

**Secretaría de Salud**

**Auditoría de TIC**

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2021-0-12100-20-0341-2022

Modalidad: Presencial

Núm. de Auditoría: 341

***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 2021 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.

***Alcance***

	<b>EGRESOS</b>
	Miles de Pesos
Universo Seleccionado	1,005,565.5
Muestra Auditada	144,714.9
Representatividad de la Muestra	14.4%

El universo seleccionado por 1,005,565.5 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 2021; la muestra auditada está integrada por 4 contratos y 10 convenios modificatorios, relacionados con los servicios de arrendamiento de equipo informático; de mantenimiento y de aplicaciones sustantivas, así como de servicios de telecomunicaciones, con pagos ejercidos por 144,714.9 miles de pesos, que representan el 14.4% del universo seleccionado.

Adicionalmente, la auditoría comprende el análisis presupuestal de la Cuenta Pública de 2021 de la Secretaría de Salud (SSA) en relación con los gastos en materia de Tecnologías de Información y Comunicaciones, la revisión de los procesos de Ciberseguridad en la infraestructura de la SSA, Continuidad de las operaciones, así como de la Estrategia de vacunación contra COVID-19. Los recursos objeto de revisión en esta auditoría se encuentran

reportados en la Cuenta de la Hacienda Pública Federal del ejercicio de 2021, Tomo III, apartado Información Presupuestaria en el "Estado Analítico del Ejercicio del Presupuesto de Egresos en Clasificación Administrativa", correspondiente al Ramo 12 "Salud".

### **Antecedentes**

La Secretaría de Salud (SSA) es la dependencia del Poder Ejecutivo que se encarga primordialmente de la prevención de enfermedades y promoción de la salud de la población. Las estrategias definidas en el Plan Sectorial de Salud 2020-2024 suponen cuatro vertientes para el incremento en la capacidad del sistema: la planeación integral del fortalecimiento; la capacidad humana en términos de suficiencia, capacitación y profesionalización; la infraestructura en la que se incluye el equipamiento y, finalmente, la relacionada con tecnologías de información y comunicación.

La Dirección General de Tecnologías de Información (DGTI) se encarga de establecer las políticas y la normativa técnica aplicables para el uso de las tecnologías de la información, así como de dirigir y operar los servicios en las unidades administrativas y órganos desconcentrados de la Secretaría de Salud, así como de detectar las necesidades de automatización o actualización tecnológica, entre otras.

Como parte del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública de 2020, se realizó la auditoría 222-DS titulada "Auditoría de TIC", en donde se validaron los servicios de arrendamiento de equipo informático; los de fábrica de software, servicios de telecomunicaciones y los de centro de datos, así como la revisión de la función de TIC en la SSA en 2020, relacionadas con Calidad de Datos, Ciberseguridad y Continuidad de las Operaciones.

Con la información proporcionada por la entidad se determinó que, entre 2017 y 2021, la Secretaría de Salud ha invertido 1,064,741.5 miles de pesos en materia de Tecnologías de la Información (TIC), y se observaron inconsistencias respecto a las cifras presentadas en la Auditoría número 222-DS correspondiente a la fiscalización superior de la Cuenta Pública de 2020, como se muestra a continuación:

DIFERENCIA RECURSOS INVERTIDOS EN MATERIA DE TIC – CUENTA PÚBLICA DE 2020 VS CUENTA PÚBLICA DE 2021

(Miles de pesos)

Periodo de inversión	2016	2017	2018	2019	2020	2021	Total
Cuenta Pública 2020	437,933.5	405,915.4	427,100.8	62,435.1	267,425.3	N/A	<b>1,600,810.1</b>
Cuenta Pública 2021	N/A	425,813.4	447,961.4	64,607.1	44,837.7	81,521.9	<b>1,064,741.5</b>
<b>Diferencia</b>	<b>N/A</b>	<b>- 19,898.0</b>	<b>- 20,860.6</b>	<b>- 2,172.0</b>	<b>222,587.6</b>	<b>N/A</b>	

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Cabe señalar que la integración proporcionada contempla partidas presupuestarias no relacionadas con gastos de TIC, aunado a que la información sólo corresponde a la Dirección General de Tecnologías de Información, siendo que ésta no es la única Unidad Administrativa que eroga presupuesto en las contrataciones de Tecnologías de Información en la Secretaría de Salud.

En el análisis de la gestión de las TIC efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados, con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones y la función de las TIC sujetas de revisión, y determinar el alcance, naturaleza y muestra de la revisión del cual, se obtuvieron los resultados que se presentan en este informe.

## **Resultados**

### **1. Análisis Presupuestal**

De acuerdo con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal de 2021, publicado en el Diario Oficial de la Federación el 30 de noviembre de 2020, a la Secretaría de Salud (SSA) se le aprobó un presupuesto de 145,414,570.9 miles de pesos.

Respecto del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2021, la SSA tuvo un presupuesto ejercido de 9,062,071.7 miles de pesos en el capítulo 3000, de los cuales, 1,005,565.5 miles de pesos corresponden a recursos relacionados con las Tecnologías de Información y Comunicaciones (TIC), lo que representa el 11.1% del presupuesto ejercido, como se muestra a continuación:

#### RECURSOS EJERCIDOS EN CONTRATACIONES RELATIVAS A LAS TIC EN LA SSA DURANTE 2021

(Miles de pesos)

		A	B	C= B/A
Capítulo	Descripción	Ejercido	Ejercido TIC	%
3000	Servicios Generales	9,062,071.7	1,005,565.5	11.1
<b>TOTAL</b>		<b>9,062,071.7</b>	<b>1,005,565.5</b>	<b>11.1</b>

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Los recursos ejercidos en materia de TIC por 1,005,565.5 miles de pesos se integran de la manera siguiente:

INTEGRACIÓN DEL GASTO DE LAS CONTRATACIONES RELACIONADAS CON LAS TIC EN 2021 EN LA SSA

(Miles de pesos)

Capítulo / P. Presupuestaria	Subpartida	Descripción	Presupuesto Ejercido
<b>3000</b>		<b>Servicios Generales</b>	
3100		<b>Servicios básicos</b>	<b>365,895.0</b>
	31602	Servicios de telecomunicaciones	117,190.3
	31603	Servicios de internet	18,404.6
	31701	Servicios de conducción de señales analógicas y digitales	16,946.6
	31901	Servicios integrales de telecomunicación	26,779.6
	31904	Servicios integrales de infraestructura de cómputo	186,573.9
3200		<b>Servicios de Arrendamiento</b>	<b>160,077.0</b>
	32301	Arrendamiento de equipo y bienes informáticos	139,164.3
	32303	Arrendamiento de equipo de telecomunicaciones	2,478.3
	32701	Patentes, derechos de autor, regalías y otros	18,434.4
3300		<b>Servicios profesionales, científicos, técnicos y otros servicios</b>	<b>471,418.9</b>
	33301	Servicios de desarrollo de aplicaciones informáticas	42,628.0
	33304	Servicios de mantenimiento de aplicaciones informáticas	45,128.0
	33606	Servicios de digitalización	143.3
	33903	Servicios integrales	383,519.6
3500		<b>Servicios de instalación, reparación, mantenimiento y conservación</b>	<b>8,174.6</b>
	35301	Mantenimiento y conservación de bienes informáticos	8,174.6
<b>TOTAL</b>			<b>1,005,565.5</b>

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Del universo seleccionado en 2021 por 1,005,565.5 miles de pesos, que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 144,714.9 miles de pesos en 4 contratos y 10 convenios modificatorios que representan el 14.4% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS EJERCIDOS DURANTE 2021 POR LA SSA  
(Miles de pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Ejercido
				De	Al	Mínimo	Máximo	
Contrato Marco	DGRMSG-DCC-S-045-2021	Ofi Productos de Computación, S.A. de C.V.	Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6.	01/07/2021	31/12/2023	10,957.6	27,394.0	5,610.5
Contrato Marco	DGRMSG-DCC-S-055-2021	Mainbit, S.A. de C.V.	Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E1 y E2.	11/09/2021	31/12/2023	16,206.0	40,516.0	0.0
Adjudicación Directa	DGRMSG-DCC-S-008-2018	Consortio Red Uno, S.A. de C.V., Triara.Com, S.A. de C.V., Scitum, S.A. de C.V., Prestaciones Profesionales Empresariales, S.A. de C.V. y Servicios Especializados Scitum, S.A. de C.V.	Servicio Integral de Telecomunicaciones (SINTEL)	13/04/2018	31/03/2021	383,144.2	957,860.6	
	Primer Convenio Modificadorio 01/21		Ampliación de la vigencia.	01/04/2021	30/06/2021	N/A	N/A	
	Segundo Convenio Modificadorio 02/21		Ampliación de la vigencia.	01/07/2021	30/09/2021	N/A	N/A	
	Tercer Convenio Modificadorio 03/21		Ampliación de la vigencia.	01/10/2021	31/12/2021	N/A	N/A	119,229.8
	Cuarto Convenio Modificadorio 04/21		Ampliación de la vigencia.	01/01/2022	31/03/2022	N/A	N/A	
	Quinto Convenio Modificadorio 05/21		Ampliación de la vigencia.	31/03/2022	30/06/2022	N/A	N/A	
				<b>Subtotal</b>		<b>383,144.2</b>	<b>957,860.6</b>	<b>119,229.8</b>
Contratación entre Entes Públicos	DGRMSG-DCC-S-020-2020		Servicio para Mantenimiento y Desarrollo de Aplicaciones Sustantivas	29/05/2020	31/12/2020	13,680.6	34,201.4	
	Primer Convenio Modificadorio 01/20		Ampliación de la vigencia.	23/12/2020	31/03/2021	N/A	N/A	
	Segundo Convenio Modificadorio 02/21	Centro de Investigación e Innovación en Tecnologías de la Información y	Ampliación de la vigencia.	31/03/2021	30/06/2021	N/A	N/A	19,874.6
	Tercer Convenio Modificadorio 03/21	Comunicación (INFOTEC)	Ampliación de la vigencia.	30/06/2021	31/12/2021	N/A	N/A	
	Cuarto Convenio Modificadorio 04/21		Ampliación del monto y vigencia.	31/12/2021	31/03/2022	2,736.1	6,840.3	
Quinto Convenio Modificadorio 05/22		Ampliación de la vigencia.	01/04/2022	30/06/2022	N/A	N/A		
				<b>Subtotal</b>		<b>16,416.7</b>	<b>41,041.7</b>	<b>19,874.6</b>
				<b>Total</b>		<b>426,724.5</b>	<b>1,066,812.3</b>	<b>144,714.9</b>

FUENTE: Contratos y facturas proporcionadas por la SSA.

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. Contratos DGRMSG-DCC-S-045-2021 y DGRMSG-DCC-S-055-2021 “Servicio de Arrendamiento de Equipo de Cómputo Personal y Periféricos”

El 17 de junio de 2020, la Secretaría de Salud formalizó el “Contrato Marco para la contratación del Arrendamiento de Equipo de Cómputo Personal y Periféricos para las Dependencias y Entidades de la Administración Pública Federal”, mediante el procedimiento de invitación a cuando menos tres personas número IA-012000991-E87-2021, con fundamento en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); en los artículos 17, 24, 26, fracción II, 26 Bis, fracción II, 27, 28, fracción I, 29, 40, 41, fracción XX, 43 y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); y en los artículos 14, 39, 71, 77, 78 y 85 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP); con vigencia al 31 de diciembre de 2023, dicho contrato considera equipo de cómputo distribuido en 32 partidas y 5 contratos específicos.

El alcance de los trabajos de fiscalización abarcó los contratos núm. DGRMSG-DCC-S-045-2021 y DGRMSG-DCC-S-055-2021. El detalle se muestra a continuación:

CONTRATOS DEL SERVICIO DE ARRENDAMIENTO DE EQUIPO DE CÓMPUTO PERSONAL Y PERIFÉRICOS						
Contrato	Prestador de servicios	Objetivo	Vigencia	Monto del contrato	Ejercido 2021	
				(Miles de pesos)		
DGRMSG-DCC-S-045-2021	Ofi Productos de Computación, S.A. de C.V.	Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6.	Del 1 de julio de 2021 al 31 de diciembre de 2023.	mínimo 10,957.6 máximo 27,394.0	5,610.5	
DGRMSG-DCC-S-055-2021	Mainbit, S.A. de C.V.	Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E1 y E2.	Del 11 de septiembre de 2021 al 31 de diciembre de 2023.	mínimo 16,206.0 máximo 40,516.0	0.0	

FUENTE: Elaborado con base en la información proporcionada por la SSA.

En los contratos señalados anteriormente, se revisó la factibilidad de su contratación y se identificó lo siguiente:

### Proceso de Contratación

- No se identificaron las actividades ejecutadas por la SSA para evitar que, en el procedimiento de adhesión al Contrato Marco, los servidores públicos que intervinieron no se aprovecharan de su cargo para favorecer a alguna(s) de las personas que hayan presentado cotización y que se exigiera de éstas la misma conducta.

- Se observó que el Órgano Interno de Control (OIC) en la Secretaría de Salud recomendó designar a personal de nivel mando medio para que éste realizara la gestión y administración del proyecto; no obstante, la Dirección General de Tecnologías de Información (DGTI) de la SSA asignó a personal de soporte administrativo.
- La justificación para solicitar la autorización presupuestal para la contratación plurianual del Arrendamiento de Equipo de cómputo personal y periféricos carece de fecha de elaboración y autorización, por lo que no fue posible verificar el cumplimiento del plazo establecido en el artículo 147, fracción I, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (RLFPRH), ni del segundo párrafo del numeral 12.2. Contratos y pedidos plurianuales de sus Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público (POBALINES).
- En la revisión al procedimiento de contratación de invitación a cuando menos tres personas, se identificó lo siguiente:
  - No se estableció en la convocatoria la definición de si la totalidad de bienes o servicios objeto de la licitación serían adjudicados a un solo licitante, o si se efectuaría mediante el procedimiento de abastecimiento simultáneo.
  - El Acta correspondiente a la celebración de Presentación y Apertura de Propositiones carece de la firma autógrafa del representante del OIC.
  - Se carece de las solicitudes de cotización y las invitaciones a cuando menos tres personas que permitan acreditar que éstas cumplen con lo establecido en la Cláusula Sexta. “De la Selección del proveedor”, apartado B. “Para la Invitación a Cuando Menos Tres Personas”, fracción II, del Contrato Marco.

#### **Contrato DGRMSG-DCC-S-045-2021 “Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6.”**

La SSA formalizó el contrato específico núm. DGRMSG-DCC-S-045-2021 con la empresa Ofi Productos de Computación, S.A. de C.V., con objeto de prestar el servicio de “Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6”; con vigencia del 01 de julio de 2021 al 31 de diciembre de 2023, por un monto mínimo de 10,957.6 miles de pesos y un máximo de 27,394.0 miles de pesos.

#### **Alcance del Servicio**

El contrato se formalizó con el propósito de contar con el arrendamiento de equipo de cómputo personal y periféricos para las partidas E4, E6 y P6, las cuales contemplan lo siguiente:

ALCANCE DE LOS SERVICIOS DEL CONTRATO ESPECÍFICO NÚM. DGRMSG-DCC-S-045-2021

Partida	Contrato marco		Descripción de la partida	Cantidad	
	ID Partida	Perfil		Mínimo	Máximo
E4	16	"L3"	Computadora portátil especializada (laptop Workstation) con estación de trabajo para laptop.	1,110	2,275
E6	18	"M2"	Apple de Escritorio iMac.	50	125
P6	29	"P09"	Video Proyector.	184	460

FUENTE: Elaborado con base en la información proporcionada por la SSA.

### Pagos

Durante 2021 se realizaron pagos por 5,610.5 miles de pesos y con recursos del ejercicio 2022 un pago por 84.5 miles de pesos, correspondiente a los servicios de diciembre de 2021; en la información analizada se observó lo siguiente:

- El pago de una factura por un importe de 84.5 miles de pesos no se realizó dentro de los 20 días naturales contados a partir de la entrega del Comprobante Fiscal Digital por Internet (CFDI).
- No se cuenta con las memorias de cálculo que permitan acreditar que las penas convencionales por 730.0 miles de pesos, calculadas por la Dirección de Red y Telecomunicaciones (DRT) por atrasos del proveedor en la entrega de equipos, son correctas. Asimismo, se detectó que para los meses de enero y febrero de 2022 también se aplicaron penas convencionales por atrasos en la entrega de equipos.

### Cumplimiento técnico y funcional de los servicios y entregables establecidos en el anexo técnico del contrato

- No se han realizado actividades de análisis de activos de hardware y software a los equipos de arrendamiento, por medio de la herramienta provista por el proveedor; asimismo, ésta únicamente permite gestionar el encendido y apagado de los equipos de cómputo con sistema operativo Windows (Laptop L3) conectados a la red de la secretaría.
- El prestador de servicios administra y actualiza el inventario del equipamiento (laptops especializadas [Dell Latitude], video proyectores y equipos de escritorio iMac) de forma manual a través de documentos en Excel.
- El control de altas, bajas, cambios, reasignaciones y reubicaciones de los equipos de arrendamiento para actualizar el inventario no se realiza periódicamente; tampoco se cuenta con un procedimiento documentado y formalizado para llevar a cabo dichos procesos.

- No se observó el tipo de configuración básica que se aplicó en los equipos de cómputo, incluyendo el software autorizado y configuraciones de seguridad mínimas requeridas por la secretaría.
- Las actualizaciones del sistema operativo en equipos de cómputo, emitidas por el fabricante, son aplicadas sin que la secretaría verifique de manera previa la compatibilidad y su funcionamiento.
- No se identificó la fecha en que concluyó la fase de despliegue del equipamiento solicitado por la secretaría, ni se cuenta con evidencia que demuestre que el administrador del contrato efectuó la evaluación inicial de equipos arrendados, para acreditar que éstos fueron instalados en el plazo establecido en el anexo técnico del contrato.
- A la fecha de la auditoría (septiembre 2022), el proveedor no ha entregado a la DRT la dirección del sitio web para la descarga de manuales.
- El administrador del contrato no verificó el monto al que ascienden los servicios mensuales, únicamente dio su visto bueno a la prefactura emitida por el proveedor.
- No se cuenta con procedimientos para realizar los mantenimientos (preventivos, correctivos o por casos de emergencia) al equipo arrendado, en donde se describan las actividades, responsables, frecuencia de éstos, así como sus alcances. A la fecha de la auditoría (septiembre 2022), no se han ejecutado mantenimientos al equipamiento.
- Se carece de un procedimiento formalizado para la gestión de incidencias relacionadas a desperfectos, robos, extravío o descomposturas en el equipamiento como consecuencia de casos fortuitos (incendios, desastres naturales o ciberataques).
- No se identificaron los mecanismos utilizados por el administrador del contrato para evaluar el desempeño del proveedor, con respecto a la gestión de fallas, solicitudes, así como para los casos de atrasos relevantes en la entrega de equipos.
- Se carece de mecanismos para notificar las inconsistencias detectadas por el administrador del contrato en la documentación proporcionada por el proveedor como parte de los entregables mensuales.
- En el contrato marco y específico no se establecieron penalizaciones por atrasos en la atención de incidentes por parte del proveedor.
- El plan de trabajo del proyecto no se encuentra formalizado y no incluye las fechas de los hitos importantes (fase de inicio, evaluación inicial y conclusión del despliegue);

tampoco cuenta con documentación en donde se acredite la instalación y puesta en marcha de los equipos con los usuarios finales.

- No se realizó el análisis de necesidades detallado, por unidad administrativa de la secretaría, en el cual se justificara la elección de los equipos por perfil y que demostrara que los usuarios requerían el equipamiento solicitado para la ejecución de sus actividades, como fue el caso de los equipos de la marca Apple.
- La secretaría carece de mecanismos de control que mitiguen la pérdida o robo de activos.
- De un total de 1,402 equipos de cómputo y componentes (laptops especializadas, equipos de escritorio iMac y video proyectores), se seleccionó una muestra aleatoria de 446 equipos (31.8%) suministrados al 31 de diciembre de 2021, de los cuales se realizó la validación de las especificaciones técnicas requeridas en el anexo técnico del contrato. En la revisión realizada, se observó lo siguiente:
  - No se acreditó la existencia de 17 equipos (3.8% de la muestra) por los que se pagaron 97.0 miles de pesos.
  - Existen 93 equipos (20.9% de la muestra) que se encontraban en almacén o en su embalaje original (sin abrir) por lo que, desde el momento de su entrega por parte del proveedor y a la fecha de la auditoría (septiembre 2022), éstos no están en operación ya que no han sido instalados ni configurados por el prestador de servicios, en consecuencia, no fueron utilizados por personal de la secretaría para el desempeño de sus actividades; no obstante, se han realizado pagos por 216.4 miles de pesos.
  - 13 videoproyectores no cuentan con su resguardo.
  - El listado de equipos de arrendamiento proporcionado por la DRT no contiene la actualización respecto al domicilio de las unidades administrativas de la secretaría.

Se concluye que existieron deficiencias en la supervisión del contrato, toda vez que no se cuenta con la documentación que acredite que el administrador del mismo estableció mecanismos de control que documentaran los procesos de entrega e implementación del equipo arrendado; no se llevó a cabo un análisis de necesidades para determinar el equipamiento a requerir; existen deficiencias en el inventario de equipos; el contrato no contempló los procedimientos para la ejecución de actividades relevantes para el servicio como lo son: mantenimientos, gestión de solicitudes, mecanismos de supervisión a la mesa de servicios, así como para el reemplazo de equipos; no se realizó una validación de los equipos entregados ni un seguimiento del cumplimiento del contrato, en consecuencia, se identificó equipamiento que se encontraba en almacén o en su embalaje original, por el que

se realizaron pagos por 216.4 miles de pesos; asimismo, la secretaría no pudo demostrar la existencia de 17 equipos por los que realizó pagos por 97.0 miles de pesos.

### **Contrato DGRMSG-DCC-S-055-2021 “Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E1 y E2.”**

La SSA formalizó el contrato específico núm. DGRMSG-DCC-S-055-2021 con la empresa Mainbit, S.A. de C.V., con objeto de prestar el servicio de “Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E1 y E2”; con vigencia del 11 de septiembre de 2021 al 31 de diciembre de 2023, por un monto mínimo de 16,206.0 miles de pesos y un máximo de 40,516.0 miles de pesos.

El 30 de junio de 2021 la secretaría emitió el fallo de los proveedores seleccionados; el 10 de septiembre de 2021, se celebró el “Acta de notificación de reposición de fallo” debido a la inconformidad por las partidas E1 y E2 que presentó la empresa Mainbit, S.A. de C.V., ante el OIC en la Secretaría de Salud, ya que éstas habían sido adjudicadas a otro proveedor; una vez realizadas nuevas evaluaciones a sus propuestas, la secretaría determinó que ambas eran aceptables; no obstante, la empresa Mainbit, S.A. de C.V., cumplió técnicamente con lo solicitado en la Convocatoria y ofertó los mejores precios unitarios, por lo que se le adjudicaron las partidas E1 y E2.

### **Alcance del Servicio**

El contrato se formalizó con el propósito de contar con el arrendamiento de equipo de cómputo personal y periféricos para las partidas E1 y E2, las cuales contemplan lo siguiente:

ALCANCE DE LOS SERVICIOS DEL CONTRATO ESPECÍFICO NÚM. DGRMSG-DCC-S-055-2021					
Partida	Contrato marco		Descripción de la partida	Cantidad	
	ID Partida	Perfil		Mínimo	Máximo
E1	5	"D3"	Computadora de escritorio intermedia	4,103	10,258
E2	9	"D5"	Computadora de escritorio avanzada	3,664	9,160

FUENTE: Elaborado con base en la información proporcionada por la SSA.

### **Pagos**

Al 14 de febrero de 2022, no se han realizado pagos por los servicios prestados en el 2021 debido a que el proveedor no ha presentado facturas relacionadas con los servicios prestados en 2021.

La DRT indicó que el proveedor presentó atrasos en la entrega de los equipos, iniciando su entrega e instalación hasta el 2022, lo que incumplió el plazo de 45 días naturales establecido en el anexo técnico (26 de octubre de 2021). Por lo anterior, se le notificaron al proveedor penas convencionales por 6,013.7 miles de pesos, correspondientes al periodo de octubre a

diciembre de 2021; sin embargo, no se proporcionaron las memorias de cálculo que permitan verificar los montos referidos por la secretaría.

### **Cumplimiento técnico y funcional de los servicios y entregables establecidos en el anexo técnico del contrato**

- No se cuenta con un procedimiento para realizar reportes de monitoreo o evaluaciones del desempeño de la mesa de servicio; tampoco para el borrado seguro de un equipo de cómputo ni la definición del responsable de efectuarlos.
- Se carece de un procedimiento para llevar a cabo mantenimientos (preventivos o correctivos) al equipamiento; así como para realizar el reemplazo de equipos de cómputo o periféricos.
- No se entregó la relación de configuraciones para los equipos de cómputo, del licenciamiento propuesto por el proveedor para la prestación del servicio de arrendamiento, ni el listado en donde se observen los números de serie de CPU, monitor, teclado y mouse de los equipos.
- No existe evidencia de que el administrador del contrato verifique los entregables mensuales proporcionados por el proveedor.
- De la herramienta para realizar el diagnóstico y administración de los equipos de cómputo, se observó lo siguiente:
  - La SSA no realizó pruebas en la herramienta para verificar que ésta permite la gestión del inventario, así como el reporte del estado de cifrado y analíticas de uso, incluyendo los casos de cambio de sistema operativo de los equipos.
  - No se cuenta con el manual de operación de la herramienta, para identificar las alertas que emite ésta ante eventos de reubicación de equipos, funcionalidad de rastreo y su seguimiento; así como para ejecutar altas y bajas de equipos de cómputo.
  - Se carece de un procedimiento y políticas para la gestión de accesos a la herramienta.
  - No cuenta con mecanismos para identificar los equipos de cómputo que no se encuentran conectados a la red de la secretaría, sus accesorios, ni para indicar la fecha en que fue dado de alta un equipo.
- La gestión de altas, bajas, cambios, reasignaciones, reubicaciones y fallas en los equipos, así como su seguimiento, la realiza cada enlace informático por medio de la mesa de servicios; sin embargo, no se proporcionó evidencia que lo acredite.

- No se identificaron los motivos del atraso en la implementación de los equipos y sus accesorios. A la fecha de la auditoría (septiembre 2022), no se ha pronunciado el prestador de servicios para indicar la fecha en la que concluirá la implementación de los equipos de cómputo.

Se concluye que existieron deficiencias en la revisión y seguimiento del contrato núm. DGRMSG-DCC-S-055-2021, toda vez que se carece de la evidencia de las actividades realizadas por el administrador del contrato para supervisar la entrega e implementación de los equipos solicitados y garantizar la prestación del servicio; no se cuenta con procedimientos para la gestión (altas, bajas o cambios) de los equipos de cómputo y sus accesorios; para la administración de la herramienta y sus usuarios; para ejecutar mantenimientos y para su borrado seguro; así como para identificar fallas en los equipos, realizar su seguimiento o en su caso, el reemplazo del equipo y sus accesorios. El proveedor no realizó la entrega e instalación de los equipos de cómputo durante el ejercicio 2021 y no ha realizado el pago de las penas convencionales determinadas por la DRT; por lo que no es posible aseverar que la estrategia de contratación bajo un contrato marco cumplió con el objetivo de brindar las mejores condiciones al Estado, debido a que los atrasos en la implementación de los equipos y en la gestión de pagos por la aplicación de penas convencionales han afectado a los usuarios de la secretaría y, por ende, sus tareas operativas.

#### 2021-0-12100-20-0341-01-001 **Recomendación**

Para que la Secretaría de Salud realice un análisis de las funciones y actividades del personal de la secretaría, el cual permita identificar el equipamiento tecnológico necesario para los usuarios finales, en donde se establezcan los perfiles y las características mínimas de hardware y software requeridas para cada uno de éstos, con la finalidad de que cuenten con un rendimiento óptimo y funcional, y con una eficiencia operativa. Además, que se realice y documente el análisis del dimensionamiento de equipamiento tecnológico requerido por la secretaría, para garantizar que se soliciten únicamente los equipos de cómputo o infraestructura de hardware y software necesarios para el cumplimiento de las funciones del personal, a fin de evitar tener equipos almacenados en bodega y no aprovechados. Asimismo, que establezca mecanismos de seguimiento con los enlaces informáticos de las unidades administrativas de la secretaría y con el proveedor, a fin de que el inventario de equipamiento se encuentre actualizado y acorde con los usuarios responsables de esta infraestructura.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### 2021-0-12100-20-0341-01-002 **Recomendación**

Para que la Secretaría de Salud implemente medidas de control, adicionales a las realizadas por los proveedores, para la infraestructura de hardware, software y servicios, a fin de supervisar y garantizar que los entregables, reportes, inventarios y actividades del proveedor

se realicen conforme a lo establecido en el contrato y esto sirva de apoyo para la aplicación de deductivas y penalizaciones correspondientes; que documente y formalice los procedimientos complementarios a la gestión de servicios de arrendamiento relacionados a los procesos de mantenimiento de los equipos; altas, bajas y reubicaciones de equipos; comunicación y procesos de atención con la mesa de servicios; prevención y mitigación ante robos o siniestros, con la finalidad de asegurar la integridad, salvaguarda y funcionamiento del equipo de arrendamiento. Asimismo, que defina, actualice y difunda procedimientos, lineamientos y manuales de usuario que contengan el detalle y descripción de las actividades por realizar en las herramientas tecnológicas utilizadas para la gestión del equipamiento tecnológico, así como que éstos sean considerados por los proveedores en la prestación del servicio.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-01-003 Recomendación**

Para que la Secretaría de Salud fortalezca los controles establecidos durante el proceso de contratación para que se evalúe la pertinencia de adherirse a Contratos Marco, con la finalidad de que no sólo se asegure el beneficio económico, sino que se garantice la actualización tecnológica que requieren los usuarios para el desempeño de sus funciones y mejorar la eficiencia operativa de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-06-001 Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 313,410.54 pesos (trescientos trece mil cuatrocientos diez pesos 54/100 M.N.), por los pagos realizados al amparo del contrato DGRMSG-DCC-S-045-2021, celebrado con la empresa Ofi Productos de Computación, S.A. de C.V., con vigencia del 1 de julio de 2021 al 31 de diciembre de 2023, para la prestación del servicio de Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6, debido a que se identificó que en el periodo comprendido en los meses de agosto a diciembre de 2021, 93 equipos (laptops y videoproyectores) se encontraban almacenados en bodega, por lo que no fueron instalados ni configurados por el proveedor, y no estaban en operación, en consecuencia, no fueron utilizados por los usuarios finales a los que se asignaron; no obstante, se pagaron 216,374.57 pesos (doscientos dieciséis mil trescientos setenta y cuatro 57/100 M.N.); asimismo, la Secretaría de Salud no demostró la existencia de 17 equipos, por los que pagaron 97,035.97 pesos (noventa y siete mil treinta y cinco pesos 97/100 M.N.), en incumplimiento de la Ley

Federal de Presupuesto y Responsabilidad Hacendaria, Art. 1, Par. 2; del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Art. 93; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Art. 66, Frac. I y III; del Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias, Art. 3; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, del apartado III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; actividad APRO 3, Factor Crítico 3; del Reglamento Interior de la Secretaría de Salud, Art. 32, Frac. III y VIII; del Manual de organización específico de la Dirección General de Tecnologías de la Información, objetivo y funciones 3, 5, 7 de la sección Dirección de Redes y Telecomunicaciones; del Contrato núm. DGRMSG-DCC-S-045-2021, cláusula segunda, párrafo segundo; cláusula tercera; cláusula décima tercera, y del Anexo único del contrato núm. DGRMSG-DCC-S-045-2021, numeral 2 y sus requerimientos 6, 9, 12, 13 y 15.

### **Causa Raíz Probable de la Irregularidad**

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

### **3. Contrato DGRMSG-DCC-S-008-2018 “Servicio Integral de Telecomunicaciones (SINTEL)”**

Se formalizó el contrato número DGRMSG-DCC-S-008-2018 con la empresa Uninet, S.A. de C.V., en participación conjunta con Consorcio Red Uno, S.A. de C.V., Triara.Com, S.A. de C.V., Scitum, S.A. de C.V., Prestaciones Profesionales Empresariales, S.A. de C.V., y Servicios Especializados Scitum, S.A. de C.V., mediante adjudicación directa, con fundamento en los artículos 22, fracción II, 25, 26, fracción III, 40, 41, fracción III y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), y artículos 71, 72, fracción III, y 85 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP), con vigencia del 13 de abril de 2018 al 31 de marzo de 2021, por un monto mínimo de 383,144.2 miles de pesos y un máximo de 957,860.6 miles de pesos, con el objeto de prestar el “Servicio Integral de Telecomunicaciones (SINTEL)”.

- El 31 de marzo de 2021 se formalizó el Primer Convenio Modificatorio que amplió la vigencia del contrato al 30 de junio de 2021.
- El Segundo Convenio Modificatorio se suscribió el 30 de junio de 2021 para ampliar la vigencia del contrato al 30 de septiembre de 2021.
- El 30 de septiembre de 2021 se formalizó el Tercer Convenio Modificatorio que amplió la vigencia del contrato al 31 de diciembre de 2021.
- Para el 21 de diciembre de 2021 se formalizó el Cuarto Convenio Modificatorio que amplió la vigencia del contrato al 31 de marzo de 2022.

- El 31 de marzo de 2022 se formalizó el Quinto Convenio Modificatorio para ampliar la vigencia del contrato al 30 de junio de 2022.

### **Alcance del Servicio**

El contrato contempló la prestación de servicios de comunicaciones para voz, datos y video, así como su seguridad asociada, a través de enlaces digitales de internet, conmutación de etiquetas multiprotocolo (MPLS), seguridad perimetral, red de voz, datos y video, mediante un esquema de servicios administrados para que los funcionarios cuenten con servicios de telecomunicaciones.

### **Pagos**

Durante el 2021 se realizaron pagos por 119,229.8 miles de pesos por los servicios prestados; en la información analizada se observó lo siguiente:

- No se proporcionaron las memorias de cálculo de las facturas, por lo que no fue posible validar su correcta determinación en función de los precios pactados contractualmente.
- No se cuenta con evidencia de la entrega de las facturas y su aceptación a través del Sistema Integral de Administración Financiera Federal (SIAFF), por lo que no fue posible verificar que el pago se realizara en un plazo de 20 días naturales.
- No se cuenta con la evidencia que permita verificar que las deductivas por 17.8 miles de pesos, determinadas por la Dirección de Red y Telecomunicaciones (DRT) derivadas del incumplimiento parcial o deficiente en la calidad de los servicios provistos son correctas. Asimismo, éstas no fueron deducidas del importe a facturar.
- En marzo de 2019 se requirió al proveedor la baja del servicio de arreglo de equipos de control de acceso a la red (NAC); no obstante, el proveedor siguió facturándolo del 2019 al 2021. De lo anterior y como resultado de la auditoría número 222–DS correspondiente a la fiscalización superior de la Cuenta Pública de 2020 realizada por la ASF, la secretaría determinó penalizaciones por 12,095.6 miles de pesos (4,398.4 miles de pesos correspondientes al ejercicio 2021) antes de impuestos y retenciones, y se requirió al proveedor en febrero de 2022 el reintegro respectivo; sin embargo, no se proporcionó evidencia que acredite su pago.

### **Cumplimiento técnico y funcional de los servicios y entregables establecidos en el anexo técnico del contrato.**

- Referente al servicio de enlace de Internet de 10 Megabits por segundo (Mbps) con protección de denegación de servicio (DoS) y seguridad perimetral:

- No se identificó la herramienta utilizada para llevar a cabo la contención de ataques.
- Se carece de la documentación que describa los medios utilizados por el proveedor para informar de los eventos identificados en las herramientas de seguridad perimetral, no se precisó el responsable de comunicar y dar seguimiento a los mismos, y también se carece de un procedimiento formalizado para la gestión de incidentes.
- Para el equipo del sistema de nombres de dominio (DNS) dedicado, no se cuenta con un:
  - Diagrama o documento donde se describa la funcionalidad del método de direccionamiento y enrutamiento de red (anycast) para el DNS.
  - Listado de usuarios que pueden realizar el bloqueo de zonas en los equipos DNS, por medio de la herramienta de monitoreo.
- Acerca del Sistema de monitoreo de desempeño de los componentes de red para 2,000 elementos:
  - Se carece de un procedimiento de monitoreo de red por parte del Centro de Operaciones de Redes de Clientes (CNOOC); no se precisó el responsable de realizar la validación de las características técnicas o especificaciones del sistema de monitoreo, así como de su implementación.
  - La herramienta de monitoreo no tiene configurados umbrales de disponibilidad y velocidad del enlace.
- El administrador del contrato no validó que los equipos o componentes tecnológicos estuvieran en óptimas condiciones al momento de su implementación, ni se cuenta con la relación de cambios realizados en los equipos como resultado de fallas o desperfectos durante el 2021.
- El proveedor no realizó inspecciones al sistema de alimentación eléctrica y a las alarmas en equipos, ni ejecutó rutinas de diagnóstico.
- La secretaría no demostró que los equipos de telecomunicaciones cuenten con las actualizaciones más recientes liberadas por el fabricante, ni las acciones que se llevaron a cabo en caso de presentarse alguna anomalía en éstas.
- Se carece de mecanismos para validar que los equipos solicitados fueron nuevos y que contaron con soporte por parte del fabricante, además no presentan anuncios de fin de venta o fin de soporte durante la vigencia del contrato.

- El proveedor no presentó el plan de trabajo correspondiente a la etapa 2 de la operación del servicio durante 2021.
- De la visita al cuarto de telecomunicaciones (MDF e IDS) de la secretaría, se observó lo siguiente:
  - Para los equipos que dan soporte a la red MPLS (tráfico de voz, tráfico de video, tráfico de datos y tráfico administrativo) la evidencia fotográfica no permitió validar el etiquetado ni su ubicación.
  - En el lugar donde reside la infraestructura que da soporte al servicio se identificó que existe material inflamable como: cajas de cartón, papeles, muebles y piñatas, por lo que existe el riesgo de que, en caso de un incidente, los equipos puedan verse afectados, lo cual impactaría en la disponibilidad, integridad y confidencialidad de la información de la secretaría.
  - No se localizaron los equipos Controlador de Borde de Sesión (SBC).

Se concluye que existieron deficiencias en la gestión del contrato núm. DGRMSG-DCC-S-008-2018, debido a que se carece de la evidencia de las actividades realizadas por el administrador del contrato para la validación de la prestación del servicio, no se demostró que los equipos contaran con las actualizaciones más recientes liberadas por el fabricante; en cuanto al monitoreo de la mesa de servicio y CNOC no hay evidencia de procedimientos, reportes de incidentes y su seguimiento; no se validó que los equipos contratados hayan sido nuevos, contaran con soporte por parte del fabricante y no presentan anuncios de fin de venta o fin de soporte durante la vigencia del contrato; no se localizaron los equipos relacionados con los servicios de telecomunicaciones (MDF e IDS) con el debido etiquetado; se determinaron deducivas por los servicios no recibidos con la calidad requerida por la secretaría por 17.8 miles de pesos; sin embargo, no fue posible verificar el cálculo realizado; asimismo, se identificó que para los servicios NAC se efectuaron pagos aproximadamente por 4,398.4 miles de pesos (antes de impuestos y retenciones); sin embargo, el proveedor no presta este servicio desde el año 2019.

#### 2021-0-12100-20-0341-01-004 **Recomendación**

Para que la Secretaría de Salud, en futuras contrataciones en materia de Tecnologías de la Información y Comunicaciones (TIC), fortalezca los controles de supervisión, seguimiento y validación por parte del administrador del contrato y por el personal autorizado para la vigilancia y supervisión del instrumento jurídico, realizando revisiones independientes a las efectuadas por el proveedor sobre los servicios prestados y documentando de manera formal dichas actividades, lo que garantice el cumplimiento de las obligaciones derivadas de los contratos relacionados con los servicios de Tecnologías de Información y Comunicaciones y asegurar que son proporcionados en su totalidad, y que cumplen en tiempo y forma con los requerimientos, características técnicas y necesidades de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-01-005 Recomendación**

Para que la Secretaría de Salud lleve a cabo revisiones periódicas a los sites (MDF e IDF) de la secretaría, con la finalidad de verificar que éstos se encuentran en óptimas condiciones y no cuentan con material inflamable en su interior, lo que garantice la seguridad, confidencialidad, integridad y disponibilidad de la información, así como de la infraestructura de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-06-002 Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 4,398,400.32 pesos (cuatro millones trescientos noventa y ocho mil cuatrocientos pesos 32/100 M.N.), por los pagos realizados al amparo del contrato DGRMSG-DCC-S-008-2018, celebrado con la empresa Uninet, S.A. de C.V., en participación conjunta con Consorcio Red Uno, S.A. de C.V., Triara.Com, S.A. de C.V., Scitum, S.A. de C.V., Prestaciones Profesionales Empresariales, S.A. de C.V., y Servicios Especializados Scitum, S.A. de C.V., con vigencia del 13 de abril de 2018 al 30 de junio de 2022, para la prestación del Servicio Integral de Telecomunicaciones (SINTEL), debido a que se identificó que la Secretaría de Salud solicitó la baja del servicio de arreglo de equipos de control de acceso a la red (NAC) desde 2019; sin embargo, el proveedor siguió facturando este servicio en 2021 y se carece de la evidencia que acredite que el proveedor realizó el reintegro correspondiente, en incumplimiento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Art. 1, Par. 2; del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Art. 93; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Art. 66, Frac. I y III; del Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias, Art. 3; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, del apartado III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; de la actividad APRO 3, Factor Crítico 3; del Reglamento Interior de la Secretaría de Salud, Art. 32, Frac. XI; del Manual de Organización General de la Secretaría de Salud, apartado VI. Funciones de la Dirección General de Tecnologías de la Información, funciones 1, 4, 5 y 8; del Manual de Organización Específico de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, apartado VI. Descripción de Funciones, de la sección

Dirección de Red y Telecomunicaciones, funciones 4, 5, 6, 7, 8, 11 y 12; del Contrato núm. DGRMSG-DCC-S-008-2018, Declaración I.6; cláusula Octava; cláusula Novena; del Anexo único del contrato núm. DGRMSG-DCC-S-008-2018, numerales I. Objeto de la contratación; II. Descripción de los servicios, Apartados A. Características técnicas de los servicios, 5) Enlace de Internet 10 Mbps con protección DoS y seguridad perimetral (FW UTM), 6) Equipo DNS dedicado, 8) Sistema de monitoreo de desempeño de los componentes de red para 2,000 elementos; D. Mantenimiento, incisos 1) Mantenimiento preventivo y correctivo y 2) Actualizaciones del sistema y su hardware, H. Metodología e I. Plan de trabajo, y del Apéndice 2. Distribución de los servicios.

#### **Causa Raíz Probable de la Irregularidad**

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

#### **4. Contrato DGRMSG-DCC-S-020-2020 “Servicio para Mantenimiento y Desarrollo de Aplicaciones Sustantivas”**

La Secretaría de Salud formalizó el contrato número DGRMSG-DCC-S-020-2020 con el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), mediante contratación entre entes públicos, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); 1°, quinto párrafo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), y 4° del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP); con vigencia del 29 de mayo al 31 de diciembre de 2020, por un monto mínimo de 13,680.6 miles de pesos y un máximo de 34,201.4 miles de pesos, con el objeto de prestar el “Servicio para Mantenimiento y Desarrollo de Aplicaciones Sustantivas”.

- El 23 de diciembre de 2020 se formalizó el Primer Convenio Modificadorio 01/20 que amplió la vigencia del contrato al 31 de marzo de 2021.
- El Segundo Convenio Modificadorio 02/21 se suscribió el 31 de marzo de 2021 para ampliar la vigencia del contrato al 30 de junio de 2021.
- El 30 de junio de 2021 se formalizó el Tercer Convenio Modificadorio 03/21 que extendió la vigencia del contrato al 31 de diciembre de 2021.
- Para el 31 de diciembre de 2021 se suscribió el Cuarto Convenio Modificadorio 04/21 que amplió la vigencia al 31 de marzo de 2022 e incrementó el monto mínimo a 16,416.7 miles de pesos y el monto máximo a 41,041.7 miles de pesos.
- El 1 de abril de 2022 se formalizó un Quinto Convenio Modificadorio 05/22 que amplía la vigencia del contrato al 30 de junio de 2022.

### **Alcance del Servicio**

El contrato contempló la prestación de servicios para mantenimiento y desarrollo de aplicaciones sustantivas, con la finalidad de proporcionar a la secretaría capacidades adicionales especializadas en materia de Tecnologías de Información y Comunicaciones (TIC), bajo un modelo operativo de órdenes de servicio que le permitieran atender la gestión de los proyectos, requerimientos y productos relacionados con el mantenimiento de las aplicaciones, desarrollo evolutivo de software, así como la mejora de las aplicaciones sustantivas para la secretaría y otros servicios adicionales.

### **Pagos**

Durante el 2021 se realizaron pagos por 19,874.6 miles de pesos, de la información analizada se observó lo siguiente:

- No se proporcionaron las memorias de cálculo de las facturas, por lo que no fue posible validar su correcta determinación en función de los precios pactados contractualmente.
- No se cuenta con evidencia de la entrega de las facturas y su aceptación a través del Sistema Integral de Administración Financiera Federal (SIAFF), por lo que no fue posible verificar que el pago se realizara en un plazo de 20 días naturales.
- En la documentación proporcionada no se identificó la expedición de los CFDI con "Complemento para recepción de pagos".

### **Cumplimiento técnico y funcional de los servicios y entregables establecidos en el anexo técnico.**

- Se carece de la evidencia que demuestre la revisión del administrador del contrato a las estimaciones de servicios efectuadas por el proveedor para la atención de requerimientos; tampoco se documentó ni se realizó una validación a los montos y horas hombre reportadas por el proveedor, que permitan verificar que los pagos efectuados a éste corresponden a las actividades realizadas y a la calidad de su servicio. Tampoco se proporcionó el listado de órdenes de servicio totales generadas en 2021.
- Con relación a las órdenes de servicio gestionadas en 2021, no se generó el diseño detallado del aplicativo que se desarrolló, considerando por lo menos, requerimientos del negocio, de seguridad de la información, de privacidad y protección de datos personales, técnicos, casos de uso, y matriz de trazabilidad.
- No se identificó evidencia que demostrara que el proveedor contara con la certificación solicitada en el anexo técnico.

- Para los desarrollos y mantenimientos generados en 2021, la secretaría no realizó su inscripción ante el Registro Público de la Propiedad y de Comercio; tampoco se realizaron actividades de transferencia de conocimiento; ni la elaboración de cronogramas de trabajo para las aplicaciones generadas por medio del servicio de desarrollo evolutivo.
- No se generaron órdenes de servicio relacionadas con procesos de pruebas (estrés o desempeño, integrales, de funcionalidad, usuario, vulnerabilidades o de código estático) para aplicativos de terceros.
- No se implementaron mecanismos de seguridad dentro del código de aplicativos.
- La Dirección General de Tecnologías de Información (DGTI) no efectuó actividades de diagnósticos, análisis de impacto al negocio y de capacidades de infraestructura tecnológica, en alcance a los servicios proporcionados por el proveedor.
- No se realizó el seguimiento a los compromisos contractuales por medio de la lista de verificación solicitada en el anexo único del contrato, no proporcionó evidencia que valide que las órdenes de servicio generadas durante 2021 fueron cerradas a satisfacción de las áreas usuarias ni de que el proveedor entregara los procedimientos formalizados para la administración de problemas y cambios, así como el plan de calidad.
- No se cuenta con evidencia de la formalización de los cambios de administradores por parte de la entidad y del proveedor.
- No se identificaron los controles utilizados para entregar el acceso a los ambientes de desarrollo y calidad al proveedor, así como las cuentas con correos institucionales utilizadas.
- No se cuenta con la documentación que acredite que el proveedor generó para las órdenes de servicio, los entregables asociados a los requerimientos de la solución tecnológica de TIC, alcance de la orden y estrategia de servicio, y la notificación de la autorización o rechazo de la orden, los cuales formaban parte de la etapa de análisis de las órdenes de servicio. Tampoco aquellos asociados al cronograma de trabajo y, en los casos que aplique, el control de cambio de la orden de servicio.
- Se carece de las actas de liberación de cada uno de los mantenimientos y desarrollos de software realizados por el proveedor; tampoco se cuenta con los “Reportes mensuales de servicios devengados” establecidos en el anexo único del contrato.
- No se cuenta con la evidencia que acredite las actividades realizadas por el administrador del contrato para verificar los entregables proporcionados por el proveedor, únicamente validó el funcionamiento de los aplicativos construidos o modificados; tampoco consideró mecanismos de garantía posteriores a la entrega

formal de cada uno de los desarrollos y mantenimientos de software efectuados por el proveedor.

- No se identificó que en las minutas de trabajo proporcionadas por la secretaría se contemplara la revisión, por parte del administrador del contrato, del cumplimiento de horas máximas por cada uno de los perfiles.
- El administrador del contrato no cuenta con la documentación que acredite la revisión de documentación y su autorización a los cambios de roles por alta o reemplazo por parte del proveedor.
- La DGTI no suscribió acuerdos de confidencialidad con el personal del proveedor respecto al manejo de la información de la secretaría durante la vigencia del servicio; tampoco verificó que el proveedor contara con un mecanismo de respaldo de los repositorios de código fuente.
- No se cuenta con un comité de cambios en materia de TIC que evalúe y apruebe los cambios en infraestructura, así como actualizaciones a sistemas, software y hardware.
- Para los servicios de desarrollo o mantenimiento de aplicativos, la DGTI no generó cronogramas específicos para la ejecución de pruebas, ni evidencia que permita demostrar que el proveedor dio atención y mitigó las incidencias identificadas en el proceso de pruebas y que atendía fallas en aplicativos una vez liberados y puestos en producción.
- El administrador del contrato no demostró que el proveedor contemplara la participación del usuario final en el proceso de pruebas, así como de que éste diera su aprobación a las funcionalidades entregadas.
- No se identificó el nombre de la herramienta y versión utilizada por el proveedor para la gestión de pruebas de vulnerabilidades.
- La DGTI no realizó una calendarización para las pruebas de vulnerabilidades al software ni proporcionó evidencia de haberlas ejecutado.
- En la revisión del aplicativo Ambiente para la administración y manejo de atenciones (AAMATES), en donde el proveedor le daría atención por medio de servicios de fábrica de software, se identificó lo siguiente:
  - No se cuenta con un versionamiento de los cambios efectuados a los módulos modificados o construidos por parte del proveedor al aplicativo AAMATES, ni con la documentación que valide la gestión de órdenes de servicio relacionadas a dicho aplicativo.

- No se llevaron a cabo pruebas de estrés, de usuario, de funcionalidades, integrales, de vulnerabilidades o pruebas de código estático al aplicativo AAMATES y sus respectivos módulos.
  - La DGTI no dio seguimiento a posibles incidencias identificadas en pruebas de software efectuadas al aplicativo AAMATES, tampoco se elaboraron órdenes de servicio relacionadas con el refuerzo de la seguridad del mismo.
  - Los únicos mecanismos de cifrado utilizados para el AAMATES y sus respectivos módulos son los provistos por la infraestructura tecnológica que ofrece el servicio integral del centro de datos.
  - El administrador del contrato no indicó si por medio de los servicios del contrato se realizaron ajustes al aplicativo AAMATES relacionados con los requerimientos siguientes: Aplicación de funcionalidad en modo fuera de línea y consolidación de información de forma asíncrona, así como para la consolidación de bases de datos.
- Se seleccionó una muestra aleatoria de ocho solicitudes de desarrollo o mantenimientos (22.9%) de un universo de 35; de lo anterior, la secretaría no proporcionó la documentación probatoria que acredite la ejecución de las actividades de mantenimiento y desarrollo por parte del proveedor; no se demostró la generación, autorización y entrega de las órdenes de servicio de los aplicativos seleccionados por el grupo auditor; tampoco la recepción de servicios y entregables comprometidos en dichas órdenes, ni la aprobación de los servicios asociados a éstas; no obstante, se realizaron pagos por 19,874.6 miles de pesos.

Se concluye que existieron deficiencias en la revisión, autorización y seguimiento del contrato núm. DGRMSG-DCC-S-020-2020; toda vez que el administrador del contrato no realizó acciones para dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en el contrato, no se cuenta con mecanismos para la verificación de las horas, hombre referidas por el proveedor de la ejecución de los servicios de desarrollo de software, ni para la revisión de los entregables; no se llevaron a cabo análisis de vulnerabilidades previo a la liberación de desarrollos de software y no proporcionó evidencia que valide que todas las órdenes de servicio generadas durante 2021 con el proveedor fueron cerradas a satisfacción de las áreas usuarias; tampoco sus entregables ni la documentación probatoria que valide la ejecución de las actividades de mantenimiento y desarrollo por parte del proveedor; no obstante, se realizaron pagos por 19,874.6 miles de pesos.

#### 2021-0-12100-20-0341-01-006 **Recomendación**

Para que la Secretaría de Salud realice un análisis de vulnerabilidades o pruebas de penetración a los aplicativos críticos antes de su salida al ambiente productivo de la Secretaría; que defina los mecanismos necesarios para gestionar las actividades de control de cambios y formalice la integración de un comité que evalúe los impactos y dé su visto bueno

a la aplicación de los mismos; establezca procedimientos para la validación de las horas/hombre para servicios de desarrollo; que solicite cartas de liberación de los desarrollos de software especificando sus componentes, fecha, versión y ambiente, y que defina garantías posteriores a la entrega formal de cada uno de los desarrollos y mantenimientos de software efectuados por el proveedor.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-06-003 Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 19,874,569.22 pesos (diecinueve millones ochocientos setenta y cuatro mil quinientos sesenta y nueve pesos 22/100 M.N.), por los pagos realizados al amparo del contrato DGRMSG-DCC-S-020-2020, celebrado con el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), con vigencia del 29 de mayo del 2020 al 30 de junio de 2022, para la prestación del Servicio para Mantenimiento y Desarrollo de Aplicaciones Sustantivas, debido a que se carece de la documentación probatoria que demuestre que se ejecutaron las fases de análisis, construcción, pruebas, puesta en marcha, aprobación y recepción de los servicios por parte del proveedor para las órdenes de servicio de mantenimiento para aplicativos generadas en 2021, en incumplimiento del Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias, artículos 3, 10, fracción IX y 26; del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, del apartado III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; actividad APRO 3, Factor Crítico 3; del Reglamento Interior de la Secretaría de Salud, artículo 32 fracciones III y VIII; del Manual de Organización Específico de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, Apartado VI. Descripción de Funciones, de la sección Dirección de Red y Telecomunicaciones, funciones 6, 7, 8 y 9; del Contrato No. DGRMSG-DCC-S-020-2020, Cláusulas Primera; Tercera; Octava, y Décima Tercera, y del Anexo único del contrato No. DGRMSG-DCC-S-020-2020, numerales 3, 5, 6, 7, 8, 9, 10, 11 y 20.

#### **Causa Raíz Probable de la Irregularidad**

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

**La(s) acción(es) vinculada(s) a este resultado se presenta(n) en el(los) resultado(s) con su(s) respectiva(s) acción(es) que se enlista(n) a continuación:**

Resultado 3 - Acción 2021-0-12100-20-0341-01-004

## 5. Ciberseguridad

Se revisó la información proporcionada por la Secretaría de Salud (SSA) relacionada con la administración y operación de los controles de Ciberseguridad para la infraestructura de hardware y software de la entidad; se analizaron las directrices, infraestructura y herramientas informáticas en esta materia.

Se utilizó como referencia el documento “Center for Internet Security (CIS) Controls IS Audit/Assurance Program”, en el cual se establecen 20 controles de ciberdefensa, integrados por 171 actividades de control para evaluar e identificar las estrategias, políticas, procedimientos y controles de ciberdefensa implementados en la secretaría. En el análisis realizado se identificó que 3 controles se requieren fortalecer y 17 carecen de control, como se muestra a continuación:

SEMÁFORO DE MADUREZ DE LOS CONTROLES DE CIBERSEGURIDAD EN LA SECRETARIA DE SALUD DURANTE 2021	
Control	Indicador
CSC Control 1: Inventario y control de activos de hardware	●
CSC Control 2: Inventario y control de activos de software	●
CSC Control 3: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	●
CSC Control 4: Evaluación continua de la vulnerabilidad y solución	●
CSC Control 5: Uso controlado de privilegios administrativos	●
CSC Control 6: Mantenimiento, monitoreo y análisis de bitácoras de auditoría	●
CSC Control 7: Protección de correo electrónico y navegador web	●
CSC Control 8: Defensa contra software malicioso (malware)	●
CSC Control 9: Limitación y control de puertos de red, protocolos y servicios	●
CSC Control 10: Capacidad de recuperación de datos	●
CSC Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	●
CSC Control 12: Seguridad Perimetral	●
CSC Control 13: Protección de datos	●
CSC Control 14: Control de acceso basado en necesidad de conocimiento	●
CSC Control 15: Control de acceso inalámbrico	●
CSC Control 16: Supervisión y monitoreo de cuentas	●
CSC Control 17: Implementar un programa de concientización y entrenamiento de seguridad	●
CSC Control 18: Seguridad del Software de Aplicación	●
CSC Control 19: Respuesta y Manejo de Incidentes de Ciberseguridad	●
CSC Control 20: Pruebas de penetración y ejercicios de equipo rojo	●

FUENTE: Elaborado con información proporcionada por la SSA.

Indicador: ● Cumplimiento aceptable ● Requiere fortalecer el control ● Carencia de control

Las observaciones de los controles que no cumplieron o cumplieron parcialmente se muestran a continuación:

### Inventario y control de activos hardware

- Se carece de una herramienta para la identificación de equipos de cómputo conectados a la red de la secretaría, para identificar, gestionar, bloquear o desconectar activos no autorizados y para actualizar el inventario de activos de hardware; tampoco se tienen mecanismos compensatorios para efectuar estas actividades.

- No se tiene un inventario que contemple la totalidad de activos de hardware de la secretaría (estén o no conectados a la red).
- No se cuenta con mecanismos de gestión de direcciones IP de la infraestructura tecnológica que soporta los servicios de TIC, que permita la actualización de inventarios de hardware y el bloqueo de direcciones que no estén autorizadas.

#### **Inventario y control de activos software**

- No se cuenta con un inventario del software autorizado; tampoco con una herramienta que permita documentar y actualizar todo el software requerido en la secretaría, incluidos los sistemas operativos instalados en los activos de hardware.
- La Secretaría no cuenta con mecanismos que permitan garantizar que sólo se utilice software autorizado ni un proceso para la eliminación del no autorizado; tampoco ha implementado la categorización de librerías que aseguren que sólo se ejecuten aquellas que están autorizadas.
- Se carece de evidencia que acredite que se utilizan sistemas separados física o lógicamente para aislar y ejecutar aquel software que es requerido para fines de negocio, pero que conlleva un mayor riesgo para la organización.

#### **Configuración segura para hardware y software**

- Existen oportunidades de mejora en los mecanismos de gestión, almacenamiento y monitoreo de las configuraciones de hardware y para el licenciamiento de software de la secretaría.

#### **Gestión continua de vulnerabilidades**

- No se cuenta con una herramienta para la gestión automatizada de actualizaciones de seguridad (parches) de sistemas operativos de la secretaría.
- Existen oportunidades de mejora en los mecanismos implementados en la secretaría para la evaluación, ejecución, documentación y seguimiento para la gestión de las vulnerabilidades.

#### **Uso controlado de privilegios**

- No se utilizan herramientas automatizadas para inventariar las cuentas con privilegios de administración de la secretaría.
- Existen oportunidades de mejora en los mecanismos de acceso, uso, monitoreo y alerta implementados en las cuentas de administración en los sistemas e infraestructura de la SSA.

- Se identificaron debilidades en la administración de privilegios.

#### **Mantenimiento, monitoreo y análisis de logs de auditoría**

- Se carece de documentación que acredite la implementación de fuentes de sincronización de tiempo en la infraestructura de la secretaría.
- Se identificaron áreas de oportunidad en relación con los mecanismos para el registro, monitoreo y análisis de bitácoras de auditoría de los aplicativos de la secretaría, así como en el uso de herramientas que permitan identificar, analizar y recuperar de manera centralizada los eventos de seguridad que pudieran presentarse en los sistemas de la SSA.

#### **Protección de correo electrónico y navegador web**

- Se identificaron debilidades en la protección de correo electrónico y navegador web.

#### **Defensa contra malware**

- No se cuenta con mecanismos de análisis, restricción y bloqueo de medios extraíbles que se ejecuten de forma automática, cuando éstos se conectan a los equipos de cómputo o servidores.
- Se detectaron debilidades en defensa contra malware.

#### **Limitación y control de puertos de red, protocolos y servicios**

- Se carece de controles para que en cada sistema se ejecuten solo los puertos de red, los protocolos y los servicios requeridos y autorizados por la secretaría.
- No se cuenta con evidencia que muestre que la SSA realiza el escaneo automático de puertos de forma periódica en todos sus sistemas.

#### **Capacidad de recuperación de datos**

- No se proporcionó la documentación en donde se especifiquen los alcances de los respaldos, lugares dispuestos para el resguardo de cintas y sus mecanismos de protección, los cuales son contemplados en los servicios prestados por el proveedor del contrato núm. DGRMSG-DCC-S-008-2018 para el “Servicio Integral de Telecomunicaciones (SINTEL).

#### **Configuración segura de los equipos de red**

- Se identificaron áreas de oportunidad relacionadas con los mecanismos utilizados para el acceso a los equipos de red de la Secretaría de Salud.

- Se carece de documentación que acredite que la secretaría utiliza segmentación de red por medio de redes de área local virtuales (VLANS).

#### **Seguridad Perimetral**

- Se detectaron deficiencias en la seguridad perimetral.

#### **Protección de datos**

- Se identificaron áreas de oportunidad en relación con el uso de herramientas y mecanismos para la prevención de pérdida de datos y para el monitoreo del tráfico que sale de la organización con la finalidad de proteger la información sensible.
- Existen oportunidades de mejora en los mecanismos de protección de la información implementados para el uso de dispositivos USB; así como en los existentes para prevenir la fuga de información crítica a través de medios extraíbles.

#### **Control de acceso basado en necesidad de conocimiento**

- Se identificaron deficiencias en los mecanismos implementados para limitar y cifrar la comunicación entre dispositivos de diferentes segmentos de la red.

#### **Control de acceso inalámbrico**

- Existen áreas de oportunidad en los mecanismos implementados para la gestión de redes inalámbricas, la transmisión de información a través de éstas, así como en la configuración de los dispositivos que se conectan a dichas redes.

#### **Supervisión y monitoreo de cuentas**

- Se identificaron áreas de mejora en los mecanismos utilizados para el monitoreo y alertamiento de los inicios de sesión en los sistemas de la secretaría.

#### **Implementar un programa de concientización y entrenamiento de seguridad**

- Se carece de un plan de concientización en materia de seguridad de la información, tampoco se cuenta con la evidencia del método para medir la eficacia de las actividades de capacitación en la secretaría.

#### **Seguridad del software de aplicación**

- No se capacita al personal del área de desarrollo de la secretaría en temas relacionados con la escritura de código seguro, así como en sus responsabilidades específicas para el correcto cumplimiento de sus funciones.

- Existen oportunidades de mejora en los mecanismos implementados por la secretaría para garantizar la seguridad del código de las aplicaciones.

#### **Respuesta y manejo de incidentes**

- Se carece de la definición de un procedimiento de respuesta a incidentes de ciberseguridad.
- No se realizan pruebas de escenarios de incidentes de seguridad cibernética con los usuarios de la SSA, con la finalidad de validar que la estrategia de respuesta definida por la secretaría es adecuada y suficiente en caso de una contingencia.
- Se identificaron áreas de mejora en los mecanismos utilizados para la gestión de incidentes de ciberseguridad en la secretaría.

#### **Pruebas de penetración y ejercicios de equipo rojo**

- No se proporcionó evidencia de los usuarios que tienen acceso a la herramienta de escaneo de vulnerabilidades utilizada por la secretaría; tampoco se tiene una cuenta dedicada para realizar dichos escaneos.

Por lo anterior, se concluye que existen deficiencias en los controles de ciberdefensa para la infraestructura de hardware y software de la secretaría, relacionadas con las directrices, infraestructura y herramientas informáticas en esta materia, dichas deficiencias podrían afectar la integridad, disponibilidad y confidencialidad de la información, poniendo en riesgo la operación de la Secretaría de Salud.

#### **2021-0-12100-20-0341-01-007 Recomendación**

Para que la Secretaría de Salud realice las acciones necesarias para implementar actividades de administración y monitoreo automáticas sobre los activos de información a nivel hardware y software, con la finalidad de contar con inventarios precisos y actualizados que le permitan identificar elementos no autorizados, así como reforzar los controles que se tienen para la gestión y acceso de cuentas administrativas con la finalidad de proteger dichos activos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-01-008 Recomendación**

Para que la Secretaría de Salud implemente acciones para reforzar los procedimientos relacionados con la revisión periódica de puertos, protocolos y conexiones de red que le permitan identificar posibles brechas de seguridad; adicionalmente, que implemente mecanismos con la finalidad de dar seguimiento a la corrección de vulnerabilidades y que

defina y formalice procedimientos para la atención de incidentes de seguridad que le permitan proteger la integridad, confidencialidad y disponibilidad de la información; que realice el seguimiento a los programas de concienciación y entrenamiento en materia de seguridad informática, y que mida la eficacia de las actividades de capacitación, con el objetivo de conocer si dichas capacitaciones están funcionando.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-01-009 Recomendación**

Para que la Secretaría de Salud implemente políticas y lineamientos de seguridad de la información, así como las configuraciones necesarias en relación con los servicios de internet, correo electrónico y dispositivos extraíbles, con la finalidad de limitar el tipo de información que puede ingresar o salir de la secretaría, así como la instalación de software malicioso en servidores y estaciones de trabajo que pudiera afectar la integridad, confidencialidad y disponibilidad de los sistemas de información.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

#### **2021-0-12100-20-0341-01-010 Recomendación**

Para que la Secretaría de Salud defina y formalice estándares de seguridad y configuraciones para los sistemas e implemente mecanismos para proteger dichas configuraciones y evitar modificaciones no autorizadas; que refuerce los mecanismos para el registro y monitoreo de bitácoras de auditoría con la finalidad de asegurar la consistencia e integridad de los reportes que se generen; finalmente, que considere la implementación de herramientas automáticas para la identificación de información sensible, con el objetivo de generar un inventario de la misma e implementar los controles necesarios para preservar su integridad y confidencialidad.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

## **6. Continuidad de las Operaciones**

Como parte de los trabajos de auditoría se verificaron las condiciones que la Secretaría de Salud (SS) presenta en el Proceso de Continuidad de las Operaciones de Tecnologías de la

Información y Comunicaciones (TIC) para garantizar la disponibilidad de la información y continuidad de los servicios. En el análisis realizado se observó lo siguiente:

- La secretaría no cuenta con un documento formalizado donde se establezcan las áreas y puestos de los responsables de definir los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC.
- El catálogo de servicios de TIC no se encuentra formalizado; no se identificó al responsable de su administración y actualización; tampoco la información relacionada con la arquitectura empresarial y sus componentes (procesos, aplicaciones e infraestructura tecnológica requerida).
- El catálogo de servicios de TIC de la secretaría no incluye los servicios de operación de trámites y de ventanilla única nacional, mesa de servicio, reportes estadísticos de la gestión de trámites y servicios, de apertura de información pública en formato abierto, autenticación de certificados digitales, de mensajes y validación de documentos con firma digital, módulo de firmado electrónico de documentos, así como aplicaciones únicas de sustitución de uso de papel.
- No se tiene definido un responsable del diseño de los servicios de TIC; no se realiza un análisis de requerimientos para servicios existentes o nuevos, ni la integración de un expediente del diseño de los servicios.
- No se cuenta con un programa de capacidad de los servicios, tampoco se realizan actividades para identificar los activos de TIC que requieren actualizarse, mejorarse o sustituirse, así como las fechas propuestas y costos estimados en cada caso.
- No se proporcionó evidencia que demuestre que la secretaría ha formalizado y definido acciones a implementar cuando la capacidad y rendimiento de la infraestructura de TIC no estén en el nivel requerido.
- La Secretaría de Salud no incluye en sus programas de continuidad las características de capacidad y rendimiento de cada componente de la infraestructura de TIC.
- No se informa a los responsables de los procesos de la DGTI, las oportunidades identificadas para mejorar la capacidad de la arquitectura tecnológica, los niveles de servicios alcanzados, el medio utilizado para llevar a cabo dicha comunicación, así como, la periodicidad con la que se lleva a cabo.
- No existe una metodología para realizar un análisis de impacto al negocio, en el que se identifiquen los procesos críticos de la operación y sus impactos al materializarse un riesgo; ni en el que se definan tiempos máximos tolerables de interrupción (MTO), tiempos y puntos objetivos de recuperación (RTO y RPO), así como la frecuencia para la revisión y actualización de dicho análisis.

- Se carece de un método (cualitativo o cuantitativo) para calificar el impacto potencial de los riesgos; y no se realizan estimaciones de los impactos cuantitativos de las contingencias operativas.
- No se proporcionó evidencia que acredite que se consideran todos los factores de riesgo y la criticidad de los activos de información, tampoco se contemplan los escenarios relativos a la verificación de posibles contingencias operativas.
- El Plan de Continuidad del Negocio (BCP) no cuenta con estrategias, procedimientos ni actividades a realizar para cada escenario de contingencia.
- No se cuenta con procedimientos, actividades y notificaciones por realizar para cada una de las emergencias derivadas de la materialización de amenazas de seguridad cibernética.
- No se cuenta con un Plan de Recuperación en Caso de Desastres (DRP) formalizado, en donde se contemplen notificaciones de inicio y fin de contingencia, roles y responsabilidades, un árbol de llamadas que incluya la información de contacto del personal a cargo de gestionar las actividades de recuperación, procedimientos para la restauración de sistemas en sitio alterno; asimismo, no se identificó si el DRP forma parte del Plan de Continuidad del Negocio.
- Se carece de una herramienta para realizar respaldos, así como del análisis a través del cual determinaron las políticas de respaldo, su frecuencia y mecanismos de protección y resguardo.
- No cuenta con un procedimiento documentado y formalizado para la restauración de respaldos.
- Se carece de políticas y procedimientos para la ejecución de pruebas a la estrategia de continuidad del negocio.
- No se cuenta con un calendario de ejecución de pruebas de recuperación ni la documentación de las acciones a seguir en caso de presentarse fallas o desviaciones en la ejecución de las mismas.

De la revisión de los controles implementados para asegurar la Continuidad de las Operaciones de TIC, los principales riesgos por la carencia o inconsistencia de éstos y sus consecuencias potenciales para las operaciones y activos de la Secretaría de Salud son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE CONTROLES DE CONTINUIDAD DE LAS OPERACIONES

Factor crítico	Riesgo
Planeación de la Capacidad	Los recursos no se aprovechan adecuadamente y se realizan acciones incorrectas en mantenimiento y administración, que pudieran no ser suficientes, lo que podría derivar en la degradación de la calidad del servicio.
Planeación de la disponibilidad de la infraestructura de cómputo	La gestión de la disponibilidad de la infraestructura de cómputo es responsable de optimizar y monitorizar los servicios para que éstos funcionen ininterrumpidamente y de manera fiable, cumpliendo los niveles de servicio y todo ello a un costo razonable, al carecer de una adecuada gestión de la disponibilidad se incrementa el riesgo de no poder asegurar que los servicios estén disponibles y funcionen correctamente en el marco de los niveles de servicio establecidos, lo que podría impactar en las operaciones de la SSA.
Programa de Continuidad	Los planes de continuidad no son probados y no son acordes a los cambios que han sufrido las infraestructuras tecnológicas y los aplicativos sustantivos, lo cual podría provocar el riesgo de que ante un desastre, los mecanismos de recuperación podrían presentar fallas sustanciales y el tiempo objetivo de recuperación (RTO) sería mucho mayor al requerido por la secretaría, lo cual afectaría las operaciones de la secretaría.
Definición del Análisis de Impacto al Negocio (BIA), Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)	Al carecer de la implementación de un Análisis de Impacto al Negocio, de planes de continuidad y recuperación de desastres, no es posible estimar la afectación que podría padecer la secretaría como resultado de la ocurrencia de algún incidente o un desastre, debido a que no se tendrían identificados los posibles impactos que pudiera sufrir, lo que no permite establecer acciones preventivas ni planes para la recuperación de las operaciones críticas de la SSA, en caso de que se presente la interrupción de uno o más servicios de TIC.
Activos críticos, productos y servicios esenciales	La falta de identificación de los procesos críticos y activos de información representa un riesgo para la secretaría, debido a que no se tendrían controles que de manera adecuada aseguren la disponibilidad, confidencialidad e integridad de los activos de información crítica.
Políticas y procedimientos de Respaldo y Recuperación	Al no contar con un procedimiento definido, documentado y formalizado para la ejecución y resguardo de respaldos; así como para llevar a cabo pruebas de restauración, se incrementa el riesgo de que los medios de respaldo no funcionen adecuadamente en caso de presentarse una contingencia, comprometiendo la continuidad de las operaciones.

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Por lo anterior, se concluye que la secretaría no ha definido ni implementado medidas y controles que le permitan asegurar la continuidad de las operaciones y la restauración de los sistemas en caso de presentarse una contingencia o eventualidad; tampoco lleva a cabo actividades para vigilar el correcto cumplimiento de las disposiciones normativas en materia de tecnologías de información y comunicaciones correspondientes.

### Centro de Datos

Durante el 2021, la Secretaría de Salud contó con el Servicio Integral de Centro de Datos proporcionado por el proveedor Triara.com, S.A. de C.V., en participación conjunta con Uninet, S.A. de C.V., Scitum, S.A. de C.V., Compañía de Teléfonos y Bienes Raíces, S.A. de C.V., Prestaciones Profesionales Empresariales, S.A. de C.V., Servicios Especializados Scitum, S.A. de C.V. y B Drive IT, S.A. de C.V., con la celebración del contrato núm. DGRMSG-DCC-S-006-2021. En el análisis realizado se observó lo siguiente:

- No se cuenta con una matriz de riesgos del centro de datos formalizada.
- No se cuenta con procedimientos documentados para el control de acceso físico y lógico; tampoco con políticas y procedimientos sobre la atención de incidentes de ambiente físico.

- No se cuenta con controles de seguridad implementados para garantizar el acceso físico a las áreas reservadas del centro de datos.
- Las puertas del centro de datos no cuentan con alamas, monitoreo, pruebas, cerraduras para llaves o biométricos, y se carece de señalizaciones de seguridad.
- No se identificó a los responsables de recibir la señal de alerta en caso de incendio; así como de quién realiza y supervisa las actividades de configuración de los dispositivos, pruebas de los equipamientos y controles de cambios.
- No fue posible verificar el funcionamiento, características y estado de los sistemas de aire acondicionado, prevención de daños por inundación, eléctrico, ni de los sistemas de alimentación ininterrumpida (UPS) con los que cuenta el centro de datos. Tampoco de los controles implementados para prevenir y mitigar incendios en el centro de datos.
- No se pudo verificar que los servidores y mainframes ubicados en el centro de datos no estuvieran obsoletos; la frecuencia establecida para realizar el cambio de los mismos; así como que los activos se encuentren inventariados.
- No se tiene evidencia que garantice que los dispositivos del centro de datos no tienen salida a impresoras, que no existen computadoras de escritorio o laptops dentro del centro de cómputo.
- Se carece de políticas y procedimientos sobre carpetas compartidas, uso de contraseñas y control de accesos de emergencia; de manuales documentados y formalizados de atención a contingencias, operación de dispositivos para evitar, detectar o corregir los riesgos físicos; procedimientos para efectuar el retiro, transporte y almacenamiento de activos de TIC de forma segura, así como para la aplicación de mantenimientos sobre los mismos.
- No se cuenta con políticas de borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, que sean retirados del ambiente operativo, por daño o reemplazo; tampoco las políticas para la clasificación de la información.
- Se carece de la definición de un plan de capacidad que le permita evitar la saturación del uso de los centros de datos; no se cuenta con un centro de datos alternativo; tampoco se proporcionó la evidencia que acredite el mecanismo utilizado para llevar a cabo las liberaciones de cambios de aplicativos en el ambiente productivo.
- No se acreditó que se cuente con respaldos fuera del centro de datos; se carece de un procedimiento para la ejecución de respaldos, recuperación de información, pruebas a los respaldos, destrucción, reutilización o restauración de cintas magnéticas.

- No se encuentran formalizadas y autorizadas las bitácoras de monitoreo para los servidores físicos y virtuales, así como las de respaldo de información; se carece de bitácoras para la destrucción y liberación de medios magnéticos realizados en el centro de datos durante 2021.
- Se identificaron áreas de oportunidad en la configuración de antivirus de los activos, así como en el cifrado de los medios de almacenamiento de las bases de datos de la secretaría.
- No se cuenta con evidencia que demuestre que durante 2021 se llevaron a cabo adquisiciones recientes o cambios en el centro de datos; tampoco se especificó la frecuencia con la que realiza la actualización del directorio del personal del centro de datos.

En la revisión de los controles de seguridad física y lógica del servicio integral del Centro de Datos contratado por la SSA, los principales riesgos por la carencia o inconsistencia de éstos y sus consecuencias potenciales para sus operaciones y activos son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE SEGURIDAD FÍSICA Y LÓGICA EN EL CENTRO DE DATOS

Factor crítico	Riesgo
Procedimientos de clasificación de información	Al no contar con mecanismos para clasificar la información, no es posible para la secretaría determinar los niveles apropiados de control para mantener la confidencialidad e integridad de la información, en consecuencia, la SSA desconoce la cantidad y ubicación de la información sensible que posee y genera; asimismo, el carecer de un nivel de protección en la información aumenta el riesgo de que la información se vea comprometida, lo que pudiera afectar en la toma de decisiones y operación de la Secretaría de Salud.
Mecanismos de control de incendios y para la mitigación de daños contra inundación	La falta de implementación o mantenimiento de dispositivos para el control de incendios e inundación puede ocasionar que en caso de presentarse algún incidente no se lleven a cabo acciones con oportunidad que permitan contener el fuego y agua en su zona de origen reduciendo los daños en su entorno más inmediato y evitar la propagación a zonas adyacentes, y en consecuencia presentarse un daño a la infraestructura tecnológica de la SSA que pudiera impactar la operación de la misma.
Replicación del almacenamiento a sitios alternos	No se cuenta con un centro de datos alternativo y los respaldos no son probados sistemáticamente para detectar fallas en la grabación de los datos, en consecuencia, en caso de un evento o desastre, el punto objetivo de recuperación (RPO) de información sería mucho mayor al estimado, lo que podría afectar la disponibilidad, integridad y confidencialidad de la información de la secretaría.
Carencia de un Plan de Recuperación de Desastres (DRP)	Al carecer de la implementación de un plan de recuperación de desastres, no es posible estimar la afectación que podría padecer la secretaría como resultado de la ocurrencia de algún incidente o un desastre, debido a que no se tendrían identificados los posibles impactos que pudiera sufrir, lo que no permite establecer acciones preventivas ni planes para la recuperación de las operaciones críticas de la SSA, en caso de que se presente la interrupción de uno o más servicios de TIC.
Políticas y procedimientos institucionales	La carencia de políticas y procedimientos provoca que no se formalice el uso adecuado de los activos de TIC por parte de los usuarios finales y administradores de tecnologías, ya que, al no contar con procedimientos oficializados, se desconoce cómo actuar ante situaciones de riesgo y no es posible aplicar sanciones o identificar las responsabilidades del personal.
Cifrado de dispositivos	La falta de implementación de cifrado de dispositivos deja expuesta la información y pone en riesgo la integridad, disponibilidad y confidencialidad de los activos de la SSA, el mecanismo de cifrado permite aislar la información de personal no autorizado dentro y fuera de la secretaría, y a la vez minimizar las consecuencias indeseadas que éstos puedan generar con el uso indebido de los datos.

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Por lo anterior, se concluye que existieron deficiencias en los controles de seguridad física y lógica del Centro de datos, en incumplimiento de lo establecido en el III.C. Proceso de Administración de la Operación (AOP), Actividad AOP 4, del Manual 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 y sus reformas del 23 de julio de 2018; así como de los artículos 42, 47, inciso c; 48, incisos a, c y d; 76, Incisos c, d, e y f, del Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, publicado en el DOF el 6 de septiembre de 2021.

**2021-0-12100-20-0341-01-011 Recomendación**

Para que la Secretaría de Salud implemente, formalice y mejore los controles para la administración de los servicios de Tecnologías de la Información y Comunicaciones (TIC), que consideren la identificación y actualización de los activos y servicios de TIC; que verifique la capacidad y rendimientos de la infraestructura de las Tecnologías de la Información y Comunicaciones para determinar si es suficiente para prestar los servicios de Tecnologías de la Información y Comunicaciones con los niveles acordados y que informe a los responsables de los dominios tecnológicos de la secretaría de las oportunidades y recomendaciones emitidas para mejorar la capacidad de la arquitectura tecnológica.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**2021-0-12100-20-0341-01-012 Recomendación**

Para que la Secretaría de Salud elabore un Análisis de Impacto al Negocio, que considere la totalidad de las actividades y que permita identificar los tipos de impacto, las afectaciones y consecuencias sobre los procesos críticos de la secretaría y a partir del cual se defina un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación en caso de Desastres (DRP); que defina la frecuencia con la que se van a revisar, probar y actualizar los análisis de impacto realizados al negocio, con el propósito de reflejar los cambios en los sistemas o en la operación de los procesos críticos de la secretaría; que defina escenarios para la verificación de posibles contingencias operativas, como enfermedades infecciosas, indisponibilidad de recursos humanos, materiales o técnicos, interrupciones ocurridas en servicios prestados por terceros; adicionalmente, que implemente mecanismos de prueba que permitan validar la efectividad de la estrategia de continuidad al menos semestralmente y, en caso necesario, realizar las modificaciones necesarias para corregir las desviaciones identificadas y mejorar el tiempo objetivo de recuperación (RTO) de las operaciones de la Secretaría de Salud; finalmente, que defina un árbol de llamadas con la información de contacto del personal responsable de gestionar las actividades de recuperación.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**2021-0-12100-20-0341-01-013 Recomendación**

Para que la Secretaría de Salud elabore e implemente una metodología, política o procedimiento para la generación y restauración de respaldos de información, en donde se defina a los responsables de solicitarlos y autorizarlos, y que mantenga actualizados y bajo resguardo los respaldos de información.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**2021-0-12100-20-0341-01-014 Recomendación**

Para que la Secretaría de Salud refuerce los controles físicos y lógicos necesarios dentro de su Centro de Datos para garantizar la continuidad y disponibilidad de las operaciones, así como la confidencialidad e integridad de la información de la secretaría e implemente una matriz de riesgos físicos, lógicos y ambientales del centro de datos, así como de las políticas para su actualización, con la finalidad de identificar los peligros y establecer las acciones preventivas para mitigar los riesgos que pudieran afectar las operaciones de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**2021-0-12100-20-0341-01-015 Recomendación**

Para que la Secretaría de Salud implemente controles y mecanismos en los Centro de Datos de la secretaría para contar con cifrado en los medios de almacenamiento, que defina el listado de los operadores responsables de su resguardo y mantenimiento; que elabore, actualice e implemente políticas o lineamientos de seguridad física y lógica para los Centros de Datos, en los que se considere la atención de incidentes del ambiente físico, el ingreso, instalación, configuración y retiro del equipamiento tecnológico.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

## 7. Estrategia de Vacunación Covid-19

Como parte de los trabajos de auditoría se verificaron las condiciones con las que la Secretaría de Salud realizó la administración de los sistemas y bases de datos involucrados en la adquisición, gestión y distribución de las vacunas para la atención a la pandemia generada por el virus SARS-CoV-2 (COVID-19), con el objetivo de comprobar la disponibilidad de la información y continuidad de los servicios. En el análisis realizado se observó lo siguiente:

El 4 de diciembre de 2020, la Secretaría de Gobernación (SEGOB), la Secretaría de Salud (SSA), la Secretaría de Bienestar (SB), la Secretaría de Educación Pública (SEP), el Instituto Mexicano del Seguro Social (IMSS), el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), el Instituto de Salud para el Bienestar (INSABI) y el Sistema Nacional para el Desarrollo Integral de la Familia (DIF) celebraron el “Convenio General de Colaboración para coadyuvar en las acciones inherentes a la atención de la pandemia causada por la COVID-19 en México, incluyendo la implementación de las políticas, medidas y acciones para la vacunación contra el virus SARS-COV-2”, con objeto de establecer los mecanismos correspondientes entre los participantes, en el ámbito de sus respectivas competencias para dar cumplimiento a las disposiciones emitidas por la Secretaría de Salud para la atención de dicha pandemia.

Dentro de dicho convenio, en la cláusula Segunda “Instrumentación”, se estableció en el numeral III los compromisos específicos de la SSA:

### *“III. Compromisos específicos de “SALUD”*

*[...]*

*b. Concentrar la información la información que requiera de “LAS PARTES”, para fortalecer la atención de las medidas para mitigar los efectos de la pandemia causada por el virus SARS-CoV-2; incluyendo la implementación de las campañas de vacunación derivadas de esta.*

*[...]*

*f. Intercambiar y mantener actualizada la información del personal de salud, tanto de instituciones a nivel local y federal, así como del ámbito privado, sin importar su categoría o tipo de contratación, que permita llevar el registro y seguimiento de éstos, respecto de la aplicación de la vacuna en contra de la enfermedad COVID-19.*

*g. Vigilar y supervisar que en todo momento se cumpla con lo establecido en el presente Convenio General de Colaboración.*

*h. Proporcionar a “GOBERNACIÓN” el listado de personas, conteniendo la CURP o aquellos datos de identidad jurídica que permitan identificar a las personas candidatas vacunales o que hayan sido vacunadas contra el COVID-19, a efecto de que se confronte y valide la CURP y/o sus datos de identidad jurídica, con base en el anexo de ejecución suscrito por “LAS PARTES” involucradas.*

La SSA informó de la existencia de los sistemas denominados “Ambiente para la Administración y Manejo de Atenciones en Salud (AAMATES)”, Plataforma CV COVID (con sus respectivas bases de datos), y la copia de la base de datos denominada “Mi Vacuna”, desarrollados y empleados en diferentes etapas del proceso de vacunación y proporcionó la información que a su consideración daba cumplimiento a los requerimientos de este ente fiscalizador, así como también proporcionó una extracción de su información para el análisis por parte del personal auditor de la ASF. De lo anterior, se obtuvo lo siguiente:

### Ambiente para la Administración y Manejo de Atenciones en Salud (AAMATES)

#### Características Generales

AAMATES es un sistema desarrollado por la SSA desde hace varios años, para gestionar los insumos hospitalarios, expedientes electrónicos y otros procesos de la operación sanitaria de los diversos nosocomios que dependen directamente de ella. Dentro de dicho sistema se cuenta con un módulo denominado “Inventario”, en el cual para atención de la pandemia, en febrero de 2021, se registró el catálogo de insumos y vacunas adquiridos para la atención a la pandemia generada por el virus SARS-CoV-2 (COVID-19) y fue utilizado durante el transcurso de dicha pandemia. A continuación, se describen las características de este módulo:

CARACTERÍSTICAS PRINCIPALES DEL MÓDULO INVENTARIO DEL AAMATES

Objetivo	Llevar la administración eficiente del movimiento y conteo de los insumos adquiridos.
Fecha de inicio de su funcionamiento	Febrero de 2021.
Número de usuarios	2,326 (octubre de 2021).
Administración de usuarios	La Dirección General de Tecnologías de la Información (DGTI) de la SSA es la encargada de dar de alta los usuarios que solicite cada uno de los “encargados correccaminos” de cada una de las entidades federativas.
Adquisiciones de bienes o servicios	No.
Vinculación con otros sistemas	Ninguna.
Cantidad de registros (tabla principal)	63,990

FUENTE: Elaborado con base en la información proporcionada por la SSA.

NOTA: Encargados correccaminos, se refiere a las 32 personas (una por entidad federativa) responsables, entre otras cosas, de la administración de usuarios del sistema AAMATES, así como de coordinar su uso en la Unidades Médicas de su competencia.

En la información proporcionada se observó lo siguiente:

- No se proporcionó el Modelo Entidad- Relación o cualquier otra representación gráfica donde se identifiquen las tablas utilizadas por el módulo de inventario, con la finalidad de identificar la interrelación de la información en los distintos almacenes de datos.
- No se entregó el diccionario de datos de las tablas utilizadas por el sistema.

- No se identificaron los servidores, sistemas operativos, bases de datos, su ubicación, componentes de conectividad, módulos que integran la aplicación y diagramas lógicos de las bases de datos.
- No se cuenta con reglas de operación y criterios de validación de la información contenida en el sistema AAMATES y su base de datos.
- No se entregaron las políticas, lineamientos y procedimientos utilizados para la administración y validación de usuarios y contraseñas del sistema AAMATES, ni el listado de usuarios, con sus roles y privilegios.
- No se identificó el seguimiento a las salidas del almacén de las vacunas a aplicar, el personal que realiza dicha actividad, ni si en el módulo de inventario se registra el destino final de las vacunas.

### **Análisis de Calidad de Datos**

El 25 de mayo el personal auditor de la ASF se presentó en las instalaciones de la DGTI de la secretaría con la finalidad de extraer, con corte a esa fecha, la totalidad de registros de la base de datos del módulo de inventario de AAMATES, mismos que fueron analizados por el personal auditor de la ASF para determinar la consistencia y calidad de la información contenida en dichas bases, y obtuvieron los resultados siguientes:

- Se identificó que 145,506,201 registros de vacunas fueron recibidas (entradas) o distribuidas (salidas) en las Unidades Médicas, dichas vacunas se encontraban en presentaciones de “ampolleta”, “envase” o “vial”.
- Se observó que existen 11,701 registros con fechas de entrada y salida correspondientes a los meses de julio a diciembre de 2022, periodo que no coincide con la fecha en que se obtuvo la información (mayo 2022).
- De las 145,506,201 vacunas registradas en la base de datos de movimientos, 320,002 (0.2%) corresponden a vacunas con fechas de entradas y salidas en los años 2012, 2016, 2018, 2019, 2023 y 2024, lo cual no es consistente con las fechas de atención a la pandemia generada por el virus SARS-CoV-2 (COVID-19).
- Del total de vacunas registradas como recibidas (86,286,072) sólo se registró la distribución del 68.3% (58,900,126) de las mismas, por lo que existe una diferencia de 31.7% (27,385,946) que corresponderían a vacunas que presuntamente no han salido de las Unidades Médicas donde se almacenan.
- La estructura de los datos contenidos en el campo “fecha movimiento” no se encuentra estandarizada; se observó que la fecha se capturó con formatos distintos y se cuenta con registros sin fecha.

- Se visualizaron inconsistencias en las fechas de creación del registro debido a que, para algunas vacunas, éstas son posteriores a la fecha en que se realizó un movimiento; así como en la captura del campo “Lote”.

## Plataforma CV COVID

### Características Generales

Plataforma web diseñada para la generación de los certificados de vacunación en contra del SARS-CoV-2 (COVID-19), (<https://cvcovid.salud.gob.mx/>). El personal de la DGTI manifestó que la “Secretaría de Salud cuenta con la plataforma CV Covid que, si bien no participa de la distribución de las vacunas, en ésta se integra toda la información de las vacunas efectivamente aplicadas para poder emitir el certificado de vacunación. Para ello cuenta con dos fuentes de información:

- *Plataforma “mivacuna.gob.mx”:* Desarrollada y operada por la Secretaría del Bienestar, en la que se registra la vacunación de la población en general, desde el preregistro web y hasta la captura de los comprobantes de vacunación por parte de la brigada correcaminos. La Secretaría de Salud no administra esta plataforma y solo recibe una copia de la información que se actualiza de manera incremental cada 20 minutos mediante una conexión segura.
- *Plataforma de vacunación del personal del sector de la salud (https://vacunasovid.gob.mx):* Sistema desarrollado y administrado por el Instituto Mexicano del Seguro Social, utilizada para el registro del personal del sector salud vacunado. La Secretaría de Salud no administra esta plataforma y solo recibe una copia de la información que se actualiza de manera incremental cada 24 horas mediante una conexión segura.”

A continuación, se describen las características de esa plataforma web:

CARACTERÍSTICAS PRINCIPALES CV COVID

Objetivo	Generación del certificado de vacunación directo al usuario final.
Número de usuarios	No cuenta con usuarios registrados, debido a que éste es un proceso automatizado.
Administración de plataforma	La DGTI de la SS es la encargada de administrar la plataforma, misma que opera mediante consultas a su plataforma web sin necesidad de autenticarse.
Vinculación con otros sistemas	Bases de datos de la Secretaría del Bienestar en las cuales realizó el registro de las personas vacunales, así como de las personas efectivamente vacunadas. Base de datos del Instituto Mexicano del Seguro Social (IMSS), en la cual se llevó a cabo el registro del personal del sector salud de todo el país que recibió las vacunas correspondientes.
Cantidad de registros (tabla principal)	85,414,696.

FUENTE: Elaborado con base en la información proporcionada por la SSA.

En la información proporcionada se observó lo siguiente:

- No se proporcionó el Modelo Entidad-Relación utilizado por la plataforma CV Covid, su diccionario de datos, ni las reglas de operación y criterios de validación de la información contenida en la plataforma y sus bases de datos.
- No se cuenta con la arquitectura lógica y física de la plataforma CV Covid, que permita identificar sus componentes tecnológicos.
- No se entregaron las políticas, lineamientos y procedimientos utilizados para la administración y validación de usuarios y contraseñas de la plataforma CV Covid.

### **Análisis de Calidad de Datos**

El 25 de mayo y el 15 de junio de 2022, personal auditor de la ASF asistió a las instalaciones de la DGTI para extraer la totalidad de los registros de la plataforma CV Covid, encargada de la recopilación de la información de personas vacunales, personas de la población general vacunados (en ambos casos, información proporcionada por la Secretaría del Bienestar); así como de las personas del sector salud vacunadas (información proporcionada por el IMSS) para la generación y envío de las constancias de vacunación, , mismos que fueron analizados por el personal auditor de la ASF para determinar la consistencia y calidad de la información contenida en dichas bases, y se obtuvieron los resultados siguientes:

- La Clave Única de Registro de Población (CURP) es el identificador principal de cada registro de la base de datos; sin embargo, éste no corresponde a un campo obligatorio. Se identificaron 2 valores no válidos (valores nulos) en el campo “Curp”.
- Existen registros de personas vacunadas con edades que van desde los 122 años hasta los 0 años, de lo anterior se observó que:
  - Existen 13,826,870 de personas vacunadas con más de 110 años, lo cual es inconsistente con lo reportado por el Instituto Nacional de Estadística y Geografía (INEGI), en donde para el 2020 señaló que para los Estados Unidos Mexicanos existen 18,295 hombres y mujeres con 100 años y más.
  - En el apartado del campo “Curp” donde se registra el año de nacimiento de las personas, se muestran los dígitos “00”; por lo que los registros no cuentan con la calidad esperada y la información no es consistente.
- El campo “fecha\_caducidad\_vacuna” no cuenta con una estructura estandarizada, debido a que hay errores en su estructura.
- Se identificaron inconsistencias para 1,003 registros en la captura del nombre de las vacunas (por ejemplo AstraZeneca, ASTRA ZENECA, Astra Ze0, Astra Zeca, Sputnik V, Sputnik1, Cans, Cansino y Cansin0) debido a que no se encuentran homologados.

- Se detectaron valores nulos en los campos “id\_dosis” (1,647,990) y “idRegistro” (1,644,822), así como inconsistencias en los datos registrados en “id\_dosis”.
- En el campo “sexo” se capturaron 67 valores (M, H, N, -, 1, entre otros); sin embargo, en el formato para el registro de las personas candidatas vacunales sólo se pedía especificar entre mujer (M) y hombre (H).
- Existen 20,510,646 registros (24.0%), sin nombre, primer y segundo apellido, fecha de nacimiento, nacionalidad ni sexo de la persona registrada.
- De los 85,414,696 de registros, se identificó la aplicación de un total de 83,768,374 vacunas de acuerdo con la información revisada. Para los 1,646,322 registros faltantes, se observó que cuentan con valores nulos o con inconsistencias en su captura.
- No fue posible verificar el número de personas que cuentan con el registro de su esquema completo de vacunación, para la generación del certificado correspondiente, debido a que sólo se proporcionó información referente a la aplicación de la primera dosis.
- No se cuenta con la evidencia que acredite la validación de la Clave Única de Registro de Población (CURP) en el Registro Nacional de Población (RENAPO).

### **Mi Vacuna (mivacuna.gob.mx)**

#### **Características Generales**

Plataforma que fue desarrollada, administrada y es operada por la Secretaría del Bienestar pero que otorga a la secretaría una copia incremental de la información cada 20 minutos. Esta copia incluye los datos del pre registro web que realizó la ciudadanía a través del portal web mivacuna.gob.mx. La SSA manifestó contar con una copia de esta base de datos y precisó que no realiza ninguna operación de escritura o borrado de esta información y solo consulta los datos para poder enviar las constancias generadas en la plataforma CV Covid a los correos y teléfonos registrados. A continuación, se describen las características de esta base:

## CARACTERÍSTICAS PRINCIPALES DE LA BASE DE DATOS RELACIONADA CON LA PLATAFORMA MI VACUNA

Objetivo	Registro de la vacunación de la población en general, desde el preregistro web y hasta la captura de los comprobantes de vacunación por parte de la brigada correccaminos.
Fecha de inicio de su funcionamiento	La SSA lo desconoce.
Número de usuarios	No está en el ámbito de competencia de la SSA, debido a que es responsabilidad de la Secretaría de Bienestar.
Administración de usuarios	Secretaría de Bienestar.
Vinculación con otros sistemas	Bases de datos de la Secretaría del Bienestar en las cuales realizó el registro de las personas vacunales, así como de las personas efectivamente vacunadas.
Cantidad de registros (tabla principal)	85,435,369.

FUENTE: Elaborado con base en la información proporcionada por la SSA.

### Análisis de Calidad de Datos

Como parte de las labores de auditoría, el 15 de junio del 2022, personal auditor de la ASF visitó las instalaciones de la DGTI para extraer la totalidad de los registros del repositorio de información de Mi vacuna, en donde se recopila la información del pre-registro de las personas vacunales correspondientes a la población general, así como del personal vacunado (información proporcionada por la Secretaría del Bienestar), mismo que fue analizado por la el personal auditor de la ASF para determinar la consistencia y calidad de la información contenida en dicha base, se observó lo siguiente:

- La base de datos relacionada con Mi vacuna tiene 85,435,369 registros, sin contar con un campo llave como identificador único.
- La base de datos contiene el registro de las personas candidatas vacunales de la población en general, por lo que únicamente contempla los datos de contacto, datos personales sensibles, correo electrónico y CURP. No obstante, no se proporcionaron las CURP, teléfonos, ni correos electrónicos de los 85,435,369 registros de personas vacunales.
- Existen registros de personas vacunadas con edades que van desde los 122 años hasta los 0 años.
- En el campo "Sexo" se observaron 61 valores (M, H, N, \*, -, 1, entre otros).

Por todo lo anterior, se concluye que la secretaría no cuenta con información exacta, completa y confiable en las bases de datos del módulo inventario de AAMATES, CV Covid y Mi Vacuna; toda vez que se identificaron los siguientes errores relacionados con la calidad de los datos:

INCONSISTENCIAS ASOCIADAS A LA CALIDAD DE LOS DATOS AAMATES, CV COVID Y MI VACUNA

Características	Descripción	Observación
Exactitud	El grado en que los datos tienen atributos que representan correctamente el verdadero valor del atributo previsto de un concepto o evento en un contexto de uso específico.	No se cuenta con controles de entrada de datos, impactando en la exactitud de los datos cargados, tanto semántica, como sintácticamente; debido a que no reflejan la realidad de la situación de su titular, es decir, no son verdaderos o fieles. Por ejemplo, errores en la estructura de la CURP, así como los diferentes valores en el género de las personas.
Complejidad	El grado en que los datos del sujeto asociados con una entidad, tienen valores para todos los atributos esperados e instancias de entidades relacionadas en un contexto de uso específico. Cuando no falta ningún dato personal que se requiera para las finalidades para las que se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular.	No es posible garantizar que las bases de datos de los sistemas utilizados para la atención de la pandemia generada por el virus SARS-COV-2 contemplen el universo de datos y los campos requeridos en éstas; debido a que se identificaron campos vacíos en los campos para determinar el número de dosis, fechas de movimientos, CURP, correos electrónicos o teléfonos.
Consistencia	La consistencia entre los formatos del campo y los registros.	Se identificaron valores en 0, errores de captura y valores incorrectos en los campos de las bases de datos. Por ejemplo, errores de captura en la CURP, edad, sexo, marca de vacuna, número de dosis y fechas; no se tienen definidos los tipos de datos para los campos de las bases de datos.
Correctos	Cuando los datos personales no tienen errores o defectos y por ello cumplen con todas las características previas, es decir, son exactos, completos, pertinentes y actualizados.	Se identificaron errores de captura y valores incorrectos en los campos de las bases de datos. Por ejemplo, errores de captura en la CURP, edad, sexo, número de dosis, marca de vacuna.

FUENTE: Elaborado con base en la información proporcionada por la SSA.

Por lo que no es posible asegurar que la información concentrada por la Secretaría de Salud, en las bases de datos del módulo inventario de AAMATES, CV Covid y Mi Vacuna, así como la que es proporcionada a la Secretaría de Gobernación, sea confiable e íntegra, lo cual impacta en los procesos de identificación de las personas candidatas vacunales (población general y personal del sector salud) que hubieran hecho su pre registro o en su caso, que hayan sido vacunadas contra el SARS-CoV-2 (COVID-19), y se les haya generado su certificado de vacunación; asimismo, se carece de mecanismos para la validación de los datos registrados y no se han adoptado las medidas convenientes para procurar que los datos cumplan con las características de exactitud, completitud y consistencia, con el fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la población general, así como personal del sector salud se vea impactado por esta situación; por lo que se vio afectado el cumplimiento de los compromisos y obligaciones señalados en el numeral III, incisos b, f, g y h del Convenio General de Colaboración para Coadyuvar en las Acciones Inherentes a la Atención de la Pandemia causada por la COVID-19 en México, incluyendo la implementación de las Políticas, Medidas y Acciones para la Vacunación contra el Virus SARS-COV-2 del 4 de diciembre de 2020; así como lo establecido en los artículos 16, 23 y 24 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**2021-0-12100-20-0341-01-016 Recomendación**

Para que la Secretaría de Salud defina, implemente o en su caso refuerce sus mecanismos y controles para garantizar que los datos e información contenida en sus sistemas, plataformas, aplicativos y bases de datos utilizados, sean exactos, completos, pertinentes, actualizados y correctos, con la finalidad de que no se altere la veracidad e integridad de la información y así mitigar los riesgos que pudieran afectar las operaciones de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

**2021-0-12100-20-0341-01-017 Recomendación**

Para que la Secretaría de Salud defina, actualice e implemente políticas o lineamientos para la gestión y validación de usuarios y contraseñas de los sistemas y bases de datos de la secretaría, así como que identifique y documente la información requerida para la operación y funcionamiento de las bases de datos, en los que se considere la arquitectura lógica y física, incluyendo los servidores, sistemas operativos, bases de datos, ubicación física de servidores, componentes de conectividad, módulos que integran la aplicación, diccionarios de datos, reglas de operación y diagramas lógicos de las bases de datos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

***Montos por Aclarar***

Se determinaron 24,586,380.08 pesos pendientes por aclarar.

***Buen Gobierno***

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

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

Se determinaron 7 resultados, de los cuales, en uno no se detectó irregularidad y los 6 restantes generaron:

17 Recomendaciones y 3 Pliegos de Observaciones.

### **Consideraciones para el seguimiento**

Los resultados, observaciones y acciones contenidos en el presente informe 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 de auditoría se encuentran sujetas al proceso de seguimiento, por lo que, debido a la información y consideraciones que en su caso proporcione la entidad fiscalizada podrán atenderse o no, solventarse o generar la acción superveniente que corresponda de conformidad con el marco jurídico que regule la materia.

### **Dictamen**

El presente dictamen se emite el 13 de octubre de 2022, 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 Salud cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En la revisión del contrato número DGRMSG-DCC-S-045-2021, cuyo objeto fue proporcionar el Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E4, E6 y P6, celebrado con Ofi Productos de Computación, S.A. de C.V., se determinó lo siguiente:
  - Se estima un probable daño o perjuicio por 313.4 miles de pesos debido a que se identificó equipamiento que se encontraba en almacén o en su embalaje original, por los que se realizaron pagos por 216.4 miles de pesos; asimismo, la secretaría no pudo demostrar la existencia de 17 equipos, por los que realizó pagos por 97.0 miles de pesos.
  - Existieron deficiencias en la supervisión del contrato, toda vez que no se cuenta con la documentación que acredite que el administrador del contrato estableció mecanismos de control que documentaran los procesos de entrega e implementación del equipo arrendado; no validó los equipos recibidos ni realizó un seguimiento del cumplimiento del contrato.

- En la revisión del contrato número DGRMSG-DCC-S-055-2021, cuyo objeto fue proporcionar el Arrendamiento de Equipo de Cómputo Personal y Periféricos para las partidas E1 y E2, celebrado con Mainbit, S.A. de C.V., respectivamente, se determinó lo siguiente:
  - Se carece de la evidencia de las actividades realizadas por el administrador del contrato para supervisar la entrega e implementación de los equipos solicitados y garantizar la prestación del servicio.
  - El proveedor no realizó la entrega e instalación de los equipos de cómputo durante el ejercicio de 2021 y no ha realizado el pago de las penas convencionales determinadas por la secretaría; por lo que los atrasos en la implementación de los equipos han afectado a los usuarios de la secretaría y por ende sus tareas operativas.
  
- En la revisión del contrato número DGRMSG-DCC-S-008-2018, cuyo objeto fue prestar el Servicio Integral de Telecomunicaciones (SINTEL), celebrado con Uninet, S.A. de C.V. en participación conjunta con Consorcio Red Uno, S.A. de C.V., Triara.Com, S.A. de C.V., Scitum, S.A. de C.V., Prestaciones Profesionales Empresariales, S.A. de C.V. y Servicios Especializados Scitum, S.A. de C.V., se determinó lo siguiente:
  - Se estima un probable daño o perjuicio por 4,398.4 miles de pesos debido a que se identificó que se efectuaron pagos por el servicio de arreglo de equipos de control de acceso a la red (NAC) durante 2021; sin embargo, el proveedor no presta este servicio desde el año 2019.
  - La secretaría determinó deductivas por 17.8 miles de pesos por los servicios recibidos con una calidad menor a la requerida; sin embargo, no se proporcionó la evidencia para verificar el cálculo realizado.
  - Se carece de la documentación que acredite que el administrador del contrato realizó la supervisión, administración y vigilancia del contrato, servicios y documentación generada por el proveedor para la prestación de los servicios.
  
- En la revisión del contrato número DGRMSG-DCC-S-020-2020, cuyo objeto fue prestar el Servicio para Mantenimiento y Desarrollo de Aplicaciones Sustantivas, celebrado con el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), se determinó lo siguiente:
  - Se estima un probable daño o perjuicio por 19,874.6 miles de pesos debido a que se carece de la evidencia que valide que todas las órdenes de servicio generadas durante 2021 con el proveedor, fueron cerradas a satisfacción de las áreas usuarias; que se cuenta con sus entregables, así como con la

documentación probatoria que valide la ejecución de las actividades de mantenimiento y desarrollo por parte del proveedor.

- El administrador del contrato no verificó las horas/hombre referidas por el proveedor de la ejecución de los servicios de desarrollo de software, tampoco se ejecutaron análisis de vulnerabilidades antes de la liberación de los desarrollos de software.
- Se identificaron deficiencias en la administración y operación de los 20 controles de Ciberseguridad para la infraestructura de hardware y software de la secretaría, revisados conforme lo establecido en el documento “Center for Internet Security (CIS) Controls IS Audit/Assurance Program”, toda vez que 3 controles se requieren fortalecer y 17 carecen de control; lo anterior podría afectar la integridad, disponibilidad y confidencialidad de la información, poniendo en riesgo la operación de la SSA.
- Existieron deficiencias en los controles de seguridad física y lógica del Centro de Datos, por lo cual, en caso de una contingencia, no es posible garantizar la continuidad de las operaciones de la secretaría, así como la restauración de los sistemas críticos.
- Se identificaron áreas de mejora en las bases de datos (del módulo inventario de AAMATES, CV Covid y Mi Vacuna) utilizadas en los procesos de identificación de las personas candidatas vacunales (población general y personal del sector salud) que hubieran hecho su pre registro o en su caso, que hayan sido vacunadas contra el SARS-CoV-2 (COVID-19), y se les haya generado su certificado de vacunación.

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

Director de Área

Director General

C. Jazmín Gabriela Pantoja Soto

Mtro. Roberto Hernández Rojas Valderrama

***Comentarios de la Entidad Fiscalizada***

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

elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

## **Apéndices**

### *Procedimientos de Auditoría Aplicados*

1. Verificar que para los Capítulos del gasto relacionados con las TIC las cifras reportadas en la Cuenta Pública se corresponden con las registradas en el estado del ejercicio del presupuesto y que están de conformidad con las disposiciones y normativas aplicables; analizar la integración del gasto ejercido en materia de TIC en los Capítulos asignados de la Cuenta Pública fiscalizada.
2. Validar que el estudio de factibilidad comprenda el análisis de las contrataciones vigentes; la determinación de la procedencia de su renovación; la pertinencia de realizar contrataciones consolidadas; los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.
3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo a las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones; verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.
4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permitan su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como las penalizaciones y deductivas en caso de incumplimientos.
5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, servicios administrados para la operación de infraestructura y sistemas sustantivos, telecomunicaciones y demás relacionados con las TIC para verificar: antecedentes; beneficios esperados; entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento/sustantivas); implementación y soporte de los servicios; verificar la gestión de riesgos, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de vulnerabilidades, entre otros.
7. Verificar la gestión de los programas de continuidad de las operaciones; evaluar la seguridad física y lógica del Centro de Datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).
8. Verificar la evaluación de la calidad y la arquitectura de las bases de datos; asimismo, verificar el control de accesos y privilegios, segregación de funciones, controles de las cuentas funcionales y privilegiadas, trazabilidad y monitoreo de las operaciones de los sistemas de información empleados para la adquisición y distribución de vacunas COVID-19.

#### *Áreas Revisadas*

La Unidad de Administración y Finanzas, la Dirección General de Recursos Materiales y Servicios Generales, la Dirección General de Tecnologías de Información, la Dirección de Red y Telecomunicaciones, y la Dirección de Sistemas e Infraestructura, todas adscritas a la Secretaría de Salud.

#### *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: Art. 1, Par. 2.
2. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Art. 93.
3. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 66, Frac. I y III.
4. Otras disposiciones de carácter general, específico, estatal o municipal: Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias, Art. 3; Art. 10, Frac. IX; Art. 11 Frac. II; Art. 18 Frac. II;

Art. 27; Art. 26; Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; actividad APRO 3, Factor Crítico 3; II.C. Proceso de Administración de la Seguridad de la Información (ASI), Actividad ASI 5, factor crítico 5; Actividad ASI 6, factor crítico 1, incisos i), j), k), l), m), n), o), p), q); II.A. Proceso de Administración de Servicios (ADS), Actividades ADS 1, factor crítico 1, inciso g, (subinciso iii); ADS 2, factor crítico 3, incisos a y b; ADS 3, factores críticos 1, inciso d, 2, 3, 4, 5 y 6, incisos a y b y ADS 4, factores críticos 1, 3, 4, 5, 6 y 7; apartado III.C. Proceso de Administración de la Operación (AOP), objetivos específicos 1 y 2, Actividad AOP 4; ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, Art.42; Art. 47, inciso a, c, d; Art. 48, incisos a, c y d; Art. 75, segundo párrafo; Art. 76, incisos c, d, e, f y g; Contrato núm. DGRMSG-DCC-S-045-2021, cláusula segunda párrafo segundo; cláusula tercera; cláusula décima tercera; Anexo único del contrato núm. DGRMSG-DCC-S-045-2021, numeral 2 y sus requerimientos 6, 9, 12, 13 y 15; Contrato núm. DGRMSG-DCC-S-055-2021, numeral 1.12 del apartado Declaraciones I. De La Dependencia; Anexo único del contrato núm. DGRMSG-DCC-S-055-2021, numeral 2; numeral 3; numeral 4; numeral 5; numeral 9; Reglamento Interior de la Secretaría de Salud, Art. 32, Frac. III; Frac. VIII; Frac. XI; Manual de organización específico de la Dirección General de Tecnologías de la Información, objetivo y funciones 3, 4, 5, 6, 7, 8, 11 y 12, de la sección Dirección de Redes y Telecomunicaciones; Manual de Organización General de la Secretaría de Salud, apartado VI. Funciones de la Dirección General de Tecnologías de la Información, Objetivo, funciones 1, 4, 5, 6, 7, 8, 15; Contrato núm. DGRMSG-DCC-S-008-2018, Declaración I.6; cláusula Octava; cláusula Novena; Anexo único del contrato núm. DGRMSG-DCC-S-008-2018, numerales I. Objeto de la contratación; II. Descripción de los servicios, Apartados A. Características técnicas de los servicios, 5) Enlace de Internet 10 Mbps con protección DoS y seguridad perimetral (FW UTM), 6) Equipo DNS dedicado, 8) Sistema de monitoreo de desempeño de los componentes de red para 2,000 elementos; D. Mantenimiento, incisos 1) Mantenimiento preventivo y correctivo y 2) Actualizaciones del sistema y su hardware, H. Metodología e I. Plan de trabajo; y Apéndice 2. Distribución de los servicios; Contrato No. DGRMSG-DCC-S-020-2020, Cláusulas Primera; Cláusulas Tercera; Cláusulas Octava, Cláusulas Décima Tercera; Anexo único del contrato No. DGRMSG-DCC-S-020-2020, numerales 3, 5, 6, 7, 8, 9, 10, 11 y 20; Convenio General de Colaboración para Coadyuvar en las Acciones Inherentes a la Atención de la Pandemia causada por la COVID-19 en México, numeral III, incisos b, f, g y h; Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Art. 16; Art. 23; Art. 24.

*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.