Secretaría del Trabajo y Previsión Social

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-0-14100-15-0405-2018

405-DE

Criterios de Selección

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

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

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

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

En el caso de los Estados de la República:

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

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

Objetivo

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

Consideraciones para el seguimiento

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

En tal virtud, las recomendaciones y acciones que se presentan en este informe individual de auditoría se encuentran sujetas al proceso de seguimiento, por lo que en razón de la

información y consideraciones que en su caso proporcione la entidad fiscalizada, podrán confirmarse, solventarse, aclararse o modificarse.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	436,152.8
Muestra Auditada	131,033.1
Representatividad de la Muestra	30.0%

El universo seleccionado por 436,152.8 miles de pesos corresponde al total de recursos asignados en Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2017; la muestra auditada se integra por cuatro contratos para prestar los Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo; Modernización de Aplicativos con una Fábrica de Software y Arrendamiento de Equipo de Cómputo y Bienes Informáticos con pagos ejercidos por 131,033.1 miles de pesos, que representan el 30.0% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Secretaría del Trabajo y Previsión Social (STPS) en 2017, relacionada con el Gobierno y Administración de las TIC, Gestión de la Seguridad de la Información, Continuidad de las Operaciones y Centro de Datos, entre otras.

Antecedentes

La Secretaría del Trabajo y Previsión Social (STPS) tiene como misión fortalecer la política laboral, a partir de cuatro ejes rectores dirigidos a lograr que los mexicanos tengan acceso a empleos formales y de calidad, con prestaciones y derechos plenos, a través de la democratización de la productividad, la plena salvaguarda de sus derechos y el de las personas en situación de vulnerabilidad, además de asegurar el acceso a la justicia laboral.

Durante el 2017, la STPS contó con cinco proyectos estratégicos en materia de TIC: Centro de Contacto E-Multimedia para la atención de los usuarios del Servicio Nacional de Empleo y del Portal de Empleo; Servicios Administrados de Seguridad de la Información; Servicio del Centro de Tecnologías de la Información y Comunicaciones (CTIC); Red Nacional de Servicios Integrales Administrados de Voz, Datos, Internet y Videoconferencia; así como los Servicios Integrales de Tecnología para el Servicio Nacional de Empleo (SNE).

Entre 2013 y 2017, en la STPS se han invertido más de 2,667,997.5 miles de pesos en sistemas de información, telecomunicaciones e infraestructura tecnológica, entre otros, integrados de la manera siguiente:

Recursos invertidos en materia de TIC

(Miles de pesos)

PERIODO DE INVERSIÓN	2013	2014	2015	2016	2017	TOTALES
MONTO POR AÑO	341,476.2	542,123.9	812,994.1	535,250.5	436,152.8	2,667,997.5

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

Resultados

1. Análisis Presupuestal

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2017, la STPS tuvo un presupuesto de 3,864,317.8 miles de pesos, de los cuales 436,152.8 miles de pesos corresponden a recursos relacionados con las TIC, lo que representan el 11.3% del total, como se muestra a continuación:

Recursos ejercidos en 2017

(Cifras en Miles de Pesos)

Capítulo	Descripción	Presupuesto Ejercido	Presupuesto Ejercido TIC	%
1000	Servicios personales	2,151,492.1	24,462.8	1.1
2000	Materiales y suministros	24,266.4	919.0	3.8
3000	Servicios generales	1,063,262.0	410,771.0	38.6
4000	Transferencias, asignaciones, subsidios y otras ayudas	625,297.3	-	-
	TOTAL	**3,864,317.8**	**436,152.8**	**11.3**

Fuente: Elaborado con la información proporcionada por la STPS.

Los recursos ejercidos en materia de TIC por 436,152.8 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2017 STPS
(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**24,462.8**
2000		**MATERIALES Y SUMINISTROS**	**919.0**
3000		**SERVICIOS GENERALES**	**410,771.0**
	31401	Servicio Telefónico Convencional	2,093.4
	31501	Servicio de Telefonía Celular	1,877.1
	31601	Servicio de Radiolocalización	131.8
	31602	Servicios de telecomunicación	93,438.6
	31603	Servicios de internet	24.0
	31701	Servicios de conducción de señales analógicas y digitales	10,749.1
	32301	Arrendamiento de Equipo y Bienes Informáticos	90,610.8
	32701	Patentes, derechos de autor, regalías y otros	39,445.3
	33104	Otras asesorías para la operación de los programas	1,949.7
	33301	Servicios de desarrollo de aplicaciones informáticas	141,842.2
	33303	Servicios relacionados con certificación de procesos	57.4
	33903	Servicios integrales	28,021.0
	35201	Mantenimiento y conservación de mobiliario y equipo	518.1
	35301	Mantenimiento y conservación de bienes informáticos	12.5
		TOTAL	**436,152.8**

Fuente: Elaborado con la información proporcionada por la STPS.

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 24,462.8 miles de pesos durante el ejercicio fiscal 2017; considerando 65 plazas, el promedio anual por persona fue de 376.4 miles de pesos.

Del total ejercido en 2017 por 436,152.8 miles de pesos que corresponde al total de recursos asignados en materia de TIC, se erogaron 131,033.1 miles de pesos en cuatro contratos que representan el 30.0% del universo, el cual se integra de la siguiente manera:

Muestra de Contratos Ejercidos durante 2017
(Miles de Pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2017
				Del	Al	Mínimo	Máximo	
Adjudicación directa bajo el Artículo 1, antepenúltimo párrafo (LAASSP)	Contrato CE-043-2015	INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación	Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo	17/08/2015	31/12/2015	33,718.9	47,676.2	21,467.4
	1° Convenio modificatorio		Ampliación de vigencia y monto del contrato	01/01/2016	30/06/2016	0.00	5,000.0	
	2° Convenio modificatorio		Ampliación de vigencia y monto del contrato	01/07/2016	31/12/2016	0.00	15,000.0	
	3° Convenio modificatorio		Ampliación de vigencia y monto del contrato	01/01/2017	31/05/2017	1,295.3	19,859.2	

Proceso de Contratación	Contrato	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2017
				Del	Al	Mínimo	Máximo	
	4° Convenio modificatorio		Ampliación de vigencia y monto del contrato	01/06/2017	31/08/2017	3,207.1	8,017.8	
				Subtotal		38,221.3	95,553.2	21,467.4
Adjudicación directa	Contrato RF-050-2017	Valores Corporativos SOFTTEK, S.A. de C.V.	Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo	01/09/2017	31/12/2018	23,545.1	58,862.8	6,956.5
Adjudicación directa bajo el Artículo 1, antepenúltimo párrafo (LAASSP)	Contrato RF-041-2017	Empresa 1	Servicio de "Modernización de Aplicativos de la STPS-Fabrica de Software"	14/07/2017	31/12/2017	29,749.9	73,374.9	34,935.6
Adjudicación directa	Contrato RF-112-2015	Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., de manera conjunta con otros proveedores	Servicio de Arrendamiento de Equipo de Cómputo y Bienes Informáticos, así como mantenimiento preventivo y correctivo del mismo	16/11/2015	15/11/2018	106,440.5	266,101.2	67,673.6
				Total		**197,956.8**	**493,892.1**	**131,033.1**

Fuente: Información proporcionada por la STPS.

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

2. Contrato CE-043-2015 “Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo”

Se analizó el Contrato Administrativo CE-043-2015 celebrado con el fideicomiso público INFOTEC (Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación), mediante adjudicación directa bajo el artículo 1°, antepenúltimo párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), así como cuatro convenios modificatorios para ampliar la vigencia y monto del contrato, con vigencia del 17 de agosto de 2015 al 31 de agosto de 2017, por un monto mínimo de 38,221.3 miles de pesos y monto máximo de 95,553.2 miles de pesos, con objeto de prestar los “Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo”; durante el ejercicio 2017 se realizaron pagos por 21,467.4 miles de pesos, se determinó lo siguiente:

Alcance

El contrato incluyó seis servicios con costo fijo: Servicio de Licenciamiento y Soporte; Servicio de Administración de Bases de Datos; Servicio Semantic Web Builder; Soporte en Sitio a la operación de la Coordinación General del Servicio Nacional de Empleo (CGSNE); Mesa de Servicios y Administración de Proyectos, así como ocho servicios bajo demanda: Operación de soluciones web; Mejora de soluciones web; Mantenimiento de aplicaciones; Soporte en

sitio a la operación de la CGSNE; Diagnóstico y verificación de perfiles del personal del Servicio Nacional de Empleo (SNE); Despliegue de capacitación presencial y en línea; Pruebas y mejoras aplicadas en campo sobre el módulo automatizado de perfilamiento de vacantes y buscadores de empleo; así como la implementación y mejora de procesos.

Proceso de Contratación

- No se proporcionó el Estudio de Factibilidad de los "Servicios Integrales de Tecnología para el Servicio Nacional de Empleo".
- En la comparación de los requerimientos técnicos que señala la investigación de mercado, no se observó un análisis para determinar que todos los proveedores participantes cumplían.
- No se cuenta con el resultado de la investigación de mercado.
- Se carece de documentación que acredite la capacidad técnica, material y humana del proveedor adjudicado para la realización del objeto del contrato.

Servicios Fijos

En relación con el servicio Semantic Web Builder, compuesto por el reporte de trabajo, sesiones de entendimiento, sesiones de transferencia de conocimiento y visita a las instalaciones del cliente; únicamente fueron solicitados los reportes de trabajo de los eventos atendidos durante cada mes, no fueron solicitadas las sesiones de transferencia de conocimiento ni de entendimiento sobre lo que se administraba en la instancia del servicio, tampoco se solicitó al proveedor realizar las visitas a las instalaciones de la dependencia, aun cuando ya estaban incluidas en el alcance.

Servicios Bajo Demanda

Sobre el Servicio de Mantenimiento de Aplicaciones y el Servicio de Soporte en Sitio a la operación de la CGSNE, la STPS no contaba con la información relativa a las propuestas de servicio y los entregables para cotejar que los pagos fueron efectivamente devengados; en consecuencia, la ASF solicitó al proveedor del contrato (INFOTEC) la misma información que no tenía la dependencia y de esta manera comprobó que los servicios fueron prestados.

Para cumplir con los servicios de empleo a la población, la Coordinación General del Servicio Nacional de Empleo requiere de una plataforma robusta y eficiente para la operación de las soluciones web, por ello resulta prioritario asegurar que cuente con todos los entregables y sus especificaciones para responder en caso de cambios o contingencias en los sistemas, con la finalidad de mantener de manera óptima el nivel de disponibilidad de sus aplicaciones.

2017-0-14100-15-0405-01-001 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social instrumente los mecanismos de control para verificar que cuenta con todos los entregables pactados en los contratos, con la finalidad de tener todas las especificaciones para responder oportunamente a los cambios en el entorno de los sistemas, así como contar con el debido soporte de los pagos devengados.

3. Contrato RF-050-2017 "Servicio Integral de Tecnologías para el Servicio Nacional de Empleo"

Se analizó el contrato RF-050-2017 celebrado con Valores Corporativos SOFTTEK, S.A. de C.V. (Softtek), mediante la contratación de adjudicación directa con fundamento en los artículos 26, fracción III, 40, 41, fracción III, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, con vigencia del 1 de septiembre de 2017 al 31 de diciembre de 2018, por un monto mínimo de 23,545.1 miles de pesos y máximo de 58,862.8 miles de pesos, con objeto de prestar los "Servicios Integrales de Tecnologías para el Servicio Nacional de Empleo" para la STPS; durante el ejercicio 2017 se realizaron pagos por 6,956.5 miles de pesos, se determinó lo siguiente:

Alcance

El contrato consistió en mantener, actualizar e integrar los servicios que actualmente proporciona el SNE a la ciudadanía y empleadores, en materia de intermediación laboral a través de medios electrónicos y presenciales por medio del soporte, desarrollo y mantenimiento de aplicaciones del SNE, así como mitigar el riesgo de interrupción de la continuidad de implementaciones de los aplicativos y portales, que contribuyen a alcanzar las metas establecidas sobre la integración de sistemas de vinculación laboral, integración de procesos de atención y apoyos con subsidio que se otorgan en el marco del Programa de Apoyo al Empleo.

Contratación y Entregables

Se revisó, validó y analizó el procedimiento de contratación, anexos, entregables y pagos; se revisó la documentación correspondiente a la Continuidad Operativa (Mantenimientos Menores) y al Servicio de Mantenimientos Mayores y Nuevos Desarrollos, y no se identificaron desviaciones importantes respecto al cumplimiento del contrato y anexo técnico; se obtuvo documentación que acredita la gestión y validación de la entrega del servicio y sus niveles acordados por parte de los administradores de este contrato.

4. Contrato RF-041-2017 "Servicio de Modernización de Aplicativos de la STPS – Fábrica de Software"

Se analizó el Contrato Administrativo RF-041-2017, celebrado con la Empresa 1 mediante adjudicación directa bajo el artículo 1°, antepenúltimo párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con vigencia del 14 de julio al 31 de diciembre de 2017, por un monto mínimo de 29,749.9 miles de pesos y máximo de 73,374.9 miles de pesos, con objeto de prestar el "Servicio de Modernización de Aplicativos de la STPS - Fábrica de Software"; durante 2017 se realizaron pagos por 34,935.6 miles de pesos, se determinó lo siguiente:

Alcance

Contar con un servicio de desarrollo de software para la creación, mantenimiento y soporte de sistemas de información, de acuerdo a la arquitectura y plataforma tecnológica de la STPS, mediante un modelo operativo maduro, basado en procesos, metodologías, niveles de atención y capacidades técnicas que den cumplimiento a la normatividad de TIC.

Proceso de Contratación

- Se identificó una diferencia de 1,000.0 miles de pesos entre el monto máximo del contrato y el desglose de los precios unitarios señalados en el anexo técnico.

Modelo de Gobierno

- El administrador del contrato no implementó ningún mecanismo para conciliar la bitácora de actividades del equipo de trabajo de desarrollo, la cual carece de las horas trabajadas por cada actividad, con las horas informadas por el proveedor en el "Reporte de Órdenes de Trabajo", lo que impide verificar las horas devengadas.

- Para el servicio de "Administración de Programas y Proyectos", el administrador del contrato sólo verificó el cumplimiento de forma general de las órdenes de trabajo, sin validar el detalle de los entregables, en consecuencia, no se tienen elementos para determinar si la calidad y el desempeño de los servicios fueron satisfactorios, y tampoco se aseguró de que los entregables estén libres de defectos que comprometan su funcionamiento.

Implementación del Sistema Integral de Conciliación y Registro Laboral (SICREL)

- La Unidad de Enlace de la Reforma del Sistema de Justicia Laboral de la STPS solicitó el apoyo de la Dirección General de Tecnologías de la Información (DGTI), para desarrollar un sistema que atienda lo dispuesto en la reforma publicada en el Diario Oficial de la Federación el 24 de febrero de 2017, sobre el "DECRETO" por el que se declaran reformadas y adicionadas diversas disposiciones de los artículos 107 y 123 de la Constitución Política de los Estados Unidos Mexicanos, en materia de "Justicia Laboral", en preparación de la puesta en marcha del organismo descentralizado que estará a cargo de la función conciliatoria y las funciones de registro de todos los contratos colectivos de trabajo y las organizaciones sindicales, así como los procesos administrativos relacionados.

- A la fecha de la auditoría (agosto 2018), está pendiente la aprobación de la reforma laboral, no se ha nombrado al titular del Instituto de Justicia Laboral ni se ha formado un equipo que opere los aplicativos desarrollados; por lo anterior, el sistema entrará en funciones en el momento que se ponga en marcha el organismo para el que fue diseñado.

Ciclo de Vida del Desarrollo de Soluciones Tecnológicas

En la revisión del Manual de Organización y Procesos de la Dirección General de Tecnologías de la Información de la STPS y las normativas del MAAGTICSI con su anexo sobre las mejores prácticas del ciclo de vida del desarrollo de software, se identificó lo siguiente:

- La Dirección de Servicios de Información (DSI) no tiene implementada una metodología formalizada para gestionar los procesos de Desarrollo de Aplicaciones Sustantivas y Administrativas de la STPS, que incluya políticas, normas y procedimientos a seguir por las diferentes áreas responsables en desarrollo de aplicaciones, para asegurar que los productos de software cumplan con estándares mínimos de calidad y funcionalidad.

- No se cuenta con una metodología para determinar la duración y el costo de las actividades para el desarrollo de sistemas, ni para asignar el número de recursos necesarios en cada orden de servicio.

- Para la gestión de incidentes de los sistemas no se cuenta con una base de conocimientos que sirva para clasificar el nivel de atención necesario para su análisis y remediación.

- Se carece de un procedimiento para la gestión de los recursos humanos que participan en los desarrollos, mantenimientos y cambios de los aplicativos, con la finalidad de detectar los perfiles idóneos, realizar una evaluación de desempeño y medir el grado de cumplimiento de los objetivos individuales y grupales.

- Los administradores de proyectos no aplican una metodología para la planeación de los desarrollos, ni cuentan con los planes subsidiarios desde su inicio hasta su cierre, que sean actualizados de manera periódica para reportar los avances, riesgos y desviaciones de los trabajos hasta su finalización.

- Se carece de indicadores para evaluar el nivel de cumplimiento de las unidades de desarrollo de sistemas conforme a los tiempos y requerimientos funcionales de las órdenes de servicio y tampoco se tiene un mecanismo para valorar el nivel de satisfacción de los usuarios.

- No se cuenta con una administración de riesgos para los nuevos desarrollos o controles de cambios, que generen iniciativas para el tratamiento de los mismos, ni la evaluación del impacto que pueda afectar a los demás aplicativos e infraestructura de la entidad.

- Los sistemas no se encuentran diseñados en una Arquitectura Orientada a Servicios, en consecuencia, no se cuenta con funcionalidades reutilizables e interoperables entre diversas áreas de la Dependencia o con Instituciones del Gobierno Federal.

- No se tiene implementada una metodología para la verificación de la calidad del código fuente de los desarrollos de software efectuados por los proveedores.

- Se carece de planes que consideren diversos tipos de pruebas como unitarias, integrales, stress, seguridad y regresivas, entre otras, a los aplicativos antes de su liberación al ambiente productivo.

- No se aplican procedimientos formales para la generación de datos de pruebas con la finalidad de sustituir datos sensibles y de esta manera evitar poner en riesgo su privacidad.

- Se carece de una herramienta para el control de versiones, establecimiento de líneas base, repositorio consolidado y organizado de todos los documentos generados durante el proyecto de desarrollo de sistemas.

- Se carece de un procedimiento de control de cambios para el desarrollo de soluciones tecnológicas, que considere estándares de documentación, requerimientos de calidad y aprobación de las áreas involucradas.

- Para el cierre de solicitudes de los desarrollos de software, se carece de un informe que contenga la valoración de los resultados y los beneficios obtenidos, tampoco se hace constar en actas la aceptación de las unidades administrativas solicitantes del servicio.

- No se tiene evidencia de la aplicación de pruebas de vulnerabilidades a los cambios o nuevos desarrollos de software antes de liberarse al ambiente de producción, por ende, no se generan acciones para remediar los riesgos potenciales.

De la revisión de los manuales y normativas relacionadas con el desarrollo de soluciones tecnológicas, se concluyó que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la entidad son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS	
Factor crítico	**Riesgo**
Análisis de Vulnerabilidades	La falta de ejecución de un análisis de vulnerabilidades a los sistemas antes de su puesta a producción, podría representar un riesgo en la seguridad y funcionalidad de la aplicación, debido a que no se están protegiendo los recursos que forman parte del sistema a nivel hardware, software, telecomunicaciones y datos.
Análisis de Riesgos	Se carece de la evaluación de los riesgos de los módulos desarrollados y el impacto que podrían tener sobre los procesos, de manera que se obtengan planes de remediación para definir los controles a implantar de acuerdo a las capacidades y recursos del área de desarrollo, para mantener aceptable el nivel de riesgo y evitar la materialización de las amenazas detectadas.
Plan de pruebas	Al no contar con diversos tipos de pruebas que aseguren el cumplimiento de los requerimientos del usuario, se tiene el riesgo de que el sistema no funcione de acuerdo con su diseño y que los controles internos no trabajen de acuerdo a las políticas de la entidad.
Datos para pruebas	Debido al uso de datos de prueba no enmascarados, se pone en riesgo la privacidad de la información.
Administración de Cambios	La carencia de un procedimiento para el control de cambios, podría impactar en el desempeño del sistema y aplicativos relacionados, comprometiendo la disponibilidad y seguridad de la operación.
Plan de Calidad	No se cuenta con planes para el aseguramiento de la calidad del desarrollo de software, en consecuencia, no se cumple con estándares de codificación ni metodologías de desarrollo para la revisión de los resultados y productos entregados en cada fase, así como la confirmación del cumplimiento de los requerimientos, lo que podría derivar en riesgos de incompatibilidad con otros sistemas, presentando deficiencias y brechas de seguridad en su operación.
Gestión de Código Fuente	Se carece de procedimientos para el control de versiones del código fuente de los programas, con la finalidad de contar con la capacidad de revertirlos cuando se requiera, asimismo, se carece de un registro histórico de las acciones realizadas con cada versión de código fuente, lo que puede causar afectaciones a la funcionalidad de las aplicaciones e impactos a los activos de información.
Cierre de Proyectos	Se carece de las actas de aceptación de entregables firmadas por los usuarios finales que participaron en los proyectos, lo que pone en riesgo el cumplimiento de los requerimientos.

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

La falta de aplicación de una metodología para el Desarrollo de Soluciones Tecnológicas, propicia sistemas de baja calidad, insatisfacción de los usuarios, errores de procesamiento, falta de protección contra códigos maliciosos, entre otros, y pone en riesgo la operación del Sistema de Seguimiento del Proceso Inspectivo, Directorio Nacional de Empresas y el Sistema Integral de Conciliación y Registro Laboral, entre otros.

2017-0-14100-15-0405-01-002 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social estipule en los contratos o convenios que se celebren en materia de TIC, aun en aquellos realizados entre entidades de la administración pública, los apartados de penalizaciones, deductivas, fianzas y garantías para los casos de incumplimiento de los servicios; asimismo, establezca un mecanismo de validación para asegurar la capacidad técnica, material y humana de los proveedores para la realización de los contratos.

2017-0-14100-15-0405-01-003 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente controles para verificar la calidad del código fuente de los desarrollos de software, y formalice la aceptación de las pruebas por parte de las Unidades Administrativas Solicitantes para asegurar el cumplimiento de los requerimientos de las solicitudes de servicios. Asimismo, instrumente controles sobre

las horas trabajadas por parte del equipo del prestador de servicios para validar que las horas propuestas por el proveedor sean las óptimas para la atención de los requerimientos.

2017-0-14100-15-0405-01-004 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente los mecanismos de control para la elaboración de políticas, normas y procedimientos para el Desarrollo de Soluciones Tecnológicas, a fin de estandarizar la entrega de productos de software, con la finalidad de garantizar un adecuado funcionamiento y mantenimiento de los mismos, considerando las mejores prácticas para contar con elementos como Análisis de Vulnerabilidades, Análisis de Riesgos, Plan de pruebas, Datos para pruebas, Administración de Problemas, Administración de Cambios, Plan de Calidad, Gestión de Código Fuente y Cierre de Proyectos.

2017-9-14115-15-0405-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en la Secretaría del Trabajo y Previsión Social o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión del Contrato RF-041-2017 y el Desarrollo de Soluciones Tecnológicas propiciaron irregularidades vinculadas con las responsabilidades de los titulares de la Dirección de Servicios de Información y la Subdirección de Diseño y Construcción de Sistemas, debido a las deficiencias en los controles para el cumplimiento de la vigilancia para evitar desviaciones y riesgos en el cumplimiento de las especificaciones técnicas; la verificación de entregables funcionales de las ordenes de trabajo; la carencia de procedimientos de conciliación de las horas trabajadas por parte del proveedor; el Análisis de Vulnerabilidades; el Análisis de Riesgos; el Plan de pruebas; los Datos para pruebas; la Administración de Cambios; el Plan de Calidad; la Gestión de Código Fuente y el Cierre de Proyectos.

5. Contrato RF-112-2015 “Servicio de Arrendamiento de Equipo de Cómputo y Bienes Informáticos”

Se analizó el contrato RF-112-2015 celebrado de manera conjunta entre las empresas Tecnoprogramación Humana de Veracruz, S.A. de C.V., Tecnoprogramación Humana Especializada en Sistemas Operativos, S.A. de C.V., Soporte y Capacitación S.A. de C.V., Tecnología en Service Desk, S.A. de C.V. y Servicios de Integración y Garantías S.A. de C.V., a través de una adjudicación directa con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 26, fracción III, 40, 41, fracción III, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), y 72, fracción III, y 85 de su Reglamento, con vigencia del 16 de noviembre de 2015 al 15 de noviembre de 2018, por un monto mínimo de 106,440.5 miles de pesos y monto máximo de 266,101.2 miles de pesos, con objeto de la prestación del “Servicio de Arrendamiento de Equipo de Cómputo y Bienes Informáticos”; durante el ejercicio 2017 se realizaron pagos por 67,673.6 miles de pesos, se determinó lo siguiente:

Alcance

Proporcionar el servicio de arrendamiento de equipos de cómputo, servicios de soporte, asistencia técnica, mantenimientos preventivos y correctivos, gestión de servicios, así como contar con un punto único de contacto para el levantamiento de incidentes o servicios por parte de los usuarios de la dependencia.

Proceso de Contratación

La Dirección General de Tecnologías de la Información (DGTI) señaló que se llevó a cabo un proceso de análisis para definir las características necesarias en cada uno de los diferentes tipos de equipos requeridos, no obstante, durante los recorridos de prueba se identificó lo siguiente:

- Se detectó que 829 equipos Portátiles Tipo B cuentan con accesorios adicionales como docking station, monitor, teclado y mouse, los cuales son para uso intensivo del equipo; cabe señalar que 760 (91.7%) de éstas computadoras, son utilizadas por personal de Inspección que se dedica a visitar empresas y está fuera de la oficina la mayor parte del tiempo.
- De un total de 22 computadoras Apple Mac, se identificaron 6 (27.3%) que están asignadas a usuarios con un perfil de puesto que no justifica el uso de este tipo de equipos para llevar a cabo sus funciones, de tal manera que las actividades por desarrollar por estos usuarios pueden ser realizadas con equipos más económicos, para los cuales la STPS tiene contratos vigentes; al comparar los costos entre equipos equivalentes más económicos, se concluyó que la dependencia pudo obtener un ahorro de 233.5 miles de pesos anuales.

Revisión de las Especificaciones de Equipos

En la revisión de las especificaciones de los equipos estipuladas en los Anexos Técnicos del contrato, se identificaron las observaciones siguientes:

- Los 12 servidores contratados (100.0%) contaban con procesadores ES-2620v3 @ 2.4GHz, cuando de acuerdo con el contrato debían tener procesadores ES-2640 @ 2.6GHz.
- En el caso de 151 equipos Portátiles Tipo A, se detectó que 5 (3.3%) cuentan únicamente con 4 GB RAM en lugar de los 8 GB contratados.
- En el caso de 110 equipos Portátiles Tipo B, se identificó que 2 (1.8%) tienen únicamente 4 GB RAM en lugar de los 8 GB contratados.

A pesar de lo anterior, estos incumplimientos no fueron penalizados, debido a que el contrato señala que para el caso en que los equipos aprovisionados no cumplan con las especificaciones técnicas requeridas, la STPS deberá notificar al proveedor, quien tendrá un lapso de 3 días para sustituir los equipos. Sin embargo, los incumplimientos señalados no habían sido detectados a la fecha de la auditoría, por ende, tampoco habían sido comunicados al proveedor para su reemplazo.

La STPS, en el transcurso de la auditoría y con motivo de la intervención de la ASF, instruyó las acciones de control necesarias para corregir las desviaciones señaladas, las cuales son las siguientes:

- La DGTI notificó al proveedor del servicio, a través del oficio 513.4/28.05.2018/198 de fecha 28 de mayo de 2018, las observaciones encontradas por la ASF; en consecuencia, se realizaron los cambios necesarios para los equipos de cómputo que no contaban con la memoria RAM que indica el contrato, y se reemplazaron los procesadores por componentes superiores a las características señaladas en el Anexo Técnico.
- Con el oficio No. 513.2/13.08.2018/127 con fecha 13 agosto de 2018, se notificó al proveedor el pago de deductivas por los incumplimientos señalados, y como resultado de lo anterior, la STPS proporcionó el Recibo Bancario de Pago de Contribuciones, Productos y Aprovechamientos Federales de fecha 17 de agosto de 2018 por 61.0 miles de pesos correspondiente a las deductivas aplicadas.

Se deben fortalecer las evaluaciones de los procedimientos y actividades realizadas por los funcionarios para evitar la subutilización de los recursos de cómputo que propicia el derroche de recursos económicos; asimismo, se requiere mejorar los mecanismos de monitoreo y supervisión del funcionamiento de la infraestructura tecnológica para evitar omisiones en las especificaciones técnicas entregadas por parte de los prestadores de servicios.

2017-0-14100-15-0405-01-005 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social evalúe los procedimientos y actividades realizadas por los funcionarios para asignar las características del equipo de cómputo adecuado para el desempeño de sus actividades, con la finalidad de asegurarse de las capacidades de los equipos estén alineadas a las necesidades de procesamiento de los perfiles de puesto y de esta manera cumplir con los criterios de economía y eficiencia en beneficio del Estado.

2017-0-14100-15-0405-01-006 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente mecanismos de control y revisión para validar que los equipos cumplan con las características establecidas en el contrato y anexo técnico al ser entregados por el prestador de servicios y que se mantengan con dichas especificaciones a lo largo de la vida del contrato, con la finalidad de asegurarse de cumplir con los requerimientos de las áreas usuarias para el óptimo desempeño de sus actividades.

6. Gobierno y Administración de las TIC

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

Establecer la gobernabilidad de las operaciones

- La DGTI no cuenta con planes alternativos en caso de que los proyectos se desfasen o tengan incumplimientos, con el riesgo de la falta de identificación de los problemas, en consecuencia, no se tienen los datos suficientes para definir acciones alternativas.
- Se carece de una Matriz RACI (Responsable, Encargado, Consultado, Informado), o documento similar, en donde se asegure que para el desarrollo de proyectos se asignen las actividades a los funcionarios o equipos de trabajo pertinentes, en consecuencia, no se tiene una adecuada segregación de funciones.
- No se tiene implementado un procedimiento formalizado para determinar las fortalezas, oportunidades, debilidades y amenazas del ámbito de las TIC en la STPS.
- Se carece de un procedimiento formalizado y continuo para el análisis de capacidades y servicios de TIC, considerando factores internos y externos, para detectar las áreas sujetas a cambios o mejoras, por lo cual no se asegura que los recursos de TIC se encuentren alineados a las necesidades de la dependencia.
- No se cuenta con el procedimiento formalizado de las actividades que se llevan a cabo para establecer, priorizar y definir la fuente de financiamiento y la autorización de la Planeación Estratégica de TIC.

Proceso de administración de proyectos

- No se tiene un proceso formal para designar a un representante de la DGTI con los conocimientos técnicos suficientes para dar respuesta clara y precisa a las solicitudes de aclaración de los licitantes en las juntas de aclaraciones en materia de contratos de TIC.

Datos Abiertos

- En relación con el cumplimiento del cronograma de implementación en la STPS, no se tiene evidencia de las actividades siguientes:

  - Publicación e inicio de acciones de los Planes de Acción de Datos Abiertos
  - Cronograma de publicación de datos abiertos 2017
  - Revisión y modificación de reglamentos internos
  - Mecanismos para seguridad y privacidad de datos
  - Capacitación impartida al personal

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

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL GOBIERNO Y ADMINISTRACIÓN DE LAS TIC	
Factor crítico	**Riesgo**
Segregación de funciones	Se carece de la segregación de funciones en las actividades operativas y sustantivas de las áreas de las TIC, para la detección de deficiencias que pueden resultar en una mayor posibilidad de

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES PARA EL GOBIERNO Y ADMINISTRACIÓN DE LAS TIC	
Factor crítico	**Riesgo**
	fraude, errores, irregularidades en los procesos, en el procesamiento de transacciones y en los reportes financieros.
Metodología FODA	La Matriz FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) favorece el cumplimiento de los objetivos y procesos de la dependencia, el carecer de una metodología para su implementación, impide tener un proceso de mejora continua para incrementar la calidad de los aplicativos sustantivos e infraestructura tecnológica, aunado a la falta de detección de debilidades para crear planes de acción para su tratamiento y erradicación.
Análisis de Capacidades y Servicios de TIC	Debido a la carencia del análisis de capacidades de los servicios de TIC, la dependencia no asegura el cumplimiento de los niveles de servicio acordados ni el crecimiento previsto de la demanda, en consecuencia, no se detectan ni monitorean las capacidades y recursos necesarios para desarrollar la estrategia de TI alineada a las necesidades de la dependencia.

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

Para cumplir con los objetivos y metas de la Secretaría en materia de TIC, así como elaborar proyectos de innovación y desarrollo tecnológico, a fin de determinar su viabilidad y compatibilidad tecnológica para su posible desarrollo e incorporación a la Dependencia, es fundamental contar con mecanismos para la adecuada segregación de funciones que fortalezca la metodología para determinar las fortalezas y oportunidades de mejora que se requieren para la instrumentación de los proyectos de innovación tecnológica.

2017-0-14100-15-0405-01-007 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente procedimientos para determinar las fortalezas, oportunidades, debilidades y amenazas del ámbito de las TIC que impacten en sus actividades; instrumente la adecuada segregación de funciones en las operaciones de TIC, así como un análisis continuo de las capacidades y servicios de TIC con la finalidad de contar con elementos para evaluar las tecnologías existentes y emergentes para definir la dirección tecnológica apropiada que permita materializar los objetivos y estrategias de TIC de acuerdo con las necesidades de la dependencia.

7. Gestión de la Seguridad de la Información

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

Políticas y Manejo de Contraseñas

- La política de contraseñas no establece condiciones que obliguen a construir contraseñas robustas, y carece de procedimientos específicos que normen la composición y tiempo de vida de las contraseñas.
- Las contraseñas no son almacenadas de manera segura, únicamente son enmascaradas utilizando cálculos diseñados internamente sin algoritmos de cifrado.
- Las credenciales de los sistemas se exponen cuando son transmitidas hacia los servidores para su autenticación, debido a que no utilizan certificados digitales.

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

- Los procedimientos de administración de usuarios de aplicaciones no se encuentran documentados, autorizados ni formalizados por la Dependencia; además, la administración de usuarios está a cargo de las áreas usuarias y no es una actividad monitoreada, ni supervisada por la Dirección de Seguridad de la Información y Comunicaciones (DSIC).

Recertificación de Usuarios y Protección de Cuentas Privilegiadas

- Debido a que la administración de usuarios está a cargo de las áreas usuarias y no es una actividad monitoreada, ni supervisada por la DSIC, esta última desconoce si se ejecuta de forma periódica una recertificación de usuarios y sus privilegios.

Análisis de Vulnerabilidades

- La DSIC ha generado requerimientos de cambio para atender las vulnerabilidades detectadas, sin embargo, la evidencia proporcionada no permite asegurar que las 400 vulnerabilidades críticas y 1,613 de riesgo alto hayan sido mitigadas o erradicadas.

Comunicaciones Seguras

- Los aplicativos que navegan por internet no utilizan certificados digitales, al estar expuestos en la nube, podrían estar sujetos a ataques que buscan ganar acceso a la aplicación o tener acceso a información reservada.
- En relación con los túneles de redes privadas virtuales establecidos entre la Dependencia y terceros, no se tiene evidencia de la configuración del cifrado dentro del canal de comunicación, por lo que pueden existir riesgos de exposición de información.

Líneas Base de Configuración

- La DSIC señaló que los proveedores son los responsables de reducir las vulnerabilidades de los equipos que estén bajo su administración, sin embargo, la dependencia manifestó que no ha validado la aplicación del endurecimiento de la configuración de los sistemas operativos, equipos de comunicaciones y máquinas virtuales, entre otros.

Monitoreo y Supervisión

- Durante 2017 y a la fecha, la herramienta para prevenir la pérdida de datos (DLP) se encuentra funcionando en modo de monitoreo, por lo tanto, la STPS únicamente podría actuar de forma reactiva en caso de fuga de información.
- La DSIC no revisa las bitácoras para supervisar las actividades ejecutadas por el proveedor, quien al tener el rol de administrador de las herramientas de seguridad podría, intencionalmente o por error, ejecutar acciones que expongan a la dependencia a incidentes de seguridad.

Pruebas de Seguridad

- Se logró acceder a sitios que fueron restringidos por la dependencia mediante las herramientas de filtrado; asimismo, algunos servidores presentaron vulnerabilidades de riesgo alto en el soporte de seguridad y algoritmos de cifrado de las páginas web.

Roles Funcionales con Actividades en Materia de Seguridad de la Información

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

Cumplimiento del MAAGTICSI

- Durante el diseño detallado para el desarrollo de los aplicativos, no se incluyen requerimientos de seguridad de la información, y tampoco se efectúa el análisis de vulnerabilidades antes de poner en operación de los sistemas.
- En las contrataciones relacionadas con los servicios de Internet, no se cuenta con mecanismos de protección contra ataques de denegación de servicios, desde la propia red del proveedor e independientemente de los controles de seguridad de la información que implemente la Dependencia.
- El Grupo Estratégico de Seguridad de la Información (GESI), en coordinación con las unidades administrativas de la Dependencia, no ha diseñado la estrategia de seguridad de la información, por lo que se carece de lo siguiente:
  - Métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los activos de información.
  - Controles de seguridad que impidan que el código de las soluciones tecnológicas, sus componentes y productos, y demás elementos relacionados, se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.
- El GESI con apoyo de las unidades administrativas competentes de la Dependencia, requiere reforzar el Sistema de Gestión de Seguridad de la Información (SGSI), a través de ampliar el alcance, documentar, implementar, supervisar y mejorar, lo correspondiente a la gestión de controles de seguridad necesarios para contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos; asimismo, identificar las posibles amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información.

De la revisión de los procedimientos para la Gestión de la Seguridad de la Información, se obtuvo que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la STPS, son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	
Factor	**Riesgo**
Administración de usuarios	Debido a que no se tienen procedimientos formalizados para la gestión de claves de usuarios, éstos podrían tener permisos para acceder a información que no le corresponde de acuerdo con sus funciones y responsabilidades; en consecuencia, se pierde la confidencialidad en la

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	
Factor	**Riesgo**
	información y se pueden ejecutar transacciones no autorizadas que ponen en riesgo la integridad de los activos de la institución.
Privacidad de la Información	No se asegura el cifrado de datos, ni redes con protocolos seguros para la transferencia de información; tampoco se consideran pruebas de seguridad en los aplicativos; en consecuencia, se podrían tener alteraciones en la información, borrado o mal uso de los datos, así como operaciones no autorizadas al no asegurar que los nuevos desarrollos integren funciones de seguridad.
Monitoreo de las pistas de auditoría y bitácoras de los aplicativos y bases de datos	No se realiza una revisión periódica de las pistas de auditoría y las bitácoras de los aplicativos sustantivos y de toda la plataforma tecnológica (bases de datos, sistemas operativos, software de intercambio entre aplicativos), ni que impidan borrar o alterar éstas, a fin de detectar oportunamente movimientos irregulares o cambios no autorizados, en consecuencia, existe la probabilidad de que usuarios maliciosos puedan ejecutar transacciones no autorizadas que comprometan la integridad de los activos y no se deje trazabilidad.
Seguridad del Perímetro de Internet	En las contrataciones relacionadas con los servicios de Internet, no se asegura que se cuente con mecanismos de protección a ataques de denegación de servicios, lo que implica riesgos que pueden impactar en la disponibilidad del servicio al cliente y afectación a la reputación de la imagen pública, entre otros.
Mecanismos de Seguridad en los aplicativos sustantivos	No se asegura el cifrado de datos, ni redes con protocolos seguros para el envío de información, asimismo, no se adicionan componentes de seguridad a los desarrollos de aplicativos de cómputo, tampoco se ejecuta un análisis de vulnerabilidades al código fuente antes de su puesta en producción; esto implica posibles alteraciones, mal uso de los datos, así como operaciones no autorizadas al no incluir en los nuevos desarrollos validaciones de seguridad de la información.
Sistema de Gestión de Seguridad de la Información (SGSI)	Se debe fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), así como su programa de implementación y operación, con la finalidad de mitigar y controlar diversos riesgos, principalmente la pérdida de la confidencialidad de la información que puede utilizada por personas que no tienen autorización; la falta de integridad de la información ya que los datos pueden ser alterados, provocando pérdidas económicas y fraudes, así como la afectación a la disponibilidad de los servicios que impide que los usuarios accedan a las aplicaciones cuando lo requieran para cumplir con los objetivos de la Dependencia.

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

La DGTI tiene entre sus funciones la administración de la infraestructura de TIC, así como supervisar la instalación, operación, mantenimiento y control de las redes de procesamiento electrónico de datos y evaluar su operación, aplicando las medidas correctivas que procedan; por lo anterior, resulta prioritario fortalecer la administración de usuarios; asegurar la privacidad de la información; ejecutar el monitoreo de las pistas de auditoría y bitácoras de los aplicativos; mejorar la seguridad del perímetro de internet e implementar mecanismos de seguridad en los aplicativos sustantivos, con la finalidad de que la estrategia de seguridad de la información facilite el cumplimiento de los objetivos de la Dependencia.

2017-0-14100-15-0405-01-008 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social implemente políticas y procedimientos para la administración de contraseñas de los usuarios considerando una adecuada segregación de funciones, recertificaciones de accesos y el manejo de cuentas con privilegios especiales. Asimismo, implementar políticas para la composición y tiempo de vida de las contraseñas de los aplicativos, sistemas operativos y equipos de infraestructura tecnológica, asegurando que las credenciales de autenticación estén cifradas y se utilicen certificados digitales para su transmisión durante el proceso de autenticación.

2017-0-14100-15-0405-01-009 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social fortalezca los controles de seguridad de la información en las configuraciones de línea base de la infraestructura tecnológica para prevenir que las vulnerabilidades sean explotadas; corrija las vulnerabilidades detectadas en los servidores que albergan las aplicaciones sustantivas; implemente el uso de protocolos de cifrado para las conexiones con terceros; supervise de manera continua las actividades de los proveedores; configure las herramientas de filtrado para evitar accesos no autorizados, así como instrumente componentes de seguridad en los desarrollos de los aplicativos y ejecute un análisis de vulnerabilidades al código fuente antes de su liberación al ambiente productivo.

2017-9-14115-15-0405-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en la Secretaría del Trabajo y Previsión Social realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que en su gestión relacionada a la Seguridad de la Información propiciaron irregularidades vinculadas con las responsabilidades de los titulares de la Dirección General de Tecnologías de la Información, la Dirección de Planeación e Innovación Tecnológica y la Dirección de Seguridad de la Información y Comunicaciones, debido a las deficiencias en los controles para incluir mecanismos de seguridad en los aplicativos antes de ponerlos en operación; debilidades en el cifrado de datos para transferir la información con protocolos seguros; carencia de resguardo del código de las soluciones tecnológicas para evitar que se copien con fines distintos a su desarrollo; falta de reglas para construir contraseñas robustas en su composición y tiempo de vida; carencia del monitoreo de las bitácoras de los aplicativos para detectar accesos no autorizados y deficiencias en la administración de usuarios para una adecuada segregación de funciones, recertificaciones de accesos y manejo de cuentas con privilegios especiales.

8. Continuidad de las Operaciones y Centro de Datos

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

Análisis de Impacto al Negocio (BIA)

- Se carece de evidencias del trabajo conjunto entre la Dirección de Seguridad de la Información y Comunicaciones (DSIC) y la estructura de gobierno de las TIC sobre las actividades siguientes:

o Identificar los procesos y actividades relacionadas con la misión y objetivos de la entidad, su interacción con los activos de TIC, así como sus dependencias y elementos de entrada (insumos).

o Establecer las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la STPS que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como su impacto y consecuencias.

- Definir los recursos y actividades requeridas para reestablecer las operaciones a un nivel aceptable, en función del periodo de interrupción definido por las necesidades y particularidades de la Dependencia.
- Informar los resultados obtenidos en los puntos anteriores para la toma de decisiones de la Alta Dirección.

- La carencia de las directrices de la Alta Dirección de la dependencia para la elaboración del análisis de impacto al negocio deriva en deficiencias y falta de alineación para la implementación del Plan de Continuidad del Negocio (BCP) y Plan de Recuperación en caso de Desastres (DRP), debido a que no se cuenta con la visión estratégica para definir los recursos relevantes y la tolerancia al impacto que pueden sufrir en caso de contingencias.

Plan de Continuidad del Negocio (BCP)

- No se lleva a cabo una revisión del contenido conjuntamente con los involucrados en el programa de continuidad, al menos cada seis meses, para conocer de manera indubitable cuál será su desempeño en las diversas actividades que habrán de realizarse en caso de requerirse la aplicación del plan.
- Se carece de pruebas de recuperación del programa de continuidad para confirmar que los servicios de TIC puedan ser recuperados de forma efectiva, que las deficiencias serán atendidas y comprobar su vigencia o efectuar la actualización que sea pertinente.
- En 2017, no se cuenta con evidencia de capacitación del Plan de Continuidad.

Plan de Recuperación en caso de Desastres (DRP)

- La Dependencia tiene implementado el DRP para el Sistema de Información del Programa de Apoyo al Empleo, en cuyo análisis se observó lo siguiente:

- No incluye los criterios para determinar el estado de un incidente de seguridad, cuando éste no se puede resolver y se considera como un desastre.
- Carece de mecanismos de atención ante contingencias y tareas diseñadas para la recuperación de la operación, debido a la falta de las acciones siguientes:

- Diseño de procedimientos de respuesta y recuperación, incluyendo actividades de resolución a un evento de interrupción.
- Activación del plan de acción.
- Recuperación de procesos críticos de negocio.
- Creación de planes para la reconstrucción y recuperación de los recursos de los sistemas a su estado original.
- Generación del plan de concientización y capacitación a las áreas involucradas sobre la ejecución del plan.
- Identificación de los sistemas periféricos que pueden ser afectados ante una contingencia.

- El Responsable del proceso de Administración de Servicios no tiene implementado un mecanismo formal que asegure que el hardware y el software de recuperación utilizado en la aplicación del programa de continuidad sea funcional, para restablecer, probar y renovar los respaldos al menos semestralmente.

- No se cuenta con un centro de datos alterno.

Administración de la Capacidad

- Debido a que el BIA no se realizó en conjunto con la estructura de gobierno de las TIC, el Programa de Capacidad implementado por la DSIC no asegura que todos los servicios de TI están soportados en una infraestructura tecnológica con capacidades acordes con las necesidades de la dependencia.

- No se tiene documentado el diseño de acciones por implementar cuando la capacidad y rendimiento de la infraestructura de TIC no están en el nivel requerido, como ajustar la prioridad de las tareas de los componentes de la infraestructura de TIC e instaurar los mecanismos de recuperación en caso de fallas, entre otras.

- No se mantiene informados a los responsables de los dominios tecnológicos de las oportunidades identificadas para mejorar la capacidad de la arquitectura tecnológica en operación y realizar recomendaciones sobre los incidentes por falta de capacidad de la infraestructura de TIC.

Catálogo de Servicios

- El catálogo de servicios de TIC no está alineado con las necesidades prioritarias de la STPS, debido a que la estructura de Gobierno de TIC no participó en su definición ni aprobación, en consecuencia, no se tiene la certeza de que los servicios y la disponibilidad tecnológica cumplan con los objetivos de la entidad.

Clasificación de la información

- No se tiene evidencia de que el Responsable de la Seguridad de la Información Institucional (RSII) y el Grupo Estratégico de Seguridad de la Información (GESI), trabajaron en conjunto con la estructura de Gobierno de las Tecnologías de la Información, en la clasificación de la información reservada, confidencial y pública, en consecuencia, no se garantiza que la información este clasificada de acuerdo al valor para la entidad, ni que sea respaldada y restaurada en el momento en que se requiera.

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

PRINCIPALES RIESGOS POR LA CARENCIA DE CONTROLES EN LOS PROGRAMAS DE CONTINUIDAD DE LAS OPERACIONES	
Factor Crítico	**Riesgo**
Análisis de Impacto al Negocio (BIA)	La carencia de alineación con los objetivos y prioridades de la Alta Dirección, deriva en el riesgo de no tener identificadas las funciones, actividades, unidades administrativas, así como los servicios relevantes que proporciona la STPS, los cuales podrían resultar afectados por la interrupción de uno o más servicios de TIC, asimismo, se carece de la estimación del impacto técnico, económico y reputacional para la dependencia.
Programa de Continuidad de las Operaciones (BCP)	Se carece de la definición de prioridades por parte de la Alta Dirección para las situaciones de recuperación para evitar el restablecimiento de servicios de menor impacto y asegurarse de que la respuesta y la recuperación se encuentren alineadas con las necesidades de la dependencia, asimismo, no se cuenta con la evidencia de pruebas de recuperación, al menos semestralmente, para confirmar que los servicios de TIC puedan ser recuperados de forma efectiva.
Plan de Recuperación de Desastres (DRP)	No se cuenta con la identificación de las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, por lo tanto, los puntos objetivos de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) de la información, serían mucho mayores a los requeridos para la continuidad de las operaciones de la dependencia.
Planeación de la capacidad	La falta de alineación con las necesidades prioritarias de la STPS, incrementa el riesgo de que los servicios no se vean respaldados por una capacidad adecuada de procesamiento y almacenamiento, por lo tanto, los recursos podrían ser desaprovechados con acciones equivocadas en cuanto a su mantenimiento y administración, teniendo como consecuencia una probable degradación de la calidad del servicio.

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

La dependencia debe asegurar los servicios de intranet, internet y correo electrónico, así como evaluar el desempeño de los sistemas en operación y bases de datos, los cuales se encuentran en riesgo en caso de contingencia, si no se toman acciones para mitigar las deficiencias detectadas en el análisis de impacto al negocio, la planeación de la capacidad de la infraestructura y la recuperación de los servicios ante desastres.

2017-0-14100-15-0405-01-010 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social rediseñe e implemente el Análisis de Impacto al Negocio (BIA), el Programa de Continuidad de las Operaciones del Negocio (BCP) y el Plan de Recuperación en caso de Desastres (DRP), para adecuarlo a las necesidades, prioridades y metas de la alta dirección de la secretaría, con la finalidad de garantizar la continuidad operativa de los procesos críticos, aplicativos sustantivos e infraestructura tecnológica acorde a la misión y objetivos de la dependencia.

2017-0-14100-15-0405-01-011 **Recomendación**

Para que la Secretaría del Trabajo y Previsión Social fortalezca los procedimientos para la elaboración del Plan de Capacidad de la infraestructura tecnológica, con la finalidad de garantizar que todos los servicios de TIC estén alineados con los requerimientos de la entidad, asimismo, que cuenten con un correcto dimensionamiento para la prestación de los servicios, con el objetivo de que los recursos sean aprovechados adecuadamente y que éstos aseguren los niveles de servicio requeridos para una óptima operación de la entidad.

Recuperaciones Operadas

En el transcurso de la revisión se recuperaron recursos por 61,039.00 pesos, con motivo de la intervención de la ASF.

Resumen de Observaciones y Acciones

Se determinaron 6 observaciones las cuales generaron: 11 Recomendaciones y 2 Promociones de Responsabilidad Administrativa Sancionatoria.

Dictamen

Con base en los resultados de la auditoría practicada a la Secretaría del Trabajo y Previsión Social (STPS), cuyo objetivo consistió en fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada por 131,033.1 miles de pesos que se establece en el apartado relativo al alcance, se concluye que en términos generales cumplió con las disposiciones legales y normativas que son aplicables en la materia, y se identificaron deficiencias de importancia, entre las que destacan las siguientes:

- Se carece de una metodología para el Desarrollo de Soluciones Tecnológicas, lo que ocasiona deficiencias en el cumplimiento de las especificaciones técnicas de los sistemas debido a la falta de elementos como el análisis de riesgos para el diseño de los desarrollos; el plan de pruebas para asegurar su operatividad; el plan de calidad para cumplir con estándares de las mejores prácticas; la gestión del código fuente para mantener su trazabilidad y la administración de cambios para garantizar su consistencia y actualización.

- Se tienen deficiencias para elaborar proyectos de innovación y desarrollo tecnológico, debido a las carencias en los mecanismos para una adecuada segregación de funciones y a la falta de una metodología para determinar las fortalezas y oportunidades de mejora que se requieren para la instrumentación de los proyectos de modernización tecnológica.

- La operación de la infraestructura tecnológica, aplicativos sustantivos y el control de las redes de procesamiento electrónico de datos se encuentran en riesgo debido a las deficiencias en la seguridad de la información, identificadas en los mecanismos para la administración de las contraseñas de usuarios, el monitoreo de las pistas de auditoría

y bitácoras de los aplicativos, el cifrado de datos para transferir la información con protocolos seguros, así como el resguardo del código fuente de los aplicativos, entre otros.

- La carencia de alineación del Análisis de Impacto al Negocio con los objetivos y prioridades de la Alta Dirección, deriva en el riesgo de no tener identificadas las funciones, actividades y servicios relevantes que proporciona la Secretaría, los cuales podrían resultar afectados por la interrupción de uno o más servicios de TIC; por lo tanto, la recuperación de la información y el tiempo que se tome para el restablecimiento de los servicios no serían los adecuados para la continuidad de las operaciones de la dependencia.

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

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

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Lic. Genaro Hector Serrano Martínez	Ing. Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinados por la Auditoría Superior de la Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

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

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

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

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

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

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

7. Evaluar el nivel de gestión que corresponde a los procesos relacionados con la dirección, el control y la administración de riesgos en materia de tecnologías de la información y comunicaciones; analizar el diagnóstico de las funciones sustantivas y administrativas de las TIC que lleva a cabo la entidad fiscalizada; evaluar el nivel de alineación de la estrategia de TIC con los objetivos de la Organización, así como de los mecanismos de medición, seguimiento y cumplimiento de sus metas; revisar el avance en la implementación del MAAGTICSI o, en su caso, la normativa que se aplique. Revisar el cumplimiento de las disposiciones en materia de Datos Abiertos.

8. Evaluar los mecanismos que permitan la administración de la seguridad de la información que potencialmente podrían afectar los objetivos de la institución o constituir una amenaza para la seguridad nacional; evaluar el nivel de cumplimiento en

la optimización del riesgo; verificar la gestión de seguridad de la información y gestión de los programas de continuidad de las operaciones; revisar el control de accesos y privilegios, segregación de funciones, controles de las cuentas funcionales y privilegiadas en los aplicativos y bases de datos sustantivos; verificar los mecanismos implementados para la transferencia de datos sobre canales seguros, así como los estándares aplicados para el cifrado de datos en operación.

9. Evaluar los mecanismos que permitan disminuir el impacto que puede sufrir la entidad a causa de eventos adversos y/o desastres que atenten contra la continuidad de las operaciones. Evaluar la seguridad física del Centro de Datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).

Áreas Revisadas

La Dirección General de Tecnologías de Información, la Coordinación General del Servicio Nacional del Empleo y la Dirección General de Programación y Presupuesto de la STPS.

Disposiciones Jurídicas y Normativas Incumplidas

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

1. Constitución Política de los Estados Unidos Mexicanos: Art. 134;
2. Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 1;
3. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 66, fracción III;
4. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 26, párrafo primero; 48, fracción II;
5. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 4, último párrafo;
6. Otras disposiciones de carácter general, específico, estatal o municipal: Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, publicado en el D.O.F. el 08 de mayo de 2014, última reforma publicada el 04 de febrero de 2016: Art. 10, inciso II, Art. 12, Art. 26; Reglas Generales numerales 2, 3, 6 y 17; Objetivo general del Proceso I.A Planeación Estratégica (PE); Objetivo general del Proceso II.A Administración de Servicios (ADS); Objetivo general del Proceso III.A Administración de Proyectos (ADP); Actividad APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos del Proceso III.B de Administración de Proveedores (APRO); Objetivo general del Proceso II.C Administración de la Seguridad de la Información (ASI); Objetivo general del Proceso III.C Administración de la Operación (AOP);Objetivo general del Proceso III.D Operación de Controles de Seguridad de la Información y del ERISC (OPEC);

Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Secretaría del Trabajo y Previsión Social: Art. 55; Art. 58; Art. 61; Art. 62; Art.73;

Contrato No. CE-043-2015: Cláusula Décima;

Anexo Técnico del Contrato no. RF-041-2017: Apartado 3.2. Modelo de Gobierno; 5.1 Administración de Programas y Proyectos; 11.4 Condiciones Técnicas de Aceptación de Entregables; 11.5 Penas Convencionales y/o Deductivas;

Fundamento Jurídico de la ASF para Promover Acciones

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

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

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