Comisión Nacional de Protección Social en Salud

Auditoría de TIC

Auditoría Financiera y de Cumplimiento: 16-5-12U00-02-0216

216-DS

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios cuantitativos y cualitativos establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2016 considerando lo dispuesto en el Plan Estratégico de la ASF 2011-2017.

Objetivo

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

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	140,667.3
Muestra Auditada	72,854.0
Representatividad de la Muestra	51.8%

Identificación

Área Auditora: 41220 DGATIC

El universo seleccionado por 140,667.3 miles de pesos corresponde al total de recursos asignados en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2016; la muestra auditada se integra de un contrato para prestar los servicios de procesamiento, almacenamiento y administración de la información con pagos ejercidos por 72,854.0 miles de pesos, que representa el 51.8% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de las acciones realizadas en materia de TIC por la Comisión Nacional de Protección Social en Salud (CNPSS) y la Secretaría de Salud (SSA) en 2016, relacionadas con el Gobierno y Administración de las TIC, Gestión de la Seguridad de la Información y Continuidad de las Operaciones, Calidad de Datos, entre otras.

Antecedentes

La Comisión Nacional de Protección Social en Salud (CNPSS), es un órgano desconcentrado de la Secretaría de Salud, con autonomía técnica, administrativa y operativa cuya función consiste en ejercer las atribuciones que se le confieren en materia de protección social en salud, tales como vigilar que se ejecuten las acciones necesarias para el acceso efectivo a los servicios de salud, a través de la afiliación de la población objetivo y que voluntariamente lo solicite, promoviendo la adecuada tutela de sus derechos, así como la administración y uso eficiente de los recursos. Entre las iniciativas más importantes de Tecnologías de Información y Comunicaciones (TIC) destaca el mantenimiento de doce aplicativos, entre los cuales se encuentra el Sistema de Gestión Financiera (SIGEFI), Sistema de Gestión de Gastos Catastróficos (SIGGC2), Sistema Nominal en Salud (SINOS) y el Sistema Único de Gestión (SUG).

Entre 2012 y 2016, en la CNPSS se han invertido 159,623.5 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la siguiente manera:

Recursos Invertidos en Materia de TIC
(Miles de Pesos)

PERIODO DE INVERSIÓN	2012	2013	2014	2015	2016	TOTALES
MONTO	107,713.9	33,122.3	13,655.3	3,508.9	1,623.1	**159,623.5**

Fuente: Elaborado por la ASF con base en la información proporcionada por la CNPSS

El presupuesto destinado en el año 2016 en relación al 2015 representa un decremento del 46.3%.

Resultados

1. Análisis Presupuestal

La CNPSS presentó la Adecuación Presupuestal número CNPSS-SICOP-06-261 realizada por la Dirección General de Programación, Organización y Presupuesto (DGPOP) de la Secretaría de Salud (SSA) sobre las partidas en materia de Tecnologías de la Información y Comunicaciones (TIC), que originalmente contaban con un presupuesto por 140,667.3 miles de pesos, con el fin de centralizar los recursos y los pagos de los servicios bajo el control de la Secretaría de Salud, en cumplimiento de las Políticas Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios (POBALINES) de la SSA, emitidos el 1 de noviembre de 2012, las cuales establecen que con la finalidad de aprovechar el volumen de compra de la Secretaría de Salud, deberá consolidar la adquisición, arrendamiento de bienes o la contratación de los servicios en la Dirección General de Tecnologías de la Información (DGTI) de la SSA; la disminución de las partidas de TIC quedó de la manera siguiente:

Adecuaciones Presupuestales del Gasto de TIC en la CNPSS
(Miles de Pesos)

Partidas	Concepto	Original	Ampliaciones	Reducciones	Presupuesto Pagado
31401	Servicio telefónico convencional	741.0	0.0	741.0	0.0
31501	Servicio de telefonía celular	173.3	0.0	173.3	0.0
31602	Servicios de telecomunicaciones	14,475.6	0.0	14,475.6	0.0
31603	Servicios de internet	11.5	0.0	11.5	0.0
31904	Servicios integrales de infraestructura de cómputo	64,683.7	0.0	64,683.7	0.0
32301	Arrendamiento de equipo y bienes informáticos	3,900.2	0.0	3,900.2	0.0
32701	Patentes, derechos de autor, regalías y otros	6,091.7	624.0	5,467.7	0.0
33301	Servicios de desarrollo de aplicaciones informáticas	46,935.7	3,030.5	43,905.2	1,591.8
	TOTAL	**137,012.7**	**3,654.5**	**133,358.2**	**1,591.8**

Fuente: Elaborado con la información proporcionada por la CNPSS

Nota: Diferencias por redondeo.

Derivado de la estrategia de centralizar los recursos económicos para los servicios de TIC bajo el control de la SSA, durante el 2016 la CNPSS ejerció únicamente 1,623.1 miles de pesos del presupuesto en materia de TIC, tampoco realizó acciones relacionadas a la vigilancia del cumplimiento de los servicios de tecnología contratados; debido a que la SSA determina los componentes tecnológicos de TI por adquirirse, así como ejecuta las acciones de monitoreo y vigilancia del otorgamiento de los mismos, sin que por parte de la Comisión sean realizadas acciones de gobernabilidad de los servicios. Por esta razón fueron revisadas las operaciones de la CNPSS y de las áreas vinculadas pertenecientes a la Secretaría de Salud.

Respecto al padrón de beneficiarios, los procesos de verificación de la información, validación de la integridad de los datos y la administración del sistema, donde es procesada la información, son actividades realizadas por la Dirección General de Afiliación y Operación, sin embargo, no se identifican mecanismos de control implementados por parte de esta Dirección General, que permitan asegurar que se cuenta con estándares y políticas en materia de seguridad de la información, que permitan salvaguardar adecuadamente la información de los beneficiarios; y que los mismos se encuentren regulados por la Dirección General de Procesos y Tecnología de la Comisión.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2016, se concluyó que a la CNPSS se le asignó un presupuesto de 75,921,355.7 miles de pesos, de los cuales únicamente ejerció 1,623.1 miles de pesos correspondientes a recursos relacionados con las TIC, que representan el 0.002% del total, como se muestra a continuación:

Recursos ejercidos en 2016 en la CNPSS
(Miles de pesos)

Capítulo	Concepto	Ejercido	Ejercido TIC	%
1000	Servicios personales	625,850.3	0.0	0.0
2000	Materiales y suministros	310,286.7	31.3	0.01
3000	Servicios generales	362,929.6	1,591.8	0.43
4000	Transferencias, asignación, subsidios y otras ayudas	74,622,289.1	0.0	0.0
	Total	**75,921,355.7**	**1,623.1**	**0.002**

Fuente: Elaborado por la ASF con base en la información de la Cuenta de la Hacienda Pública Federal 2016 de la Secretaría de Salud.

Nota: Diferencias por redondeo.

Los recursos ejercidos en materia de TIC por 1,623.1 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2016 CNPSS
(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
2000		**MATERIALES Y SUMINISTROS**	**31.3**
	21401	Materiales y útiles consumibles para el procesamiento en equipos y bienes informáticos	31.3
3000		**SERVICIOS GENERALES**	**1,591.8**
	33301	Servicios de Desarrollo de aplicaciones informáticas	1,591.8
		TOTAL	**1,623.1**

Fuente: Elaborado con la información proporcionada por la CNPSS.

Nota: Diferencias por redondeo.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC considerando 22 plazas con una percepción anual de 7,935.0 miles de pesos durante el ejercicio 2016, el costo promedio por plaza es de 360.7 miles de pesos anuales. Cabe mencionar que la CNPSS es únicamente un área que genera los reportes de incidencias del personal, ya que el control presupuestal del ejercicio de esta partida, es efectuado por la Secretaría de Salud.

Por otra parte, de los 140,667.3 miles de pesos que corresponde al total de recursos asignados a la CNPSS en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal 2016, se erogaron recursos por 72,854.0 miles de pesos en el contrato de "Procesamiento, almacenamiento y administración de la información para las unidades administrativas, y órganos administrativos desconcentrados de la Secretaría de Salud", que representa el 51.8% del total del universo mencionado, el cual se integra de la siguiente manera:

Contrato de Prestación de Servicios Ejercidos por la Secretaría de Salud en 2016

(Miles de pesos)

Proceso de Adjudicación	Contrato	Proveedor	Objeto del contrato	Vigencia Del	Vigencia Al	Monto	Ejercido 2016	%
Adjudicación Directa	DGRMSG-DCC-S-015-2016	Grupo de Tecnología Cibernética S.A. de C.V.	Procesamiento, almacenamiento y administración de la información para las unidades administrativas, y órganos administrativos desconcentrados de "La Secretaría de Salud"	15/04/2016	15/11/2016	60,953.6	60,953.6	100.0
Adjudicación Directa	Convenio Modificatorio 01/16 al Contrato DGRMSG-DCC-S-015-2016		Ampliar la fecha de término del contrato al 27 de diciembre de 2016 y el monto total del contrato.	16/11/2016	27/12/2016	11,900.4	11,900.4	100.0
					Total	**72,854.0**	**72,854.0**	**100.0**

Fuente: Contratos, facturas y soporte documental proporcionado por la CNPSS.

Nota: Diferencias por redondeo.

Se verificó en la SSA, que el pago fue reconocido en la partida presupuestaria correspondiente; el análisis del contrato de la muestra se presenta en el resultado subsecuente.

2. Contrato DGRMSG-DCC-S-015-2016

Se analizó el contrato número DGRMSG-DCC-S-015-2016 celebrado con la empresa Grupo de Tecnología Cibernética, S.A. de C.V., mediante el procedimiento de adjudicación directa, con fundamento en los artículos 25, 26 fracción III, 28 fracción I, 40 y 41, fracción V de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), así como el 71 y 72, fracción III del reglamento de la LAASSP, con objeto de prestar los servicios de procesamiento, almacenamiento y administración de la información para las unidades administrativas, y órganos administrativos desconcentrados de la Secretaría de Salud, vigente del 16 de abril al 15 de noviembre de 2016, por un monto de 60,953.6 miles de pesos; se realizó el primer convenio modificatorio número 01/16 al Contrato DGRMSG-DCC-S-015-2016, con la finalidad de ampliar la fecha de término al 27 de diciembre de 2016, por un monto de 11,900.4 miles de pesos, de los cuales se pagaron 72,854.0 miles de pesos durante el 2016, se determinó lo siguiente:

El alcance de los trabajos se integró por 18 servicios administrados de TI, los cuales consideran principalmente lo relacionado a bases de datos, gestión de almacenamiento y respaldos, virtualización y mesa de ayuda.

Las características generales del servicio son las siguientes:

- Aprovisionamiento de enlaces de red.
- Administración de sistemas operativos, bases de datos y virtualización.
- Solución de gestión de respaldos y almacenamiento.
- Transferencia de servicios.

Proceso de Contratación

En relación con la consolidación de la contratación de los servicios de Tecnologías de la Información ejecutado por la Secretaría de Salud (SSA), se carece de elementos que permitan identificar los requerimientos de cada unidad administrativa y órgano desconcentrado de la SSA a través del cual se sustentó la contratación del servicio.

Revisión de los Pagos

Los montos pagados en el año 2016 para cada uno de los servicios, de acuerdo con lo establecido en el contrato y su convenio modificatorio son los siguientes:

CONTRATO DGRMSG-DCC-S-015-2016 Y CONVENIO MODIFICATORIO 01/16 AL CONTRATO DGRMSG-DCC-S-015-2016
(Miles de Pesos)

No.	Servicio	Costo Unitario	Meses	Monto	IVA	Total
1.	Enlaces MPLS (SWAN)	508.0	8.4	4,267.5	682.8	4,950.4
2.	Servicios de Red de Área Local en Internet (SLAN)	561.4	8.4	4,715.8	754.5	5,470.3
	Servicios					
3.	Servicios de Administración de Sistemas Operativos (SASO)	232.7	8.4	1,954.4	312.7	2,267.1
4.	Servicios de Administración de base de datos (SABD)	411.8	8.4	3,458.8	553.4	4,012.2
5.	Servicios de Administración de Virtualización (SAV)	487.0	8.4	4,091.1	654.6	4,745.7
6.	Servicios de Conversión y Consolidación de Bases de Datos y Aplicaciones (SMDB)	357.6	8.4	3,003.8	480.6	3,484.4
7.	Servicios de Administración de Almacenamiento, Respaldos y Restauración (SARR)	1,256.1	8.4	10,551.0	1,688.2	12,239.1
8.	Servicio de Mesa de Ayuda (SMA)	183.9	8.4	1,544.7	247.2	1,791.8
9.	Servicio de Ingeniería en Sitio (SIS)	353.7	8.4	2,970.7	475.3	3,446.0
10.	Servicio del Centro de Operaciones de Seguridad (SOC)	225.4	8.4	1,892.9	302.9	2,195.8
11.	Servicios de Migración de Plataforma (SMP)	526.0	8.4	4,418.7	707.0	5,125.7
	Poder de Cómputo y Almacenamiento-Hardware Base					
12.	Solución para el Ambiente de Virtualización (AV)	239.97	8.4	2,015.7	322.5	2,338.2
13.	Solución para el Ambiente de Base de Datos (ABD)	975.9	8.4	8,197.5	1,311.6	9,509.1
14.	Solución para el Ambiente de SOA (ASOA)	424.4	8.4	3,564.8	570.4	4,135.2
	Otros					
15.	Transición del Servicio al término del contrato (STC)	1,251.6	1.0	1,251.6	200.2	1,451.8
16.	Solución de Gestión de Almacenamiento (SGA)	33.5	8.4	281.8	45.1	326.9
17.	Solución de Gestión de Respaldos (SGR)	41.7	8.4	350.4	56.1	406.5
18.	Servicio de Monitoreo de los Servicios (NOC)	508.8	8.4	4,273.6	683.8	4,957.7
	Total			62,804.8	10,048.9	72,853.9

Fuente: Información Proporcionada Por La CNPSS

Nota: La Suma De Los Parciales Puede No Coincidir Debido Al Redondeo Aplicado.

Revisión de servicios y entregables

De los 18 servicios de tecnología que contempla el contrato, por los cuales fueron pagados por la Secretaría de Salud por un monto de 72,584.0 miles de pesos en 2016, fueron revisados 15 servicios (83.3%) de los cuales existieron deficiencias en la revisión, verificación y validación de la infraestructura por parte de la Secretaría de Salud, así como la carencia de documentación de los entregables generados por el proveedor. Entre las principales observaciones se enlistan los siguientes:

- Para el Servicio de ***"6.1 Planeación de la Transición de los Servicios"***, no se proporcionó la información para acreditar una adecuada planeación de actividades realizadas por el proveedor en relación con los servicios contratados, así como la documentación que avale las actividades realizadas por el prestador del servicio, por lo que no se puede garantizar que esta actividad se realizó adecuadamente.
- No se cuenta con la información que permita identificar los mecanismos utilizados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA para validar el Servicio ***"6.2 Poder de cómputo y almacenamiento - hardware base",*** del mismo modo se carece de los elementos técnicos que acrediten la Lista de Verificación realizada por "La Secretaría" para validar el hardware base, proporcionada por el prestador de servicio.
- No se proporcionó el soporte documental que muestre que los Servicios ***"6.3 Servicio de administración de almacenamiento respaldo y restauración (SARR) y 6.4. Solución de gestión de respaldos, SGR"*** cumplieron con las características y funcionalidades operativas descritas en el "Anexo Único" del Contrato, por lo que no se puede garantizar que el prestador de servicios proporcionó la infraestructura establecida en el Anexo Único" del Contrato.
- La DGTI no verificó las actividades del Servicio ***"6.6. Servicio de migración de plataforma SMP",*** ya que no se contó con la documentación descrita en el "Anexo Único" del Contrato, aunado a que no es posible garantizar que el servicio se proporcionó con las características y funcionalidades operativas descritas en relación a los entregables documentados.
- Se carece de la evidencia documental que permita acreditar las actividades del Servicio ***"6.7. Servicios de gestión y monitoreo"***, en relación al análisis de la bitácora (LOG), y las recomendaciones y remediaciones derivadas de dicho análisis.
- Respecto a la revisión de los Servicios ***"6.10 Servicio de monitoreo de "los servicios", NOC y 6.11. Servicio del centro de operaciones de seguridad, SOC"*** no se proporcionó el análisis y/o la validación por parte de la DGTI de los niveles de operación por parte del SOC; en consecuencia, no es posible garantizar que el servicio proporcionado cumpla con los procedimientos y buenas prácticas de acuerdo a los estándares de ITIL (Biblioteca de Infraestructura de Tecnologías de Información).
- Se carece del análisis técnico que sustente el modelado de tráfico realizado por el prestador de servicio para el equipo Riverbed, utilizado para el Servicio ***"6.13.***

Enlaces MPLS SWAN" asimismo se carece de la información que permitan verificar las actividades realizadas por la DGTI para validar el cumplimiento de los niveles de servicio, así como la documentación que acredite la revisión de las características y su rendimiento; en consecuencia, no revisó el modelado de tráfico en función a la falta de documentación.

De lo anterior, se advierten deficiencias en las actividades de gestión del contrato para la verificación de los servicios, asimismo, no fue posible validar a través de qué mecanismos la Dirección General de Tecnologías de la Información (DGTI) de la SSA, revisó el contenido de los reportes que avalan los servicios otorgados y a través de los cuales se autorizaron los trabajos ejecutados por el proveedor respecto a lo contratado. Cabe señalar que la Dirección General de Procesos y Tecnología (DGPT) de la CNPSS, no tiene injerencia en la operación de los servicios, lo cual no es funcional y repercute en la baja calidad de los niveles de servicio que se prestan a la Comisión.

16-0-12100-02-0216-01-001 **Recomendación**

Para que la Secretaría de Salud a través de la Dirección General de Tecnologías de la Información, implemente mecanismos para la gestión y gobierno de los servicios de tecnologías de la información contratados, que permitan que los mismos puedan ser gestionados directamente por la Comisión Nacional de Protección Social en Salud, con la finalidad de asegurar que los niveles de servicio, trazabilidad de las operaciones, conformidad de los pagos y desarrollo de las operaciones cumplan con los criterios de eficacia, eficiencia y transparencia de acuerdo con las normativas vigentes, en beneficio de la calidad en el otorgamiento de los servicios para los usuarios finales.

16-9-12112-02-0216-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, del contrato DGRMSG-DCC-S-015-2016, para la prestación de los servicios de procesamiento, almacenamiento y administración de la información, se detectaron irregularidades vinculadas con las responsabilidades del Titular de la Dirección General de Tecnologías de la Información y de la Subdirección de Sistemas de la Secretaría de Salud, debido a que se carece de los elementos para validar las actividades relacionadas con la disponibilidad de la infraestructura, otorgamiento de los servicios y cumplimiento de niveles de servicio.

3. Gobierno y Administración de las TIC

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

Dirección General de Procesos y Tecnología (DGPT) de la CNPSS

- La conformación del Grupo de Trabajo para la dirección de TIC fue realizada en diciembre de 2016, en consecuencia, no se cuenta con elementos que permitan

verificar y garantizar la implementación y operación de las acciones realizadas por este Grupo de Trabajo en el periodo evaluado.

- Se carece de un modelo de toma de decisiones para la dirección y control de las TIC, asimismo, no fue posible identificar alguna acción realizada en esta materia.
- No se tiene evidencia de la evaluación de Segregación de Funciones en las actividades operativas de TIC, que permita identificar oportunamente procedimientos que pudieran impactar en fraude, irregularidades en los procesos, duplicidad de funciones, etc.
- No fue posible validar que los proyectos PETIC 2016 cuentan con una línea base y programa de trabajo.
- Se carece de indicadores de desempeño para los procesos de TIC ejecutados en 2016, que permitan identificar posibles desviaciones para mitigar los riesgos en la operación.
- No se cuenta con actividades realizadas para identificar las infraestructuras críticas y los activos claves de la Comisión.

Dirección General de Tecnologías de la Información (DGTI) de la SSA

- No fue posible validar la ejecución de algún procedimiento de revisión, previo a la contratación de un servicio TIC y que este se encuentre alineado a una proyección de los requerimientos funcionales, requerimientos no funcionales, controles de seguridad, niveles de servicio y tiempos de entrega que permitan garantizar una óptima operación y continuidad operativa de la SSA, la CNPSS y órganos administrativos desconcentrados.
- No se identificó un procedimiento formal, que permita verificar los indicadores de cumplimiento de niveles de servicio de los proveedores en relación a los contratos que dan soporte a la Secretaría de Salud, la CNPSS y órganos administrativos desconcentrados.
- Durante 2016, no se identificó la implementación de metodologías para la gestión de riesgos de TIC.
- Se carece de elementos que permitan validar un plan de capacidad de la infraestructura destinada para la operación de la SSA y órganos administrativos desconcentrados, así como de un mecanismo que permita verificar que la misma sustente eficientemente la operación y cuente con un rendimiento óptimo.
- No se cuenta con un Plan de Recuperación de Desastres (DRP) formalizado, así como se carece de elementos que permitan verificar la ejecución de pruebas durante 2016.
- Se carece de elementos que permitan verificar y garantizar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Datos Abiertos en la CNPSS

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

- No se cuenta con evidencia de la documentación y publicación al menos de una historia de éxito de la Comisión.
- No se cumplió con lo establecido en el Cronograma de implementación por parte de la Comisión, en relación a: publicación de planes de acción de Datos Abiertos que contendrá el inventario y priorización de la información, así como acciones implementadas de capacitación.

Implementación MAAGTIC-SI en la CNPSS

De la evaluación del avance en la implementación del MAAGTIC-SI, el cual fue reportado al 68.3% por la Comisión en todos sus procesos, de un universo de 48 subprocesos, la entidad fiscalizadora revisó una muestra de 16 (33.3%), y encontró para la CNPSS inconsistencias en 6 de ellos (37.5%), con lo cual como resultado de la revisión de los procedimientos se estima un 50.0% de avance en la implementación, detectándose observaciones en la identificación de infraestructuras críticas y activos clave, elaboración de análisis de riesgos y la administración de la continuidad de servicios de TIC.

Por lo anterior, para la CNPSS se identificaron deficiencias en la operación e implementación de la operación del Grupo de Trabajo de TIC; falta de implementación de la segregación de funciones en las actividades operativas y sustantivas de las áreas de TIC; validar el programa de trabajo de los proyectos PETIC; falta de implementación de indicadores de desempeño para los procesos de TIC ejecutados; incumplimiento del Decreto en materia de Datos Abiertos; identificar infraestructuras críticas y activos clave; elaborar análisis de riesgos; implementar acciones por parte del grupo estratégico de seguridad de la información; monitoreo al avance del desempeño del proveedor; administrar la continuidad se servicios de TIC.

Cabe señalar que la Dirección General de Procesos y Tecnología (DGPT) de la CNPSS se encuentra limitada para cumplir con sus facultades estipuladas en el Reglamento Interno de la CNPSS, debido a que varios de los procesos de Gobierno de TIC son manejados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA, lo cual no es operativo y provoca deficiencias en los procesos de planeación estratégica, administración de proveedores y análisis de riesgos en la Comisión.

Para la DGTI de la SSA se concluye que se carece de un procedimiento de revisión previo a la contratación de un servicio de TIC, falta de verificación de los indicadores de cumplimiento de niveles de servicio especificados en los contratos y carencia de la implementación de metodologías para la gestión de riesgos de TIC.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, la Dirección General de Procesos y Tecnología de la CNPSS, instruyó acciones de control que han sido iniciadas en conjunto con la Dirección General de Tecnologías de la Información de la SSA, como parte de las iniciativas de la CNPSS para colaborar con la SSA, con la finalidad de generar acciones enfocadas para el cumplimiento de las observaciones identificadas en la auditoría

relacionadas a Gobierno de TIC y Seguridad de la Información; entre los principales acuerdos se identifican los siguientes:

- Consulta jurídica acerca de la viabilidad de que cada Órgano Administrativo Desconcentrado de la Secretaría de Salud, realice el contrato respectivo por su área contratante, para los servicios consolidados en materia de TIC, con la finalidad de que la CNPSS administre su presupuesto y tenga gobernanza en los servicios que presta.
- Para solventar los puntos referentes a la seguridad de la información, la DGPT solicitará información a la DGTI.
- En la elaboración de los Anexos Técnicos de las contrataciones consolidadas, se involucrará a la CNPSS, para que adviertan sus necesidades y sean consideradas por la DGTI.

16-0-12100-02-0216-01-002 **Recomendación**

Para que la Secretaría de Salud implemente mecanismos que permitan asegurar una adecuada proyección de los requerimientos para la contratación de los servicios de Tecnologías de la Información, así como implementar mecanismos de gobernanza que permitan verificar el adecuado otorgamiento y cumplimiento de los niveles de servicio en relación con lo pactado contractualmente, a fin de garantizar una óptima operación y continuidad operativa de la Secretaría de Salud y órganos administrativos desconcentrados.

16-5-12U00-02-0216-01-001 **Recomendación**

Para que la Comisión Nacional de Protección Social en Salud implemente controles para la operación y seguimiento de las acciones realizadas por el Grupo de Trabajo para la dirección de Tecnologías de la Información y Comunicaciones (TIC) y la segregación de funciones de las áreas operativas de Tecnología de Información (TI), con la finalidad de identificar duplicidades en funciones, posibles conflictos de intereses en relación con la autoridad para la ejecución de transacciones sensibles, y evitar fraudes así como de la implementación de indicadores de desempeño de los procesos operativos de las áreas de tecnología de la Comisión Nacional de Protección Social en Salud (CNPSS).

16-9-12112-02-0216-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en la evaluación de los procesos de gobernabilidad y administración de TIC, se detectaron irregularidades vinculadas con la responsabilidad del Titular de la Dirección General de Tecnologías de la Información de la Secretaría de Salud (SSA), debido a que omitió implementar un procedimiento para cumplir con los requerimientos técnicos, funcionales y no funcionales que garanticen lo solicitado por la SSA, instrumentar los mecanismos de control para la identificación, cuantificación y determinación de la probabilidad de los riesgos en TIC, así como la instrumentación de un plan de mitigación para disminuir incidentes y posibles impactos en la operación de los procesos sustantivos, aplicativos e infraestructura tecnológica que sustentan la operación de la SSA.

16-9-12U00-02-0216-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en la evaluación de los procesos de gobernabilidad y administración de TIC, se detectaron irregularidades vinculadas con las responsabilidades del Titular de la Dirección General de Procesos y Tecnología, el Director General Adjunto, la Dirección de Seguimiento y Gestión de Procesos, Subdirección de Certificación de Proveedores y la Subdirección de Procesos y Logística de la CNPSS, debido a que omitieron realizar actividades relacionadas con el Gobierno de las TIC, tales como: implementar un modelo de gobierno de TIC, la segregación de funciones, documentar el plan de trabajo de los proyectos estratégicos, implementar indicadores de desempeño, instrumentar acciones en materia de Datos Abiertos y elaborar un análisis de riesgos.

4. Gestión de la Seguridad de la Información y Continuidad de las Operaciones

En la revisión y análisis de la información, relacionada con la Administración de la Seguridad de la información (ASI), la Operación de Controles de Seguridad de la información y del ERISC (OPEC), para la confidencialidad, disponibilidad e integridad de la información, se observó lo siguiente:

Seguridad de la Información

Dirección General de Procesos y Tecnología (DGPT) de la CNPSS

- Se carece de elementos que permitan validar la implementación y acciones realizadas por el Grupo Estratégico de Seguridad de la Información (GESI) durante 2016.
- Se carece de evidencia que permita validar la asignación del Responsable de Seguridad de la Información (RSII) en la Comisión.
- No fue posible verificar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Durante el 2016 no fue posible validar procedimientos o acciones que permitan gestionar las cuentas de los aplicativos y diversos componentes tecnológicos.
- No se cuenta con un catálogo de los dueños de los aplicativos de la CNPSS.
- En 2016 no fue ejecutado un procedimiento para la validación de los usuarios de los aplicativos.
- No se cuenta con evidencia de la documentación de un plan de capacidad; así como de la validación de la infraestructura proporcionada para la operación de la CNPSS.
- No fue posible verificar la implementación ni monitoreo de controles de seguridad de la información.
- Se verificó en 2016 la difusión de temas de concientización en materia de seguridad de la información a través de correo electrónico; sin embargo, se carece de

elementos que permitan identificar la implementación de acciones en materia de capacitación y concientización en la Comisión.

Dirección General de Tecnologías de la Información (DGTI) de la SSA

- Se carece de elementos que permitan identificar las sesiones y acciones realizadas por el Grupo Estratégico de Seguridad de la Información (GESI) durante 2016.
- No fue posible verificar la conformación del Equipo de Respuesta a Incidentes de Seguridad de TIC (ERISC).
- Durante el 2016 no fue realizado un análisis de riesgos de las áreas de TIC.
- Se carece de mecanismos de control que garanticen la protección física y lógica de las infraestructuras críticas.
- En relación con la atención de incidentes, no se cuenta con soporte documental que permita validar que se llevaron a cabo actividades de investigación técnica de los incidentes, erradicación de los mismos, así como la recuperación de la operación.
- Se carece de mecanismos que limiten la conexión de dispositivos electrónicos institucionales a redes inalámbricas externas.
- No fue posible validar la implementación de un procedimiento para la verificación del cumplimiento de las políticas, relacionados con la seguridad informática y tecnologías de la información.
- Se carece de políticas que permitan regular en la SSA, la CNPSS y órganos administrativos desconcentrados, la transferencia de datos sobre canales seguros.
- No fueron implementadas políticas o procedimientos que permitan garantizar una adecuada gestión de los respaldos de la información.
- No se cuenta con un procedimiento que permita gestionar la capacidad y desempeño de la infraestructura proporcionada a la SSA, la CNPSS y órganos administrativos desconcentrados.
- Se carece de políticas que regulen los procedimientos de borrado seguro.

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

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

Fuente: Elaborado por la ASF con base en la información proporcionada por la CNPSS y la SSA.

Continuidad de la Operación

Dirección General de Procesos y Tecnología (DGPT) de la CNPSS

- Durante el 2016 no fue realizado el Programa de Continuidad de la Operación.
- No fueron ejecutadas pruebas al Plan de Recuperación de Desastres (DRP).
- Se carece del Análisis del Impacto al Negocio (BIA), en el que se identifiquen las funciones, actividades, áreas, así como los servicios que proporciona la Comisión que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el impacto de las consecuencias que se generarían.

Dirección General de Tecnologías de la Información (DGTI) de la SSA

- No se cuenta con el catálogo de servicios de TIC.
- Se carece de un plan de capacidad de la infraestructura tecnológica, que le permita a la SSA, la CNPSS y órganos administrativos desconcentrados, cumplir con los niveles de servicio acordados; prever el crecimiento de la demanda de infraestructura; la mejora de los niveles de servicio y la incorporación de nuevos servicios de TIC.

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

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD EN LOS PROGRAMAS DE CONTINUIDAD DE LAS OPERACIONES	
Factor Crítico	**Principales Riesgos por su Carencia y sus Consecuencias Potenciales para las Operaciones y Activos**
Análisis de impacto al negocio y Plan de Recuperación de Desastres	Se carece de la identificación de las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias que se generarían, por lo tanto, los puntos objetivos de recuperación (RPO) y el tiempo objetivo de recuperación (RTO) de la información, serían mucho mayores a los requeridos para la continuidad de las operaciones.
Planeación de la Capacidad	La gestión de la capacidad es la encargada de que todos los servicios se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada, en ausencia de una correcta gestión de la capacidad los recursos no se aprovechan adecuadamente y se realizan acciones equivocadas en mantenimiento y administración, o aún peor, los recursos son insuficientes con la consecuente degradación de la calidad del servicio.

Fuente: Elaborado por la ASF con base en la información proporcionada por la CNPSS y la SSA.

Respecto a la CNPSS, se reflejan deficiencias en implementar el Grupo Estratégico de Seguridad de la Información (GESI) así como del Sistema de Gestión de Seguridad de la Información (SGSI); gestionar las cuentas de los aplicativos; implementar controles de seguridad de la información; así como en documentar el plan de capacidad, programa de Continuidad de la Operación y Análisis del Impacto al Negocio.

Cabe señalar que la Dirección General de Procesos y Tecnología (DGPT) de la CNPSS se encuentra limitada para cumplir con sus facultades estipuladas en el Reglamento Interno de la CNPSS, debido a que varios de los procesos de Seguridad de la Información y Continuidad de las Operaciones, son gestionados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA, lo cual no es eficiente y aumenta los riesgos en los procesos del sistema de gestión de seguridad de la información, gestión de incidentes y planes de recuperación en caso de contingencias en la Comisión.

En relación con la Secretaría de Salud, se tienen deficiencias en conformar el Equipo de Respuesta a Incidentes de Seguridad (ERISC); realizar el análisis de riesgos de las áreas de TIC; implementar mecanismos de control para la protección de las infraestructuras críticas; asegurar la transferencia de datos sobre canales seguros; gestionar la capacidad y desempeño de la infraestructura tecnológica; implementar políticas de borrado seguro y documentar el plan de capacidad.

En el transcurso de la auditoría y con motivo de la intervención de la ASF, la Dirección General de Procesos y Tecnología de la CNPSS, instruyó acciones de control que han sido iniciadas con la elaboración del Manual de Seguridad de la Información, el cual apoyará a implementar mecanismos que permitan asegurar una adecuada gestión, operación y regulación de aspectos de Seguridad de la Información; en él se encuentran descritos controles en materia de seguridad de la información relacionados a 13 dominios, entre los principales destacan los siguientes: Seguridad de la Información con colaboradores y proveedores; Seguridad en las operaciones y comunicaciones; Adquisición, Desarrollo y Mantenimiento de los Sistemas de

Información; Administración de Incidentes de Seguridad de la Información y Aspectos de Seguridad de la Información en la Continuidad del Negocio.

16-0-12100-02-0216-01-003 **Recomendación**

Para que la Secretaría de Salud implemente el Grupo Estratégico de Seguridad de la Información, a fin de realizar el análisis de riesgos y las acciones pertinentes para su tratamiento, así como el estudio de su interrelación entre la Secretaría de Salud, la Comisión Nacional de Protección Social en Salud y demás órganos administrativos desconcentrados, con la finalidad de implementar procedimientos que aseguren la ejecución de las acciones de remediación que sean necesarias.

16-5-12U00-02-0216-01-002 **Recomendación**

Para que la Comisión Nacional de Protección Social en Salud instrumente el Sistema de Gestión de Seguridad de la Información a fin de desarrollar una adecuada estrategia para la operación de los servicios de tecnologías de la información; iniciar la documentación de controles que aseguren la salvaguarda de información, protección de los componentes tecnológicos y activos críticos; así como implementar procedimientos para la gestión de las cuentas de usuario asignadas a los aplicativos, que permitan controlar los privilegios otorgados a las aplicaciones que procesan información de la Comisión.

16-9-12112-02-0216-08-003 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en la evaluación de la Administración de la Seguridad de la información, se detectaron irregularidades vinculadas con la responsabilidad del Titular de la Dirección General de Tecnologías de la Información de la SSA, debido a que omitió ejecutar acciones por parte del Grupo Estratégico de Seguridad de la información, conformar el Equipo de Respuesta a Incidentes, implementar la protección física y lógica de las infraestructuras críticas, regular el cumplimiento de las políticas y lineamientos emitidos en materia de seguridad de la información, garantizar una adecuada gestión de los respaldos, implementar una política de borrado seguro, generar el plan de capacidad de la infraestructura tecnológica, así como la mejora de los niveles de servicio y la incorporación de nuevos servicios de TIC.

16-9-12U00-02-0216-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en la evaluación de la Administración de la Seguridad de la información, se detectaron irregularidades vinculadas con la responsabilidad del Titular de la Dirección General de Procesos y Tecnología de la CNPSS, debido a que omitió implementar el Grupo Estratégico de Seguridad de la Información, implementar el Sistema de Gestión de Seguridad de la Información, documentar el plan de capacidad, ejecutar las pruebas del Plan de Recuperación de Desastres y documentar el Análisis del Impacto al Negocio.

5. Calidad de Datos

Para realizar esta evaluación se utilizó una herramienta de análisis de calidad de datos, con la cual se verificó el 10.6% de los 51,851,004 de beneficiarios contenidos en el Padrón del Sistema de Protección Social en Salud, el cual se encuentra a cargo de la Dirección General de Afiliación y Operación (DGAO) y concentra la información proveniente de todas las entidades federativas del país, se determinó lo siguiente:

- Se identificaron 1,397 registros correspondientes a beneficiarios entre 18 y 25 años de edad, catalogados como estudiantes sin el registro del comprobante de "No Derechohabiencia" ni comprobante de estudios.
- Se identificaron 81 colectividades con datos incompletos tales como "Tipo de Afiliación", "Comprobante de Colectividad", "Estado Colectividad", "Folio Colectividad", lo anterior incumple con lo descrito en los criterios de afiliación.
- Se identificaron 517 beneficiarias menores de 18 años, catalogadas como titulares y que no cuentan con registro de comprobante de embarazo, el cual es necesario para afiliarse con esta figura; de acuerdo a lo descrito en los numerales 2.4 "Titulares menores de edad", 3.2 "Diagnóstico de embarazo" del Manual y Afiliación de Operación y artículo 50 de la Ley General de los Derechos de las niñas, niños y adolescentes ***"únicamente las menores de edad que se encuentren embarazadas podrán ser titulares de un núcleo familiar, siempre y cuando no formen parte de uno o puedan formar parte de alguno".***
- De revisión de pólizas no contributivas, se identificaron 9,752 beneficiarios, los cuales se encuentran clasificados en los deciles V, VI y VII, (deciles que se encuentran catalogados con pago de cuota) y que no cuentan con el identificador de familia SMSXXI (Programa Seguro Médico Siglo XXI) y ES (Embarazo Saludable), para exentar el pago de la póliza; lo anterior en contravención a lo descrito en el numeral 4 "Cuotas familiares" del Manual y Afiliación de Operación.
- No fue posible validar la "Vigencia de la Póliza", lo que impide verificar que la duración de la misma no exceda la fecha límite de la Cédula de Características Socioeconómicas del Hogar (Cecasoeh), conforme a lo establecido en el Manual de Afiliación y Operación, punto 5 Pólizas.

Pólizas con Régimen Contributivo

De acuerdo con el artículo 77 bis 21 de la Ley General de Salud, los beneficiarios del Sistema de Protección Social en Salud, participarán en su financiamiento con cuotas familiares que serán anticipadas, anuales y progresivas, que se determinarán con base en las condiciones socioeconómicas de cada persona o familia.

Las cuotas vigentes para el Ejercicio Fiscal 2016, publicado en el DOF el 31 de marzo del 2016, corresponden a la siguiente información:

Decil de ingreso	Cuota familiar anual en pesos
I	-
I	-
III	-
IV	-
V	2,074.97
VI	2,833.56
VII	3,647.93
VIII	5,650.38
IX	7,518.97
X	11,378.86

Fuente: Manual de Afiliación y Operación de la CNPSS.

- Se identificaron 10 registros con diferencia en los pagos, correspondientes a cuatro beneficiarios, los cuales están catalogadas en los deciles ocho y nueve respectivamente; con forma de pago "núcleo familiar", y periodo trimestral, sin embargo se encuentran diferencias respecto a la información registrada en el decil y la pagada por los beneficiarios. Los hallazgos se presentan en la siguiente tabla:

DIFERENCIAS EN PÓLIZAS PAGADAS

(Cifras en pesos)

FOLIO	TIPO RÉGIMEN	CURP	NOMBRE	No DECIL	CUOTA ANUAL POR DECIL	DURACIÓN PÓLIZA	IMPORTE PAGADO	ASF IMPORTE	DIFERENCIA
2414154369	CONTRIBUTIVA	EITA820529MSPSRR02	ARACELY ESPINOZA TORRES	9	$7,518.97	Trimestral	$939.87	$1,879.74	-$939.87
2414154369	CONTRIBUTIVA	EITA820529MSPSRR02	ARACELY ESPINOZA TORRES	9	$7,518.97	Trimestral	$939.87	$1,879.74	-$939.87
2414154369	CONTRIBUTIVA	EITA820529MSPSRR02	ARACELY ESPINOZA TORRES	9	$7,518.97	Trimestral	$939.87	$1,879.74	-$939.87
2414154369	CONTRIBUTIVA	EITA820529MSPSRR02	ARACELY ESPINOZA TORRES	9	$7,518.97	Trimestral	$939.87	$1,879.74	-$939.87
2414154369	CONTRIBUTIVA	EITA820529MSPSRR02	ARACELY ESPINOZA TORRES	9	$7,518.97	Trimestral	$939.87	$1,879.74	-$939.87
2415186305	CONTRIBUTIVA	GUCM840714MSPZZY10	MAYRA ISABEL GUZMÁN CAZARES	8	$5,650.38	Trimestral	$706.30	$1,412.60	-$706.30
2415186305	CONTRIBUTIVA	GUCN160427HSPZZYA5	NEYMAR URIEL GUZMÁN CAZARES	8	$5,650.38	Trimestral	$706.30	$1,412.60	-$706.30
2415186305	CONTRIBUTIVA	GUCM840714MSPZZY10	MAYRA ISABEL GUZMÁN CAZARES	8	$5,650.38	Trimestral	$706.30	$ 1,412.60	-$706.30
2415186305	CONTRIBUTIVA	GUCN160427HSPZZYA5	NEYMAR URIEL GUZMÁN CAZARES	8	$5,650.38	Trimestral	$706.30	$1,412.60	-$706.30
2516827657	CONTRIBUTIVA	AEHY001005MDGRRSA6	YESENIA SARAHI ARREOLA HERNANDEZ	9	$ 7,518.97	Trimestral	$939.87	$1,879.74	-$939.87

Fuente: Elaborado con información proporcionada por la CNPSS.

- No fue posible validar que los "ID Familia" con estatus "pendiente" en el expediente tengan asignada una vigencia de 90 días.

Criterios de validación de la Integridad de la Información

- Se identificaron 2,994 beneficiarios sin información relacionada al campo "DOCUMENTO_IDENTIFICACIÓN".
- No fue posible verificar las incidencias registradas en la póliza, lo cual no permite identificar de manera detallada la trazabilidad de las actualizaciones a los datos de los beneficiarios del padrón.
- Se realizó la validación de que los beneficiarios cuenten con una unidad médica de adscripción; sin embargo, no es posible realizar la validación de que las claves asignadas a los beneficiarios correspondan a una Unidad Médica.
- Se identifican 125 beneficiarios que tienen el valor "0" en el campo número de integrantes.
- Se identifican 27 beneficiarios menores a un año que tienen asociado el estatus "Estudia".

De acuerdo con los resultados de la aplicación de las pruebas y tomando en consideración los objetivos de integridad, disponibilidad y calidad de la información, la alineación de la auditoría con los criterios de COBIT® 5 "Habilitando la Información", es la siguiente:

Alineación de los criterios de la Auditoría con COBIT® 5 "Habilitando la Información" en relación con los Resultados de las Pruebas a los Datos

ASF	Criterio COBIT	Definición	Observaciones
Integridad	Integridad	Mantener con exactitud la información tal cual fue generada, sin ser alterada por personas o procesos no autorizados.	Respecto a los procedimientos descritos por la Comisión, debido a que no se realiza una administración de las Bases de Datos de las entidades federativas, no se cuentan con elementos que permitan garantizar que la información contenida en cada entidad del SAP, pueda ser modificados de manera manual, con el riesgo de cometer omisiones o manejos irregulares con los datos.
	Consistencia	Se mantiene el mismo formato en los datos, al pasar de una representación a otra.	La información no es consistente, ya que se detectaron diferencias en varios campos relacionadas a criterios de incorporación, así como se identifican campos con información que no permite validar el dato.
	De fácil manejo	La actualización de la información se realiza de forma sencilla, además de que su extracción es fácil y se puede procesar en otros sistemas o aplicaciones.	La información proporcionada permitió el realizar la ejecución de las pruebas.
Disponibilidad	Actualizada	La información se encuentra actualizada en el momento en el que requiere ser consultada, cuando esto no ocurre, se pueden generar retrasos en la ejecución de los procesos.	Para realizar la extracción de la información del periodo evaluado, fue necesario el realizar la carga de la base de datos previo al procedimiento, así como también tuvo que considerarse estos aspectos para la carga de información relacionada a las pólizas contributivas.
	Disponibilidad	Condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.	La información no se encuentra centralizada, ya que durante el 2016 la consolidación de la información de cada una de las entidades federativas fue realizada de forma mensual. Así como tuvo que realizarse la carga de la información histórica del periodo evaluado y de las pólizas contributivas, previo a la extracción de la información.
Calidad	Precisión	La información no tiene error y no produce dudas en quien la utiliza.	Se identificaron múltiples escenarios que no pudieron ser validados debido a campos que no fueron proporcionados por la Comisión, así como también se encontraron diferencias en la información registrada a los beneficiarios y columnas sin datos de información que permitieran validar ese dato.
	Interpretabilidad	Las definiciones son claras, por lo tanto, la interpretación de los datos es rápida y oportuna.	La interpretación de la información facilitó la ejecución de las pruebas.

Fuente: Elaborado por la ASF con base en la información proporcionada por la CNPSS y el resultado de las pruebas de Calidad de Datos.

Verificación de los procedimientos de consolidación de la Información del Padrón de Beneficiarios y Generación de Respaldos.

La información de los beneficiarios del Sistema de Protección Social en Salud es procesada en el Sistema de Administración del Padrón (SAP), el cual es administrado por la Dirección General de Afiliación y Operación (DGAO); en relación con los procedimientos ejecutados por

parte de esta Dirección en relación al Proceso de Desarrollo del Sistema de Administración del Padrón (SAP), se identificó lo siguiente:

Proceso de Desarrollo del Sistema de Administración del Padrón (SAP)

- No se cuenta con una metodología de desarrollo que permita regular las actividades realizadas durante el ciclo de vida del desarrollo de software (análisis de requerimientos, desarrollo, pruebas, implementación, etc.) realizadas al SAP por parte de la Dirección de Sistemas de Afiliación y Operación; asimismo, se carece de evidencia que permita verificar los mecanismos a través de los cuales, esta Dirección garantiza que los procedimientos utilizados en las actualizaciones a este aplicativo, se encuentren alineados a la normatividad y controles establecidos por la Dirección General de Procesos y Tecnología (DGPT).
- Por parte de la Dirección de Sistemas de Afiliación y Operación, no es realizada ninguna documentación que permita identificar de manera puntual los entregables generados como parte del análisis de los requerimientos, pruebas y liberación de los cambios de desarrollo de software; lo cual implica un riesgo significativo en el procesamiento, salvaguarda y resguardo de la información del Padrón de Beneficiarios.
- No se tiene un mecanismo de identificación y seguimiento formal de los riesgos asociados a los requerimientos de desarrollo evolutivo y/o cambios en el Sistema de Administración del Padrón (SAP), a fin de determinar sus impactos y tratamientos.
- Se carece de un procedimiento para la evaluación de la calidad del código fuente del Sistema de Administración del Padrón (SAP), lo cual puede generar altas vulnerabilidades en materia de seguridad de la información.
- No se tiene implementada una base de conocimientos en la que se almacene información cronológica de los incidentes y problemas de la operación, que permitan la reconstrucción y análisis de las actividades ejecutadas en el desarrollo evolutivo del Sistema de Administración del Padrón (SAP).
- No se cuenta con un mecanismo y/o herramienta para efectuar el análisis de vulnerabilidades previo al inicio de la puesta en operación de un cambio al SAP.
- La infraestructura utilizada para la generación de los cambios en el código aplicativo y la ejecución de las pruebas, se encuentra bajo el resguardo del personal de la Dirección de Sistemas de Afiliación y Operación, por lo tanto, carece de las condiciones de seguridad que tiene el Centro de Datos Principal que soporta la operación de los procesos de la CNPSS.
- Se carece de mecanismos de seguridad que permitan garantizar que los equipos de cómputo utilizados para las actualizaciones al SAP, cuentan con controles de seguridad que aseguren la integridad, confidencialidad, confiabilidad y disponibilidad de la información del Padrón de Beneficiarios.
- No existe un procedimiento para la regulación de los cambios realizados a las cuentas de usuario del SAP, lo cual implica un riesgo sustantivo a la operación,

debido a la falta de vigilancia del uso de los privilegios de usuario asignados en la aplicación. Tampoco existe un procedimiento que permita regular de manera integral las actividades realizadas en esta materia en cada entidad federativa, por parte del Jefe de Administración del Padrón, así como la existencia de un procedimiento que garantice el cumplimiento de las actividades operativas de este responsable.

Consolidación de la Información del Padrón de Beneficiarios y Generación de Respaldos

- No se cuenta con procedimientos y/o mecanismos de control que garanticen la integridad y confidencialidad de los datos.
- Se carece de evidencia que permita validar la implementación de políticas para la gestión de respaldos.
- No es posible verificar controles mínimos de seguridad que permitan garantizar el adecuado resguardo de la información.
- En relación a los procedimientos ejecutados por parte de la DGAO respecto al Proceso de Desarrollo del Sistema de Administración del Padrón (SAP), no se identifican acciones de regulación en materia de Seguridad y Tecnologías de la Información realizadas por parte de la Dirección General de Procesos y Tecnología (DGPT) de la Comisión que permitan garantizar que los cambios y/o actualizaciones al SAP realizados durante 2016 fueron regulados a través de mecanismos de control que garantizaran un óptimo procesamiento y resguardo de la información del padrón de beneficiarios.

Como resultado de la revisión realizada a la calidad de los datos correspondiente a los beneficiarios adscritos al Sistema de Protección Social en Salud para el ejercicio fiscal 2016, se identificó que existieron deficiencias en los mecanismos de control para identificar la no derechohabiencia de los beneficiarios; inconsistencias en la información de las colectividades registradas; omisiones en la verificación de las mujeres embarazadas afiliadas; diferencias de los pagos realizados por los beneficiarios, en relación al decil en el cual se encuentran catalogados; omisiones de información de la documentación que acredita la identidad de los beneficiarios;-verificación de la información del catálogo de Unidades Médicas; omisiones al verificar que todas las pólizas cuenten con al menos un integrante, así como en la veracidad de la información registrada de los beneficiarios.

Asimismo, se identificaron inconsistencias por la falta de implementación de una metodología de desarrollo de software; se carece de un procedimiento para realizar análisis de vulnerabilidades de los cambios al código aplicativo del SAP; no se cuenta con un procedimiento para la gestión de los cambios de las cuentas de usuario y se carece de la implementación de políticas de respaldos.

16-5-12U00-02-0216-01-003 **Recomendación**

Para que la Comisión Nacional de Protección Social en Salud implemente acciones y mecanismos de control que aseguren la integridad de la información contenida en el Padrón de Beneficiarios, que se encuentren totalmente alineados a los procedimientos y/o mecanismos de control determinados por la Dirección General de Procesos y Tecnología, con

la finalidad de garantizar la integridad de los datos de las personas adscritas al Sistema de Protección Social en Salud, así como implemente acciones relacionadas para la utilización de la infraestructura tecnológica del Centro de Datos utilizado por la Comisión para tales fines.

16-5-12U00-02-0216-01-004 **Recomendación**

Para que la Comisión Nacional de Protección Social en Salud implemente en el Sistema de Administración del Padrón, una metodología para el desarrollo de soluciones de Tecnologías de la Información y Comunicaciones, que considere entre otros elementos, los requerimientos de los servicios, el diseño de las soluciones, las revisiones de calidad, el cierre de las iniciativas y la evaluación de los beneficios de los cambios al Sistema; asimismo, que las acciones o mecanismos de control por implementarse se encuentren alineados conforme a los lineamientos y normativas emitidos por la Dirección General de Procesos y Tecnología de la Comisión.

16-5-12U00-02-0216-01-005 **Recomendación**

Para que la Comisión Nacional de Protección Social en Salud implemente los mecanismos de control que permitan que la Unidad de Tecnologías de Información y Comunicaciones (UTIC) de la Comisión, gobierne y administre el uso de las tecnologías de información en todas las áreas de la Comisión; asimismo, que la UTIC inicie con las acciones para coordinar y administrar los sistemas informáticos que procesan la información del Padrón de Beneficiarios.

16-9-12U00-02-0216-08-003 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en relación con la evaluación de la calidad de datos, se detectaron irregularidades vinculadas con las responsabilidades de los Titulares de la Dirección de Planeación y Administración del Padrón y la Dirección de Sistemas de Afiliación y Operación, debido a que del análisis de la información de los beneficiarios, se presentaron inconsistencias tales como verificar la información de los beneficiarios en relación a la acreditación de la no derechohabiencia de las personas adscritas; validar la integridad de la información de los beneficiarios; implementar mecanismos para resguardar el almacenamiento de las actualizaciones realizadas a la información de los beneficiarios; mitigar las inconsistencias entre la categorización del decil asignado a los beneficiarios y el pago realizado; así como verificar que la totalidad de las pólizas cuenten con al menos un integrante.

16-9-12U00-02-0216-08-004 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa para que el Órgano Interno de Control realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente, por las irregularidades de los servidores públicos que, en su gestión, en relación con la evaluación de la calidad de datos, se detectaron irregularidades vinculadas con las responsabilidad de los Titulares de la Dirección de Planeación y Administración del Padrón y la Dirección de Sistemas de Afiliación y Operación, debido a que omitieron definir e implementar una metodología para el Sistema

de Administración del Padrón que establezca las actividades de desarrollo, mantenimiento y control de cambios en los sistemas; carencia de la segregación de funciones entre ambientes de operación y de desarrollo; falta de análisis y evaluación de cada uno de los requerimientos de cambios, nuevos desarrollos, mantenimientos a los sistemas, diseño, construcción, pruebas y aprobación, considerando a las áreas usuarias; carencia de un plan de aseguramiento de calidad del software a fin de garantizar el cumplimiento de los criterios de aceptación y gestión del código fuente para el adecuado procesamiento de la información, así como la mitigación de posibles vulnerabilidades del mismo.

Resumen de Observaciones y Acciones

Se determinó (aron) 4 observación (es) la (s) cual (es) generó (aron): 8 Recomendación (es) y 7 Promoción (es) de Responsabilidad Administrativa Sancionatoria.

Dictamen

Con base en los resultados de la auditoría practicada a la Comisión Nacional de Protección Social en Salud, cuyo objetivo consistió en fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada por 72,854.0 miles de pesos, se concluye que en términos generales cumplió con las disposiciones legales y normativas que son aplicables en la materia excepto por los resultados descritos en el presente informe de auditoría, que arrojaron deficiencias y debilidades que son importantes, entre las que destacan las siguientes:

- La Dirección General de Procesos y Tecnología (DGPT) de la CNPSS se encuentra limitada para cumplir con sus facultades estipuladas en el Reglamento Interno de la CNPSS, debido a que varios de los procesos de Gobierno de TIC son manejados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA, lo cual no es operativo y provoca deficiencias en los procesos de planeación estratégica, administración de proveedores y análisis de riesgos en la Comisión. De la misma manera, varios de los procesos de Seguridad de la Información y Continuidad de las Operaciones, son gestionados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA, lo cual aumenta los riesgos en los procesos del sistema de gestión de seguridad de la información, gestión de incidentes y planes de recuperación en caso de contingencias.

- Se advierten deficiencias en las actividades de gestión de los contratos para la verificación de los servicios, debido a que no fue posible validar los mecanismos ejecutados por la Dirección General de Tecnologías de la Información (DGTI) de la SSA para la revisión de los reportes que avalan los servicios. Cabe señalar que la Dirección General de Procesos y Tecnología (DGPT) de la CNPSS no tiene injerencia en la operación de los servicios, lo cual no es funcional y repercute en la baja calidad de los niveles de servicio que se prestan a la Comisión.

- La Dirección General de Procesos y Tecnología (DGPT) de la CNPSS no cuenta con evidencia de la evaluación de Segregación de Funciones en las actividades operativas de TIC, que permita identificar oportunamente procedimientos que pudieran impactar en fraude, irregularidades en los procesos, duplicidad de funciones, etc.
- De la revisión realizada a la calidad de los datos de los beneficiarios adscritos al Sistema de Protección Social en Salud, se identificaron deficiencias en los mecanismos de control implementados tales como la verificación de la no derechohabiencia de los beneficiarios; inconsistencias en la información de las colectividades registradas; omisiones en la verificación de las mujeres embarazadas afiliadas; diferencias de los pagos realizados por los beneficiarios, en relación al decil en el cual se encuentran catalogados; omisiones para acreditar la identidad de los beneficiarios, así como la falta de integridad en la información registrada en el padrón.
- En relación con el Sistema de Administración del Padrón (SAP) de beneficiarios, se carece de una metodología de desarrollo de software; no se cuenta con un procedimiento para realizar análisis de vulnerabilidades de los cambios al código aplicativo del SAP; no existe un procedimiento para la gestión de los cambios de las cuentas de usuario y se carece de la implementación de políticas de respaldos.

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

El presente dictamen se emite el 27 de octubre de 2017, fecha de conclusión de los trabajos de auditoría correspondientes a la Cuenta Pública 2016, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable.

Servidores públicos que intervinieron en la auditoría:

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la cuenta pública correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; análisis del gasto ejercido en materia de tic en los capítulos contables de la cuenta pública fiscalizada.
2. Validar que el estudio de factibilidad comprenda el análisis de las contrataciones vigentes; la determinación de la procedencia de su renovación; la pertinencia de realizar contrataciones consolidadas; los costos de mantenimiento, soporte y operación que

impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como el estudio de mercado.

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo a las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el programa anual de adquisiciones, arrendamientos y servicios; 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 realizados por los trabajos contratados estén debidamente soportados, cuenten con controles que permitan su fiscalización, correspondan a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización 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 a la infraestructura tecnológica, telecomunicaciones y aplicativos sustantivos para verificar: antecedentes; investigación de mercado; adjudicación; beneficios esperados; análisis de entregables (términos, vigencia, entrega, resguardo, operación, penalizaciones y garantías); pruebas de cumplimiento y sustantivas; implementación y post-implementación.

6. Evaluar el nivel de gestión que corresponde a los procesos relacionados con la dirección, el control y la administración de riesgos en materia de tecnologías de la información y comunicaciones; análisis del diagnóstico de las funciones sustantivas y administrativas de las tic que lleva a cabo la entidad fiscalizada; evaluación del nivel de alineación de la estrategia de tic con los objetivos de la organización, así como de los mecanismos de medición, seguimiento y cumplimiento de sus metas; revisión del avance en la implementación del MAAGTIC-SI o en su caso, la normativa que aplique; revisión del cumplimiento de las disposiciones en materia de datos abiertos.

7. Evaluar los mecanismos que permitan la administración de la seguridad de la información, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar los objetivos de la institución o constituir una amenaza para la seguridad nacional; evaluar el nivel de cumplimiento en la optimización del riesgo; verificar la gestión de seguridad de la información y gestión de los programas de continuidad de las operaciones; revisar el control de accesos y privilegios, segregación de funciones, controles de las cuentas funcionales y privilegiadas en los aplicativos y bases de datos sustantivos; verificar los mecanismos implementados para la transferencia de datos sobre canales seguros, así como los estándares aplicados para el cifrado de datos en operación. Evaluación de la seguridad física del centro de datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).

8. Verificar que los procesos guardan relación con lo definido en las "reglas de negocio" de la entidad; la implementación y operación de las acciones realizadas por el grupo de trabajo 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 Procesos y Tecnología (DGPT), la Dirección General de Afiliación y Operación (DGAO), ambas de la Comisión Nacional de Protección Social en Salud (CNPSS), así como la Dirección General de Tecnologías de la Información (DGTI) de la Secretaría de Salud (SSA).

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. Otras disposiciones de carácter general, específico, estatal o municipal: Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y, en la de Seguridad de la Información (MAAGTICSI), publicado el 04 de febrero del 2016 en el Diario Oficial de la Federación (DOF): Artículos 26, 27; Procesos: I.A Planeación Estratégica; II.A. Proceso de Administración de Servicios (ADS) Actividades: ADS 2, ADS 3 y ADS 4; II.C. Proceso de Administración de la Seguridad de la Información (ASI) Actividades: ASI 1, ASI 2, ASI 3, ASI 5 Factores críticos 4, 5, 6 y 8, ASI 6 y ASI 7; I.B Proceso de Administración del Presupuesto y las Contrataciones (APCT); III.A Proceso de Administración de Proyectos (ADP), Actividad ADP 2; III.B Proceso de Administración de Proveedores (APRO); III.D Proceso de Operación de los Controles de Seguridad de la Información y del ERISC (OPEC), Actividad OPEC 2;

Contrato No. DGRMSG-DCC-S-015-2016: Cláusula Quinta y Octava; Convenio modificatorio número 01/16; Anexo Único del Contrato No. DGRMSG-DCC-S-015-2016: numerales, 2, 6.1, 6.2, 6.3, 6.4, 6.6, 6.7, 6.8, 6.10, 6.11, 6.13 y 6.14;

Reglamento Interno de la Comisión Nacional de Protección Social en Salud, última reforma publicada en el Diario Oficial de la Federación el 11 de octubre de 2012: Artículo 8 Fracciones VII y VIII y Artículo 10 Bis 4;

Guía de Implementación de la Política de Datos Abiertos, publicada en el DOF el 18 de junio de 2016; Proceso de Publicación e inicio de acciones de los Planes de Acción de Datos Abiertos en cada entidad que contendrán el inventario, procesos de priorización, Catálogo de datos públicos y cronograma de apertura de los mismos.

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, párrafo primero, de la Constitución Política de los Estados Unidos Mexicanos.

Artículos 9, 10, 11, 14, fracción III, 15, 17, fracciones XV, XVI y XVII, 34, fracción V, 36, fracción V, 37, 39, 40, 49 y 67, fracciones I, II, III y IV, de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

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 esta entidad fiscalizadora para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.