precisa de las razones para prescindir de un servicio.

2019-1-19GYN-20-0215-01-004 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado incluya en su Manual del Organización General las acciones y responsabilidades de la Subdirección de Recursos Materiales y Servicios Generales para que fortalezca los mecanismos y controles que garanticen un adecuado manejo, consulta y salvaguarda de expedientes derivados de los procedimientos a su cargo tales como procesos de contratación, terminación anticipada, y recisión de contratos, que permitan conocer el estado de cada contratación y la documentación que los conforman.

2019-1-19GYN-20-0215-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 87,470,867.20 pesos (ochenta y siete millones cuatrocientos setenta mil ochocientos sesenta y siete pesos 20/100 M.N.), por pagos realizados al contrato número AD-CS-DA-SRMS-257/2016, porque no se prestaron los servicios objeto del contrato tales como instalación de aplicativos en el ambiente de desarrollo, carga de datos de prueba, administración de accesos, gestión de solicitudes de soporte, configuración de aplicaciones, base de datos, sistemas operativos/técnicos y cuentas en ambientes de pruebas y el proceso de creación de sistemas en el ambiente de desarrollo; el ambiente solicitado no fue utilizado y su beneficio fue casi nulo al ser poco aprovechado por la Subdirección de Coordinación de Proyectos tal como se estableció en la terminación anticipada de la contratación la cual determinó que no era esencial para las operaciones del Instituto en incumplimiento del artículo 9, inciso IV, 10, inciso I, del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y de Seguridad de la Información; así como del Manual de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 04 de febrero de 2016; de la Regla 5, del proceso I.B. Proceso de Administración del Presupuesto y las Contrataciones (APCT), Actividad 4 de proceso APCT 3 Estudios de Factibilidad, del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información publicado en el Diario Oficial de la Federación el 04 de febrero de 2016; de las funciones 1, 6, 7 y 12, del numeral 8 Dirección de Tecnología y Estrategia Digital, funciones 1, 3 y 5, del numeral 8.1 Subdirección de Tecnología de la Información, del Manual de Organización General del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado publicado en el Diario Oficial de la Federación el 11 de julio de 2018, y de los artículos 41, fracción III, y 54 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con última reforma publicada en el Diario Oficial de la Federación el 10 de noviembre de 2014.

**Causa Raíz Probable de la Irregularidad**

No existe monitoreo ni supervisión de los compromisos contractuales, tampoco de los lineamientos y disposiciones para el desarrollo de sistemas de información, aunado a una deficiente gestión de riesgos del organismo lo que impidió que los servicios se prestaran en tiempo y forma y se cumpliera con el fin contratado.

**3. Contrato Número AD-CS-DA-SRMS-311/2016 Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos**

Se revisó el Contrato Plurianual número AD-CS-DA-SRMS-311/2016 celebrado con Axtel, S.A.B. de C.V., en participación conjunta con Ultrasist, S.A. de C.V., mediante el procedimiento de contratación por adjudicación directa con fundamento en los artículos 22 fracción ll, 26, fracción III, 40, 41, fracción III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 71 y 72, fracción III, de su Reglamento, con el objeto de prestar el "Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos", con vigencia del 01 de noviembre de 2016 al 31 de diciembre de 2019, por un monto de 165,366.0 miles de pesos, con pagos realizados en 2019 por 65,003.4 miles de pesos, de los cuales 12,305.2 miles de pesos correspondieron a los servicios devengados por octubre, noviembre y diciembre de 2018, y 52,698.2 miles de pesos por servicios de enero a noviembre de 2019, se aplicaron deductivas por 3,088.5 miles de pesos, y se determinó lo siguiente:

**Antecedentes**

En el anexo técnico del contrato se hace referencia a la situación siguiente:

*"El ISSSTE actualmente (2016) cuenta con servicios de ambientes de seguridad administrada, los cuales son objeto de servicios en demanda de un contrato existente y fueron habilitados conforme a las necesidades del ISSSTE; sin embargo, se requirió que dichos servicios cumplan con mejores condiciones de niveles de servicio sobre la infraestructura de seguridad, que ante un evento de indisponibilidad hacia los sistemas sustantivos del instituto permitan un tiempo de recuperación menor al que actualmente se otorga. Adicionalmente se requiere que el proveedor cumpla con estándares internacionales y nacionales de seguridad como: ISO27001:2005, ITIL V3 y MAAGTICSI por mencionar algunos.*

*Por tal motivo, el ISSSTE requiere que los servicios de Seguridad Administrada se otorguen a través de un nuevo contrato por un periodo plurianual que garantice los niveles de servicio al ISSSTE para la continuidad y operación de los mismos".*

**Investigación de mercado**

En el resultado de la investigación de mercado elaborada por la Subdirección de Tecnologías de Información, adscrita a la Dirección de Tecnología y Estrategia Digital (DTED), se observa lo siguiente:

- No se amplió el rango de búsqueda a más proveedores que contaran con la misma capacidad técnica y operativa para ofrecer los servicios requeridos, sólo se acotó a 4 proveedores para que participaran en el proceso y no se precisó en la investigación de mercado el método de búsqueda en Internet, ni los criterios por los cuales se seleccionaron.

- Al momento de realizar la investigación de mercado, el ISSSTE contaba con el servicio de "Infraestructura de Centro de Datos" formalizado a través del contrato número AD-CS-DA-SRMS-286/2014 con el proveedor Sixsigma Networks México, S.A. de C.V. (KIO), con vigencia del 04 de noviembre de 2014 al 17 de octubre de 2017, y su alcance consistía en proporcionar la infraestructura integral de servicios que entre otros, incluía servicios de administración, sistemas de almacenamiento, sistemas de respaldo de información, sistema de monitoreo, recursos humanos para la administración de los ambientes propuestos, consolidación y virtualización de ambientes, mejora continua, gestión de desempeño, gestión de continuidad del negocio y todo lo necesario para proporcionar el Servicio de Infraestructura de Centro de Datos; dada la naturaleza de los servicios proporcionados, este proveedor podía cubrir el requerimiento solicitado por el ISSSTE, sin embargo, no fue considerado en la investigación de mercado.

- Axtel, S.A.B. de C.V., en respuesta a la solicitud de propuesta de los servicios requeridos, envió la cotización manifestando que cumplía bajo los mismos términos y condiciones de precio y calidad de los servicios requeridos, y que además prestaba los servicios de "Ventanilla Única de Comercio Exterior Mexicana 2 (VUCEM 2)", mediante la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E00001-E1-2016 suscrita con el Servicio de Administración Tributaria (SAT), y que de acuerdo a ellos cumplía con los términos y condiciones solicitados por el ISSSTE para los "Servicios administrados de Infraestructura de Seguridad en el Centro de Datos", sin embargo, el documento no contenía un comparativo de los precios cotizados que prevalecían en el mercado y los ofrecidos en la licitación.

- La Subdirección de Tecnología de la Información tomó como base la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E00001-E1-2016 suscrita con el Servicio de Administración Tributaria para los servicios de "Ventanilla Única de Comercio Exterior Mexicana 2 (VUCEM 2)", del Contrato Número CS-300-LP-I-P-FC-026/16, aun cuando los servicios correspondieron, entre otros, a Servicios Administrados de Infraestructura, de Procesamiento en la Nube, Almacenamiento Físico en Sitio, Seguridad de la Infraestructura de Comunicaciones, Servicio de Gestión, Operación, Monitoreo, Mantenimiento, Soporte y Seguridad de

Infraestructura y a Servicios de Implementación de Infraestructura para la Red Inalámbrica, Servicio de Energización, Servicio de Interconexión así como diversos procesos de capacitación, cambio organizacional, enrolamiento y administración de gafetes, los cuales eran de distinta naturaleza a la necesidades requeridas por el ISSSTE.

- La ASF realizó una búsqueda en la base de los contratos listados y cargados en CompraNet durante el año 2016 y encontró un contrato similar a los servicios solicitados por el ISSSTE, con un costo anual menor al proporcionado por Axtel, S.A.B. de C.V. Este contrato no fue considerado en la investigación de mercado.

- La investigación de mercado fue acotada a 4 proveedores (Axtel, S.A.B. de C.V., Orben Comunicaciones, S.A.P.I. de C.V., Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., y Nuga SYS, S.A. de C.V.) de los cuales el ISSSTE no presentó los criterios por los que fueron seleccionados como proveedores potenciales para proporcionar el servicio solicitado; cabe señalar que estos proveedores fueron los mismos que se escogieron en el contrato AD-CS-DA-SRMS-257/2016 “Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales”.

**Justificación de excepción a la Licitación Pública**

La Subdirección de Tecnología de la Información no realizó un dictamen técnico donde se refleje el análisis de cada uno de los servicios prestados en la licitación contra las necesidades solicitadas por el Instituto en el que se demostrara la coincidencia de los servicios, cobertura e igualdad de precios.

Asimismo, la justificación se fundamentó en el artículo 41, fracción III, de la LAASSP “*Existan circunstancias que puedan provocar pérdidas o costos adicionales importantes, cuantificados y justificados*”, no obstante, este servicio, como se menciona en los antecedentes, ya lo proporcionaba previamente otro proveedor, y con esta contratación el ISSSTE requería mejorarlo, por lo que no se comprobó que este servicio ponía en riesgo al Instituto y que por la falta de este servicio pudiera llegar a tener problemas operativos o pérdidas económicas.

**Comparativa entre los servicios proporcionados por la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E0000-E1-2016 y los servicios requeridos por el ISSSTE**

La Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E0000-E1-2016 ofrecía, entre otros, Servicios Administrados de Infraestructura, de Procesamiento en la Nube, almacenamiento físico en sitio y seguridad de la Infraestructura de Comunicaciones, y en el caso específico del “Servicio de Gestión, Operación, Monitoreo, Mantenimiento, Soporte y Seguridad de Infraestructura” se refiere a Servicios de Implementación de Infraestructura para la Red Inalámbrica, Servicio de Energización, Servicio de Interconexión

así como diversos procesos de Capacitación, cambio organizacional, enrolamiento y administración de gafetes. El ISSSTE señaló que el "Servicio de gestión, operación, monitoreo mantenimiento, soporte y seguridad de Infraestructura", así como el "Servicio de comunicaciones" eran los que cumplían con sus necesidades.

- La ASF realizó el análisis para identificar las coincidencias de los servicios, y se observó que los de análisis forense, pruebas DDoS (Ataque de denegación de servicio), gestión del modelo de seguridad de la información y de borrado seguro no estaban ofertados en la licitación.

- El contrato número AD-CS-DA-SRMS-311/2016 consta de 18 servicios, de los cuales sólo 7 son similares a los proporcionados en la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E0000-E1-2016, y son los siguientes: Servicio de programa de concienciación y capacitación de seguridad informática, Servicio de firewall perimetral, Servicio de IPS (Sistema de prevención de intrusos) de red, Servicio administrado de SOC (Centro de Operaciones de Seguridad) y el Servicio de detección de Respuesta a Incidentes, Servicio de análisis de vulnerabilidades, Servicio de pruebas de penetración y Servicios de análisis de riesgos de activos. Por lo tanto, la licitación solo cumplió con el 38.9 % de los servicios requeridos por el Instituto y no era justificable adherirse a este contrato.

- En la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E00001-E1-2016 y en el contrato suscrito con el Servicio de Administración Tributaria (SAT) los servicios no se encuentran descritos de manera general, no obstante, en la contratación del ISSSTE no se estipuló de la misma forma.

En análisis anterior, se observa lo siguiente:

- De las necesidades solicitadas por el ISSSTE se observó que en la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E0000-E1-2016, sólo coinciden 7 de 18 servicios.

- El ISSSTE no llevó acabo un comparativo de los servicios ofertados mediante el contrato del servicio de "Ventanilla Única de Comercio Exterior Mexicana 2 (VUCEM2)", respecto a sus necesidades y así acreditar la viabilidad de realizar una contratación con servicios bajo demanda y se demostrara que eran equiparables y representarán la mejor opción para el Instituto.

**Cumplimiento Técnico y Funcional de los Servicios y Entregables Establecidos**

- El Jefe de Servicios de Evaluación y Desarrollo de Proyectos realizó la revisión y validación de entregables del Contrato Plurianual número AD-CS-DA-SRMS-311/2016, sin contar con las facultades legales establecidas en la cláusula Décima Sexta de la Contratación.

- Para el "Servicio de gestión de usuarios privilegiados", durante el periodo de octubre de 2018 a diciembre de 2019, el proveedor le indicó al ISSSTE que su solución no se adecuaba a las necesidades para la gestión de las diversas cuentas privilegiadas de la infraestructura del centro de datos principal, por lo que se aplicaron penalizaciones en el mismo periodo por el incumplimiento de dicho servicio; no fue hasta septiembre de 2019 cuando el ISSSTE le indicó al proveedor que debería solucionar esta incompatibilidad. Lo anterior confirma que no se realizó un análisis este servicio y de la herramienta propuesta respecto a las necesidades del Instituto previo al proceso de contratación, ni se gestionó un convenio modificatorio para ajustar el alcance del servicio y el monto del contrato, por lo que se realizaron pagos injustificados por 3,782.9 miles de pesos.

- El ISSSTE no supervisó las actividades realizadas por el proveedor en relación con la configuración y gestión de reglas de las herramientas firewall e IPS (sistema de prevención de intrusos, por sus siglas en ingles), ni las actividades realizadas por la mesa de servicio ubicada en Monterrey, Nuevo León, con el objetivo de asegurarse de que las configuraciones y procedimientos que fueron solicitados en el contrato se aplicaran.

- Para el Centro de Servicios de Seguridad (SOC por su sigla en inglés), no hay evidencia de que se hayan proporcionado las actividades de Funcionalidades de seguridad, Gestión de incidentes de seguridad y Respuesta mínima a los incidentes.

- No se definió un precio individual por cada uno de los componentes y servicios ofertados en este Contrato Plurianual número AD-CS-DA-SRMS-311/2016.

- A la fecha de la auditoría (agosto de 2020), el Contrato Plurianual número AD-CS-DA-SRMS-311/2016 ya no se encuentra vigente, el ISSSTE decidió agrupar dichos servicios con el proveedor actual, el cual administra su centro de datos principal bajo el concepto de servicios bajo demanda, lo que le ha significado un mejor costo, cabe mencionar que dicho proveedor no fue contemplado en la investigación de mercado.

- El entregable del Servicio de Análisis de Riesgos (el cual no cuenta con las firmas por parte proveedor y del ISSSTE) menciona que se realizó esta actividad a los 8 dominios tecnológicos del ISSSTE, lo que arrojó un nivel de riesgo medio y señaló que el ISSSTE podría estar expuesto a la materialización de 2 a 4 incidentes de seguridad por año, se incluyeron 30 recomendaciones tecnológicas y 14 recomendaciones para el Sistema de Gestión de Seguridad de la Información. A la fecha de la auditoría (agosto 2020) no se han realizado acciones por parte del ISSSTE para atender los hallazgos y riesgos identificados.

- Durante la vigencia del contrato sólo se utilizó una vez el Servicio de Análisis forense, no obstante, el entregable proporcionado no incluía la metodología bajo la cual se realizó, ni se señala la cadena de custodia generada y los mecanismos que se

aplicaron para la recolección y protección de la información. Asimismo, en el entregable se señala que el análisis se vio limitado dado que el equipo analizado no tenía activa la generación de bitácoras en el sistema operativo.

- El Servicio de pruebas DDoS no se solicitó durante la vigencia del contrato.

- El Servicio de Borrado Seguro se tenía que ejecutar a petición del ISSSTE y una vez concluida la vigencia del contrato. No se realizaron peticiones durante la vigencia del contrato. El 31 de diciembre de 2019, finalizó la vigencia del contrato, no obstante, se hizo la petición al proveedor hasta el 12 de marzo de 2020, el ISSSTE indicó que debido a la situación que originó la pandemia no se ha podido concluir.

**Conclusiones**

Por lo anterior, se observa que la investigación de mercado incluyó sólo a 4 proveedores (Axtel, S.A.B. de C.V., Orben Comunicaciones, S.A.P.I. de C.V., Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V. y Nuga SYS, S.A. de C.V.) sin justificar como se seleccionaron, no se realizó una búsqueda en CompraNet donde existía al menos un proveedor que ofrecía servicios similares a los requeridos por el ISSSTE, tampoco se realizó un análisis comparativo de las necesidades requeridas por el ISSSTE respecto a los servicios que se ofrecieron en la Licitación Pública Internacional Abierta Electrónica de Servicios No. LA-006E00001-E1-2016 y que demostrara que se prestarían en igualdad de condiciones en cuanto a precio y calidad; no se justificó que la entidad podría haber tenido pérdidas económicas por optar por un procedimiento de contratación distinto al de adjudicación directa. Asimismo, existieron deficiencias en la supervisión de las actividades realizadas al proveedor, así como en el seguimiento y en la entrega de los servicios solicitados bajo este contrato.

Se identificaron pagos injustificados por 3,782.9 miles de pesos relacionados con el servicio de administración de usuarios privilegiados debido a la incompatibilidad de la solución propuesta por el proveedor con la infraestructura del ISSSTE, por lo que se incumplió con los objetivos específicos 1 y 2 del Proceso de administración de proveedores (APRO) del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, con última reforma publicada en el Diario Oficial de la Federación el 23 de julio de 2018; del numeral 8.1, Objetivo y funciones 1 y 5, 8.1.4 función 2 del Manual de Organización General del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, con última reforma publicada el Diario Oficial de la federación el 11 de julio de 2018.

Al respecto, se procederá en los términos del Artículo 22 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2019-1-19GYN-20-0215-01-005 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado fortalezca los controles que permitan verificar que en los procesos de contratación en materia de TIC las investigaciones de mercado realizadas por la Subdirección de Tecnologías de la Información sean acordes a las necesidades del Instituto y que, en los casos de excepción a la licitación pública, los servicios por contratar deriven de necesidades totalmente justificadas por medio de un dictamen técnico, el cual se integrará al expediente de la investigación de mercado; asimismo, que siempre se incluyan los criterios por los cuales se determinó la selección de proveedores, se establezcan criterios de búsqueda en CompraNet que sean acordes a los servicios solicitados y, en caso de considerar licitaciones públicas efectuadas por otras entidades, se elabore un documento formalizado en donde se identifiquen de manera específica las similitudes de los servicios proporcionados.

2019-1-19GYN-20-0215-01-006 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado recabe y defina sus necesidades antes de celebrar las contrataciones en materia de TIC a fin de que se encuentren fundamentadas desde su celebración y de esta forma evitar subjetividades en las solicitudes de servicios realizadas a los proveedores, realice el análisis por medio del cual se determinen los factores tecnológicos para clasificar los aplicativos, infraestructura y software requeridos; se investiguen las mejores alternativas para solicitar servicios administrados y servicios bajo demanda; realice las comparaciones entre los servicios ofertados en contratos o licitaciones públicas y los requeridos por el Instituto y sean plasmadas en un documento formal adjunto a las investigaciones de mercado. Asimismo, se asegure de que los servicios solicitados en los contratos sean acordes al objeto y naturaleza de los servicios requeridos y se establezcan desagregados los precios por servicio para garantizar las mejores condiciones para el Estado.

2019-1-19GYN-20-0215-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 3,782,881.54 pesos (tres millones setecientos ochenta y dos mil ochocientos ochenta y un pesos 54/100 M.N.), por pagos injustificados relacionados con el contrato Número AD-CS-DA-SRMS-311/2016 Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos, por el Servicio de Gestión de Usuarios Privilegiados el cual no fue proporcionado en el periodo comprendido del 01 de octubre de 2018 al 30 de noviembre de 2019, pagados con recursos de la cuenta pública 2019, en razón de las incompatibilidades de la solución propuesta por el proveedor con la infraestructura tecnológica del centro de datos principal del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, ante las cuales ni el administrador del contrato ni la Subdirección de Tecnología de la Información emitieron una opinión técnica ni realizaron las acciones pertinentes para modificar el alcance de la contratación en incumplimiento de los objetivos específicos 1 y 2, del Proceso de administración de proveedores (APRO), del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de

Seguridad de la Información, con última reforma publicada en el Diario Oficial de la Federación el 23 de julio de 2018; del numeral 8.1 Objetivo, funciones 1 y 5, numeral 8.1.4, función 2, del Manual de Organización General del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, con última reforma publicada el Diario Oficial de la federación el 11 de julio de 2018; y de las cláusulas tercera, decima sexta, y del numeral 5.3.1.7 del anexo técnico del contrato número AD-CS-DA-SRMS-311/2016.

**Causa Raíz Probable de la Irregularidad**

Falta supervisión y control en el seguimiento de entrega de servicios por parte del proveedor.

**4. Contrato Número AD-CS-DA-SRMS-141/2015 “Servicio Administrado de Equipo de Cómputo Personal (SAECP)"**

Se revisó el Contrato Plurianual número AD-CS-DA-SRMS-141/2015, celebrado con Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., Servicios de Integración y Garantías, S.A. de C.V. y Tecnología en Service Desk, S.A. de C.V., en participación conjunta, con fundamento en los artículos 22, fracción II, 25, primer párrafo, 26, fracción III, 40, 41, fracción III, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 71 y 72, fracción III, de su Reglamento; con vigencia del 1º de abril de 2015 al 31 de julio de 2018, con el objeto de contratar la prestación del “Servicio administrado de equipo de cómputo personal (SAECP)”, con un monto mínimo de 1,061,742.9 miles de pesos y un máximo de 2,294,616.0 miles de pesos. A través de la celebración del Segundo Convenio Modificatorio con número CM-CS-DA-SRMS-015/2018, de fecha 11 de julio de 2018, se amplió la vigencia del contrato al 31 de agosto de 2019, modificando también la cláusula segunda correspondiente al precio por un monto mínimo de 1,274,091.6 miles de pesos y un máximo de 2,753,539.2 miles de pesos, con pagos realizados en 2019 por 599,153.4 miles de pesos, se determinó lo siguiente:

**Alcance**

Los servicios requeridos en la modalidad de servicio administrado incluyeron equipo de cómputo, periféricos y servicios operativos. El proveedor fue responsable de todas las actividades durante la prestación de los servicios, incluyendo el desplazamiento de personas y equipos, herramientas, refacciones y demás elementos necesarios para cumplir con el servicio.

**Convenios modificatorios**

Mediante el primer convenio modificatorio se incrementó el número de tabletas y notebooks por suministrar para quedar en un máximo de 3,000 dispositivos, con el fin de equipar a 123 Estancias de Bienestar y Desarrollo Infantil del ISSSTE. Con el desarrollo de un segundo convenio modificatorio se aumentó el monto mínimo y máximo en un 20.0 %, quedando en 1,274,091.6 miles de pesos y 2,753,539.1 miles de pesos, respectivamente,

ampliando su vigencia al 31 de agosto de 2019. Por medio de un tercer convenio modificatorio se actualizó la cláusula décima séptima “Verificación de las Especificaciones y Aceptación de los Servicios”.

**Investigación de mercado**

La investigación de mercado fue elaborada por la DTED ahora Subdirección de Tecnología de la Información. En su análisis se observó lo siguiente:

- El ISSSTE solicitó propuestas a 4 proveedores, no precisó el método de búsqueda en Internet ni los criterios por los cuales solo se eligieron a estos proveedores.

- No se realizó un análisis comparativo de los componentes, capacidades y características de los posibles proveedores.

- Se tomó como base la Licitación Pública Nacional Electrónica número LA-019GYN905-N3-2014 del Fondo de Vivienda del ISSSTE (FOVISSSTE), en la cual el proveedor fue Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V. (Theos).

**Justificación de Excepción a la Licitación Pública**

El Comité de Adquisiciones, Arrendamientos y Servicios (CAAS) dictaminó favorablemente la excepción al procedimiento de licitación, al considerar que el proveedor Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., acreditaba una mejor oferta de servicio en cuanto a calidad y oportunidad al considerar que éste aceptó ofrecer las mismas condiciones ofertadas en la Licitación Pública Nacional Electrónica número LA-019GYN905-N3-2014 con FOVISSSTE y como consecuencia, se evitarían pérdidas o costos adicionales, y se obtendrían así las mejores condiciones para el Estado, en este sentido se observó:

- No se presentó evidencia de que los servicios base y sobre demanda se hayan presentado en igualdad de condiciones dado que fueron adicionales o bajo esquemas diferentes de servicio.

- No se realizó un análisis técnico en el que se hayan comparado los servicios y características requeridas por el ISSSTE y los ofrecidos en dicha licitación.

- En la licitación se ofrecían, entre otros, el Servicio Administrado de Replicador de Puertos Docking Station y el Servicio Administrado de Sistemas de Energía Interrumpida (UPS, por sus siglas en inglés) con el esquema bajo demanda, mientras que el ISSSTE los formalizó como servicios base. Asimismo, de los 19 servicios ofertados en dicha licitación, el ISSSTE adicionó 5 servicios más que no eran parte de la licitación.

**Pagos**

En desglose de las facturas se identificó:

- Ni el contrato ni en su anexo técnico se describen las actividades, características o entregables asociados al “Servicio de Administración”; en la factura se incluye dicho servicio el cual tiene un costo mensual de 6,612.0 miles de pesos, sin embargo, no hay evidencia de que este servicio haya sido prestado por el proveedor.

- Se identificó que el proveedor emitió facturas a nombre del ISSSTE por los meses de enero a agosto de 2019 por 50,366.8 miles de pesos, sin embargo, el ISSSTE no proporcionó los pagos asociados a dichas facturas ni confirmó que pertenecieran a este contrato.

**Supervisión**

- El total de actas de entrega-recepción y cédulas de supervisión fueron firmadas y autorizadas por personal que no contaba con las facultades legales requeridas, dado que no eran los administradores del contrato.

**Servicios Administrados**

- Mediante la herramienta BMC Client Management se gestionó la administración de los activos de cómputo, la ASF analizó la información de 54 de 62 sedes, a fin de identificar el número de equipos asignados y su estado. Se observó que no se cumplió con lo estipulado en el contrato de acuerdo con lo siguiente:

    - El ISSSTE no supervisa las altas, bajas, cambios y reubicaciones de equipos de cómputo ejecutados por el proveedor.

    - La administración de los proyectores, teclados, mouse, sistemas de energía interrumpida (UPS, por sus siglas en inglés), tabletas, escaneres, cámaras y servidores no se llevó a cabo de forma unificada a través de la herramienta de gestión del proveedor.

    - Sólo se detectan equipos de cómputo con agente instalado y sólo se identifican equipos Windows. No se mostró que la herramienta soporte las tecnologías MacOS y Linux

    - La herramienta no descubre equipos de cómputo nuevos conectados a la red, tales como impresoras, switches o ruteadores.

    - La herramienta no gestiona el software de forma unificada.

    - No se cuenta con mecanismos para la planeación de presupuesto, solicitado a través del Anexo Técnico No.1 del contrato.

- A la fecha de la auditoría (agosto de 2020), los niveles de servicio no se encontraron configurados en la herramienta.

- No se cuenta con trazabilidad que permita identificar la ubicación final de 2,538 equipos de escritorio, 225 computadoras portátiles, 962 impresoras, 145 escáneres, 84 proyectores, 61 cámaras, 3 plóteres y 2 servidores, correspondientes a la Dirección Médica, Dirección de Prestaciones Económicas, Sociales y Culturales, Dirección Jurídica y Dirección de Tecnología y Desarrollo Institucional, solicitados en el Anexo Técnico No. 1 del contrato.

- Los equipos asignados a SUPERISSSTE, PENSIONISSSTE y TURISSSTE no son monitoreados por la herramienta de administración de equipos del proveedor. Esto corresponde a un total de 1,270 computadoras de escritorio, 1,240 sistemas de energía interrumpida (UPS, por sus siglas en inglés), 62 laptops, 57 docking station, 28 proyectores, 26 cámaras fotográficas y 3 computadoras de diseño (MAC) asignadas a tales unidades; a pesar de que dichos equipos se encuentran considerados en la facturación y pago mensual realizado al proveedor.

- Respecto a la Gestión de activos y configuraciones (CMBD), los equipos no pueden ser “escaneados en tiempo real” para evaluar las configuraciones vulnerables o no seguras a fin de remediarlas automáticamente.

- No se proporcionó evidencia de la distribución de parches de seguridad en los equipos de cómputo.

- El módulo de Administración del conocimiento no fue utilizado.

- El Instituto realizó un dimensionamiento deficiente en relación con sus necesidades; se comprobó que utilizó cantidades inferiores a los mínimos estipulados en el Servicio administrado de cómputo de escritorio, Servicio administrado de cómputo portátil y Servicio administrado de replicador de puertos; asimismo, el servicio de clientes ligeros fue requerido inicialmente y después se descartó, sin que haya generado un pago adicional.

- Para cinco servicios bajo demanda, no se proporcionó información para determinar si llegaron al mínimo.

- Se identificó un total de 15 tabletas que fueron asignadas a las oficinas de las Direcciones de Administración, Comunicación Social, a la Dirección General y a la Subdirección de Tecnología de la Información, sin que se justificara dicha asignación.

**Entregables**

Conforme a los entregables estipulados contractualmente se identificaron las observaciones siguientes:

- No se proporcionó evidencia de la revisión conjunta del equipo de cómputo activo/inactivo en la herramienta de administración del proveedor. La inactividad del equipo de cómputo no es considerada en la evaluación de necesidades del Instituto.

- No se llevó a cabo la actividad de certificación inicial de la totalidad de las aplicaciones institucionales.

- Durante la vigencia del contrato el proveedor manejó las mismas imágenes de software institucional desde su creación (2015) y utilizó sistemas operativos que ya no contaban con soporte del fabricante, sin que el ISSSTE hubiera objetado el servicio, dado que esto compromete su infraestructura.

- En junio, agosto y diciembre de 2019 no se tuvo disponibilidad de la herramienta para las sedes Centro Médico Nacional 20 de noviembre, Zona Norte 2 y Fianzas Patriotismo. No se comprobó la existencia de medios alternos de atención para los sitios que no fueron alcanzados por la herramienta BMC Client Management por fallas en el servicio.

- A principios de 2019 los periféricos (teclados, mouse) y sistemas de energía interrumpida (UPS, por sus siglas en inglés) reportaron fallas, para el caso de los UPS, se encontraban en espera de garantía sin que a la fecha de la auditoría (agosto 2020) se haya presentado evidencia de su reemplazo.

- No se cuenta con información que asegure que el proveedor proporcionó las actividades de transferencia de conocimientos, destrucción de información y retiro de infraestructura una vez que el contrato concluyó, conforme se estipuló en la Fase IV. Cierre.

- No se proporcionaron los entregables del Proceso de Administración de Configuración (ACNF), Administración de Servicios (ADS) y Proceso de Administración de la Operación (AOP) para la operación de la mesa de servicios.

**Conclusiones**

Por lo anterior, se observó que no hubo un análisis y dimensionamiento de las necesidades por parte del ISSSTE ya que se solicitaron algunos servicios que no fueron utilizados. En relación al contrato Número AD-CS-DA-SRMS-141/2015 Servicio Administrado de Equipo de Cómputo Personal (SAECP), se determinaron pagos injustificados por 87,279.1 miles de pesos por el Servicio de Administración, y 523.7 miles de pesos, relacionados al concepto de

Memoria de cómputo tradicional y el rubro de Unidades de Suscripción de Software, lo que incumplió con lo establecido en los artículos 1, segundo párrafo y 51, tercer párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su última reforma publicada en el Diario Oficial de la Federación el 19 de noviembre de 2019; de la fracción III del artículo 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria con última reforma publicada en el Diario Oficial de la Federación el 30 de diciembre de 2015; de los artículos 7 y 8, fracción I de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y su última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2009; del numeral 7.2 párrafo octavo inciso b) de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del ISSSTE publicadas en el Diario Oficial de la Federación el 02 de marzo de 2012; del numeral 4.3.1.1.4 del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público y su última reforma publicado en el Diario Oficial de la Federación el 03 de febrero de 2016; del apartado III.B Proceso de Administración de Proveedores (APRO), actividad del proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factor crítico 1 del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, y sus reformas publicadas el 23 de julio de 2018; de las Cláusulas Séptima, Octava y Décima Séptima, y el Anexo Técnico No. 1 del Servicio Administrado de Equipo de Cómputo Personal.

Al respecto, se procederá en los términos del Artículo 22 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**Contrato núm. AD-CS-DNAF-SRMS-434/2019 “Servicio Administrado de Equipo de Cómputo Personal (SAECP)"**

Se analizó el contrato número AD-CS-DNAF-SRMS-434/2019 celebrado con Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V. como representante común de la participación conjunta con Servicios de Integración y Garantías, S.A. de C.V. y Tecnología en Service Desk, S.A. de C.V. para el “Servicio Administrado de Equipo de Cómputo Personal (SAECP)", mediante procedimiento de adjudicación directa con fundamento en los artículos 40 y 41 fracción V de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con una vigencia de septiembre a diciembre de 2019, por un monto mínimo de 159,345.2 miles de pesos y un máximo de 180,000.0 miles de pesos, sin embargo, el ISSSTE no reportó pagos durante 2019. Se determinó lo siguiente:

- Mediante este contrato se dio continuidad a los servicios prestados en el contrato número AD-CS-DA-SRMS-141/2015, el cual fue adjudicado al mismo proveedor.

- El Instituto no proporcionó el estudio de factibilidad que acredite la pertinencia del “Servicio administrado de equipo de cómputo personal (SAECP)”, por lo que no fue posible validar la determinación de la procedencia de su renovación con el mismo proveedor.

- El estudio de mercado presentado por el ISSSTE y el formato FO-CON-05 “Resultado de la investigación de mercado” no reflejaron los importes totales de las propuestas económicas presentadas por los proveedores. No se proporcionó el “Estudio Costo-Beneficio”.

- El Instituto “fundamentó” la contratación con la “proximidad” de la fecha de conclusión; es decir, el Instituto no previno la terminación de los servicios del contrato número AD-CS-DA-SRMS-141/2015 y sus convenios modificatorios ya que, de acuerdo con la documentación del estudio de mercado, lo hizo un mes antes de que concluyera el contrato (agosto 2019).

- Al ser una nueva contratación no se especificó si se utilizaron los mismos componentes del contrato número AD-CS-DA-SRMS-141/2015.

- Respecto de la continuidad del servicio para el año 2020, el ISSSTE indicó la existencia del contrato número AD-CSDNAF-013/2020, sin señalar si era con el mismo proveedor; sin embargo, a la fecha de la auditoría (agosto 2020) no se proporcionó evidencia de la formalización de dicha contratación. El proveedor Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., sigue en las instalaciones del ISSSTE, proporcionando el servicio con el mismo equipamiento del contrato número AD-CS-DA-SRMS-141/2015.

**Justificación al procedimiento de Excepción**

- La justificación no se sometió a dictaminación por parte del Comité de Adquisiciones, Arrendamientos y Servicios.

- Dicha justificación no consideró un apartado en el que se incluyera al servidor público que la suscribió (Director Normativo de Administración y Finanzas) y dictaminó como procedente la no celebración de la Licitación Pública.

**Conclusiones**

Por lo anterior se observa que el ISSSTE no realizó de forma anticipada un levantamiento de necesidades con el cual pudiera realizar una investigación de mercado conforme a sus necesidades. La justificación del procedimiento de excepción no cuenta con la aprobación del responsable.

2019-1-19GYN-20-0215-06-003 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 87,279,125.00 pesos (ochenta y siete millones doscientos setenta y nueve mil ciento veinticinco pesos 00/100 M.N.), por por pagos injustificados relacionados con el Servicio de Administración incluido en el contrato número AD-CS-DA-SRMS-141/2015, del cual no se proporcionó evidencia que indique que este servicio fue prestado por el

proveedor; ni el contrato ni en la facturación se describen las actividades y el número de entregables que amparan los pagos efectuados por dicho servicio en incumplimiento de los artículos 1, segundo párrafo, y 51, tercer párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su última reforma publicada en el Diario Oficial de la Federación el 19 de noviembre de 2019; del artículo 66, fracción III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria con última reforma publicada en el Diario Oficial de la Federación el 30 de diciembre de 2015; de los artículos 7 y 8, fracción I, de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y su última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2009; del numeral 7.2, párrafo octavo, inciso b), de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del ISSSTE publicadas en el Diario Oficial de la Federación el 02 de marzo de 2012; del numeral 4.3.1.1.4 del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público y su última reforma publicado en el Diario Oficial de la Federación el 03 de febrero de 2016; del apartado III.B Proceso de Administración de Proveedores (APRO), actividad del proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factor crítico 1, del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, y sus reformas publicadas el 23 de julio de 2018, y de las Cláusulas Séptima, Octava y Décima Séptima y el Anexo Técnico No. 1 del Servicio Administrado de Equipo de Cómputo Personal.

**Causa Raíz Probable de la Irregularidad**

Falta supervisión y control en el seguimiento de entrega de servicios por parte del proveedor.

2019-1-19GYN-20-0215-06-004 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 523,696.50 pesos (quinientos veintitrés mil seiscientos noventa y seis pesos 50/100 M.N.), por pagos injustificados realizados al proveedor, los cuales se integran por 76,299.00 pesos por el concepto de Memoria de cómputo tradicional y 447,397.50 pesos por el rubro de Unidades de Suscripción de Software (con precio unitario de 7,012.50 pesos) de los cuales no se demostró qué tipo de software se adquirió y tampoco que se haya instalado de acuerdo a lo solicitado en el contrato número AD-CS-DA-SRMS-141/2015 en incumplimiento del artículo 51, párrafo III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; de los artículos 1 y 51, tercer párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su última reforma publicada en el Diario Oficial de la Federación el 19 de noviembre de 2019; del artículo 66, fracción III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su última reforma publicada en el Diario Oficial de la Federación el 30 de diciembre de 2015; de los artículos 7 y 8, fracción I, de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y su última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2009; numeral 7.2, párrafo octavo, inciso b), de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del ISSSTE publicadas en el Diario Oficial de la

Federación el 02 de marzo de 2012; del numeral 4.3.1.1.4 del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público, y su última reforma publicada en el Diario Oficial de la Federación el 03 de febrero de 2016; del apartado III.B Proceso de Administración de Proveedores (APRO), actividad del proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factor crítico 1, del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, y sus reformas publicadas el 23 de julio de 2018, y de las cláusulas Séptima, Octava y Décima Séptima y el Anexo Técnico No. 1, numerales 5 y 7, del Servicio Administrado de Equipo de Cómputo Personal.

**Causa Raíz Probable de la Irregularidad**

Falta supervisión y control en el seguimiento de entrega de servicios por parte del proveedor.

## 5. Ciberseguridad

**Evaluación de Ciberseguridad en el ISSSTE**

Para evaluar la ciberseguridad del Instituto la ASF utilizó 2 marcos de referencia internacionales específicos en la materia, el marco CIS (Controles Críticos de Seguridad del Centro de Seguridad de Internet, por sus siglas en inglés) para la infraestructura crítica de TIC (Centro de Datos, Telecomunicaciones, Seguridad Perimetral, Ambientes de Desarrollo y Controles de Acceso) y el marco NIST (Instituto Nacional de Estándares y Tecnología, por sus siglas en inglés) 1800-24 para la infraestructura Securing Picture Archiving and Communication System (PACS) que dan soporte a los sistemas que forman parte de los procesos y equipos médicos dentro del Instituto (Imagenología, Anatomía Patológica y Mastografía).

**Evaluación de Ciberseguridad basada en CIS.**

La ASF utilizó los Controles CIS versión 7.1, que está conformado por 20 controles de ciberdefensa, integrados por 171 actividades de control disponibles para detectar, prevenir, responder y mitigar el daño, desde el más común al más avanzado, de ataques relacionados con la seguridad de la información y ciberseguridad.

**Tabla 1. Controles Críticos de Seguridad del Centro de Seguridad de Internet (Controles CIS)**

| Tipo de Control | No. | CIS Controls IS Audit/Assurance Program |
|---|---|---|
| Básico | CSC 1 | Inventario de dispositivos autorizados y no autorizados |
| Básico | CSC 2 | Inventario de software autorizado y no autorizado |
| Básico | CSC 3 | Gestión continua de vulnerabilidades |
| Básico | CSC 4 | Uso controlado de privilegios administrativos |
| Básico | CSC 5 | Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores |
| Básico | CSC 6 | Mantenimiento, monitoreo y análisis de logs de auditoría |
| Fundamentales | CSC 7 | Protección de correo electrónico y navegador web |
| Fundamentales | CSC 8 | Defensa contra malware |
| Fundamentales | CSC 9 | Limitación y control de puertos de red, protocolos y servicios |
| Fundamentales | CSC 10 | Capacidad de recuperación de datos |
| Fundamentales | CSC 11 | Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores |
| Fundamentales | CSC 12 | Defensa en borde |
| Fundamentales | CSC 13 | Protección de datos |
| Fundamentales | CSC 14 | Control de acceso basado en la necesidad de conocer |
| Fundamentales | CSC 15 | Control de acceso inalámbrico |
| Fundamentales | CSC 16 | Monitoreo y control de cuentas |
| Organizacionales | CSC 17 | Implementar un programa de concienciación y capacitación en seguridad |
| Organizacionales | CSC 18 | Seguridad del software de aplicación |
| Organizacionales | CSC 19 | Respuesta y gestión de incidentes |
| Organizacionales | CSC 20 | Pruebas de penetración y ejercicios de Equipo Rojo |

**Fuente.** Controls Center for Internet Security (CIS) v7.1.

## Alcance de la revisión bajo los controles CIS

El análisis se aplicó en el centro de datos principal, infraestructura de telecomunicaciones, estaciones de trabajo, seguridad perimetral, aplicativos médicos (SICOR [Sistema de Control de Recetas], RALM [Registro Automatizado de Licencias Médicas], el SIMEDIS [Sistema Médico de Evaluación de Enfermedades Discapacitantes], el PREVENISSTE, el STICMA [Sistema de Cita Telefónica para Mastografía]), el servicio de correo electrónico, la base de datos y servicios web.

## Medición

Para determinar el nivel de cumplimiento de cada control se evaluó cada subcategoría que lo componen; en color verde se muestran los controles con el 100.0% de cumplimiento de las subcategorías, en caso de superar el 50.0% de las subcategorías se considera parcial en color amarillo, y si es menor del 50.0%, no cumple con la estimación requerida, en color rojo.

**Tabla 2. Principales observaciones y riesgos por la carencia o deficiencias de los controles de ciberseguridad**

| Factor crítico / Subcategoría | Observación / Riesgo | % Cumplimiento en base a 100% por subcategoría | Nivel de Cumplimiento |
|---|---|---|---|
| Inventario de dispositivos autorizados y no autorizados | CIS 1. Al no administrar (inventariar, rastrear y corregir) el hardware de la infraestructura tecnológica podría ocasionar que el hardware nuevo que se instale en la red no sea monitoreado generando deficiencias en la planificación y ejecución de copias de seguridad, respuesta a incidentes y recuperación de sistemas. | 0% | |
| Inventario de software autorizado y no autorizado | CIS 2. Cuando no se administra (rastrear y corregir) el software que opera en la infraestructura tecnológica puede ocasionar que la infraestructura se encuentre vulnerable a ataques en los cuales se exploten vulnerabilidades de versiones (obsoletas) de software que puedan ingresar a datos sensibles de forma remota y que este pueda ejecutarse sin restricciones en cualquier dispositivo conectado en la red creando una brecha de alto impacto. | 20% | |
| Gestión continua de vulnerabilidades | CIS 03. Al no documentar la información relacionada con la atención y seguimiento de las vulnerabilidades identificadas en toda la infraestructura tecnológica; no se puede identificar de manera oportuna a los sistemas más vulnerables para los atacantes y solucionarlos o mitigar las deficiencias identificadas.<br><br>El no contar con una herramienta para la actualización de parches de software que automatice las actualizaciones, se ven comprometidos los sistemas que operaran en la infraestructura tecnológica. | 29% | |
| Uso controlado de privilegios administrativos | CIS 04. Cuando no se cuentan con procesos definidos para la configuración de los privilegios administrativos, un atacante puede controlar completamente un equipo e instalar keylogger, sniffers y software de control remoto para buscar contraseñas administrativas y otros datos confidenciales del Instituto, que podría exponer información confidencial del ISSSTE y de sus derechohabientes. | 11% | |
| Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores | CIS 05. No administrar e implementar una configuración de seguridad de dispositivos, se compromete a la infraestructura al ser más factible que se puedan explotar los servicios y configuraciones vulnerables de los equipos conectados a la infraestructura tecnológica. | 20% | |
| Mantenimiento, monitoreo y análisis de logs de auditoría | CIS 06. No documentar y analizar los registros de auditoría, puede provocar que actividades ilícitas puedan pasar desapercibidas indefinidamente y crear daños particulares en la infraestructura tecnológica irreversiblemente y en consecuencia, existe oportunidad para que los usuarios maliciosos puedan extraer datos que comprometa información confidencial. | 25% | |
| Protección de correo electrónico y navegador web | CIS 07. Cuando no se monitorea ni se detecta actividad maliciosa en las aplicaciones ocasiona que los aplicativos se encuentren expuestos a ataques sin que sean detectados. | 60% | |
| Defensa contra malware | CIS 08. No supervisar las configuraciones de los equipos que se encuentran operando en la red, compromete la capacidad para tomar acciones correctivas/proactivas para mitigar las vulnerabilidades y/o ataques detectados. | 63% | |
| Limitación y control de | CIS 09. No contar con mecanismos para controlar el acceso a puertos de red, protocolos y distintos servicios, deja expuesto los servicios de red remotamente | 20 % | |

| Factor crítico / Subcategoría | Observación / Riesgo | % Cumplimiento en base a 100% por subcategoría | Nivel de Cumplimiento |
|---|---|---|---|
| puertos de red, protocolos y servicios | accesibles para que puedan ser vulnerables a una explotación. | | |
| Capacidad de recuperación de datos | CIS 10. El carecer de procesos para el respaldo adecuado de la información crítica podría comprometer la capacidad del ISSSTE de restaurar su operación en caso de una contingencia. | 20 % | |
| Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores | CIS 11. Al no utilizar mecanismos que permitan supervisar la configuración de manera administrada en los equipos de la infraestructura tecnológica, permite tener brechas de seguridad que pueden ser utilizados para penetrar las defensas de cualquier infraestructura. | 21% | |
| Defensa en borde | CIS 12. No corregir y prever una buena gestión en la defensa en el borde ocasiona que se puedan explotar los sistemas alcanzables a través de internet incluyendo no solo a la seguridad perimetral, sino también extraer contenido de internet a través de los límites de la red. Es posible que se pueda robar o cambiar información o establecer una presencia persistente para realizar ataques posteriores. | 21% | |
| Protección de datos | CIS 13. El no contar con una protección de datos, un atacante pudiera lograr acceder a la red, y extraer fácilmente información importante, causando un daño físico o interrumpir operaciones críticas. | 0% | |
| Control de acceso basado en la necesidad de conocer | CIS 14. Al no tener procesos para el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) basados en roles puede provocar la pérdida de control sobre los datos protegidos o sensibles lo que se convertiría en una grave amenaza para las operaciones principales. | 6% | |
| Control de acceso inalámbrico | CIS 15. Tener procesos deficientes sobre el control de puntos de acceso no autorizados y no contar con la detección oportuna de intrusos en la red inalámbrica puede ocasionar que se infecten los sistemas a través de la explotación remota, asimismo también se pueden utilizar como puertas traseras derivado a que no requieren conexiones físicas directas. | 65% | |
| Monitoreo y control de cuentas | CIS 16. Cuando no se gestiona correctamente el monitoreo y control de cuentas de usuarios y de aplicaciones, aumentan las posibilidades de sufrir ataques o tener deficiencias en la detección de acciones ilícitas o de usuarios no autorizados. | 19% | |
| Implementar un programa de concienciación y capacitación en seguridad | CIS 17. El no tener un programa de concientización y entrenamiento de seguridad, provoca que el personal desconozca los principios básicos de cómo proteger su equipo y su información representando un gran riesgo. | 0% | |
| Seguridad del software de aplicación | CIS 18. El no contar con controles de seguridad durante el desarrollo del ciclo de vida de las aplicaciones internas o software comercial adquirido que ayude a prevenir, detectar y corregir las debilidades de seguridad hace que sean más susceptibles a recibir ataques de inyección de lenguaje estructurado de consulta (Structured Query Language -SQL), cross-site scripting (XSS), cross-site request forgery (CSRF) y click-jacking de código para obtener control sobre máquinas vulnerables físicas y virtuales. | 14% | |
| Respuesta y gestión de incidentes | CIS 19. No contar un plan de respuesta a incidentes integral que abarque la infraestructura tecnológica a nivel nacional, podría provocar que en caso de una contingencia no se pudiera contener de manera efectiva el daño, ni mitigar o recuperarse en el tiempo óptimo para no sufrir daños operacionales y económicos. | 0% | |

| Factor crítico / Subcategoría | Observación / Riesgo | % Cumplimiento en base a 100% por subcategoría | Nivel de Cumplimiento |
|---|---|---|---|
| Pruebas de penetración y ejercicios de Equipo Rojo | CIS 20. No contar con un equipo rojo para probar la fortaleza de forma general de la defensa en la organización y el no hacer pruebas de penetración provoca que no se detecte ni se corrijan vulnerabilidades en la infraestructura tecnológica podría ocasionar que un atacante pueda hallar deficiencias y realizar un ataque fácilmente. | 0% | |

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

En análisis de la revisión de los Controles CIS, se observó que, de los 20 controles, el ISSSTE tiene deficiencias en 17, de los cuales 5 están en 0.0%, lo que indica que se tienen brechas de vulnerabilidad importantes.

**Evaluación de Ciberseguridad basada en el NIST Cybersecurity Framework v1.1 1800-24. Securing Picture Archiving and Communication System (PACS). Cybersecurity for the Healthcare Sector**

La Auditoría Superior de la Federación complementó la revisión a la ciberseguridad realizada al ISSSTE con base en un marco de referencia específico para el sector salud el NIST Cybersecurity Framework v1.1 1800-24 Securing Picture Archiving and Communication System (PACS). Cybersecurity for the Healthcare Sector, el cual evalúa 19 subcategorías específicas del marco NIST (Instituto Nacional de Estándares y Tecnología, por sus siglas en inglés y compuesto de 108 subcategorías) para la evaluación de ciberseguridad e infraestructura que soporta la operación de servicios de Imagenología con apoyo de las TIC.

Este marco de referencia identifica como PACS (Securing Picture Archiving and Communication System) a un sistema de almacenamiento digital, transmisión y descarga de imágenes radiológicas. Los sistemas PACS se componen de software y hardware, que directamente se comunican con equipos de captura de imagen (mastógrafos, escaneo de rayos X, equipo de resonancia magnética, ultrasonidos). Las imágenes son transferidas a una estación de trabajo (workstation) para su visualización y emisión de informes radiológicos.

Las imágenes médicas son un componente fundamental en la prestación de atención al paciente. El sistema permite la aceptación, transferencia, visualización, almacenamiento y procesamiento digital de imágenes médicas y es casi omnipresente en los entornos sanitarios.

El ecosistema que rodea a los PACS incluye equipos de obtención de imágenes médicas interconectados que generalmente son los Sistemas de Información Radiológica (RIS), los Sistemas de Información Sanitaria (HIS) o Historia Clínica Electrónica (EHR); así como estaciones de trabajo de visualización y administración.

Estos sistemas a su vez son parte de una clasificación de activos denominados EPHI’s (Información de Salud Protegida Electrónica, por sus siglas en ingles) de los cuales la

mayoría de los médicos y hospitales archivan electrónicamente imágenes, resultados de pruebas, medicamentos, alergias y otros datos, lo que como parte del proceso les permite ver los datos en computadoras.

**Alcance**

Se analizó el alcance del contrato número LPNE-CS-DA-SRMS-298/2017 "Servicio de Gestión, del Almacenamiento y Distribución de Imágenes Médicas de Imagenología (Radiología), Endoscopia y Anatomía", a cargo del proveedor TESI de México, S.A. de C.V., por el cual se pagó un monto total de 992,351.7 miles de pesos, con la supervisión de la Subdirección de Infraestructura.

Los servicios de este contrato corresponden a:

Servicio de gestión almacenamiento y distribución de imágenes y estudios clínicos consistente en la dotación de equipos, software, accesorios, servicios y materiales requeridos para la digitalización, almacenamiento, distribución y visualización de imágenes y reportes de interpretación en las áreas de imagenología (radiología), endoscopia y anatomía patológica.

Dada la función que realiza el ISSSTE y el volumen de atención que otorga a su derechohabiencia, requiere que el cúmulo de imágenes de estudios, médicos- clínicos, se encuentre almacenado en un sitio seguro y disponibles en un esquema de 24 por 365 días para que el personal médico autorizado que requiera esta información pueda tener acceso ilimitado sin importar el lugar en el que se encuentre ubicado.

Debido a la criticidad e importancia de estos servicios, se revisaron los controles que el ISSSTE tiene implementados en cuestión de seguridad en la infraestructura que los soportan.

**Medición**

El resultado de la evaluación para cada subcategoría del NIST (Instituto Nacional de Estándares y Tecnología por sus siglas en inglés) que conforma el marco 1800-24 fue en función del cumplimiento a los requerimientos solicitados por la ASF, entre mayor cumplimiento diera la institución a estos requerimientos se calificaría conforme a los criterios siguientes:

- Atendió todos los requerimientos: Cumple.
- Atendió el 50.0% o más de los requerimientos: Cumple Parcialmente.
- No atendió ningún requerimiento: No Cumple.

Con el análisis realizado por la ASF se evaluó el cumplimiento de cada una de las subcategorías del marco de referencia NIST 1800-24, como se presenta a continuación:

**Tabla 3. Resultados de la evaluación conforme al Marco 1800-24.**

| Función | Categoría | Subcategoría del NIST aplicable | Evaluación |
|---|---|---|---|
| Identificar (ID) | ID.AM - Gestión de Activos | ID.AM-4: Los sistemas de información externos están catalogados | |
| | | ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial. | |
| | ID.RA - Evaluación de Riesgos | ID.RA-6: Las respuestas al riesgo se identifican y priorizan. | |
| Proteger (PR) | PR.AC - Gestión de Identidad y Control de Acceso | PR.AC-4: Se gestionan los permisos y autorizaciones de acceso, incorporando los principios de menor privilegio y separación de funciones. | |
| | | PR.AC-5: La integridad de la red está protegida (por ejemplo, segregación de red, segmentación de red). | |
| | | PR.AC-7: Los usuarios, dispositivos y otros activos están autenticados (p. Ej., Factor único, factor múltiple) proporcionales al riesgo de la transacción (p. Ej., Riesgos de seguridad y privacidad de las personas y otros riesgos organizacionales). | |
| | PR.DS - Protección de Datos. | PR.DS-1: Los datos en reposo están protegidos. | |
| | | PR.DS-5: Se implementan protecciones contra las filtraciones de datos. | |
| | | PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información. | |
| | PR.IP- Procesos y procedimientos de protección de la información | PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima | |
| | | PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información. | |
| | | PR.IP-6: Los datos son eliminados de acuerdo con las políticas. | |
| | | PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres). | |
| | | PR.IP-10: Se prueban los planes de respuesta y recuperación. | |
| | PR.PT - Tecnología de Protección | PR.PT-4: Las redes de comunicaciones y control están protegidas. | |

| Función | Categoría | Subcategoría del NIST aplicable | Evaluación |
|---|---|---|---|
| Detectar (DE) | DE.AE - Anomalías y Eventos | DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque. | |
| | DE.CM - Monitoreo continuo de la seguridad | DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética. | |
| Responder (RS) | RS.RP - Planificación de respuesta | RS.RP-1: El plan de respuesta se ejecuta durante o después de un evento. | |
| Recuperar (RC) | RC.RP - Planificación de recuperación | RC.RP-1: El plan de respuesta se ejecuta durante o después de un incidente de ciberseguridad. | |

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

Respecto al estándar NIST 1800-24, el ISSSTE cumplió de forma parcial con la evaluación de 13 (68.0%) subcategorías de un total de 19, del marco, asimismo, no cumplió con la evaluación de 6 subcategorías (32.0%).

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:

**Tabla 4. Principales observaciones y riesgos por la carencia o deficiencias de los controles de ciberseguridad**

| Factor crítico / Subcategoría | Observación / Riesgo |
|---|---|
| ID.AM - Gestión de Activos | El no contar con un catálogo de infraestructuras críticas no permite al instituto tener mapeados a los activos que debe de dar prioridad de atención en caso de presentarse un evento o incidente, que afecten sus procesos y operaciones incluidos los que dan soporte a los servicios de salud del instituto.<br>No tener identificados y clasificados los sistemas externos que tienen interacción con la infraestructura del instituto, en caso de una eventualidad podría retrasar los procesos de investigación de origen de fallas o incidentes. |
| ID.RA - Evaluación de Riesgos | No contar con mecanismos de evaluación de riesgos de TIC, no le permite al instituto verificar de manera periódica los hallazgos identificados, así como la exposición de la organización a éstos, y si es que ante cualquier cambio que se realice en etapas tempranas un análisis del impacto en la infraestructura de la organización. |
| PR.AC - Gestión de Identidad y Control de Acceso | No contar con una adecuada gestión de contraseñas vulnera al instituto en que se puede ingresar a sistemas y aplicativos críticos por personal no autorizado.<br>No contar con un plan integral de la seguridad con alcance institucional expone al instituto a no contar con los controles suficientes para afrontar posibles vulnerabilidades derivadas del poco control de infraestructura y mal uso de esta por los usuarios, principalmente en el sector salud donde la información que es procesada tiene un carácter crítico para los derechohabientes.<br>El no contar con políticas y procedimientos institucionales, así como depender de las que generen sus proveedores, no garantiza que se dé cumplimiento a los objetivos institucionales con respecto al uso de las tecnologías de la información. |
| PR.DS - Protección de Datos. | El no establecer políticas para el uso correcto y adecuado de la información entre el personal del instituto, así como a proveedores abre una brecha de que esta información no sea tratada y |

| Factor crítico / Subcategoría | Observación / Riesgo |
|---|---|
| | procesada de manera en que se asegure su confidencialidad e integridad.<br>El no establecer mecanismos de prevención de extracción de datos y fuga de información en los sistemas, así como en las estaciones de trabajo que gestionan o procesan información de la salud, puede comprometer a que personas ajenas a los procesos de atención a pacientes hagan un mal uso de información sensible de pacientes o puedan comprometer la exactitud e integridad de expedientes clínicos.<br>No aplicar mecanismos de cifrado a la información proveniente de dispositivos médicos no da la certeza de que se cuente con la seguridad adecuada para su almacenamiento y en caso de requerirse para su consulta que esta se encuentre con la integridad y fiabilidad adecuada y se solicitada solo por el personal o servicios autorizados.<br>El no contar con controles de verificación a la integridad del firmware y software el instituto se expone a que a través de estos activos se encuentren vulnerabilidades que pueden ser explotadas por atacantes y en su caso pueden ser invadidos por software malicioso |
| PR.IP- Procesos y procedimientos de protección de la información | El no realizar análisis de vulnerabilidades a nivel código fuente no permite al instituto a que se identifique de forma oportuna código malicioso que puede encontrarse inmerso o escondido en las aplicaciones definidas como críticas.<br>No contar con un plan de continuidad del negocio institucional en el que se identifique a la toda infraestructura de TIC que soporta procesos críticos para las operaciones, incluidas las ajenas a las Subdirección de Tecnología de la Información, debilita al instituto frente un supuesto en que las operaciones fallen y se vean afectados procesos críticos incluidos los relacionados con la atención a pacientes. Así mismo no ejecutar pruebas de recuperación a la infraestructura tales como servidores o equipamiento de telecomunicaciones no garantiza que estos no se encuentren funcionando de forma óptima ante un supuesto de continuidad del negocio.<br>El no definir a los responsables de comunicar y dar atención a los procesos de respuesta a incidentes y continuidad del negocio, entorpecería dichos procesos ya que el personal involucrado no tendría conocimiento de a quien comunicarse ante un supuesto.<br>No contar con la definición de líneas base a nivel institucional ni con políticas y procedimientos institucionales para su gestión, limita al instituto en cuanto el control de la infraestructura (incluyendo a la proporcionada por proveedores) y a que no sean aplicadas las configuraciones que el instituto requiere para una adecuada seguridad en la información |
| PR.PT - Tecnología de Protección | No realizar auditorías al funcionamiento de los aplicativos relacionados con la salud no garantiza que se encuentren implementación de mecanismos de seguridad adecuados, ni que se atiendan en forma oportuna posibles brechas de seguridad antes de que sean aprovechadas por personas malintencionadas. |
| DE.AE - Anomalías y Eventos | No contar con un procedimiento institucional para la gestión de actividades de monitoreo, así como para las actividades de gestión de incidentes en infraestructuras de TIC críticas, vulnera al instituto con respecto a que personal interno y externo no conozcan los procesos de comunicación, así como las actividades de atención que garanticen la oportuna detección y gestión de eventos que comprometan la operación de procesos críticos en la institución |
| DE.CM - Monitoreo continuo de la seguridad | El no supervisar los mecanismos y resultados de las actividades de monitoreo que efectúan los proveedores de las distintas soluciones de dispositivos médicos, no le permite al instituto tener un panorama total de sobre la seguridad a la información de su propiedad que se gestionan en sus distintas áreas y en su caso poder aplicar los mecanismos de atención pertinentes para asegurar el adecuado funcionamiento de estas soluciones. |
| RS.RP - Planificación de respuesta | El no tener identificada toda la infraestructura critica de TIC que soporta las operaciones del instituto incluida la que da soporte a sistemas relacionados con la información de la salud, limita la atención a los procesos que requieran una mayor prioridad y por ende que se entorpezcan las actividades de atención a pacientes. |
| RC.RP - Planificación de recuperación | El no tener identificado las interdependencias de sistemas críticos en el instituto, puede representar un problema ante una falla en los procesos de recuperación, ya que entorpecería el proceso de investigación de las causas por las cuales no puede ser puesto en marcha un servicio crítico.<br>El delegar todas las responsabilidades de los procesos de recuperación a los proveedores, limita al instituto a que no se tenga conocimiento de posibles incidentes que se presenten en estos procesos. |

**Fuente:** Elaborado por la ASF con base en la información que proporcionó por el ISSSTE.

Por lo anterior se concluye lo siguiente:

- Las políticas de seguridad de la información se limitan a la Subdirección de Tecnologías de la Información y no son de carácter general en el Instituto para cualquier área que utilice TIC, algunas de las políticas proporcionadas son propias de los proveedores de cada ámbito tecnológico (Centro de Datos, Telecomunicaciones, Seguridad, Equipos de Cómputo).

- No se cuenta con una estructura de Seguridad o Ciberseguridad, las funciones se encuentran inmersas en las diferentes jefaturas, no existe una figura responsable de la Seguridad Informática en el Instituto.

- Ni la Subdirección de Tecnologías de la información ni la Jefatura de Servicios de Evaluación y Desarrollo de Proyectos participan en las definiciones de controles de seguridad que deben de aplicarse en las contrataciones de dispositivos médicos que hacen uso de TIC. Tampoco se encuentran asignados en dichas contrataciones como responsables de verificar que dichos dispositivos y la infraestructura tecnológica que los soporta cumple con las configuraciones de seguridad permitidas por el Instituto.

- Respecto a la gestión de accesos, configuración de herramientas e infraestructura, así como a las actividades de monitoreo, actividades que son realizadas por diversos proveedores, el ISSSTE limita sus revisiones a los entregables definidos en los respectivos contratos sin que haya un monitoreo activo.

- La entidad no cuenta con una clasificación formal para sus aplicativos médicos que procesan EPHIS (Información de salud protegida electrónica, por sus siglas en ingles), éstos son los únicos activos en relación con la información de la salud a los que la Subdirección de Tecnología de la Información supervisa y da seguimiento.

- El ISSSTE cuenta con aplicativos médicos con el carácter de legados, que carecen de documentación, por lo que desconoce qué tipos de configuraciones fueron implementadas por sus desarrolladores originales.

- La Jefatura de Servicios de Evaluación y Desarrollo de Proyectos no realiza tareas de supervisión en materia de seguridad informática a los distintos proveedores que ofrecen servicios de dispositivos médicos al Instituto, tal es el caso del Contrato número LPNE-CS-DA-SRMS-298/2017 “Servicio de Gestión, del Almacenamiento y Distribución de Imágenes Médicas de Imagenología (Radiología), Endoscopia y Anatomía”, el cual a pesar de contar con mecanismos de seguridad como firewall, o mecanismos de respaldos a la información, mecanismos de control de cambios y actualizaciones; no recibe retroalimentación o comentarios de las áreas expertas en el Instituto en la aplicación de estos controles.

- La Jefatura de Servicios de Evaluación y Desarrollo de Proyectos no se involucra en la gestión de mecanismos de seguridad tales como el Hardening o la aplicación de

antivirus en estaciones de trabajo y en dispositivos móviles que hagan uso del "Servicio de Gestión, del Almacenamiento y Distribución de Imágenes Médicas de Imagenología (Radiología), Endoscopia y Anatomía", incluso los proveedores aplican sus propias configuraciones sin alinearse a las políticas institucionales.

- El "Servicio de Gestión, del Almacenamiento y Distribución de Imágenes Médicas de Imagenología (Radiología), Endoscopia y Anatomía" es un servicio independiente que cumple únicamente con la funcionalidad de generar imágenes para diversos procesos médicos, y no integra esta información a los sistemas de expedientes clínicos de los derechohabientes del ISSSTE.

- La información utilizada en los procesos de prueba o calidad es una copia de los datos de producción, sin que exista un enmascaramiento de los datos personales de los usuarios.

- El ISSSTE ha celebrado diversas contrataciones en el periodo comprendido de 2016 a 2020 por un monto total estimado de 2,043,707.0 miles de pesos relacionados con el Servicio de Infraestructura de Centro de Datos, Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales, Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos y Servicio Administrado de Equipo de Cómputo Personal (SAECP), los cuales dentro de sus alcances han considerado diversos mecanismos para al apoyo a la seguridad de la información que se procesa en el Instituto, el detalle de ellos se encuentran en los resultados con números 2, 3 y 4, sin embargo, en ninguno de ellos se contemplan a los aplicativos médicos críticos para las operaciones con derechohabientes del ISSSTE.

2019-1-19GYN-20-0215-01-007 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado implemente controles para administrar los dispositivos autorizados y no autorizados; tener un inventario actualizado de software; llevar a cabo un análisis continuo de vulnerabilidades; elaborar un proceso de control de acceso a los activos críticos e implementar mecanismos auditables que permitan comprobar el proceso; tener líneas bases propias de configuración de los dispositivos; realizar análisis de logs; contar con una capacidad de recuperación de datos; implementar mecanismos de protección para los datos críticos o sensibles; supervisar y validar cualquier actividad que ejecuten los proveedores relacionados con infraestructura crítica, verificar que se ajusten a las políticas internas establecidas por el Instituto; y mitigar los riegos detectados en la evaluación de los Controles Críticos del Centro de Seguridad de Internet (CIS por su siglas en inglés).

2019-1-19GYN-20-0215-01-008 **Recomendación**

Para que el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado implemente políticas y procedimientos donde se delegue a la Subdirección de Tecnología de

la Información la responsabilidad de monitorear o supervisar las configuraciones de seguridad de la información y de telecomunicaciones empleadas para el uso de los dispositivos médicos soportados por infraestructura de TIC (imagenología, radiología, mastografía, endoscopia, anatomía patológica, entre otros); desarrollar controles para el resguardo de la información que generan dichos dispositivos en el Instituto; ser partícipe, con un rol de supervisor, en los proyectos que por su naturaleza están relacionados con la aplicación de tecnologías en el sector médico, así como mitigar los riesgos detectados en la evaluación de los controles del marco NIST 1800-24.

***Montos por Aclarar***

Se determinaron 179,056,570.24 pesos pendientes por aclarar.

***Buen Gobierno***

Impacto de lo observado por la ASF para buen gobierno: Controles internos y Vigilancia y rendición de cuentas.

***Resumen de Resultados, Observaciones y Acciones***

Se determinaron 5 resultados, de los cuales, 5 generaron:

8 Recomendaciones y 4 Pliegos de Observaciones.

***Dictamen***

El presente se emite el 19 de octubre de 2020, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado no cumplió con las disposiciones legales y normativas aplicables en la materia, entre cuyos aspectos observados destacan los siguientes:

- El ISSSTE realizó 3 adjudicaciones directas bajo el mismo esquema, basándose en licitaciones que tienen pocas o nulas similitudes a las necesidades de los servicios por contratar. Se solicitaron servicios ajenos a la naturaleza de los objetos de los contratos que no se ocuparon o tuvieron poca utilidad, sin embargo, al ser

contratados bajo un esquema de servicio administrado, incrementan el volumen de servicios lo que encarece los contratos.

- Con la revisión del contrato número AD-CS-DA-SRMS-257/2016 para prestar el Servicio administrado de ambientes de prueba y calidad para aplicativos institucionales, celebrado con Axtel, S.A.B., de C.V., Alestra Comunicación, S. de R.L. de C.V. y Avantel, S. de R.L. de C.V, se determinó lo siguiente:

  - No se demostró que se hubieran realizado los servicios objeto del contrato; tres meses antes de concluir su vigencia, se realizó la terminación anticipada del contrato, por lo cual se presume que esta contratación no tuvo utilidad ni beneficio para el ISSSTE y generó erogaciones en 2019 por 87,470.9 miles de pesos.

- Con la revisión del contrato número AD-CS-DA-SRMS-311/2016 para prestar el Servicio Administrado de Infraestructura de Seguridad en el Centro de Datos, celebrado con las empresas Axtel, S.A.B. de C.V., y Ultrasist, S.A. de C.V, se determinó lo siguiente:

  - Se presumen pagos no justificados por un monto de 3,782.9 miles de pesos en relación con el servicio de administración de usuarios privilegiados, el cual no fue proporcionado debido a la incompatibilidad de la infraestructura del ISSSTE y la solución propuesta por el proveedor.

- Con la revisión del contrato número AD-CS-DA-SRMS-141/2015 para prestar el Servicio Administrado de Equipo de Cómputo Personal, celebrado con las empresas Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., en participación conjunta con Servicios de Integración y Garantías, S.A. de C.V. y Tecnología en Service Desk, S.A. de C.V., se determinó lo siguiente:

  - Se presumen pagos injustificados por un monto de 87,279.1 miles de pesos relacionados con el “Servicio de Administración” ya que no se integró el detalle de las actividades o entregables que amparan el pago de dicho servicio.

  - Se presumen pagos injustificados por un monto de 523.7 miles de pesos debido que no se demostró que se hayan recibido los servicios de Memoria de cómputo tradicional y el tipo de software que se prestaría para las Unidades de Suscripción de Software.

- Con la evaluación realizada a la ciberseguridad, se determinó lo siguiente:

  - En la revisión de los Controles Críticos de Seguridad del Centro de Seguridad de Internet (Controles CIS por sus siglas en inglés), con el cual se evaluó la infraestructura tecnológica crítica de la entidad, se observó que, de los 20 controles del CIS, el ISSSTE presentó niveles muy bajos en 17, de los cuales 5

están en 0.0%, lo que indica que se tienen brechas de vulnerabilidad importantes.

- Con el estándar NIST 1800-24 (Instituto Nacional de Estándares y Tecnología, por sus siglas en inglés) se evaluaron las condiciones de ciberseguridad de los sistemas de almacenamiento digital, transmisión y descarga de imágenes radiológicas, en el cual el ISSSTE cumplió de forma parcial con la evaluación de 13 subcategorías del marco (68.0%) asimismo, no cumplió con la evaluación de 6 subcategorías (32.0%).

- El ISSSTE ha celebrado diversas contrataciones de 2016 a 2020, por un monto total estimado en 2,043,707.0 miles de pesos relacionados con Servicios de ambientes de prueba y calidad para aplicativos institucionales, de Infraestructura de Seguridad en el Centro de Datos y de Arrendamiento de Equipo de Cómputo Personal, en los cuales se identificaron deficiencias tales como un centro de cómputo específico para un ambiente de pruebas que no fue utilizado y servicios de seguridad que no tuvieron seguimiento por parte del Instituto. Estas deficiencias no han permitido al ISSSTE contar con esquemas de seguridad de la información y de ciberseguridad.

***Servidores públicos que intervinieron en la auditoría:***

| Director de Área | Director General |
|---|---|
| C. Valderrama Roberto Hernández Rojas | 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, para los Capítulos del gasto relacionados con las TIC, las cifras reportadas en la Cuenta Pública correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

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

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo a las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones; verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados estén debidamente soportados, cuenten con controles que permitan 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 las penalizaciones y deductivas en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, servicios administrados para la operación de infraestructura y sistemas sustantivos, telecomunicaciones y demás relacionados con las TIC para verificar: antecedentes; beneficios esperados; entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento/sustantivas); implementación y soporte de los servicios; verificar la gestión de riesgos, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua

de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de vulnerabilidades, entre otros.

*Áreas Revisadas*

Las Subdirecciones de Tecnología de la Información, de Coordinación de Proyectos, de Recursos Materiales y Servicios Generales, así como la de Programación y Presupuesto adscritas a la Dirección Normativa de Administración y Finanzas del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.

*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 General de Contabilidad Gubernamental:

2. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público:

3. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público:

4. Otras disposiciones de carácter general, específico, estatal o municipal: Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos con última reforma publicada en el Diario Oficial de la Federación el 27 de agosto de 2018; artículos 26, 41, fracción III, 42, 51, párrafo III, y 54 Bis, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público con última reforma publicada en el Diario Oficial de la Federación el 10 de noviembre de 2014; Artículos 29, y 102, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público con última reforma publicada en el Diario Oficial de la Federación el 28 de julio de 2010; Fracción III, del artículo 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria con última reforma publicada en el Diario Oficial de la Federación el 30 de diciembre de 2015; Artículos 7, y 8, fracción I, de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos con última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2009; artículos 16, 19, fracción III, 38, fracción I, y 52, de la Ley General de Contabilidad Gubernamental con última reforma publicada en el Diario Oficial de la Federación el 12 de noviembre de 2012; Artículos 77 Bis, 37, fracción X, y 103 Bis 3, de la Ley General de Salud con última reforma publicada en el Diario Oficial de la Federación el 24 de diciembre de 2018; artículos 10, y 68, fracciones II, y VI, de la Ley General de Transparencia y Acceso a la Información Pública y su última reforma publicada en el Diario Oficial de la Federación el 04 de mayo de 2015; artículos 3, 11, fracción VI, 97, 98, 99, y 113, de la Ley Federal de Transparencia y Acceso a la Información Pública con última reforma publicada en el Diario Oficial de la Federación el 27 de enero de 2017; artículos 4, 6, 11, 18, 19, 20, 21, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32,33, 34, 35, 36, 37, 38, 39, 40, 41 y 42, de la Ley General de Protección de Datos Personales en Posesión de

los Particulares publicada en el Diario Oficial de la Federación el 26 de enero de 2017; Artículo 220, fracción VI, de la Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado con última reforma publicada en el DOF el 04 de junio de 2019; artículo 7, fracción IX, del Estatuto Orgánico del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado publicado en el Diario Oficial de la Federación el 1 de febrero de 2019; numerales 5.5, 5.15, y 7.2 párrafo octavo inciso b) de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del ISSSTE publicadas en el Diario Oficial de la Federación el 02 de marzo de 2012; numerales 4.2.4.1.1, 4.3.1.1.4, 4.3.4.1.2, y Tercer párrafo del numeral 4.2.1.1.10, del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público con última reforma publicada en el Diario Oficial de la Federación el 03 de febrero de 2016; artículo 9, inciso IV y 10 inciso I, del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual de Aplicación General en dichas materias, con última reforma publicada en el Diario Oficial de la Federación el 23 de julio de 2018; objetivos específicos 1, y 2, apartado III.B Proceso de Administración de Proveedores (APRO), actividad del proceso APRO 1 Generar lista de verificación de obligaciones, factor crítico 1, actividad APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factor crítico 1; numeral 5.2, funciones 7, 9, 12, 15; numeral 6.2, función 7, y 6.2.1, numeral 8, Objetivo, funciones 3, 5 y 13; numeral 8.1, Objetivo y funciones 1, 3, y 5, numeral 8.2, Objetivo y funciones 3, 4, y 6, numeral 8.1.4, función 2, y 9 del Manual de Organización General del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, con última reforma publicada en el Diario Oficial de la Federación el 11 de julio de 2018; cláusula séptima, octava y décima séptima del contrato número AD-CS-DA-SRMS-141/2015, apartado A, anexo técnico No. 1, del Servicio Administrado de Equipo de Cómputo numerales 5, y 7; cláusulas décima, vigésima segunda, vigésima novena y numerales 4.2.1, y 4.2.15, del anexo técnico del contrato número AD-CS-DA-SRMS-257/2016; cláusulas tercera, decima sexta, y numeral 5.3.1.7, del anexo técnico del contrato número AD-CS-DA-SRMS-311/2016.

*Fundamento Jurídico de la ASF para Promover Acciones y Recomendaciones*

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.