Secretaría de Bienestar

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2019-0-20100-20-0239-2020

239-DS

Criterios de Selección

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

Objetivo

Fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

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	437,250.2
Muestra Auditada	116,355.6
Representatividad de la Muestra	26.6%

El universo seleccionado por 437,250.2 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal 2019; la muestra auditada está integrada por dos contratos para prestar el servicio integral de comunicaciones, así como por el servicio para el desarrollo del inventario, control y seguimiento de la entrega-recepción de las tarjetas de Bienestar, con pagos ejercidos por 116,355.6 miles de pesos, que representan el 26.6% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Secretaría de Bienestar (BIENESTAR) en 2019, relacionada con la Ciberseguridad y Continuidad de las Operaciones.

Antecedentes

En la auditoría número 261-DS "Auditoría de TIC", correspondiente a la fiscalización de la Cuenta Pública 2017, se observó la carencia de mecanismos para asegurar la seguridad de la información contenida en los dispositivos de almacenamiento, tampoco se contaba con una metodología para tener modelos de información con bases de datos íntegras, confiables y disponibles; en relación con la Ciberseguridad, no se contaba con mecanismos de control para la evaluación continua de las vulnerabilidades, privilegios administrativos, políticas de contraseñas y línea base para la configuración de los equipos, aunado a la falta de personal especializado en la materia.

Durante la revisión de la Cuenta Pública 2018, en la auditoría 287-DS "Contratación de Servicios con Terceros", se identificó que no se cumplió con el Servicio de Aprovisionamiento de Dispositivos Móviles con el fin de llevar a cabo el Servicio de Recolección de Información Socioeconómica y atención a los Beneficiarios, incluyendo la Transmisión de Datos al Hosting de la Secretaría de Desarrollo Social, debido a que no se realizó el servicio de recolección de información socioeconómica y demográfica de los beneficiarios de los distintos Programas Sociales a través de los Dispositivos Móviles, derivado de la falta de implementación de ocho módulos del Servicio Integral de Información y de Apoyo Tecnológico que facilite la operación del Programa de Pensión para Adultos Mayores, por lo que se presumen pagos injustificados por 154,474.7 miles de pesos. Asimismo, no fue posible verificar en sitio el soporte y mantenimiento a través de la plataforma para la Gestión de Datos Maestros y Gobierno de Datos del Sistema de Información Social Integral (SISI), ni el servicio Data warehouse, BI para el Sistema de Información Social, asistencia técnica y mantenimiento, tampoco los diseños e implementación de los modelos de análisis estadístico de participantes y componentes geográficos, por lo que se presumen pagos injustificados por 44,493.8 miles de pesos.

Entre 2015 y 2019, se han invertido más de 2,650,392.0 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

Recursos invertidos en materia de TIC
(Miles de pesos)

PERIODO DE INVERSIÓN	2015	2016	2017	2018	2019	TOTALES
MONTO POR AÑO	340,678.2	350,902.6	588,583.6	909,838.0	460,389.6	**2,650,392.0**

Fuente: Elaborada con base en la información proporcionada por BIENESTAR.

Resultados

1. Análisis Presupuestal

En relación con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019, publicado en el Diario Oficial de la Federación el 28 de diciembre de 2018, se autorizó al Ramo Bienestar (20) un presupuesto de 150,606,037.7 miles de pesos, del cual se asignó a la Secretaría de Bienestar un presupuesto de 127,703,586.8 miles de pesos.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2019, se concluyó que la Secretaría de Bienestar (Sector Central) tuvo un presupuesto ejercido de 143,439,112.9 miles de pesos, de los cuales 460,389.6 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 0.3% del presupuesto, como se muestra a continuación:

RECURSOS EJERCIDOS EN LA SECRETARÍA DE BIENESTAR DURANTE 2019
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recursos relativos a las TIC
1000	Servicios personales	6,125,514.8	**23,139.4**
2000	Materiales y suministros	130,433.4	0.0
3000	Servicios generales	1,969,662.9	**437,250.2**
4000	Transferencias, asignaciones, subsidios y otras ayudas	134,835,003.4	0.0
8000	Participaciones y Aportaciones	378,498.4	0.0
	TOTAL	**143,439,112.9**	**460,389.6**

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

Los recursos ejercidos en materia de TIC por 460,389.6 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2019 EN LA SECRETARÍA DE BIENESTAR (SECTOR CENTRAL)
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**23,139.4**
3000		**SERVICIOS GENERALES**	**437,250.2**
	31401	Servicio Telefónico Convencional	1,188.6
	31501	Servicio de telefonía celular	47.0
	31701	Servicios de Conducción de Señales Analógicas y Digitales	176,035.2
	31904	Servicios Integrales de Infraestructura de Cómputo	101,294.6
	32301	Arrendamiento de Equipo y Bienes Informáticos	128,739.6
	33301	Servicios de Desarrollo de Aplicaciones Informáticas	29,945.2
		TOTAL	**460,389.6**

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

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 23,139.4 miles de pesos durante el ejercicio fiscal 2019; considerando 76 plazas, el promedio anual percibido por persona fue de 304.5 miles de pesos.

Del total ejercido en 2019 por 437,250.2 miles de pesos que corresponden al total de pagos asignados en contratos relacionados con las TIC, se erogaron 116,355.6 miles de pesos en dos contratos que representan el 26.6% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS EJERCIDOS DURANTE 2019
(Miles de pesos)

Procedimiento de contratación	Contrato/Convenio	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2019
				Del	Al	Mínimo	Máximo	
Licitación Pública Electrónica Nacional	411.413.31701.033BIS1/2017	Axtel S.A.B de C.V. en participación conjunta con Servicios Axtel, S.A. de C.V., Alestra S. de R.L., Servicios Alestra S.A. de C.V., B Drive IT, S.A. de C.V. e Integraciones Profesionales S.A. de C.V.	Servicio Integral de Comunicaciones para el Desarrollo Social (SICODES)	01/04/2017	31/03/2020	80,486.7	201,216.8	91,656.5
	1er. Convenio Modificatorio		Ampliación de vigencia del Contrato Abierto Plurianual 411.413.31701.033BIS1/2017					
	2do. Convenio Modificatorio		Ampliación en un 20% de los montos mínimo y máximo, así como de la vigencia del Contrato Abierto Plurianual 411.413.31701.033BIS1/2017					
Adjudicación Directa (Artículo 1 LAASSP)	DGTIC-413-33301-002-2019	INFOTEC, Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación	Servicios para el Desarrollo del Inventario, Control y Seguimiento de la Entrega-Recepción de las Tarjetas de Bienestar	10/06/2019	19/07/2019	0.0	24,699.1	24,699.1
		Totales				**80,486.7**	**225,915.9**	**116,355.6**

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

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

2. Contrato número 411.413.31701.033BIS1/2017 " Servicio Integral de Comunicaciones para el Desarrollo Social (SICODES) para los ejercicios 2017, 2018 y 2019" (Partida 2).

Se analizó la información del contrato número 411.413.31701.033BIS1/2017 y sus convenios modificatorios, celebrados con Axtel, S.A.B. de C.V., en participación conjunta con Servicios Axtel, S.A. de C.V.; Alestra, S. de R.L.; Servicios Alestra, S.A. de C.V.; B Drive IT, S.A. de C.V., e Integraciones Profesionales, S.A. de C.V., mediante licitación pública electrónica nacional de conformidad con los artículos 24, 25, primer párrafo, 26, fracción I, 26 BIS, fracción II, 27, 28, fracción I, 29, 30, 45 y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); 39, 81 y 85 del Reglamento de la LAASSP, con vigencia del 1 de abril de 2017 al 31 de marzo de 2020, por un monto mínimo de 80,486.7 miles de pesos y máximo de 201,216.8 miles de pesos, con el objeto de prestar el "Servicio Integral de Comunicaciones para el Desarrollo Social (SICODES) para los ejercicios 2017, 2018 y 2019" (Partida 2); con recursos del ejercicio 2019 se realizaron pagos por 91,656.5 miles de pesos; se determinó lo siguiente:

Alcance del servicio

Fortalecer la arquitectura tecnológica con soluciones de última generación que permitan la intercomunicación entre las áreas operativas y administrativas de la Secretaría, con servicios administrados de voz y datos, centro de operaciones de red (NOC) y cableado estructurado; el detalle de los servicios es el siguiente:

Servicios del contrato número 411.413.31701.033BIS1/2017
(Miles de pesos)

Descripción	Cantidad mínima total	Precios unitarios
SWITCH CORE TIPO 2	2	75.9
SWITCH DEPARTAMENTAL DE 24 PUERTOS PoE	60	5.6
SWITCH DEPARTAMENTAL DE 48 PUERTOS PoE	20	9.15
CONMUTADOR IP TIPO 1 (CORPORATIVO) HASTA 5000 USR	2	134.3
GATEWAY DE VOZ IP TIPO 1 (REMOTO) HASTA 100 USR	17	13.9
GATEWAY DE VOZ IP TIPO 2 (REMOTO) HASTA 50 USR	31	9.8
TELEFONO IP EJECUTIVO	10	0.3
TELEFONO IP SEMIEJECUTIVO	86	0.2
TELEFONO IP BASICO	1381	0.2
SOFTPHONE	25	0.1
CLIENTE MOVIL PARA SMARTPHONE	20	0.1
DIADEMA	25	0.1
MENSAJERIA UNIFICADA PARA CORREO ELECTRÓNICO Y CORREO DE VOZ	1102	0.1
TARIFICADOR DE LLAMADAS	4102	0.1
ACCESS POINT	50	2.6
CONTROLADORA WIRELESS	1	87.8
CABLEADO ESTRUCTURADO (NODOS DE COBRE)	6000	0.1
CABLEADO ESTRUCTURADO (NODOS DE FIBRA)	50	2.1
SERVICIO DE SUPERVISIÓN DE RED	3	49.9
MESA DE SERVICIO	1	18.8

Fuente: Información proporcionada por BIENESTAR mediante el oficio UAF/DGPP/410/0168/2020 de fecha 21 de enero de 2020.

Proceso de Contratación

En el estudio de factibilidad no se consideraron los costos de mantenimiento, soporte y operación que implican la contratación, vinculados con el factor de temporalidad más adecuado para determinar la conveniencia de adquirir, arrendar o contratar servicios; asimismo, no se estableció una cantidad máxima de bienes o servicios en el anexo de la convocatoria, únicamente se requirieron cantidades mínimas.

Pagos del Contrato

Las facturas no describen la cantidad, unidad de medida, concepto y precio unitario de cada uno de los componentes definidos en el detalle de los servicios del contrato, tampoco las actas de entrega-recepción de los entregables.

Entregables periódicos

- Los reportes de respaldos de los conmutadores de red de abril y junio de 2019 presentan inconsistencias ya que señalan fechas del año 2020.

- Se identificó que los reportes de tarificación correspondientes a enero, junio, agosto, septiembre y octubre de 2019, de conformidad con los metadatos (datos que describen el contenido informativo) de los archivos, fueron presentados en una fecha posterior a la entrega estipulada en la propuesta técnica.

Verificación de Equipos y Dispositivos

- De 1,978 servicios de telefonía IP se identificaron 56 dispositivos (2.8%) con número de serie repetido.

- En la revisión de las bitácoras del "Switch Core tipo 24 puertos PoE", no se identificó actividad durante nueve meses, lo que representó un riesgo para la seguridad de la información.

- Se detectaron 16 equipos con características inferiores a las establecidas en el Contrato.

Servicio del Centro de Operaciones de Red

- No se cuenta con un registro proactivo de solicitudes del sistema de monitoreo que indique la hora y el dispositivo que generó el evento.

- Se carece de un mecanismo para identificar, categorizar y mantener un control estadístico de la causa raíz de los problemas.

- El NOC no tiene la capacidad de aislar y solucionar los problemas presentados en los elementos de los nodos de red.

Mesa de servicio

- Del análisis efectuado a 77 solicitudes de servicio, 42 (54.5%) incumplen con los niveles de servicio establecidos del 99.98% y 99.90%. Se obtuvo que el monto de las deductivas representa en promedio el 3% sobre el importe del servicio, sin embargo, existen reportes que no fueron atendidos durante cinco meses; por lo anterior, el monto de las deductivas no es acorde con el impacto que han tenido las interrupciones en los servicios, lo que puede ocasionar la falta de atención y calidad en los servicios prestados por parte del proveedor.

- No se realizaron encuestas de satisfacción a los usuarios ni se efectuaron solicitudes de cambio por cada incidente registrado en la mesa de servicios.

- En la revisión de la herramienta de la Mesa de Servicio mediante las pruebas efectuadas por el grupo auditor, se identificó lo siguiente:

    - Carece de la funcionalidad para cambiar la prioridad de las solicitudes o incidentes de servicio.

    - No cuenta con un tablero de control central que permita proveer información y visualización en tiempo real del nivel del servicio objetivo de cada uno de los grupos de atención, reportes o usuarios.

    - No se identificó el procedimiento de cambios ni los formatos correspondientes para la operación y seguimiento de los casos.

- En la convocatoria de la licitación de los servicios se consideró la contratación de dos partidas, en las cuales se pactó la condición de contar con dos mesas de ayuda (una para cada partida), las cuales fueron adjudicadas al mismo proveedor. En las pruebas efectuadas por el grupo auditor al programa de gestión de la mesa de servicio, se identificó que se comparte la misma herramienta para el servicio prestado para ambas partidas, lo cual se confirmó con la extracción del historial de reportes, los cuales incluyen los servicios de ambos contratos; asimismo, en las propuestas técnicas presentadas por el proveedor, se observan las mismas características y especificaciones para la Mesa de Servicios; en consecuencia, se está pagando dos veces por el mismo servicio al mismo proveedor, sin que éste demuestre que se trata de dos herramientas y ambientes de servicio distintos e independientes; los pagos que se presumen duplicados son los siguientes:

Pagos duplicados asociados a la mesa de servicio del contrato número 411.413.31701.033BIS1/2017 (Partida 2)
(Pesos)

Mes	Descripción	A Mesas de servicio pagadas	B Mesas en uso	C=A-B Licencias que no se encuentran en uso	D Costos unitarios	E=C*D Pagos duplicados	Factura	Número de Cuenta por Liquidar Certificada (CLC)	Fecha de pago
nov-18	"MESA DE SERVICIOS"	2	1	1	21,779.76	21,779.76	885	5	08/04/2019
dic-18	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	891	10	22/04/2019
ene-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	905	36	27/12/2019
feb-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	933	37	27/12/2019
mar-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	934	58	31/12/2019
abr-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	956	62	31/12/2019
may-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	957	64	31/12/2019
jun-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	999	67	31/12/2019
jul-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1000	66	31/12/2019
ago-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1001	59	31/12/2019
sep-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1004	60	31/12/2019
oct-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1005	63	31/12/2019
nov-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1038	61	31/12/2019
dic-19	" MESA DE SERVICIOS "	2	1	1	21,779.76	21,779.76	1040	85-690	26/02/2020
					TOTAL	**304,916.71**			

Fuente: Información proporcionada mediante el oficio UAF/DGPP/410/0168/2020 de fecha 21 de enero de 2020 y Acta Administrativa Circunstancia de Auditoría 001/CP2019.

Lo anterior se realizó en incumplimiento de lo establecido en los artículos 1° de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 66, fracción III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; Actividad ADS 3 "Administrar la capacidad de la infraestructura de TIC" del Proceso de Administración de Servicios (ADS) del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, cláusulas tercera y décima quinta, del contrato núm. 411.413.31701.033BIS1/2017.

Se concluye que existen deficiencias en el análisis de la capacidad y disponibilidad de la infraestructura tecnológica para la contratación de los servicios; también se tienen inconsistencias en la operación de la mesa de servicios; así como fallas en la gestión del inventario de la infraestructura tecnológica; lo anterior representa un riesgo para la operación y continuidad de los servicios de comunicaciones de la dependencia.

2019-0-20100-20-0239-01-001 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los procedimientos para contar con un plan de capacidad y disponibilidad de la infraestructura tecnológica, el cual sirva como base para la definición de las especificaciones de los anexos técnicos para la contratación de servicios relacionados con la infraestructura tecnológica, así como para el análisis de las necesidades actuales y futuras de la secretaría en el uso eficiente de los recursos informáticos.

2019-0-20100-20-0239-01-002 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los controles de cambios, supervisión y validación de la gestión de inventarios y entregables de la infraestructura tecnológica, asimismo, establezca deductivas proporcionales al impacto operativo que causan los incumplimientos en los servicios, con la finalidad de asegurar el aprovisionamiento y operación de los equipos de cómputo y redes, así como mejorar la atención y calidad de los niveles de servicio para la infraestructura tecnológica y comunicaciones de la secretaría.

2019-0-20100-20-0239-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 304,916.71 pesos (trescientos cuatro mil novecientos dieciséis pesos 71/100 M.N.), por razón de pagos duplicados debido a que se identificó que se comparte la misma herramienta para la gestión de la mesa de servicios en dos contratos distintos adjudicados al mismo proveedor, cada uno de los cuales debe tener su propia mesa de servicios, lo cual se confirmó con la extracción del historial de reportes que incluyen los servicios de ambos contratos; asimismo, en las propuestas técnicas presentadas por el proveedor, se observan las mismas características y especificaciones para la mesa de servicios, aunado a que no se demostró que se trata de dos herramientas y ambientes de servicio distintos e independientes, en incumplimiento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, y su reforma publicada el 23 de julio de 2018: Proceso Administración de Servicios (ADS), Actividad ADS 3 Administrar la capacidad de la infraestructura de TIC; y del contrato 411.413.31701.033BIS1/2017, cláusulas tercera y décima quinta.

Causa Raíz Probable de la Irregularidad

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

3. Contrato número DGTIC-413-33301-002-2019 "Servicios para el Desarrollo del Inventario, Control y Seguimiento de la Entrega-Recepción de las Tarjetas de Bienestar"

Se analizó el contrato número DGTIC-413-33301-002-2019 celebrado con INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), mediante Adjudicación Directa, con fundamento en los artículos 1o, párrafo quinto, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y 4o. de su Reglamento, con vigencia del 10 de junio al 19 de julio de 2019, por un monto de 24,699.1 miles de pesos, con objeto de proporcionar los "Servicios para el desarrollo del inventario, control y seguimiento de la entrega-recepción de las tarjetas bancarias de Bienestar, para los beneficiarios de los programas sociales"; durante el ejercicio 2019 se realizaron los pagos por el monto total del contrato; se determinó lo siguiente:

Alcance de la contratación

Desarrollar una aplicación para los programas sociales de la Secretaria de Bienestar que incluya los módulos siguientes:

Módulos solicitados del Contrato número DGTIC-413-33301-002-2019

Requerimiento	Módulo
1	Inventario de tarjetas bancarias de Bienestar para los beneficiarios de programas sociales
2	Configuración de una plataforma de desarrollo, en conjunto con los componentes necesarios para la administración de usuarios y permisos
3	Control de la tarjeta Bienestar en la entrega-recepción
4	Tableros de control
5	Reportes de avance

Fuente: Elaborado con información proporcionada por BIENESTAR mediante oficio UAF/DGPP/410/0168/2020 de fecha 21 de enero de 2020.

Lo anterior consideró la automatización de los procesos de negocio asociados al manejo del inventario, así como la solicitud para la atención al Programa Pensión de Adultos Mayores que consta de 8,055,472 beneficiarios, realizada por la Dirección General de Atención a Grupos Prioritarios de la Secretaría.

Investigación de Mercado

No se cuenta con evidencia documental de un análisis de las propuestas técnicas presentadas por los proveedores que considere las condiciones en cuanto a los plazos y lugares de la prestación de los servicios; la forma y términos de pago; las características técnicas de los servicios, así como las demás circunstancias que resulten aplicables y que permitan la comparación objetiva entre servicios iguales o de la misma naturaleza. Adicionalmente, la secretaría carece de una metodología de estimación de costos de los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de las

soluciones tecnológicas, que permita acreditar la razonabilidad de los precios propuestos por los proveedores participantes.

Proceso de Contratación

- El apoderado legal de INFOTEC celebró una acta de hechos con la secretaría, en la que dio a conocer la infraestructura que tenía para el desarrollo del aplicativo e hizo entrega de 110 curriculum vitae del personal asignado al proyecto.

- El grupo auditor comparó la información del personal asignado al proyecto con la plantilla del personal que laboró en INFOTEC durante el ejercicio 2019; se detectó que de los 110 recursos humanos asignados al contrato con BIENESTAR, sólo 21 (19.0%) corresponden al personal contratado por INFOTEC.

- Por otra parte, INFOTEC presentó un Balance General de Estado de Resultados y un Estado de Situación Financiera al 31 de diciembre de 2018, donde se enlistan los activos, pasivos y patrimonio de la Institución, con utilidad negativa, por lo que no contaba con la capacidad económica para cumplir con sus obligaciones.

- Se detectó que en las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios (POBALINES) de BIENESTAR, para las contrataciones que se realicen entre entes públicos, sólo se requiere presentar un escrito bajo protesta de la persona facultada en el ente público que cuenta con la capacidad técnica, material y humana para la realización del objeto del contrato; no obstante, las POBALINES no consideran lo establecido en el Oficio Circular mediante el cual se emiten diversas directrices para los Oficiales Mayores de las dependencias y equivalentes en las entidades de la Administración Pública Federal y titulares de los Órganos Internos de Control, que deberán observarse en las contrataciones que se realicen entre entes públicos, las cuales señalan que el proveedor debe presentar los documentos en los que conste fehacientemente su capacidad para cumplir con las obligaciones.

Entregables del servicio

- Los entregables, tales como las historias de uso del sistema, casos de prueba y la memoria técnica, no cuentan con la validación técnica por parte de BIENESTAR.

- No se tienen las historias de usuarios y casos de prueba para todas las funcionalidades establecidas en el Anexo Técnico; tal es el caso de la conexión con los aplicativos “Diagnóstico” y “SIDER (Sistema Integral para el Desarrollo Regional)”; por lo tanto, no se cuenta con toda la documentación requerida para cada una de las funcionalidades solicitadas.

- Se observaron inconsistencias en las fechas de elaboración y modificación de los entregables; tal es el caso de documentos que fueron generados meses previos al

inicio del contrato, como el Backlog de requerimientos y el Manual de usuario, o entregables que fueron modificados en fechas posteriores a la entrega de los mismos, como la Historia de uso “HU5.2”, Caso de prueba “CP Administración” y la Memoria técnica de Instalación.

- En los entregables "Documento de Planeación" y "Stakeholders", el proveedor manifestó que para el desarrollo del sistema se requerían de 110 recursos humanos; al respecto, se identificó lo siguiente:

    - De la revisión de los Curriculum Vitae de dichos recursos, se obtuvo que tres personas (2.7%) no cumplen con el perfil y la experiencia requerida.

    - De los 110 recursos asignados al proyecto, únicamente se constató la participación de 11 (10.0%) en la elaboración, revisión y aprobación de los entregables, minutas de planeación y operación, así como en el desarrollo del código del sistema; de estos recursos, sólo se encontraron cinco en la plantilla del personal de INFOTEC.

    - Se carece de controles que permitan dar seguimiento a las actividades realizadas por el personal del proveedor durante la ejecución del servicio; asimismo, no se tienen bitácoras de actividades ni listas de asistencia del personal para acreditar los trabajos realizados.

Análisis del Código Fuente

- En la revisión de 45 archivos de código, se detectó que 32 (71.1%) fueron generados previamente a la firma del contrato, ocho carecen de fecha de creación y cinco se encuentran dentro de la vigencia del contrato.

- Como resultado del análisis de las líneas de código, se identificaron 124 errores del programa, 170 deficiencias en el diseño del software y 108 bloques de código duplicado.

Pruebas de la funcionalidad del sistema

Del recorrido de pruebas realizadas por el grupo auditor al sistema se identificó lo siguiente:

- De un universo de 81 pruebas para comprobar la funcionalidad del sistema, en 11 casos (14.6%) se cumplieron los criterios técnicos, 30 casos (36.6%) se efectuaron con datos de prueba que no corresponden al volumen del padrón de pensión de adultos mayores para validar el comportamiento de los programas, y en 40 casos (48.8%) no se pudo comprobar su funcionamiento de conformidad con el anexo técnico del contrato, debido a que los usuarios finales responsables de la operación del sistema no se presentaron para realizar las pruebas.

- El sistema no realiza validaciones en la carga de la información, debido a que se identificaron campos sin valores como la “fecha de recepción”, “remesa” y “responsable”; asimismo, el sistema no despliega el registro de los usuarios que acceden utilizando el Sistema Integral para el Desarrollo Regional (SIDER), lo que incumple con lo descrito en el Anexo Técnico del Contrato.

- No se cuenta con la opción "Inventario Banco" y "Carga Inventario Banco" desde el menú de Administración; por lo tanto, para consultar el inventario es necesario entrar al total de tarjetas y filtrar por banco, situación que modifica el diseño previsto del sistema; asimismo, se carece de la documentación que acredite la solicitud de dicho cambio, así como de la actualización de éste en la documentación del sistema.

- De un total de 1,769,949 tarjetas que se encuentran cargadas en el sistema, 136 están como "Tarjetas por aceptar" y sólo 23 se encuentran como "Tarjetas asignadas", las cuales tienen fecha de recepción de enero a abril 2019; esto es, fueron procesadas de manera previa a la firma del contrato. Esta situación pone de manifiesto que el aplicativo no se encuentra en operación para el cumplimiento del objeto del contrato, aunado a que el sistema fue requerido para la entrega de apoyos a beneficiarios del programa Pensión para Adultos Mayores con un padrón activo de 8,055,472 personas, y dado que sólo se han asignado 23 tarjetas y ninguna ha sido entregada, se confirma que los datos que se encuentran en el sistema son de prueba, aun cuando han pasado más de 11 meses de la terminación del contrato.

- No fue posible validar 40 funcionalidades del sistema, tales como la impresión de un acuse con código QR, las notificaciones por correo electrónico, el seguimiento de tarjetas, las transacciones a la base de datos (altas, cambios y bajas), así como la interconexión con el sistema Integral para el Desarrollo Regional (SIDER), entre otras, debido a que los funcionarios de la Dirección General de Atención a Grupos Prioritarios (DGAGP) no se presentaron para realizar las pruebas de las que son responsables de conformidad con la cláusula décima segunda del contrato, aun cuando fueron citados por la Auditoría Superior de la Federación, con la finalidad de realizar reuniones y entrevistas de trabajo para conocer el ejercicio de sus funciones durante la gestión del contrato sujeto a revisión.

Por lo anterior, no fue posible comprobar el cumplimiento de todas las funcionalidades descritas en el anexo técnico, aunado a que el sistema no ha realizado el objeto y alcance del contrato, debido a las inconsistencias en los entregables, a los errores en la programación, así como por los datos de prueba que demuestran que el sistema no se encuentra en operación en el ambiente productivo; por lo tanto, se presumen pagos injustificados por servicios no devengados con el detalle siguiente:

Pagos injustificados por el desarrollo del Sistema del Inventario, Control y Seguimiento de la Entrega-Recepción de las Tarjetas Bienestar, relativos al contrato número DGTIC-413-33301-002-2019
(Pesos)

Periodo	Concepto	Número de Cuenta por Liquidar Certificada (CLC)	Número de la factura	Fecha de pago	Importe pagado
Del 10 de junio al 19 de julio de 2019	Pago correspondiente al anticipo del 40% que se menciona en la cláusula VIII del contrato.	13	F 16445	25/06/2019	9,879,636.48
Del 10 de junio al 19 de julio de 2019	Pago correspondiente al finiquito del 60% restante	15	F 16606	30/07/2019	14,819,454.72
				Total	**24,699,091.20**

Fuente: Elaborado con información proporcionada por la Secretaría de Bienestar, mediante oficio UAF/DGPP/410/0168/2020 de fecha 21 de enero de 2020.

Lo anterior se realizó en incumplimiento de lo establecido en los artículos 1° de la Ley de Presupuesto y Responsabilidad Hacendaria; 66, fracción III, del reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; apartado "Antecedentes y “Alcance de la contratación" del formato APCT-F2 del Proceso de Administración del Presupuesto y las Contrataciones del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, última reforma publicada el 23 de julio de 2018, cláusulas primera y décima segunda, del contrato número DGTIC-413-33301-002-2019, y del apartado "Objeto del Servicio", “Descripción del Servicio o Bienes Requeridos” y “Alcance” del anexo técnico del contrato número DGTIC-413-33301-002-2019.

Desarrollo de Soluciones Tecnológicas

En la revisión de los controles para el desarrollo de soluciones tecnológicas se observó lo siguiente:

- Se carece de un procedimiento con los criterios y las actividades para la gestión y administración de cuentas de usuario y la asignación de perfiles, asimismo, no se generan cartas responsivas de los usuarios dados de alta en el sistema.

- No se cuenta con un repositorio actualizado con los parámetros o estándares de configuración para todos los componentes del sistema, así como la generación de listas de acceso, informe de cambios, configuraciones de las herramientas y scripts de pruebas.

- Se carece de un programa de capacidad que permita conocer los niveles de servicio acordados, el crecimiento previsto de la demanda de infraestructura, así como la incorporación de los nuevos servicios de TIC.

- No se tiene un procedimiento de atención y solución de los incidentes, fallas y requerimientos presentados durante el desarrollo y operación del sistema, que

permita conocer las fallas más recurrentes, así como la implementación de sus soluciones.

- No se observan mecanismos de protección para información sensible que es enviada sobre la red (interna y externa), ni se utilizan protocolos de cifrado para proteger los datos como nombres de usuario, contraseñas o datos de tarjetas de crédito; asimismo, no se tiene evidencia del análisis de vulnerabilidades previo a la puesta en operación del aplicativo.

- Se carece de pistas de auditoría y bitácoras de acceso al aplicativo, por lo que no es posible detectar oportunamente movimientos irregulares o cambios no autorizados.

Se concluye que la investigación de mercado no aseguró que se cuente con las mejores condiciones disponibles para el Estado; el proveedor no acreditó la capacidad humana y económica para cumplir con sus obligaciones; se carece de controles para acreditar las actividades desarrolladas por el prestador de servicio en el desarrollo de los sistemas; no fue posible comprobar el cumplimiento de todas las funcionalidades descritas en el anexo técnico; se detectaron inconsistencias en los entregables, errores en la programación del sistema, así como datos de prueba que confirman que el sistema no se encuentra en operación en el ambiente productivo; se tienen inconsistencias en la metodología para el desarrollo de sistemas en los controles relativos al control de accesos, análisis de vulnerabilidades de los aplicativos, seguridad de la información desde el diseño de los sistemas, así como en el monitoreo de las bitácoras y registros de auditoría.

2019-0-20100-20-0239-01-003 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los procedimientos para realizar investigaciones de mercado que consideren la forma, términos de pago y el análisis de las características técnicas de los bienes o servicios por contratar, así como implementar una metodología para la estimación del costo de los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de las soluciones tecnológicas con la finalidad de contar con una comparación objetiva entre bienes o servicios iguales o de la misma naturaleza, así como asegurar las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento y oportunidad.

2019-0-20100-20-0239-01-004 **Recomendación**

Para que la Secretaría de Bienestar homologue sus Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios, con lo establecido en el Oficio Circular mediante el cual se emiten diversas directrices para los Oficiales Mayores de las dependencias y equivalentes en las entidades de la Administración Pública Federal y titulares de los Órganos Internos de Control, que deberán observarse en las contrataciones que se realicen entre entes públicos, con la finalidad de que los servicios prestados aseguren las mejores condiciones para la secretaría.

2019-0-20100-20-0239-01-005 **Recomendación**

Para que la Secretaría de Bienestar establezca como entregables las bitácoras de actividades del personal que se asigne para la ejecución de los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de aplicativos de cómputo; asimismo, fortalezca los mecanismos de verificación en el cumplimiento de los perfiles del personal y especializaciones técnicas requeridas para el desarrollo de las actividades con la finalidad de constatar el cumplimiento de las actividades y tiempos establecidos en las estimaciones del costo de los servicios, así como asegurarse de que el personal del proveedor tiene las competencias y experiencia requeridas para la prestación de los servicios.

2019-0-20100-20-0239-01-006 **Recomendación**

Para que la Secretaría de Bienestar fortalezca la metodología de desarrollo de sistemas para considerar el control de accesos a los sistemas, análisis de vulnerabilidades de los aplicativos antes de su puesta en marcha, seguridad de la información desde el diseño de los sistemas, así como el monitoreo de las bitácoras y registros de auditoría con la finalidad de asegurar que los sistemas o servicios de TIC sean construidos, instalados, probados y desplegados eficientemente en el ambiente productivo.

2019-0-20100-20-0239-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 24,699,091.20 pesos (veinticuatro millones seiscientos noventa y nueve mil noventa y un pesos 20/100 M.N.), por razón de los pagos injustificados por servicios no devengados derivados de la falta de comprobación del cumplimiento de todas las funcionalidades descritas en el Anexo Técnico para la operación del Sistema de Inventario, Control y Seguimiento de la Entrega-Recepción de las Tarjetas Bancarias de Bienestar, aunado a que el sistema no ha realizado el objeto y alcance del contrato, debido a las inconsistencias en los entregables, a los errores en la programación, así como por la falta de operación del sistema en el ambiente productivo, aun cuando han pasado más de 11 meses de la terminación del contrato, en incumplimiento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, y su reforma publicada el 23 de julio de 2018, Apartado Antecedentes y Alcance de la Contratación del formato APCT-F2 del Proceso de Administración del Presupuesto y las Contrataciones; del contrato número DGTIC-413-33301-002-2019, cláusula primera y décima segunda, y del anexo técnico del contrato número DGTIC-413-33301-002-2019, Apartado Objeto del Servicio, Descripción del Servicio o Bienes Requeridos y Alcance.

Causa Raíz Probable de la Irregularidad

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

4. Ciberseguridad

En el análisis de la información relacionada con la administración y operación de los controles de ciberseguridad vinculados con la infraestructura y soluciones tecnológicas, de conformidad con los procesos del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, las mejores prácticas de sus apéndices, así como con las políticas y lineamientos de la secretaría, se observó lo siguiente:

Inventario y control de activos de hardware

- Se carece de herramientas de descubrimiento activo y pasivo para identificar equipos y dispositivos conectados a la red, con la finalidad de actualizar de forma automática el inventario de activos.

- El inventario de activos de hardware no registra las direcciones de red, nombre, propósito, responsable, ubicación, así como el estado del activo para estar conectado o bloqueado a la red.

- Se desconoce si los activos no autorizados se eliminan de la red, se ponen en cuarentena o se actualizan en el inventario periódicamente.

- No se tiene implementado el control de acceso a nivel de puertos para limitar y controlar los equipos que pueden autenticarse en la red, de tal forma que sólo se conecten los equipos autorizados.

Inventario y control de activos de software

- No se cuenta con listas blancas de scripts, librerías y software para las operaciones.

- Se carece de herramientas para documentar el inventario de software autorizado con atributos como nombre, versión, autor, equipo y fecha de instalación.

- No se tienen procedimientos para la eliminación de software no autorizado.

Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

- Se carece de estándares de configuración de seguridad para todos los sistemas operativos y software autorizados.

- No se cuenta con imágenes o plantillas seguras para todos los sistemas de conformidad con los estándares de configuración aprobados por la secretaría.

- No se tienen implementadas herramientas automatizadas que detecten y regresen los parámetros de configuración en los equipos y sistemas en caso de accesos no autorizados.

- No se cuenta con un sistema de monitoreo para verificar todos los elementos de configuración de seguridad, excepciones aprobadas por catálogo y que alerte cuando ocurran cambios no autorizados.

Evaluación continua de la vulnerabilidad y solución

- Se carece de una herramienta de análisis de vulnerabilidades para escanear automáticamente todos los sistemas en la red de manera periódica, para identificar las vulnerabilidades potenciales en los sistemas de la secretaría.

- No se realizan comparaciones de los resultados del análisis de vulnerabilidades para verificar que se hayan remediado de manera oportuna.

- No se tiene un proceso de calificación de riesgo para priorizar la corrección de las vulnerabilidades descubiertas.

Uso controlado de privilegios administrativos

- No se tienen herramientas automatizadas para realizar el inventario de las cuentas administrativas, incluidas las cuentas de dominio y locales.

- No se asegura que las cuentas administrativas estén asignadas a funcionarios autorizados y que éstos las usen para las tareas designadas.

- No se utiliza la autenticación multi factor y canales encriptados para el acceso de las cuentas del administrador local, super-usuario o cuentas de servicio, tampoco se tiene evidencia del uso de contraseñas únicas para este tipo de cuentas.

- No se tiene una computadora dedicada (consola) para todas las tareas administrativas o aquellas que requieren acceso administrativo.

- No se restringe el acceso a las herramientas para el desarrollo de código.

- Las políticas de contraseñas no se encuentran formalizadas.

Mantenimiento, monitoreo y análisis de bitácoras de auditoría

- Los dispositivos de red no recuperan información de tiempo de manera periódica, para que las marcas de tiempo en los registros sean consistentes.

Protección de correo electrónico y navegador web

- Se carece de evidencia de la restricción del uso de lenguajes de codificación en navegadores web.

Defensa contra malware

- No se documenta, supervisa, ni limita el uso de dispositivos externos conectados a la red de la secretaría.

Capacidad de recuperación de datos

- No se realizan pruebas de la integridad de los datos en las copias de respaldo de forma periódica.

Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

- No se tienen configuraciones de seguridad estandarizadas en los equipos, ni alertas cuando se realizan modificaciones a las mismas.

- No se cuenta con la gestión de los equipos de red utilizando autenticación multi factor, ni sesiones cifradas.

- Se carece del uso automatizado de herramientas para verificar las configuraciones de dispositivos estándar, así como la detección de cambios.

Seguridad perimetral

- Se carece de sistemas de detección de intrusos (IDS).

- No se cuenta con autenticación de múltiples factores para el acceso remoto a los sistemas de la secretaría.

Protección de datos

- No se cuenta con una herramienta automatizada en el perímetro de la red para el monitoreo de la transferencia no autorizada de información sensible, así como el

bloqueo de dichas transferencias mientras alerta al personal de seguridad de la información.

- Se carece de políticas y sistemas automatizados para restringir el uso de medios extraíbles.

- No se cuenta con el cifrado de dispositivos de almacenamiento del tipo puerto de seriado universal (USB) para los datos almacenados.

Control de acceso basado en necesidad de conocimiento

- Se carece de una herramienta de descubrimiento activo para identificar toda la información sensible almacenada, procesada o transmitida por las soluciones tecnológicas de la Secretaría.

- No se cuenta con listas de control de acceso específicas para el sistema de archivos, uso compartido de redes, aplicaciones o bases de datos.

Control de acceso inalámbrico

- No se cuenta con un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.

- No se tiene deshabilitada la conexión inalámbrica de Bluetooth, ni la Comunicación de Campo Cercano (NFC) en los equipos personales.

Supervisión y monitoreo de cuentas

- No se cuenta con autenticación de múltiples factores para las cuentas de usuario en los sistemas.

- No se tiene un proceso automatizado para revocar el acceso a los sistemas mediante la desactivación de cuentas por la terminación o el cambio de responsabilidades de los empleados o proveedores, así como de la suspensión después de un período de inactividad establecido.

- Las cuentas carecen de una fecha de vencimiento forzada y no se tiene evidencia de su monitoreo.

- No se cuenta con alertas en los casos en que los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora o el día, la ubicación de la estación de trabajo y la duración de la sesión.

Implementar un programa de concientización y entrenamiento de seguridad

- La secretaría no realizó un análisis para comprender las habilidades y comportamientos del personal relativas a la seguridad de la información.

- No se cuenta con capacitación para fortalecer los conocimientos y actitudes del personal sobre la seguridad de la información.

- No se definió un programa de concientización de seguridad de la información para todo el personal involucrado, el cual debe ser actualizado y difundido de manera continua.

- No se tiene evidencia de capacitación sobre la importancia de habilitar y utilizar la autenticación segura, así como en temas de ingeniería social y suplantación de identidad.

- Se carece de capacitación para identificar, almacenar, transferir, archivar y destruir información confidencial de manera adecuada.

Seguridad del software de aplicación

- No es posible asegurar que se lleva a cabo la verificación y documentación de errores para todas las entradas de datos en los sistemas de la secretaría.

- No se verifica que la versión del software externo cuente con soporte del desarrollador.

- No se lleva a cabo una validación para utilizar componentes actualizados y de confianza en el software desarrollado por la secretaría.

- No se utilizan algoritmos de cifrado revisados y estandarizados.

- Se carece de capacitación para el personal de desarrollo de sistemas para escribir código seguro en su entorno de desarrollo y responsabilidades específicas.

- No se tienen herramientas para verificar el cumplimiento de las prácticas de codificación segura para el software desarrollado internamente.

- No se tiene definido un proceso para la aceptación y tratamiento de los reportes de las vulnerabilidades del software.

- No se cuenta con cortafuegos de aplicaciones web (WAF) con objeto de inspeccionar todo el tráfico que fluye a través de las aplicaciones en ambiente web.

- Se carece de plantillas para el endurecimiento de las configuraciones (hardening) de los sistemas críticos que soportan los procesos de la secretaría.

Respuesta y manejo de incidentes de ciberseguridad

- No se cuenta con un plan institucional de respuesta a incidentes de ciberseguridad, ni las fases documentadas para el manejo y gestión de los incidentes.

- Se carece de la definición de los cargos y responsabilidades para el manejo de incidentes, tampoco se cuenta con la documentación durante el incidente y hasta su resolución.

Pruebas de penetración y ejercicios de equipo rojo

- En la secretaría no se estableció un programa para pruebas de penetración, por lo que no se tienen definidas pruebas periódicas de intrusiones externas e internas ni equipo rojo, para identificar vulnerabilidades en los sistemas.

- Se carece de un ambiente de pruebas que imite un entorno de producción para los ensayos de penetración específicos y ataques del equipo rojo, contra elementos que normalmente no se prueban en el ambiente productivo.

Evaluación de los controles y medidas de Ciberdefensa de la Secretaría de Bienestar

Control	Indicador	Cumplimiento
Inventario y control de activos hardware	🟡	37.5%
Inventario y control de activos software	🔴	0.0%
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	🔴	20.0%
Evaluación continua de la vulnerabilidad y Solución	🟡	42.9%
Uso controlado de privilegios administrativos	🔴	0.0%
Mantenimiento, monitoreo y análisis de bitácoras de auditoría	🟢	80.0%
Protección de correo electrónico y navegador web	🟢	70.0%
Defensa contra malware	🟢	87.5%
Capacidad de recuperación de datos	🟢	80.0%
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	🟡	37.5%
Seguridad Perimetral	🟢	66.7%

Evaluación de los controles y medidas de Ciberdefensa de la Secretaría de Bienestar

Control	Indicador	Cumplimiento
Protección de datos	🔴	0.0%
Control de acceso basado en necesidad de conocimiento	🟡	44.4%
Control de acceso inalámbrico	🟡	30.0%
Supervisión y monitoreo de cuentas	🟡	38.5%
Implementar un programa de concientización y entrenamiento de seguridad	🔴	0.0%
Seguridad del Software de Aplicación	🔴	9.1%
Respuesta y Manejo de Incidentes	🟡	29.0%
Pruebas de penetración y ejercicios de equipo rojo	🔴	33.3%

Fuente: Elaborado con información proporcionada por la Secretaría de Bienestar mediante el oficio BIE/413/0158/2020 de fecha 26 de marzo de 2020 y el Acta Circunstanciada de Auditoria 008/CP2019.

🟢 Cumplimiento aceptable

🟡 Requiere fortalecer el control

🔴 Controles insuficientes

De la revisión de los procedimientos para la Gestión de la Ciberseguridad, se concluye que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la Secretaría de Bienestar son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIAS EN LOS CONTROLES DE CIBERSEGURIDAD

Control	Riesgo
Inventario y control de activos hardware	Los dispositivos no autorizados pueden no ser detectados y obtener acceso a los sistemas para realizar acciones indebidas.
Inventario y control de activos software	No se cuenta con la capacidad de evitar la instalación y ejecución de software no autorizado por la Secretaría.
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	La falta de estandarización de configuraciones de seguridad, así como la carencia de un sistema de monitoreo de las mismas, pueden propiciar que los atacantes exploten los servicios en la red, así como el software de la Secretaría.
Evaluación continua de la vulnerabilidad y Solución	La falta de escaneo de los sistemas y las redes para revisarlos de manera frecuente e identificar las vulnerabilidades, con la finalidad de remediar las debilidades encontradas, así como la falta de calificación del riesgo, pueden provocar limitaciones para identificar, remediar y minimizar la ventana de oportunidades para los atacantes.
Uso controlado de privilegios administrativos	La carencia de los controles relativos al inventario de todas las cuentas administrativas, incluidas las cuentas de dominio y locales, autenticación multi factor para el acceso administrativo, cambios de contraseñas por defecto, así como el registro y alerta de cambios, tiene el riesgo de que un posible ataque se extienda en las redes y controle los equipos críticos.

Control	Riesgo
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	Al no tener restricción del uso de lenguajes de codificación en navegadores web, se tiene la posibilidad de la explotación de configuraciones y servicios vulnerables por parte de los posibles atacantes.
Control de acceso basado en necesidad de conocimiento	La falta de monitoreo para el descubrimiento de información sensible, listas de control de acceso específicas para el sistema de archivos, uso compartido de redes, aplicaciones o bases de datos, propicia la pérdida de control sobre los datos protegidos y/o sensibles.
Control de acceso inalámbrico	No se cuenta con la capacidad de mitigar la explotación de redes vulnerables para evitar un posible robo de datos.
Supervisión y monitoreo de cuentas	La falta de gestión activa del ciclo de vida de las cuentas del sistema (creación, uso, latencia, eliminación) conlleva al incremento de oportunidades para cualquier ataque.
Implementar un programa de concientización y entrenamiento de seguridad	No se identifican los conocimientos, habilidades, brechas y capacidades de los funcionarios, las cuales son necesarias para el soporte de la seguridad de la información a través de políticas, capacitación y programas de concientización.
Seguridad del Software de Aplicación	Debido a la falta de capacidad para prevenir, detectar y corregir las debilidades de seguridad en los sistemas desarrollados por la Secretaría, es posible que se tengan vulnerabilidades que puedan ser explotadas para acciones indebidas.
Respuesta y Manejo de Incidentes	No se tienen documentados los procedimientos de respuesta a incidentes ni las fases para su preparación, detección, análisis, contención, erradicación y recuperación, lo que puede ocasionar la pérdida de la confidencialidad, integridad y disponibilidad de la información.
Pruebas de penetración y ejercicios de equipo rojo	La carencia de pruebas de penetración a la infraestructura y soluciones tecnológicas, puede poner en riesgo la operación de la dependencia al no identificar las vulnerabilidades y vectores de ataque que tienen las redes y sistemas.

Fuente: Elaborado con información proporcionada por la Secretaría de Bienestar mediante el oficio BIE/413/0158/2020 de fecha 26 de marzo de 2020 y el Acta Circunstanciada de Auditoria 008/CP2019.

Por lo anterior, se detectan irregularidades en las políticas, procedimientos y normativa interna de la secretaría relacionadas con la ciberseguridad, debido a las deficiencias en los controles de inventario de software autorizado y no autorizado; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; uso controlado de privilegios administrativos; protección de datos; implementar un programa de concientización y entrenamiento de seguridad; seguridad del software de aplicación; respuesta a incidentes y gestión, así como las pruebas de penetración y ejercicios de equipo rojo; lo anterior podría causar un impacto negativo en la seguridad de la información de la secretaría, así como en la confidencialidad, integridad y disponibilidad de la información de los beneficiarios de los diversos programas sociales a los que brinda servicios.

2019-0-20100-20-0239-01-007 **Recomendación**

Para que la Secretaría de Bienestar implemente políticas y procedimientos para el uso controlado de privilegios administrativos; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; seguridad del software de aplicación; protección de los datos, así como para la implementación de un programa de concientización y entrenamiento en seguridad de la información para los usuarios finales con la finalidad de aumentar el nivel de seguridad de

las contraseñas, estandarizar las configuraciones de seguridad de los dispositivos y equipos, corregir las debilidades de seguridad en el desarrollo de sistemas y concienciar a los usuarios sobre los mecanismos de ciberdefensa, para mejorar la gestión de la seguridad de la información en la secretaría.

2019-0-20100-20-0239-01-008 **Recomendación**

Para que la Secretaría de Bienestar fortalezca los controles y procedimientos para el inventario de software/hardware autorizado y no autorizado; el plan de respuesta a incidentes de ciberseguridad, así como las pruebas de penetración a las redes y sistemas al menos semestralmente; con la finalidad de asegurar que la operación de la infraestructura y soluciones tecnológicas se realiza de conformidad con los objetivos de la seguridad informática, para mejorar la capacidad de protección de las redes y sistemas, así como garantizar su recuperación en caso de un ataque cibernético.

2019-9-20113-20-0239-08-001 **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 ciberseguridad en la infraestructura y soluciones tecnológicas, omitieron atender las recomendaciones números 2017-0-20100-15-0261-01-005 y 2017-0-20100-15-0261-01-006 emitidas en el Informe Individual de Auditoría número 261-DS de la Fiscalización Superior de la Cuenta Pública 2017, debido a que entregaron un plan de trabajo con tres niveles de maduración donde cada nivel tendría una duración de un año, para 2019 informaron que se implementaría lo establecido en el plan de trabajo con lo elemental sobre un sistema de información social integral atendiendo a todas las recomendaciones, sin embargo, las deficiencias señaladas en las recomendaciones persisten en los controles asociados al inventario de software autorizado y no autorizado; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; uso controlado de privilegios administrativos; protección de datos; implementar un programa de concientización y entrenamiento de seguridad; seguridad del software de aplicación; respuesta a incidentes y gestión, así como las pruebas de penetración y ejercicios de equipo rojo. Lo anterior puede causar un impacto negativo en la seguridad de los activos de información, así como en la confidencialidad, integridad y disponibilidad de la información de los beneficiarios de los distintos programas sociales de la secretaría, en incumplimiento de la Ley General de Responsabilidades Administrativas, publicada en el Diario Oficial de la Federación el 18 de julio de 2016, artículo 7, fracciones I y V; del Reglamento Interior de la Secretaría de Bienestar, con última reforma publicada el 24 de abril de 2018, artículo 31, fracción I; del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual de Aplicación General en dichas materias publicado en el DOF el 8 de mayo

de 2014, con última reforma publicada en el DOF el 23 de julio de 2018, artículos 16, fracción III, y 18; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, con última reforma publicada en el DOF el 23 de julio de 2018, Numeral 9, Reglas generales; del Proceso de Administración de Servicios (ADS), Regla del proceso 2; ADS 3, Factor crítico 4; del Proceso de Administración de la Seguridad de la Información (ASI), ASI 6, Factor crítico 1, inciso a, y del Apéndice IV.B Matriz de Metodologías, Normas y Mejores Prácticas Aplicables a la Gestión de las TIC, Requerimientos de Técnicas de seguridad - Sistemas de gestión de seguridad de la información ISO/IEC FDIS 27001:2013, apartados A.7, A.7.2, A.8, A.8.1, A.8.3, A.9, A.9.4, A.12, A.12.2, A.12.6, A.12.7, A.13, A.13.1.

5. Continuidad de las Operaciones de TIC

En el análisis de la información proporcionada por la Secretaría para la Continuidad de las Operaciones, de conformidad con los controles de los Procesos de Administración de Servicios, Administración de la Operación y Administración de la Seguridad de la Información del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, se observó lo siguiente:

- Se carece de los criterios y evaluaciones para determinar los activos de información críticos.

- No se cuenta con un procedimiento para la definición, análisis, planificación, medición y mejoramiento de la disponibilidad de los servicios de TIC, por lo tanto, no se puede asegurar la pronta recuperación de la infraestructura, aplicativos y servicios críticos en caso de interrupciones.

- El programa de continuidad no describe el plan de gestión de incidentes de ciberseguridad; asimismo, en relación con el Tiempo Objetivo de Recuperación (RTO), Punto Objetivo de Recuperación (RPO) y Plazo Máximo Tolerable de Interrupción (MTPD), no se cuenta con los criterios para definir dichas métricas, tampoco se identifican los activos de información críticos a los que hacen referencia.

- No se han realizado pruebas al programa de continuidad de las operaciones ni se tiene constancia de los planes que se tienen para tal efecto.

- Se carece de un Análisis de Impacto al Negocio (BIA) para identificar las necesidades de la dependencia en términos de recuperación, sobre todo aquellas que se consideran críticas para su funcionamiento, con la finalidad de contar con la capacidad de recuperación de los procesos, sistemas y servicios que se ofrecen a la ciudadanía.

- No se tiene un Plan de Recuperación de Desastres (DRP), para reducir al máximo los efectos de un desastre en las funciones de la dependencia, de tal manera qué ante cualquier eventualidad, las áreas de Tecnologías de la Información sean capaces de reanudar rápidamente sus funciones.

- No se cuenta con un programa de capacidad que asegure la operación de los servicios de TIC, conforme a los compromisos y niveles de servicio para las actividades de monitoreo de la infraestructura tecnológica, gestión de incidentes, tendencias de las cargas de trabajo y actualización de los activos de información, entre otros.

- Se carece de políticas formalizadas para las actividades de respaldos de información, asimismo, no se tienen implementados procedimientos institucionales para la clasificación y resguardo de la información, en consecuencia, la dependencia no tiene forma de acreditar que la información a recuperarse garantiza la correcta operación de los procesos críticos.

Por lo anterior, son insuficientes las acciones para asegurar la continuidad de los servicios TIC de la secretaría, debido a la falta de análisis y medición de la disponibilidad de servicios de TI; la carencia del plan de capacidad para asegurar que la operación de los servicios se lleve a cabo conforme a los niveles de servicio requeridos; la falta del análisis de impacto al negocio en el que se identifiquen las funciones, actividades, áreas y servicios que podrían resultar afectados ante la interrupción de los servicios de TIC; así como por la carencia del plan de recuperación de desastres para contar con los mecanismos de atención ante contingencias y las tareas para la recuperación de las operaciones.

2019-0-20100-20-0239-01-009 **Recomendación**

Para que la Secretaría de Bienestar implemente las acciones necesarias para la elaboración, actualización, pruebas y difusión del Programa de Continuidad de las Operaciones, Análisis de Impacto al Negocio, Plan de Recuperación de Desastres y Plan de Capacidad de TIC, así como la actualización de las políticas y procedimientos para la realización de los respaldos de información, con la finalidad de asegurar la continuidad operativa de los procesos críticos, infraestructura y soluciones tecnológicas de la entidad.

Montos por Aclarar

Se determinaron 25,004,007.91 pesos pendientes por aclarar.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Planificación estratégica y operativa y Controles internos.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 5 resultados, de los cuales, en uno no se detectó irregularidad y los 4 restantes generaron:

9 Recomendaciones, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 2 Pliegos de Observaciones.

Dictamen

El presente se emite el 12 de octubre de 2020, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue "fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables", y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, la Secretaría de Bienestar no cumplió con las disposiciones legales y normativas que son aplicables en la materia, entre cuyos aspectos observados destacan los siguientes:

- En la gestión del contrato del Servicio Integral de Comunicaciones para el Desarrollo Social se detectaron deficiencias en el análisis de la capacidad y disponibilidad de la infraestructura tecnológica para la contratación de los servicios, así como inconsistencias en la operación de la mesa de ayuda, por lo que se presumen pagos injustificados por 304.9 miles de pesos.

- En relación con la contratación de los Servicios para el Desarrollo del Inventario, Control y seguimiento de la Entrega-Recepción de las Tarjetas de Bienestar, se carece de controles para acreditar las actividades desarrolladas por el prestador del servicio en el desarrollo del sistema, no fue posible comprobar el cumplimiento de todas las funcionalidades descritas en el Anexo Técnico, se tienen inconsistencias en los entregables, errores en la programación, así como la falta de operación del sistema en el ambiente productivo; por lo anterior, se presumen pagos injustificados por 24,699.1 miles de pesos.

- Se detectaron irregularidades en las políticas y procedimientos relacionadas con la ciberseguridad, debido a las deficiencias en los controles del inventario de software autorizado y no autorizado; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; uso controlado de privilegios administrativos; protección de datos; carencia de un programa de concientización y entrenamiento de seguridad; seguridad del software de aplicación; plan de respuesta a incidentes, así como la falta de pruebas de

penetración y ejercicios de equipo rojo. Lo anterior podría causar un impacto negativo en la confidencialidad, integridad y disponibilidad de la información de los beneficiarios de los diversos programas sociales de la secretaría.

- Son insuficientes las acciones para asegurar la continuidad de los servicios de tecnologías de información y comunicaciones de la dependencia, debido a la falta de análisis y medición de la disponibilidad de los servicios; la carencia del plan de capacidad para asegurar que la operación se lleve a cabo conforme a los niveles de servicio requeridos; la falta del análisis de impacto al negocio en el que se identifiquen las funciones, actividades, áreas y servicios que podrían resultar afectados ante la interrupción de los servicios, así como por la carencia del plan de recuperación de desastres para contar con los procedimientos y tareas para el restablecimiento de las operaciones.

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

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 estén de conformidad con las disposiciones y normativas aplicables; Analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad 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 la investigación de mercado.

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

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permiten 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, así como la pertinencia de su penalización o deductivas en caso de incumplimientos.

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

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

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

7. Evaluar la gestión de los programas de continuidad de las operaciones en sus elementos como el análisis de impacto al negocio (BIA), el plan de continuidad del negocio (BCP), el plan de recuperación ante desastres (DRP), políticas de respaldos, replicación de datos, planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros.

Áreas Revisadas

Las direcciones generales de Tecnologías de la Información y Comunicaciones; Atención a Grupos Prioritarios; Recursos Materiales; y Programación y Presupuesto de la Secretaría de Bienestar.

Disposiciones Jurídicas y Normativas Incumplidas

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

1. Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 1;

2. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 26 y 53 Bis;

3. Ley General de Responsabilidades Administrativas: publicada en el Diario Oficial de la Federación el 18 de julio de 2016, artículo 7, fracciones I y V;

4. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 3, último párrafo y 30;

5. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 66, fracciones I y III;

6. Otras disposiciones de carácter general, específico, estatal o municipal: Reglamento Interior de la Secretaría de Bienestar con última reforma publicada el 24 de abril de 2018: artículo 31, fracción I; Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Nacional, en materia de tecnologías de la información y comunicaciones, y en la seguridad de la información, así como el manual administrativo de aplicación general en dichas materias publicado en el DOF el 8 de mayo de 2014, con última reforma publicada en el DOF el 23 de julio de 2018: artículos 10, fracciones III y VII, 16, fracción III, 18, 26; Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, con última reforma publicada en el DOF el 23 de julio de 2018: numeral 9, Reglas generales; Proceso Administración de Proveedores (APRO), Actividad APRO 1 Generar Lista de Verificación de Obligaciones, Factor crítico 2, inciso c; Actividad APRO 2 Monitorear el avance y el

desempeño del proveedor, Factor crítico 1; Proceso de Administración de Servicios (ADS), numeral 1, Regla del proceso 2, Actividad ADS 1 Mantener actualizado el catálogo de servicios de TIC, Actividad ADS 2 Diseñar los Servicios de TIC, Factor crítico 3; Actividad ADS 3 Administrar la capacidad de la infraestructura de TIC, Factor crítico 4, ADS 4 Administrar la Continuidad de Servicios de TIC; Proceso Administración de la Seguridad de la Información (ASI), Reglas del proceso 8 y 9, ASI 6, Factor crítico 1, inciso a; Proceso Administración de la Operación (AOP), AOP 1 Establecer el mecanismo de operación y mantenimiento de los sistemas, Actividad AOP 3 Monitorear la infraestructura de TIC en operación, Factor Crítico 3; Proceso Administración de la Configuración (ACNF), Actividad ACNF 2 Definir la estructura del repositorio de configuraciones, Factor Crítico 1; Apartado Antecedentes y Alcance de la contratación del formato APCT-F2 del Proceso de Administración del Presupuesto y las Contrataciones; ITIL V3; ISO 20000-1:2011 (nueva versión ISO 20000-1:2018), ISO/IEC 27001:2013, ISO 9001:2008 (nueva versión ISO 9001:2015), Requerimientos de Técnicas de seguridad - Sistemas de gestión de seguridad de la información ISO/IEC FDIS 27001:2013: apartados A.7, A.7.2, A.8, A.8.1, A.8.3, A.9, A.9.4, A.12, A.12.2, A.12.6, A.12.7, A.13, A.13.1, Norma ISO 22301/2019 Seguridad y Resiliencia Gestión de la Continuidad del Negocio-Requerimientos, en sus apartados 4.3.2 Alcance de la Gestión de Continuidad del Negocio, 5.2.2 Comunicación de la Política de Continuidad de Negocio y 5.3 Roles, Responsabilidades y Autoridades del Apéndice IV.B Matriz de Metodologías, Normas y Mejores Prácticas aplicables a la Gestión de las TIC; Oficio Circular mediante el cual se emiten diversas directrices para los Oficiales Mayores de las dependencias y equivalentes en las entidades de la Administración Pública Federal y titulares de los Órganos Internos de Control, que deberán observarse en las contrataciones que se realicen entre entes públicos, publicado en el DOF el 6 de noviembre de 2017: Art. 1, inciso b y c; Manual de Organización y de Procedimientos de la Dirección General de Tecnologías de la Información y Comunicaciones de la Secretaría de Bienestar, expedido el 23 de octubre de 2018: función 10 del puesto Dirección de Desarrollo de Sistemas; contrato núm. 411.413.31701.033BIS1/2017: cláusulas primera, tercera, décima segunda y décima quinta; anexo técnico del contrato núm. 411.413.31701.033BIS1/2017: Apartado Objeto del Servicio, Descripción del Servicio o Bienes Requeridos y Alcance; Apartado Antecedentes y Alcance de la Contratación del formato APCT-F2 del Proceso de Administración del Presupuesto y las Contrataciones; contrato número DGTIC-413-33301-002-2019, cláusula primera y décima segunda y el anexo técnico del contrato número DGTIC-413-33301-002-2019, Apartado Objeto del Servicio, Descripción del Servicio o Bienes Requeridos y Alcance.

Fundamento Jurídico de la ASF para Promover Acciones y Recomendaciones

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

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

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