Secretaría de Desarrollo Social

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-0-20100-15-0261-2018

261-DS

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, así como el ejercicio del gasto de los programas sociales, su adecuado uso, operación, administración de riesgos, calidad de los datos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, procesos de 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	826,095.4
Muestra Auditada	131,457.1
Representatividad de la Muestra	15.9%

El universo seleccionado por 826,095.4 miles de pesos corresponde al total de recursos asignados en Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2017; la muestra auditada se integra por tres contratos, dos de los cuales fueron para prestar el Servicio de Centro de Contacto y el otro se refiere al Servicio Administrado de Equipo de Cómputo, Periféricos, Soporte Técnico y Mesa de Servicio con pagos ejercidos por 131,457.1 miles de pesos, que representan el 15.9% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Secretaría de Desarrollo Social (SEDESOL) en 2017, relacionada con la Ciberseguridad, la Calidad de Datos y el Ciclo de Vida del Desarrollo de los Sistemas de los programas de Estancias Infantiles y Comedores Comunitarios.

Antecedentes

La Secretaría de Desarrollo Social tiene como misión contribuir a la construcción de una sociedad en la que todas las personas, sin importar su condición social, económica, étnica, física o de cualquier otra índole, tengan garantizado el cumplimiento de sus derechos sociales y puedan gozar de un nivel de vida digno; a través de la formulación y conducción de una política de desarrollo social, privilegiando la atención a los sectores sociales más desprotegidos.

Durante el 2017, la SEDESOL dio continuidad a tres proyectos estratégicos en materia de TIC: Digitalización de Trámites y Servicios, Perfeccionamiento y Promoción del inventario de Datos Abiertos de la SEDESOL y la Prestación del Servicio Administrado de Voz y Datos para el Sector de Desarrollo Social.

Entre 2013 y 2017, en la SEDESOL se invirtieron 2,390,081.4 miles de pesos en comunicaciones, infraestructura de cómputo, arrendamiento y mantenimiento de bienes informáticos, desarrollo de aplicaciones informáticas, consultoría, 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	176,852.9	315,069.9	587,247.4	484,815.8	826,095.4	**2,390,081.4**

Fuente: Elaborado con base en la información proporcionada por SEDESOL.

Resultados

1. Análisis Presupuestal

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2017, se concluyó que la SEDESOL tuvo un presupuesto de 48,635,719.6 miles de pesos, de los cuales 826,095.4 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 1.7% del total, como se muestra a continuación:

Recursos ejercidos en 2017
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Presupuesto Ejercido TIC
1000	Servicios personales	2,256,827.1	26,678.2
2000	Materiales y suministros	111,895.4	308.7
3000	Servicios generales	2,589,718.5	799,108.5
4000	Transferencias, asignaciones, subsidios y otras ayudas	43,675,833.2	0.0
5000	Bienes Muebles, Inmuebles e Intangibles	1,445.4	0.0
	TOTAL	**48,635,719.6**	**826,095.4**

Fuente: Elaborado con base en la información proporcionada por la SEDESOL.

Los recursos ejercidos en materia de TIC por 826,095.4 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2017 SEDESOL
(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**26,678.2**
2000		**MATERIALES Y SUMINISTROS**	**308.7**
3000		**SERVICIOS GENERALES**	**799,108.5**
	31701	Servicios de conducción de señales analógicas y digitales	182,141.9
	31904	Servicios integrales de infraestructura de cómputo	132,705.3
	32301	Arrendamiento de equipo y bienes informáticos	118,023.3
	32701	Patentes, derechos de autor, regalías y otros	31,454.3
	33104	Otras asesorías para la operación de programas	3,131.0
	33301	Servicios de desarrollo de aplicaciones informáticas	80,200.7
	33303	Servicios relacionados con certificación de procesos	291.4
	33903	Servicios integrales	240,926.5
	35301	Mantenimiento y conservación de bienes informáticos	123.3
	35701	Mantenimiento y conservación de maquinaria y equipo	10,110.9
		TOTAL	**826,095.4**

Fuente: Elaborado con base en la información proporcionada por la SEDESOL.

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 26,678.2 miles de pesos durante el ejercicio fiscal 2017; considerando 76 plazas, el promedio anual por persona fue de 351.0 miles de pesos.

Del total ejercido en 2017 por 826,095.4 miles de pesos que corresponde al total de recursos asignados en materia de TIC, se erogaron 131,457.1 miles de pesos en tres contratos que representan el 15.9 % del universo, el cual se integra de la manera siguiente:

Muestra de Contratos Ejercidos durante 2017
(Miles de pesos)

Procedimiento de contratación	Contrato	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2017
				Del	Al	Mínimo	Máximo	
Adjudicación directa	Contrato número 411.413.33903.278/2015	Grupo Vanguardia en Información y Conocimiento, S.A. de C.V.	"Servicio de Centro de Contacto para la Secretaría"	1/01/2016	31/12/2016	20,972.1	52,424.4	11,610.9
	Convenio modificatorio		Ampliación del monto y plazo	1/01/2017	31/03/2017	0.0	10,484.9	
		Subtotal				20,972.1	62,909.3	11,610.9
Adjudicación directa	Contrato número 411.413.33903.044/2017	Grupo Vanguardia en Información y Conocimiento, S.A. de C.V.	"Servicio de Centro de Contacto para la Secretaría"	1/09/2017	31/12/2018	18,245.7	45,609.2	34,558.1
Adjudicación directa	Contrato 411.413.32301.262/2016	Soluciones Tecnológicas Especializadas, S.A. de C.V.	"Servicio Administrado de Equipo de Cómputo, Periféricos, Soporte Técnico y Mesa de Servicio"	1/12/2016	31/03/2019	198,409.5	317,860.7	85,288.1
					Total	**237,627.3**	**426,379.2**	**131,457.1**

Fuente: Elaborado con base en la información proporcionada por la SEDESOL.

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

2. Contratos 411.413.33903.278/2015, y 411.413.33903.044/2017 "Servicio Consolidado de Centro de Contacto para la Secretaría de Desarrollo Social"

Se analizó la información de los contratos números 411.413.33903.278/2015, convenio modificatorio 411.413.33903.278/2015 y 411.413.33903.044/2017 celebrados con Grupo Vanguardia en Información y Conocimiento, S.A. de C.V., Grupo Asis Corporativo, S.A. de C.V., KJFM Diseños y Soluciones, S.A. de C.V., Priorato Mercantil, S.A. de C.V. y Grupo de Asistencia Jurídica, S.C., mediante Adjudicación Directa, con fundamento en los artículos 17, 22 fracción II, 24, 25 primer párrafo, 26 fracción III, 40, 41 fracción III, 45 y 47 de la Ley de Adquisiciones,

Arrendamientos y Servicios del Sector Público (LAASSP) y artículos 13, 72 fracción III, 81 y 85 de su Reglamento, con vigencia del 1° de enero del 2016 al 31 de diciembre de 2018, por un monto mínimo de 39,217.8 miles de pesos y un monto máximo de 108,518.5 miles de pesos, con el objeto de prestar el "Servicio Consolidado de Centro de Contacto para la Secretaría de Desarrollo Social", con pagos realizados en 2017 por 46,169.0 miles de pesos, se determinó lo siguiente:

Alcance

El servicio del Centro de Contacto se integró para la atención de 18 Programas y sub programas sociales de la SEDESOL para: brindar información, atención de quejas, denuncias y aclaraciones; la ejecución de campañas de información, de afiliación y encuestas de satisfacción; así como para mantener la disponibilidad y continuidad del servicio.

Monitoreo de Llamadas

Para el servicio de monitoreo no se consideró ningún indicador respecto a la duración de las llamadas para saber cuántas rebasaban el limite promedio estipulado en el contrato, el cual era de 10 minutos; tampoco se tienen evidencias de la contabilización de las llamadas que se encontraban en la cola de espera.

Protección de datos personales

- Los agentes telefónicos recaban datos personales de las personas que son contactadas a través de las llamadas, como el nombre, fecha de nacimiento y lugar de la llamada; la Secretaría indicó que la fecha de nacimiento y el lugar es para fines estadísticos, en cuanto al nombre se utiliza para detectar a los beneficiarios de los distintos programas. Respecto al tratamiento de los datos personales, el proveedor debe apegarse a lo señalado en el ISO 27001:2013 como lo establece el contrato, de acuerdo a un sistema de gestión seguridad de la información para el servicio del centro de contacto, no obstante, no se tienen evidencias del cuidado que se le da a los datos recabados durante la llamada por parte del proveedor ni de la dependencia, tampoco se cuenta con una clasificación de los datos y mecanismos para protegerlos, asimismo, no se identificó la necesidad de solicitar dichos datos ya que en los reportes que entrega el proveedor sólo se presenta la edad por rangos y el sexo, además no se consulta a los beneficiarios por nombre debido a que el proveedor no tiene acceso a ningún sistema para tal efecto.
- El contrato no contempló el borrado seguro de la información, el proveedor realiza un procedimiento de borrado interno con la finalidad de optimizar el espacio en sus servidores, sin que la SEDESOL se cerciore que la información se haya eliminado por completo y no pueda ser recuperada.

Validación de los niveles de servicio

El contrato establece que la DGTIC, es la encargada de comprobar, supervisar, y verificar la correcta y eficiente prestación del servicio por medio de la Dirección de Desarrollo de Sistemas Administrativos (DDSA); sin embargo, por parte de la DDSA no se tienen evidencias para constatar que las actividades desarrolladas por el proveedor fueron las estipuladas en el

contrato y su anexo técnico; la DGTIC señaló que se planificarán controles de doble chequeo para comprobar los servicios que entrega el proveedor.

Entre las principales desviaciones respecto al cumplimiento del contrato y anexo técnico, destacan la falta de soporte para la medición del tiempo de las llamadas y aquellas en la cola de espera; no se tiene evidencia del manejo de la información recabada con respecto a la protección de los datos personales por parte del proveedor; la Secretaría no se asegura que la información sea eliminada de los dispositivos de almacenamiento del proveedor de manera correcta y no pueda ser recuperada; no se cuenta con evidencias que aseguren que los elementos de servicio facilitados por el proveedor hayan sido los establecidos en el contrato, lo anterior, genera riesgos de exposición no autorizada de los datos de los usuarios.

2017-0-20100-15-0261-01-001 **Recomendación**

Para que la Secretaría de Bienestar implemente procedimientos y mecanismos de control para asegurarse que el proveedor realice un monitoreo en tiempo real de los niveles de servicio que hayan sido acordados, con la finalidad de obtener las mejores condiciones de operación y calidad del servicio; asimismo, que sean configurados componentes que generen la trazabilidad del servicio como son las bitácoras, cifras de control, indicadores y criterios de aceptación del servicio realizado.

2017-0-20100-15-0261-01-002 **Recomendación**

Para que la Secretaría de Bienestar implemente procedimientos y mecanismos de control para dejar evidencia del manejo de la información recabada de los beneficiarios para la protección de los datos personales por parte del proveedor; asegurar que la información sea eliminada de los dispositivos de almacenamiento del proveedor de manera segura para que no pueda ser recuperada; así como establecer un protocolo que evite que los datos que gestiona el proveedor se copien, transmitan o difundan por cualquier medio, con fines distintos a los definidos en el contrato.

3. Contrato 411.413.32301.262/2016 “Servicio Administrado de Equipo de Cómputo, Periféricos, Soporte Técnico y Mesa de Servicio”

Se analizó el contrato número 411.413.32301.262/2016 celebrado con Soluciones Tecnológicas Especializadas, S.A. de C.V., mediante Adjudicación Directa, con fundamento en los artículos 17, 22 fracción II, 24, 25 primer párrafo 26 fracción III, 40, 41 fracción III y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y artículo 72 fracción III, 81 y 85 de su Reglamento, con vigencia del 1° de diciembre del 2016 al 31 de marzo de 2019, por un monto mínimo de 198,409.5 miles de pesos y un monto máximo de 317,860.7 miles de pesos, con el objeto de prestar un Servicio Administrado de Equipo de Cómputo, Periféricos, Soporte Técnico y Mesa de Servicio, con pagos realizados en 2017 por 85,288.1 miles de pesos, se determinó lo siguiente:

Alcance

Suministrar al personal de la Secretaría equipos de cómputo con tecnología de vanguardia; contar con una mesa de servicio como punto único de contacto entre el usuario final y los servicios en materia de TIC; brindar niveles de servicio adecuados que permitan solucionar y atender los requerimientos de los usuarios.

Estudio de Factibilidad

No se cuenta con el análisis de la conveniencia para la adquisición o arrendamiento con opción a compra de los bienes, para lo cual debió de considerarse entre otros aspectos los costos de mantenimiento y consumibles a pagar en cada caso.

Revisión del Equipo Suministrado por el Proveedor

- La DGTIC señaló que desconoce el proceso que se llevó a cabo para determinar las características necesarias de cada uno de los diferentes equipos requeridos, señalando que se consideró con base a las características del servicio otorgado mediante un procedimiento de adhesión del contrato JADQ-12-15 que fue celebrado por la Casa de Moneda y el prestador de servicios.
- Con base a lo señalado en el anexo técnico del contrato y en la propuesta técnica del proveedor, se llevó a cabo la revisión de su cumplimiento, detectando las observaciones siguientes: De un universo de 707 equipos Laptop, cuatro contaban con un procesador Intel Core i7-8550U a 1.80 GHz y de acuerdo con lo especificado en la propuesta técnica debió ser Intel Core i7-6500U a 2.5 GHz; ocho estaciones de trabajo contaban con monitores de escritorio de 20 pulgadas y de acuerdo con la propuesta técnica debieron ser de 24 pulgadas.
- La Secretaría erogó un precio unitario de 3.9 miles de pesos por 38 equipos Mac Book de acuerdo a lo observado en las Actas de Entrega-Recepción para la liberación de pago, no obstante, el precio unitario señalado para el equipo Mac Book en la propuesta económica del proveedor es por 2.3 miles de pesos.

Mecanismos de validación del contrato

El contrato establece que la Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC), es la encargada de comprobar, supervisar, vigilar, dar seguimiento, verificar la realización óptima, correcta y eficiente de la prestación del servicio a través de la Dirección de Servicios Informáticos o las áreas técnicas que defina la dependencia, no obstante, los servicios en los cuales se detectaron deficiencias son los siguientes: falta de reportes mensuales donde se muestre el estado que guarda la infraestructura tecnológica; los resultados de las encuestas de satisfacción; los formatos establecidos para el cumplimiento de estándares de calidad, ITIL y MAAGTICSI; no se entregó evidencia de que se realizan los procesos de gestión de problemas, cambios, liberaciones, configuraciones, gestión del conocimiento, operaciones, capacidad, continuidad, tampoco del módulo de administración de parches, portal de autoservicio, simulacros de contingencia, de las certificaciones del personal, el cumplimiento de sus funciones y los esquemas de seguridad.

En conclusión no se cuenta con el análisis de la conveniencia para la adquisición o arrendamiento con opción a compra de los bienes; no se tiene evidencia del módulo de administración de parches, portal de autoservicio, simulacros de contingencia ni certificaciones del personal; se carece de esquemas de seguridad para el borrado de información de los equipos portátiles y de escritorio, para evitar que sea recuperada la información. Lo anterior, puede impactar la calidad del servicio que requieren los usuarios de la Secretaría y de los Programas Sociales, asimismo, se podría exponer información almacenada en los equipos.

2017-0-20100-15-0261-01-003 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los mecanismos de control y supervisión en la recepción, configuración, distribución y manejo de los inventarios de equipos de cómputo, con la finalidad de detectar oportunamente los movimientos y capacidades de los equipos, para asegurar las mejores condiciones de operación de la infraestructura tecnológica. Adicionalmente, verificar el cumplimiento de los servicios a los equipos de cómputo, portal de autoservicio, los reportes de desempeño, el monitoreo y prevención de fallas, las encuestas de satisfacción y las pruebas de contingencia

4. Ciberseguridad

En la revisión y análisis de la información relacionada con la administración y operación de los controles de Ciberseguridad vinculados con la infraestructura tecnológica y sus aplicativos sustantivos, las directrices y herramientas informáticas en esta materia, así como de los procesos de Administración de la Seguridad de la Información (ASI) del MAAGTICSI, aunado a las políticas y lineamientos proporcionados por la SEDESOL, se detectaron las observaciones siguientes:

Documentación de procesos de seguridad de la información

- La información entregada por la Secretaría no permite determinar los umbrales y parámetros cuantitativos y cualitativos para definir el catálogo de infraestructuras críticas, los activos clave y los sistemas de información esenciales.
- Con relación a la designación de roles funcionales en materia de seguridad, no se tienen evidencias de sus habilidades y certificaciones, ni mecanismos para evaluar el nivel de concientización en seguridad de los usuarios de la SEDESOL.

Gestión de Cuentas de Usuarios

- Con relación a las políticas de contraseñas, su composición, actualización, bloqueo y baja por inactividad, se detectó que cada plataforma tecnológica (Sistema de Gestión de Estancias Infantiles (SGEI), Comedores Comunitarios, directorio activo, entre otras), es gestionada por cada unidad administrativa sin una configuración estandarizada a nivel transversal en la SEDESOL.
- Durante las pruebas se determinó que el directorio activo ofrece un tratamiento por igual a cuentas de cualquier nivel, pudiendo poner en riesgo aquellas que tienen un grado de autorización mayor para el manejo de información sustantiva; asimismo, se carece de la gestión integral, estandarizada y monitoreada de las cuentas de los aplicativos de la SEDESOL, así como de los diferentes sistemas operativos, bases de datos, sistemas de capa intermedia y demás herramientas utilizadas en la Secretaría.

Endurecimiento de la Configuración de Seguridad y Cifrado

- Se carece de procedimientos para robustecer la configuración de los Sistemas Operativos, Bases de Datos, Software de Capa Intermedia, Aplicaciones y Medios de comunicación, con la finalidad de cerrar las brechas en la seguridad de los datos; así como de la designación de personal dedicado a funciones de seguridad de la información tanto en el Manual como en el Reglamento de la dependencia.

- El cifrado de datos en la Secretaría no se tiene estandarizado para favorecer la protección de la información, por medio de canales seguros, su respaldo y resguardo; tampoco se cifran los respaldos de información y se desconocen las acciones que realizaron con aquellos respaldos que tuvieron algún estatus de falla.
- No se analizan de manera regular los puertos de todos los servidores críticos, así como su comparación con las líneas base de configuración, con la finalidad de generar alertas sobre posibles cambios no autorizados.
- La DGTIC no gestiona el control del software que es instalado en los equipos de cómputo de los usuarios, ni quién lo determina, cómo lo validan, cómo evitan instalaciones no autorizadas, tampoco es supervisado por herramientas de monitoreo de activos para verificar que no sea modificado.

Incidentes, Monitoreo y Bitácoras

- En relación al monitoreo de la red por parte del proveedor, no se tiene un comparativo de manera histórica, sólo se hace a petición, por lo tanto, la toma de decisiones para el óptimo desempeño del ancho de banda, memoria, procesador, redes privadas virtuales y servidores, se encuentra limitada.
- La DGTIC no coordina a los involucrados para la atención de los incidentes, tampoco tipifican el riesgo, ni la asignación de títulos de trabajo y obligaciones para su manejo; se carece de un registro de los tiempos para escalar o atender los incidentes; no se califica el desempeño de los niveles de servicio; se carece del mantenimiento, monitoreo y análisis de las bitácoras de auditoría de las aplicaciones críticas para detectar, analizar o recuperarse de un ataque; no se monitorean los incidentes de seguridad de forma transversal en la Secretaría, aunado a que el Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra desactualizado.
- La SEDESOL no integra un proceso de gestión y control de cambios de la línea base de la configuración de seguridad de todas sus plataformas, lo que puede derivar en un alto riesgo de ser modificados sin tener un marco comparativo que evite vulnerabilidades.

Análisis de Vulnerabilidades

- La DGTIC no presentó evidencias de la resolución del dictamen de la causa raíz, lecciones aprendidas y acciones realizadas tanto del proveedor como de la SEDESOL, para evitar la reincidencia de seis vulnerabilidades de nivel alto detectadas en 2017.
- No se asegura que los equipos de cómputo cuenten con antivirus, ni que cada dispositivo inalámbrico conectado a la red coincide con un perfil de configuración y de seguridad autorizado.

Filtrado de Tráfico y Contenido

- La DGTIC no tiene implementadas listas blancas de aplicaciones que permitan ejecutar el software sólo si está incluido en la lista blanca, asimismo, durante las pruebas se pudo evadir el filtrado de seguridad, ingresando a las páginas no autorizadas por medio de un programa “traductor”.

- Se efectuaron pruebas de vulnerabilidades en la infraestructura tecnológica de la Secretaría y se detectó que dos servicios tienen una falla en el software de cifrado, que podría ser utilizada para el robo de información; en el caso de otros dos servicios se identificaron problemas como certificado no válido, sitio explotable, fallas en la configuración, protocolo inseguro y desactualización de parches.

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

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIAS EN LOS CONTROLES DE CIBERSEGURIDAD	
Factor	**Riesgo**
Clasificación de Infraestructuras y Activos de Información Críticos	Se carece del análisis de los procesos existentes para determinar cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Secretaria para alcanzar sus objetivos; en consecuencia, se presenta una brecha entre las expectativas de la SEDESOL y las capacidades de TIC, al no considerar los activos de información críticos, ni los indicadores de evaluación del desempeño que son relevantes para la Secretaria, pudiendo ocasionar políticas de seguridad mal diseñadas, incumplimientos regulatorios, pérdidas financieras por proyectos mal definidos, entre otros.
Administración de usuarios	Debido a que no se tienen procedimientos formalizados y estandarizados a nivel de la Secretaria para la gestión de claves de usuarios, éstos podrían tener permisos para acceder a información que no le corresponde de acuerdo a sus funciones y responsabilidades, en consecuencia, se podría perder la confidencialidad en la información y ejecutar transacciones no autorizadas que pueden poner 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 de la información.
Monitoreo de las pistas de auditoría y bitácoras de los aplicativos y bases de datos	No se realiza una revisión periódica de las pistas de auditoría y las bitácoras de los aplicativos sustantivos, a fin de detectar oportunamente movimientos irregulares o cambios no autorizados, lo que podría dar oportunidad para que los usuarios maliciosos puedan ejecutar transacciones no autorizadas que pudieran comprometer la integridad de los activos.
Gestión de configuraciones	En la estructura de datos del repositorio de configuraciones, no se verifica que se consideren los atributos básicos relacionados con los elementos de configuración y sus componentes, así como el estado en que se encuentran, con el riesgo de que en caso de la presencia de un evento o problema, no se tenga un repositorio que permita verificar el impacto en los activos de TIC con respecto a sus características esenciales.
Sistema de Gestión de Seguridad de la Información (SGSI)	El Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra desactualizado, lo que podría traer como consecuencia, diversos riesgos: pérdida de confidencialidad de la información que puede ser conocida y utilizada por personas que no tienen autorización; falta de integridad ya que los datos pueden ser alterados, provocando pérdidas económicas y fraudes; afectación a la disponibilidad de los servicios que impide que los usuarios accedan a las aplicaciones cuando lo requieran; por otro lado, los mecanismos de seguridad de la información se mantienen estáticos, en un entorno dinámico que requiere de la aplicación de acciones preventivas y correctivas generadas por las revisiones que se efectúen al SGSI.
Alineación de la Seguridad de las TIC hacia la Secretaria	El equipo de trabajo para la identificación de infraestructuras de información esenciales y/o críticas, así como de activos clave, y las diversas áreas de la SEDESOL involucradas, no analizan los procesos existentes para determinar cuáles de éstos son críticos, considerando como tales aquellos de los que depende la Secretaria para alcanzar sus objetivos; esto es, se carece de un método y políticas para efectuar una alineación de TIC con la SEDESOL respecto a la seguridad de la información.

Resulta prioritaria la implementación y mejora de los mecanismos de control para: la evaluación continua de las vulnerabilidades; uso controlado de privilegios administrativos; contar con personal con habilidades y certificaciones en seguridad de la información; fortalecer las políticas de contraseñas, de manera estandarizada a nivel Institución; ejecutar la comparación de las líneas base de configuración de los equipos para generar alertas sobre posibles cambios no autorizados; mejorar la clasificación de infraestructuras, sistemas y activos de información críticos; lo anterior, podría impactar en la seguridad la información de más de 76 millones de beneficiarios de los diversos programas de la SEDESOL.

2017-0-20100-15-0261-01-004 **Recomendación**

Para que la Secretaría de Bienestar desarrolle e implemente una estrategia institucional de seguridad con mecanismos de control para la evaluación continua de las vulnerabilidades en las redes y equipos de cómputo, así como el monitoreo, supervisión y análisis de registros de auditoría; con la finalidad de evitar que una amenaza afecte a los activos de información e infraestructuras tecnológicas críticas.

2017-0-20100-15-0261-01-005 **Recomendación**

Para que la Secretaría de Bienestar implemente procedimientos y mecanismos de control en el uso de privilegios administrativos; la restricción y control de puertos de red, protocolos y servicios, para asegurar la protección de los datos en el intercambio de información; así como los métodos para asegurar que la información cuenta con niveles óptimos de integridad y confiablidad para la privacidad de la información.

2017-0-20100-15-0261-01-006 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los procedimientos de control para implementar la clasificación de infraestructuras y activos de información críticos, así como la actualización del Sistema de Gestión de Seguridad de la Información; con la finalidad de que por medio del análisis de riesgos y la definición de controles, determine las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.

2017-9-20113-15-0261-08-001 **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 de Bienestar 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 de la seguridad de la información, se detectaron irregularidades, debido a que se carece de la evaluación continua de las vulnerabilidades en la infraestructura tecnológica; uso controlado de privilegios administrativos; monitoreo, supervisión y análisis de registros de auditoría; restricción y control de puertos de red, protocolos y servicios; control de acceso inalámbrico; clasificación de infraestructuras y activos de información críticos; así como la actualización del Sistema de Gestión de Seguridad de la Información; lo anterior podría exponer a terceros no autorizados la información de más de 76 millones de beneficiarios de los diversos Programas de la Secretaría.

5. Calidad de Datos en los Programas de Estancias Infantiles y Comedores Comunitarios

Para realizar esta evaluación se utilizó una herramienta de análisis de calidad de datos, con la cual se verificó el 100.0% de la información de las bases de datos proporcionadas por la SEDESOL correspondientes al año 2017, relacionadas con el programa de Estancias Infantiles y Comedores Comunitarios, de lo cual se determinó lo siguiente:

Modelo de Información Integral para los datos

- Se carece de un modelo de información para los datos en la Secretaría, que cuente con los objetivos para el tratamiento de la información con sus criterios de calidad que deben de alcanzarse en cuanto a grado de eficiencia, eficacia, uso y seguridad de la información.
- Con respecto al Programa de Estancias Infantiles se requiere integrar la gestión de sus datos en un modelo de información. En el caso del Programa de Comedores Comunitarios se requerirá de mayores esfuerzos, debido a que actualmente la gestión de su información es mediante hojas de cálculo de Excel.

Evaluación de la funcionalidad y objetivos del Modelo de Información

- En el Sistema de Gestión de Estancias Infantiles (SGEI) se detectaron las siguientes inconsistencias: los controles de edición en las pantallas de captura permiten carga de información errónea en fechas y montos; se tienen campos sin parametrizar; se carece de la descripción de acrónimos; no se obtiene por interface el dato del acta de nacimiento, estado civil, colonia, último grado escolar y estado de jubilación.
- Se carece de estadísticas que permitan a la SEDESOL tomar acciones sobre la información, por ejemplo: información que no es utilizada; así como de los registros sin movimiento; datos que no integran controles de edición, que no se han parametrizado, con valoraciones personales u opcionales e indicadores que determinen que la información es correcta y confiable.
- Diversos elementos del modelo de información no están definidos, ni documentados, para obtener respuestas inmediatas que apoyen a la toma de decisiones, algunos son los siguientes: confirmación de exactitud de los datos; detectar información histórica u operativa; periodos de retención y destrucción de datos; hábitos o extrapolaciones del comportamiento de la información; actualización de la información y su frecuencia; datos que no cambian; registros confiables y correctos; datos sin uso; datos validados por interoperabilidad o tiempo real; contexto en el que la información toma sentido; datos supeditados a otras informaciones; información a ser respaldada y su clasificación de criticidad o sensibilidad.

Pruebas de Calidad de los Datos

- En el Programa de Comedores Comunitarios, se detectó que de 5,542 comedores en 1,612 (29.1%), el número de personas que recibieron el beneficio fue superior a 120 en alguno de los meses, incumpliendo lo señalado en las reglas de operación.

- Del Programa de Estancias Infantiles se identificó lo siguiente:
    - 4,446 registros (46.1%) de un total de 9,643, no contienen información en el campo horario.
    - 3,943 registros (40.9%) de un total de 9,643, no contienen información o el registro es igual a cero en el campo de capacidad instalada.
    - La estancia con clave “18580” tiene fecha de visita del 26 de enero de 2210.

Ciclo de Vida del Desarrollo de Sistemas

- La SEDESOL no cuenta con estrategias de interoperabilidad al interior de la propia Secretaría ni con otras instituciones que requieran compartir datos.
- El programa de Comedores Comunitarios no integra ninguna metodología de Desarrollo de Sistemas para gestionar sus procesos.
- El Sistema de Gestión de Estancias Infantiles (SGEI) presenta las deficiencias siguientes:
    - Se carece de la documentación y regulación para la operación de los procedimientos relacionados con la gestión de proyectos, eventos, incidentes, monitoreo, problemas, cambios, versiones, configuración, capacidad, niveles de servicio, seguridad de la información, gobierno y riesgos.
    - No se consideró desde el diseño de sistemas, la seguridad de la información y la protección de datos personales; no se tiene evidencia que los desarrollos han quedado bajo la titularidad de la Secretaría; se carece de una arquitectura orientada a servicios; asimismo, no se cuenta con un análisis de vulnerabilidades previo al inicio de la puesta en operación del sistema.
    - Se carece de criterios para clasificar el sistema como un activo clave; no se encuentra controlado en un repositorio de configuraciones; no se tiene evidencia de los niveles de servicio acordados; el sistema no forma parte de programa de continuidad de las operaciones, tampoco se tienen pruebas de recuperación en caso de contingencia.

Los principales riesgos por la carencia o inconsistencia de los controles para el desarrollo de soluciones tecnológicas y sus consecuencias potenciales para las operaciones y activos, son los siguientes:

Principales riesgos por la carencia o inconsistencia de los controles para el Desarrollo de Soluciones Tecnológicas	
Factor crítico	**Riesgo**
Análisis de Vulnerabilidades	La falta de ejecución de un análisis de vulnerabilidades a las solicitudes de desarrollo de sistemas antes de su puesta a producción, puede representar un riesgo en la disponibilidad de las funcionalidades de la aplicación, debido a que pueden no estar protegidos los recursos que forman parte del sistema a nivel hardware, software, telecomunicaciones y datos.
Análisis de Riesgos	El equipo de análisis de riesgos de desarrollo de software no detecta, clasifica y prioriza los riesgos para evaluar su impacto sobre los módulos de los sistemas, de manera que se obtengan planes de remediación y mitigación para definir los controles a implantar de acuerdo con las capacidades y recursos de las áreas, para mantener aceptable el nivel de riesgo y evitar la materialización de las amenazas.
Administración de Problemas	La falta de gestión de los problemas impide la identificación de las fallas que pudieran presentarse con mayor frecuencia, aunado a que no define el impacto que pudiera ocasionar un incidente, lo que provoca deficiencias en la prevención e identificación de riesgos, así como en los mecanismos de respuesta para controlarlos, mitigarlos y erradicarlos.
Administración de Cambios	Los cambios a los programas deben ser probados y eventualmente certificados para asegurar que realicen las funciones que se pretenden. Además de esto, si el análisis de riesgo determina que es necesario, se podrían requerir pruebas adicionales para asegurar que la funcionalidad existente, el desempeño del sistema y la seguridad del aplicativo, no se ve afectada por el cambio.
Plan de Calidad	El aseguramiento de la calidad se enfoca en aspectos formales del desarrollo de software, tales como adherirse a estándares de codificación y a la metodología de desarrollo de la entidad, la cual al no tener un procedimiento para la revisión de los resultados y productos que se deben entregar en cada etapa, así como la confirmación del cumplimiento de los requerimientos, no está asegurando la calidad del sistema debido a que no mide el grado de alineación a la metodología, con la finalidad de proponer mejoras a los procedimientos de desarrollo de sistemas.
Gestión de Código Fuente	Se carece de procedimientos para el control de versiones en el código fuente de los programas, para poder revertirlos en caso necesario, lo que impide realizar cambios sobre los elementos almacenados de código fuente; asimismo, se carece de un registro histórico de las acciones realizadas con cada versión de código fuente, lo que puede causar afectaciones a la funcionalidad de aplicaciones e impactos a los activos de información.
Manual de Mantenimiento	Debido a la carencia de un manual de mantenimiento, no están establecidas las normas y procedimientos que se utilizan en los sistemas para efectuar la función de mantenimiento en todos y cada uno de sus módulos.
Administración de Proyectos	Debido a la carencia de una administración de proyectos, no se está asegurando que todas las iniciativas cuenten al menos, con su documento de planeación del proyecto, así como los planes subsidiarios, desde su inicio hasta su cierre, con la actualización en tiempo y forma de acuerdo con los avances de los mismos. Adicionalmente, se carece de controles para dar seguimiento al alcance, tiempo, riesgos y costos que pueden impactar de manera negativa al beneficio esperado por la entidad.

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

Las principales inconsistencias que incrementan el riesgo de vulnerabilidades en el desarrollo de sistemas se deben a la carencia de una metodología para el desarrollo de soluciones tecnológicas que propicia sistemas de baja calidad, insatisfacción de los usuarios, errores de

procesamiento, falta de protección contra códigos maliciosos, lo cual no contribuye en alcanzar una mayor eficiencia en los procesos institucionales; asimismo, no se cuenta con un modelo de información con bases de datos íntegras, confiables y disponibles, debido a la falta de procedimientos para la limpieza, normalización, validación y unificación de los datos, con la finalidad de que los registros cumplan con lo establecido en la arquitectura de la información.

2017-0-20100-15-0261-01-007 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los procedimientos de control y monitoreo para implementar mecanismos que le permitan contar con un modelo de información con bases de datos íntegras, confiables y disponibles, mediante la limpieza, normalización, validación y unificación de los datos, con la finalidad de que los registros de los diversos programas sociales cumplan con las mejores prácticas y lo establecido en la arquitectura de la información.

2017-0-20100-15-0261-01-008 **Recomendación**

Para que la Secretaría de Bienestar implemente una metodología de desarrollo de soluciones tecnológicas con la finalidad de mitigar los riesgos y solventar las inconsistencias que se presentan en los procesos de Análisis de Vulnerabilidades; Análisis de Riesgos; Administración de Problemas; Administración de Cambios; Plan de Calidad; Gestión de Código Fuente; Manual de Mantenimiento y Administración de Proyectos, a fin de contar con sistemas de información con óptimos niveles de integridad, confiabilidad y disponibilidad de la información.

2017-9-20113-15-0261-08-002 **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 de Bienestar 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 de la Calidad de los Datos para los Programas de Estancias Infantiles y Comedores Comunitarios incurrieron en incumplimientos, debido a que se carece de un modelo de información para los datos que asegure la eficiencia, eficacia, uso y seguridad de la información; no se cuenta con una metodología de Desarrollo de Sistemas para la automatización de los procesos; se carece de la documentación y regulación para la operación de los procedimientos relacionados con la gestión de proyectos, eventos, incidentes, monitoreo, problemas, cambios, versiones, configuración, capacidad, niveles de servicio, seguridad de la información, gobierno y riesgos; no se consideró desde el diseño de sistemas, la seguridad de la información y la protección de datos personales; los sistemas no están diseñados con una arquitectura orientada a servicios; asimismo, se carece de un análisis de vulnerabilidades previo al inicio de la puesta en operación de los sistemas.

Resumen de Observaciones y Acciones

Se determinaron 4 observaciones las cuales generaron: 8 Recomendaciones y 2 Promociones de Responsabilidad Administrativa Sancionatoria.

Dictamen

El presente se emite el 28 de enero de 2019, 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 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 que se establece en el apartado relativo al alcance, se concluye que, en términos generales, la Secretaría de Bienestar cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con la operación del Centro de Llamadas, se detectó la falta de soporte para la medición del tiempo de las llamadas y aquellas en la cola de espera; no se tiene evidencia del manejo de la información recabada respecto a la protección de los datos personales; la dependencia no se asegura que la información sea eliminada de los dispositivos de almacenamiento del proveedor de manera correcta y que no pueda ser recuperada; lo anterior, genera riesgos de exposición no autorizada de los datos de los beneficiarios.

- Sobre la Ciberseguridad, es prioritaria la implementación de mecanismos de control para la evaluación continua de las vulnerabilidades; el uso controlado de privilegios administrativos; contar con personal con habilidades y certificaciones en seguridad de la información; fortalecer las políticas de contraseñas de manera estandarizada a nivel institucional; realizar comparativos de las líneas base de configuración de los equipos para generar alertas sobre posibles cambios no autorizados; lo anterior, podría impactar en la seguridad de la información de más de 76 millones de beneficiarios de los diversos programas de la SEDESOL.

- Se detectó la carencia de una metodología para el desarrollo de soluciones tecnológicas que propicia sistemas de baja calidad, insatisfacción de los usuarios, errores de procesamiento, falta de protección contra códigos maliciosos, lo cual no contribuye en alcanzar una mayor eficiencia en los procesos institucionales; asimismo, no se cuenta con un modelo de información con bases de datos íntegras, confiables y disponibles, debido a la falta de procedimientos para la limpieza, normalización, validación y unificación de los datos.

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

El presente dictamen se emite el 28 de enero de 2019, 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
Genaro Héctor Serrano Martínez	Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables; analizar el 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 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; análisis y pruebas de vulnerabilidades, entre otros.

8. Verificar que los procesos guardan relación con lo definido en las "reglas de negocio" de la entidad; revisar el nivel de control de los datos relacionado con la integridad, disponibilidad y calidad de la información, determinando el nivel de riesgo en sus operaciones; verificar la trazabilidad y monitoreo de las operaciones que afectan a las bases de datos (BD).

Áreas Revisadas

La Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC), y la Dirección General de Programación y Presupuesto (DGPP).

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 de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 26; Art. 48, fracción II; Art. 55;

2. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 10;

3. Otras disposiciones de carácter general, específico, estatal o municipal: 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 Administrativo de Aplicación General en dichas materias, publicado el 08 de mayo de 2014 en el Diario Oficial de la Federación, última reforma publicada el 04 de febrero de 2016: Art. 5, fracción I; Art. 8; Art. 9, fracción II; Art. 10, fracción II, V y VI; Art. 13, fracción VII; Art. 16, fracción III; Art. 17, fracción I, VIII; Art. 18, fracción III; Art. 19, fracción VI; Art. 24; 26;

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: Objetivo General del MAAGTICSI; Reglas generales, 9, 13; Proceso de Administración de Servicios (ADS), regla del proceso 2 y 5; subproceso ADS 1, factor crítico 1, inciso e); subproceso ADS 3, factor crítico 2, 3, 4, 5; subproceso ADS 4, factor crítico 3, 4 y 5; Proceso de Administración de la Seguridad de la Información (ASI), objetivo específico 2 y 4; regla del proceso 14 y 8; subproceso ASI 3, factor crítico 1, inciso e) y factor crítico 15; subproceso ASI 4, factor crítico 6; subproceso ASI 5, factor crítico 1, inciso c), d); factores críticos 5 y 16; subproceso ASI 6, factor crítico 1, incisos a), c), g), e), i), o), r) y s); Proceso de Administración de la Operación (AOP), regla del proceso 4; subproceso AOP 2, factores críticos 1, 2, 3 y 4; subproceso AOP 4, factor crítico 1, inciso c); Proceso de Administración de Configuraciones (ACNF), objetivo general, subproceso ACNF 1, factor crítico 2; Proceso de Planeación Específica (PE), regla de proceso 2;

Manual de Organización General de la Secretaría de Desarrollo Social publicado en el Diario Oficial de la Federación el 14 de julio de 2015: 3.3 Funciones, Dirección General de Tecnologías de la Información y Comunicaciones, función 1, 2, 4, 5, 6, 7, 10, 11, 12, 13 y 14;

Manual de Organización y de Procedimientos de la Dirección General de Tecnologías de la Información y Comunicaciones autorizado el 23 de febrero de 2016: Dirección de Desarrollo de Sistemas Administrativos, funciones 1, 2, 4, 5, 6, 7, 11, 12, 13, 14 y 18;

Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Secretaría de Desarrollo Social: Capitulo segundo, Fracción III;

Contrato 411.413.32301.262/2016: clausula décima sexta;

Anexo Técnico del contrato 411.413.32301.262/2016: Numerales 3.1, 4.2.3, 4.2.7, 4.2.8, 4.8.8.1.1, 4.8.8.1.2, 4.8.8.1.3, 4.8.8.1.3.18, 4.3.3, 4.3.4, 4.6.2.14, 4.7.3, 4.6.2.3, 4.6.2.11, 4.7.5, 4.8.8.2.3, 4.8.7.1.2, 5, 5.1, 6.3, 6.4, 8.5.9.11, 8.5.9.17, 8.5.6.2.3, 8.5.7, 8.5.9.3, 9, XII, XIII, 15, 16, 17, 22 inciso o) y 24;

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.