Secretaría de Salud

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2024-0-12100-20-0385-2025

Modalidad: Presencial

Núm. de Auditoría: 385

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 2024 en consideración de lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

Fiscalizar la gestión financiera de las contrataciones relacionadas con TIC, el gobierno y administración de riesgos, la ciberseguridad, la resiliencia de las operaciones, la operación de los centros de datos, los servicios de cómputo en la nube, el desarrollo de soluciones tecnológicas y el aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas, normativas y mejores prácticas aplicables.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	483,690.2
Muestra Auditada	196,310.9
Representatividad de la Muestra	40.6%

El universo seleccionado por 483,690.2 miles de pesos, corresponde al total de pagos de los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal de 2024; la muestra auditada está integrada por 2 contratos y 16 convenios modificatorios, relacionados con servicios integrales de telecomunicaciones y de centro de datos, con pagos por 196,310.9 miles de pesos que representan el 40.6% del universo seleccionado. Adicionalmente, la auditoría comprende la revisión de la Ciberseguridad de la Secretaría de Salud (SSA).

Los recursos objeto de revisión en esta auditoría se encuentran reportados en la Cuenta de la Hacienda Pública Federal del ejercicio de 2024, Tomo III Poder Ejecutivo, apartado Información Presupuestaria en el “Estado Analítico del Ejercicio del Presupuesto de Egresos en Clasificación Económica y por Objeto del Gasto”, correspondiente al Ramo 12 “Salud”.

Antecedentes

La misión de la Secretaría de Salud (SSA) es establecer las políticas de Estado para que la población ejerza su derecho a la protección a la salud.

Para lograrlo, la Dirección General de Tecnologías de la Información (DGTI) en su planeación estratégica impulsó la gestión y operación de sus comunicaciones institucionales y de su infraestructura de Tecnologías de la Información y Comunicaciones, garantizando la conectividad, interconexión y soporte a los procesos administrativos, operativos y de investigación en los Institutos Nacionales de Salud y Hospitales de Alta Especialidad. Asimismo, fortaleció la gestión documental, la operación de la Biblioteca de la Comisión Nacional de Bioética y la aplicación del Examen Nacional para Aspirantes a Residencias Médicas 2024. Estas acciones incluyeron el desarrollo de software de apoyo para diseño de imagen y comunicación digital institucional, así como la implementación del protocolo de internet IPv6, consolidando así la modernización tecnológica y la eficiencia operativa de la dependencia.

Resultados

1. Análisis Presupuestal

De acuerdo con el Decreto de Presupuesto de Egresos de la Federación para el ejercicio fiscal de 2024, publicado en el Diario Oficial de la Federación el 25 de noviembre de 2023, se autorizó a la Secretaría de Salud un presupuesto de 96,989,997.6 miles de pesos para sus unidades centrales, órganos administrativos desconcentrados y entidades Paraestatales.

Del presupuesto aprobado a las unidades centrales y órganos administrativos desconcentrados por 53,145,141.2 miles de pesos, a la SSA le correspondieron 1,597,449.2 miles de pesos en el capítulo 3000, con las ampliaciones y reducciones quedó un presupuesto modificado por 2,529,161.5 miles de pesos en dicho capítulo.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2024, se concluyó que la SSA tuvo un presupuesto ejercido de 2,529,152.5 miles de pesos y economías por 9.0 miles de pesos en el capítulo 3000, de los cuales, 501,908.2 miles de pesos, correspondieron a recursos relacionados con las Tecnologías de la Información y Comunicación (TIC), que representan el 19.8% del presupuesto en el capítulo señalado, como se muestra a continuación:

RECURSOS EJERCIDOS POR LA SECRETARÍA DE SALUD EN TIC DURANTE EL EJERCICIO DE 2024

(Miles de pesos)

Capítulo	Concepto	Presupuesto ejercido (A)	Presupuesto ejercido TIC (B)	Porcentaje C=(B*100) /A
3000	Servicios generales	2,529,152.5	501,908.2	19.8
	TOTALES	2,529,152.5	501,908.2	19.8%

FUENTE: Información proporcionada por la Secretaría de Salud.

Los recursos ejercidos en materia de las TIC por 501,908.2 miles de pesos se integran de la manera siguiente:

GASTOS EN MATERIA DE TIC DURANTE 2024 EN LA SECRETARÍA DE SALUD

(Miles de pesos)

Capítulo/ Subpartida	Descripción	Presupuesto ejercido
3000	SERVICIOS GENERALES	
31401	Servicio telefónico convencional	1,869.9
31602	Servicios de telecomunicaciones	110,050.6
31701	Servicios de internet	16,514.3
31904	Servicios integrales de infraestructura de cómputo	212,387.6
32301	Arrendamiento de equipo y bienes informáticos	94,983.6
32701	Servicios de desarrollo de aplicaciones informáticas	39,438.9
33301	Otros servicios comerciales	26,663.3
	TOTAL	501,908.2

FUENTE**:** Información proporcionada por la Secretaría de Salud.

NOTA: Diferencias por redondeo.

Del universo seleccionado en el ejercicio de 2024 por 483,690.2 miles de pesos, que corresponde al total de pagos ejercidos en los contratos relacionados con las TIC, se erogaron 196,310.9 miles de pesos en dos contratos y dieciséis convenios modificatorios que representan el 40.6% del universo seleccionado, que son los siguientes:

MUESTRA DE CONTRATOS Y CONVENIOS DE TIC EJERCIDOS DURANTE 2024
(Miles de pesos)

Tipo de Contratación	Contrato	Proveedor	Objeto	Vigencia		Monto		
				Del	Al	Mínimo	Máximo	Ejercido
Adjudicación Directa	DGRMSG-DCC-S-008-2018	Uninet, S.A. de C.V., (en su carácter de fusionante de Consorcio Red Uno, S.A. de C.V. y Prestaciones Profesionales Empresariales, S.A. de C.V.), en participación conjunta con Triara.Com, S.A. de C.V. y Scitum, S.A. de C.V., (en su carácter de fusionante de Servicios Especializados Scitum, S.A. de C.V.)	Servicio integral de telecomunicaciones (SINTEL)	27/04/2018	31/03/2021	383,144.2	957,860.6	126,564.8
	Convenio Modificatorio 01/21		Ampliación de la vigencia.	01/04/2021	30/06/2021			
	Convenio Modificatorio 02/21		Ampliación de la vigencia.	01/07/2021	30/09/2021			
	Convenio Modificatorio 03/21		Ampliación de la vigencia.	01/10/2021	31/12/2021			
	Convenio Modificatorio 04/21		Ampliación de la vigencia.	01/01/2022	31/03/2022			
	Convenio Modificatorio 05/22		Ampliación de la vigencia.	01/04/2022	30/06/2022			
	Convenio Modificatorio 06/22		Ampliación de la vigencia.	01/07/2022	30/09/2022			
	Convenio Modificatorio 07/22		Ampliación de la vigencia.	01/10/2022	31/12/2022			
	Convenio Modificatorio 08/22		Ampliación de la vigencia.	01/01/2023	31/03/2023			
	Convenio Modificatorio 09/23		Ampliación de la vigencia.	01/04/2023	30/06/2023			
	Convenio Modificatorio 10/23		Ampliación de la vigencia.	01/07/2023	30/09/2023			
	Convenio Modificatorio 11/23		Ampliación de la vigencia.	01/10/2023	31/10/2023			
	Convenio Modificatorio 12/23		Ampliación de la vigencia.	01/11/2023	31/12/2023			
	Convenio Modificatorio 13/23		Ampliación de la vigencia.	01/01/2024	31/03/2024			
	Convenio Modificatorio 14/24		Ampliación de la vigencia.	01/04/2024	31/12/2024			
	Convenio Modificatorio 15/24		Ampliación de la vigencia.	01/01/2025	31/03/2025			
Licitación Pública	DGRMSG-DCC-S-029-2022	Triara.Com, S.A. de C.V. en participación conjunta con Uninet, S.A. de C.V., B Drive It S.A. de C.V. y Engine Core, S.A. de C.V.	Servicio Integral de Centro de Datos para la Secretaría de Salud	22/07/2022	31/12/2024	137,414.7	343,536.7	69,746.1
	Convenio Modificatorio 01/24		Ampliación de la vigencia.	01/01/2025	31/03/2025			
					Total	520,558.9	1,301,397.3	196,310.9

FUENTE: Información proporcionada por la Secretaría de Salud.

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

2. Servicio Integral de Telecomunicaciones (SINTEL)

Se revisó el contrato número DGRMSG-DCC-S-008-2018 suscrito con Uninet, S.A. de C.V. (en su carácter de fusionante de Consorcio Red Uno, S.A. de C.V., y Prestaciones Profesionales Empresariales, S.A. de C.V.), en participación conjunta con Triara.Com, S.A. de C.V., y Scitum, S.A. de C.V., (en su carácter de fusionante de Servicios Especializados Scitum, S.A. de C.V.), con vigencia del 27 de abril de 2018 al 31 de marzo de 2021, por un monto mínimo de 383,144.2 miles de pesos y máximo de 957,860.6 miles de pesos, para el servicio integral de telecomunicaciones (SINTEL).

Se celebraron 15 convenios modificatorios para ampliar la vigencia al 31 de marzo de 2025 sin exceder su monto máximo original. Durante el ejercicio fiscal 2024 la Secretaría de Salud (SSA) pagó 126,564.8 miles de pesos, de los cuales se pagaron 11,224.6 miles de pesos por los trabajos de diciembre de 2023; por otra parte, por los trabajos de enero a noviembre de 2024, se erogaron 115,340.2 miles de pesos.

Alcance del servicio

Se contempló la prestación de servicios de comunicaciones para voz, datos y video de la secretaría, así como su seguridad asociada, por medio 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.

Revisión técnica, funcional y administrativa

Se revisó la documentación técnica para verificar el cumplimiento a las características del contrato y se encontró lo siguiente:

Servicios de Enlace MPLS (Conmutación de Etiquetas Multiprotocolo) de 10 Mbps

En el anexo único del contrato no se estableció un mecanismo que permitiera solicitar, atender, autorizar y verificar las solicitudes de ajuste del ancho de banda requeridas por la SSA.

Sistema de Monitoreo de desempeño de los componentes de red para 2,000 elementos

- No se demostró que el sistema de monitoreo implementado fuera compatible con los sistemas operativos y protocolos requeridos en el anexo único.

- El proveedor no acreditó que el sistema de monitoreo pudiera integrar 2,000 elementos de red ni configuró los umbrales de rendimiento y disponibilidad en el

tablero de control, lo que impidió monitorear adecuadamente el desempeño de los componentes que integran la red institucional.

- No se proporcionó evidencia de que el Sistema de Monitoreo contara con la capacidad para almacenar y conservar los registros generados por cada uno de los dispositivos monitoreados.

Servicio de Monitoreo

Centro de Operaciones de la Red (NOC)

- El NOC no contó con un plan de capacidades de infraestructura del año 2024 ni llevó a cabo los análisis semestrales sobre el desempeño de la infraestructura y los servicios del proveedor.

- El proveedor no presentó el módulo de usuarios en el tablero de control, lo que impidió verificar al personal autorizado del NOC y sus perfiles.

Centro de Operaciones de Seguridad (SOC)

- En 2024, la secretaría no realizó una visita física al SOC para verificar la ejecución de los servicios conforme a lo establecido en el anexo único del contrato.

- La SSA no validó los mecanismos implementados por el proveedor para gestionar y supervisar remotamente los dispositivos de seguridad.

- El proveedor no presentó el módulo de usuarios del tablero de seguridad, lo que impidió validar al personal autorizado y sus perfiles de acceso.

- La herramienta de monitoreo utilizada por el proveedor no tiene habilitado el envío automático de alertas ante cambios en la configuración de los equipos, lo que limita la capacidad de detección oportuna de modificaciones no autorizadas o incidentes de seguridad.

Por lo anterior, se observó que el administrador del contrato no validó las características técnicas del sistema de monitoreo, en incumplimiento 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, artículos 41, inciso d; 47, inciso c; y 48, inciso a; del contrato DGRMSG-DCC-S-008-2018, declaración I.6; y cláusula sexta, inciso c; y del Anexo Único del contrato DGRMSG-DCC-S-008-2018, apartado "II. Descripción de los servicios", subapartados A. Características técnicas de los servicios; B. Administración de los servicios; D. Mantenimiento; E. Monitoreo; H. Metodología, inciso 2. "Etapa 2. Operación del Servicio Integral de Telecomunicaciones (SINTEL)", numerales II. NOC (Centro de Operaciones de la Red) y III. SOC (Centro de Operaciones de Seguridad); así como el Manual de

Organización General de la Secretaría de Salud, función 8 de la Dirección General de Tecnologías de la Información; y el Manual de Organización Específico de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, funciones 4, 5 y 11 de la Dirección de Red y Telecomunicaciones.

Pruebas en sitio

Se realizaron visitas a los cuartos de telecomunicaciones (MDF[1] e IDF[2]) de la secretaría y se identificaron deficiencias en las condiciones de operación como la falta de ventilación o control de temperatura, la presencia de materiales inflamables, artículos de limpieza y un garrafón de agua, así como la acumulación de polvo en los *Conmutadores, Unidades de energía ininterrumpible, Cortafuegos y Enlaces de comunicación.*

La Secretaría de Salud, en el transcurso de la auditoría y con motivo de la intervención de la Auditoría Superior de la Federación, informó el retiro del material no relacionado con los servicios de red, así como la definición de bitácoras y listas de verificación mensuales; no obstante, se encuentra en proceso de su implementación en todos los cuartos de telecomunicaciones, a fin de fortalecer sus mecanismos de verificación internos para preservar la integridad de la infraestructura.

Evaluación de controles y mejores prácticas en materia de seguridad de la información

- No se presentaron evidencias documentales que acrediten la comunicación entre el proveedor y el administrador del contrato respecto a la atención de incidencias del servicio.

- Después de la notificación del proveedor sobre el cambio de personal, la SSA no verificó el cumplimiento del perfil requerido del nuevo recurso asignado para la prestación de los servicios.

- Se careció de un procedimiento documentado para la administración y uso de las controladoras de red inalámbricas.

- No se proporcionó evidencia de la validación de los monitoreos del Centro de Operaciones de la Red (NOC).
- En el Centro de Operaciones de Seguridad (SOC), el proveedor no contó con procedimientos formalizados para la gestión del monitoreo, incidentes, cambios, requerimientos extraordinarios ni para el levantamiento y cierre de tickets.

---

[1] MDF: Marco de distribución principal, es el eje central de la red de un edificio, donde se conectan los servicios externos (como internet y telefonía) a la red interna del edificio.

[2] IDF: Marco de distribución Intermedio, desempeña un papel de apoyo al MDF, actuando como un punto de retransmisión que extiende la conectividad del MDF a áreas, pisos o secciones específicas de un edificio a los que el marco de distribución principal no puede llegar directamente debido a limitaciones de distancia, facilitando las conexiones de red local para dispositivos y usuarios en sus áreas específicas.

- La secretaría no validó la implementación de las políticas de seguridad informática en sus dispositivos e infraestructura para la prestación de los servicios del SOC.

En conclusión, existieron deficiencias en la gestión, supervisión y operación de la infraestructura tecnológica y se identificaron omisiones en la validación de ajustes de ancho de banda en enlaces MPLS (Conmutación de etiquetas multiprotocolo), en el sistema de monitoreo de red, así como la falta de controles en el NOC y SOC en incumplimiento de la normativa. No existieron condiciones adecuadas en los cuartos de telecomunicaciones y no se acreditó documentalmente la comunicación con el proveedor para la gestión de incidentes.

2024-0-12100-20-0385-01-001 **Recomendación**

Para que la Secretaría de Salud fortalezca los mecanismos de supervisión, seguimiento y validación en las contrataciones de Tecnologías de la Información y Comunicaciones para establecer revisiones independientes y documentar las actividades; realizar visitas físicas a las instalaciones de los prestadores de servicios y validar los mecanismos de gestión y monitoreo implementados, con la finalidad de asegurar que los servicios contratados se presten conforme a las características técnicas y a los requerimientos 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.

2024-0-12100-20-0385-01-002 **Recomendación**

Para que la Secretaría de Salud realice revisiones periódicas a los sitios principales e intermedios de telecomunicaciones, con el objetivo de verificar que éstos se encuentren en condiciones óptimas, cuenten con ventilación adecuada para regular la temperatura de los equipos, y mantengan una limpieza general en pisos, paredes, cableado y tuberías. Asimismo, que se asegure de que no haya materiales inflamables en su interior, a fin de garantizar la seguridad y disponibilidad de la información, así como de la infraestructura tecnológica 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.

2024-0-12100-20-0385-01-003 **Recomendación**

Para que la Secretaría de Salud fortalezca los mecanismos de supervisión y seguimiento en los contratos de servicios de telecomunicaciones para que la evidencia técnica de cualquier modificación al ancho de banda, cuente con el detalle de la fecha, las horas, los parámetros

técnicos antes y después del cambio, así como los resultados de las pruebas correspondientes; además, realice y mantenga actualizado el registro de cada modificación y asegure la disponibilidad de dicho registro durante la vigencia del contrato; adicionalmente, defina métricas de desempeño con umbrales de alerta para utilizarlas en actividades de supervisión de las redes y la toma de decisiones de la operación de la infraestructura tecnológica, con la finalidad de garantizar la trazabilidad de los cambios, optimizar la gestión de los contratos y asegurar la continuidad y calidad 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.

2024-9-12112-20-0385-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación comunica la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en la Secretaría de Salud o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de las personas servidoras públicas que, en su gestión del contrato número DGRMSG-DCC-S-008-2018 "Servicio integral de telecomunicaciones (SINTEL)", no validaron ni dieron seguimiento a los servicios prestados debido a las omisiones en la validación de la compatibilidad técnica y la capacidad de integración del sistema de monitoreo; la verificación de la configuración de umbrales y el almacenamiento de registros (logs) para la trazabilidad y el control operativo; la verificación de los planes de capacidad (capacity planning) y el análisis del desempeño del Centro de Operaciones de Red (NOC); la supervisión de la implementación y el control de módulos de usuarios y perfiles en los tableros de control (dashboards) para asegurar la observabilidad y el seguimiento de métricas; así como para la realización de visitas físicas en sitio para verificar la ejecución de los servicios y constatar los mecanismos de vigilancia remota del Centro de Operaciones de Seguridad (SOC), en incumplimiento 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, artículos 41, inciso d; 47, inciso c; y 48, inciso a; del contrato DGRMSG-DCC-S-008-2018, declaración I.6; y cláusula sexta, inciso c; y del Anexo Único del contrato DGRMSG-DCC-S-008-2018, apartado "II. Descripción de los servicios", subapartados A. Características técnicas de los servicios; B. Administración de los servicios; D. Mantenimiento; E. Monitoreo; H. Metodología, inciso 2. "Etapa 2. Operación del Servicio Integral de Telecomunicaciones (SINTEL)", numerales II. NOC (Centro de Operaciones de la Red) y III. SOC (Centro de Operaciones de Seguridad); así como el Manual de Organización General de la Secretaría de Salud, función 8 de la Dirección General de Tecnologías de la Información; y el Manual de Organización Específico de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, funciones 4, 5 y 11 de la Dirección de Red y Telecomunicaciones.

3. Servicio Integral de Centro de Datos para la Secretaría de Salud

Se analizó el contrato número DGRMSG-DCC-S-029-2022 suscrito con Triara.Com, S.A. de C.V., en participación conjunta con Uninet, S.A. de C.V., B Drive IT, S.A. de C.V., y Engine Core, S.A. de C.V., con vigencia del 22 de julio de 2022 al 31 de diciembre de 2024, por un monto mínimo de 137,414.7 miles de pesos y máximo de 343,536.7 miles de pesos, para el servicio integral de Centro de Datos para la Secretaría de Salud.

Se celebró un convenio modificatorio para ampliar la vigencia al 31 de marzo de 2025 sin exceder su monto máximo original. Durante el ejercicio fiscal 2024 la Secretaría de Salud (SSA) pagó 69,746.1 miles de pesos, de los cuales se pagaron 7,046.0 miles de pesos por los servicios devengados en diciembre de 2023 y 62,700.1 miles de pesos por los servicios devengados de enero a diciembre de 2024.

Alcance del Servicio

El alcance contempló los servicios del proceso de migración como la infraestructura (centro de datos, virtualización, plataforma de contenedores y bases de datos); la gestión de sistemas operativos y bases de datos; la seguridad (*firewall* perimetral, protección contra *malware* para servidores, protección de correo electrónico, resolución de nombres de dominio externos, certificados digitales, pruebas de penetración y análisis de vulnerabilidades); el enlace a internet; el monitoreo y centro de operaciones de seguridad (SOC); la mesa de ayuda y la transición al término del contrato.

Pagos

Durante el ejercicio de 2024, se realizaron pagos por 69,746.1 miles de pesos; sin embargo, no se proporcionó la evidencia que acredite el cumplimiento del proceso de pago de los servicios establecido en la cláusula tercera del contrato.

Revisión técnica, funcional y administrativa

Servicio de infraestructura

Existieron deficiencias en la gestión y supervisión de accesos por parte de la secretaría, debido a que, en la herramienta de monitoreo de infraestructura, se identificó 1 (20.0%) de 5 usuarios que no debía estar habilitado.

Servicio de virtualización

La SSA gestionó la creación de máquinas virtuales y designó responsables por unidad administrativa; no obstante, careció de los mecanismos para verificar que las actualizaciones hayan sido aplicadas.

Servicio de seguridad

No se presentó la evidencia que demuestre la comunicación entre el administrador del contrato y el proveedor, para la solicitud, la autorización, la ejecución y la validación de los cambios en la configuración de las políticas de seguridad perimetral implementadas por el prestador del servicio.

Servicio de pruebas de penetración (caja gris y caja negra)

Los reportes de las pruebas de penetración realizadas en 2024 no contienen los hallazgos específicos, ni la evidencia que respalde la prestación del servicio de seguridad integrado por 7 subservicios con las pruebas de penetración a la infraestructura tecnológica, por los cuales se pagaron 19,633.8 miles de pesos; cabe señalar que no se cuenta con el desglose de los precios de dichos subservicios.

Lo anterior incumplió los artículos 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 14, fracción I de los Lineamientos en Materia de Austeridad Republicana de la Administración Pública, publicados en el Diario Oficial de la Federación el 18 de septiembre de 2020; 3, fracción I, 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 el 06 de septiembre de 2021; Cláusulas Primera, Tercera y Décima novena, del contrato número DGRMSG-DCC-S-029-2022; y los numerales “I. Objeto de la contratación” y “4.2.6.6 Servicio pruebas de penetración (caja gris y caja negra)”, del anexo técnico del contrato número DGRMSG-DCC-S-029-2022.

Evaluación de controles y mejores prácticas en materia de seguridad de la información

- La secretaría no dispone de un Plan de Recuperación ante Desastres ni de un centro de datos alterno, contractualmente solo cuenta con el Centro de Datos Principal del proveedor.

- La SSA no cuenta con un procedimiento documentado para la implementación de actualizaciones de seguridad en sus sistemas operativos.

- El proveedor presentó la evidencia de las acciones implementadas para restringir la navegación en internet; no obstante, no se cuenta con un procedimiento formalizado que establezca los criterios de aplicación, las restricciones específicas y los responsables de su validación.

Se concluye que no se acreditó la ejecución de las pruebas de penetración por las que se pagaron 19,633.8 miles de pesos; además, no se contó con un Plan de Recuperación ante Desastres ni procedimientos formales para la aplicación de actualizaciones de seguridad.

2024-0-12100-20-0385-01-004 **Recomendación**

Para que la Secretaría de Salud implemente controles para la gestión de accesos a las plataformas críticas para asegurar que las cuentas de usuario estén autorizadas, auditadas y eliminadas oportunamente cuando pierdan vigencia.

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.

2024-0-12100-20-0385-01-005 **Recomendación**

Para que la Secretaría de Salud desarrolle un Plan de Recuperación en caso de Desastres y un Plan de Continuidad del Negocio con base en el Análisis de Impacto al Negocio de la dependencia, que considere la totalidad de las actividades y permita identificar los tipos de impacto, las afectaciones y las consecuencias sobre sus procesos críticos; asimismo, que realice pruebas para asegurar que se cuenta con la capacidad de recuperación en caso de presentarse un incidente que ocasione la interrupción de las operaciones.

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.

2024-0-12100-20-0385-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 19,633,784.16 pesos (diecinueve millones seiscientos treinta y tres mil setecientos ochenta y cuatro pesos 16/100 M.N.), por realizar los pagos del servicio de seguridad, debido a que no se cumplió con el objetivo del servicio de las pruebas de penetración para identificar las vulnerabilidades contenidas en la infraestructura, así como para las pruebas de los controles de seguridad desde un ambiente externo (caja negra) y el ambiente interno (caja gris), con la emisión de las recomendaciones y hallazgos identificados para mejorar el nivel de seguridad, conforme lo establecido en el numeral 4.2.6.6 "Servicio pruebas de penetración (caja gris y caja negra)" del anexo técnico del contrato número DGRMSG-DCC-S-029-2022, suscrito con el proveedor Triara.Com, S.A. de C.V., en participación conjunta con Uninet, S.A. de C.V., B Drive IT, S.A. de C.V., y Engine Core, S.A. de C.V; adicionalmente, por no contar con evidencia que respalde la prestación del servicio, lo que limitó la capacidad para identificar, evaluar y mitigar vulnerabilidades en la infraestructura tecnológica de la dependencia, más los rendimientos financieros generados desde la fecha de su pago hasta la de su recuperación,, en incumplimiento del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III; de los Lineamientos en Materia de Austeridad Republicana de la Administración Pública, artículo 14, fracción I; 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, artículo 3, fracción I; del contrato número DGRMSG-DCC-S-029-2022, Cláusulas Primera, Tercera y Décima Novena; y del anexo técnico del contrato número DGRMSG-DCC-S-029-2022, numerales "I. Objeto de la contratación" y "4.2.6.6 Servicio pruebas de penetración (caja gris y caja negra)".

Causa Raíz Probable de la Irregularidad

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

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

Resultado 2 - Acción 2024-0-12100-20-0385-01-001

4. Ciberseguridad

Se analizó la información proporcionada por la Secretaría de Salud relacionada con la administración y operación de los controles de ciberseguridad vinculados con la infraestructura y soluciones tecnológicas; la revisión se realizó de conformidad con los controles del Centro de Seguridad en Internet (CIS) y con las políticas de la SSA.

La verificación tuvo por objeto proporcionar a la Secretaría de Salud una evaluación de la efectividad de la ciberdefensa con referencia a los controles críticos del CIS, con base en las mejores prácticas para la gestión de incidentes, la administración de la configuración de seguridad, la gestión y conciencia de la seguridad, la seguridad de redes y servidores, la administración de la continuidad del negocio, la gestión de la seguridad de la información, así como las relaciones con terceros y prácticas de gobernanza.

El alcance de la auditoría consideró 18 dominios de seguridad críticos que incluyeron 151 controles y 215 subcontroles para evaluar el diseño y la efectividad operativa de la ciberseguridad con sus respectivos objetivos de cumplimiento.

Para la evaluación se consideraron tres niveles, de conformidad con el porcentaje alcanzado en la evaluación de los controles y subcontroles, en los cuales el nivel “Aceptable” se alcanza con más del 67.0%, el nivel “Requiere fortalecer el control” se obtiene entre el 33.0% y el 67.0%, y el nivel “Carencia de control” se consigue con menos del 33.0%.

Como resultado de la evaluación practicada se obtuvo lo siguiente:

EVALUACIÓN DE CIBERSEGURIDAD EN LA SSA CUENTA PÚBLICA 2024

Dominio	Nivel
01 Inventario y control de activos tecnológicos	
02 Inventario y control de activos de software	
03 Protección de datos	
04 Configuración segura de activos tecnológicos y software	
05 Administración de cuentas	
06 Gestión de control de acceso	
07 Gestión continua de vulnerabilidades	
08 Gestión de registros de auditoría	
09 Protecciones de correo electrónico y navegador web	
10 Defensas contra malware	
11 Recuperación de datos	
12 Gestión de infraestructura de red	
13 Monitoreo y defensa de redes	
14 Concientización sobre seguridad y capacitación en habilidades	
15 Gestión de proveedores de servicios	
16 Seguridad del software de aplicación	
17 Gestión de respuesta a incidentes	
18 Pruebas de penetración	
	Aceptable
	Requiere fortalecer el control
	Carencia de control

FUENTE: Elaborado con información proporcionada por la Secretaría de Salud.

En conclusión, en la presente revisión se identificaron cinco dominios aceptables (27.8%), siete dominios que requieren fortalecer el control (38.9%) y seis dominios con carencia de control (33.3%).

2024-0-12100-20-0385-01-006 **Recomendación**

Para que la Secretaría de Salud fortalezca las políticas, los procedimientos y los controles en la función de identificar de la ciberseguridad para el inventario y control de activos de hardware y software, la gestión continua de vulnerabilidades, la gestión de registros de auditoría y la gestión de proveedores de servicio, a fin de mejorar la comprensión del contexto organizacional, identificar los activos y software que respaldan los procesos críticos de la operación y gestionar adecuadamente los riesgos asociados para mitigar afectaciones en la secretaría y su 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.

2024-0-12100-20-0385-01-007 **Recomendación**

Para que la Secretaría de Salud fortalezca las políticas, los procedimientos y los controles en la función de proteger de la ciberseguridad para la protección de datos, la gestión de control de acceso, las defensas contra malware, la gestión de infraestructura de red, la concientización sobre seguridad y capacitación en habilidades y la seguridad del software de aplicación, con el propósito de robustecer la implementación de mecanismos orientados a salvaguardar los procesos y los activos de la organización, independientemente de su naturaleza 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.

2024-0-12100-20-0385-01-008 **Recomendación**

Para que la Secretaría de Salud fortalezca las políticas, los procedimientos y los controles en la función de responder de la ciberseguridad para la gestión de respuesta a incidentes, a fin de robustecer los mecanismos de prevención, detección, contención y erradicación en caso de un ataque cibernético.

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.

2024-0-12100-20-0385-01-009 **Recomendación**

Para que la Secretaría de Salud fortalezca las políticas, los procedimientos y los controles en la función de recuperar de la ciberseguridad para la recuperación de los datos, con la finalidad de mejorar los planes y las actividades para restaurar los procesos y servicios en caso de un incidente informático.

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 19,633,784.16 pesos pendientes por aclarar.

Buen Gobierno

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

Resumen de Resultados, Observaciones, Acciones y Recomendaciones

Se determinaron 4 resultados, de los cuales, en uno no se detectó irregularidad y los 3 restantes generaron:

9 Recomendaciones, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 1 Pliego 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 2025, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada 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 TIC, el gobierno y administración de riesgos, la ciberseguridad, la resiliencia de las operaciones, la operación de los centros de datos, los servicios de cómputo en la nube, el desarrollo de soluciones tecnológicas y el aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas, normativas y mejores prácticas 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 las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con el servicio integral del centro de datos para la Secretaría de Salud, los informes de pruebas de penetración no dan constancia de su ejecución ni integran hallazgos específicos para que la dependencia realice las acciones pertinentes para mitigar las vulnerabilidades identificadas; no obstante, se llevaron a cabo pagos por 19,633.8 miles de pesos por el servicio de seguridad.

- Con respecto al servicio integral de telecomunicaciones, se observaron deficiencias en el monitoreo de red, debido a que no fueron configurados los umbrales y a la falta de evidencia sobre la compatibilidad técnica del sistema. Asimismo, se detectaron debilidades en los controles aplicados en el Centro de Operación de Red (NOC) y el de Seguridad (SOC), así como en la supervisión de los cambios relacionados con los anchos de banda requeridos por la secretaría y con la infraestructura de los cuartos de telecomunicaciones.

- En cuanto a la Ciberseguridad, se identificaron cinco dominios aceptables (27.8%), siete dominios que requieren fortalecer el control (38.9%) y seis dominios con carencia de control (33.3%).

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Ing. Nohema Lara Blanco	Mtro. Genaro Héctor Serrano Martínez

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 que atiende parcialmente los hallazgos de la auditoría y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe de Auditoría.

El Informe de Auditoría puede consultarse en el Sistema Público de Consulta de Auditorías (SPCA).

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública se correspondieron con las registradas en el estado del ejercicio del presupuesto y que cumplieron las disposiciones

y normativas aplicables, así como analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que fueron identificadas las necesidades de bienes, arrendamientos o servicios requeridos para el cumplimiento de las atribuciones del ente público; revisar la estimación de los precios de los bienes, arrendamientos o servicios con base en la información existente en el sistema CompraNet o la histórica del ente público, actualizada conforme a los precios oficiales y de la competencia que sean aplicables, así como comprobar que la integración del Programa Anual de Adquisiciones, Arrendamientos y Servicios fue con base en los requerimientos de las áreas contratantes.

3. Constatar que la investigación de mercado verificó la oferta de bienes, arrendamientos o servicios y la existencia de proveedores a nivel nacional o internacional, así como que actualizó el precio de referencia del requerimiento específico; validar que se tuvo la suficiencia presupuestaria para cubrir el pago de la requisición de bienes, arrendamientos o servicios y que los licitantes no se encontraban inhabilitados para participar en los procedimientos de contratación, de igual manera validar que las evaluaciones técnicas y económicas cumplieron con los criterios de aceptación y las mejores condiciones de economía, eficacia y eficiencia para el ente público.

4. Comprobar que los precios marcados en la contratación se correspondan con los asentados en los comprobantes de pago y que las erogaciones fueron por trabajos efectivamente devengados que justificaron las facturas pagadas y que éstas cumplieron con los requisitos fiscales; verificar que fueron aplicadas las penas pactadas en el contrato por los atrasos del proveedor en la entrega del servicio, así como las deductivas que resulten procedentes por el incumplimiento parcial o la deficiente prestación de los servicios.

5. Realizar pruebas de cumplimiento a las contrataciones de las TIC para verificar que los bienes, arrendamientos o servicios recibidos correspondieron en sus características con las especificaciones contratadas, contenidas en las bases de licitación, contratos y anexos técnicos, que se contó con el soporte documental que acreditó la recepción del entregable conforme a lo establecido en la contratación.

6. Realizar pruebas sustantivas a las contrataciones de las TIC para comprobar que los entregables pactados en las bases de licitación, contratos y anexos técnicos cumplieron con los beneficios esperados, las especificaciones técnicas, la vigencia de los servicios, la entrega en las instalaciones, el resguardo de los bienes, el cumplimiento de las garantías, la implementación de las soluciones e infraestructura tecnológica y el soporte de los servicios.

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

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

Áreas Revisadas

Las direcciones generales de Programación y Presupuesto, y de Tecnologías de la Información, ambas adscritas a la Subsecretaría de Administración y Finanzas dependiente de la Secretaría de Salud.

Disposiciones Jurídicas y Normativas Incumplidas

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

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

2. Otras disposiciones de carácter general, específico, estatal, local o municipal: 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, artículos 3, fracción I, 41, inciso d, 47, inciso c, y 48, inciso a.

Reglamento Interior de la Secretaría de Salud, artículo 32, fracciones I, II, III, IV, V, VI y XI.

Manual de Organización General de la Secretaría de Salud, función 8 de la Dirección General de Tecnologías de la Información.

Manual de Organización Específico de la Dirección General de Tecnologías de la Información de la Secretaría de Salud, funciones 4, 5, y 11 de la Dirección de Red y Telecomunicaciones.

Lineamientos en Materia de Austeridad Republicana de la Administración Pública, artículos 14, fracción I.

Contrato número DGRMSG-DCC-S-008-2018, declaración I.6; y cláusula sexta, inciso c.

Anexo Único del contrato DGRMSG-DCC-S-008-2018, apartados "II. Descripción de los servicios", subapartados "A. Características técnicas de los servicios", numerales "1) Enlaces de MPLS 10 Mbps", "3) Enlace de Internet en HA 200 Mbps, con protección DoS y seguridad perimetral", "B. Administración de los servicios", "D. Mantenimiento", "E. Monitoreo", "H. Metodología", incisos 1 "Etapa 1. Implementación del Servicio Integral de Telecomunicaciones (SINTEL)" y 2 "Etapa 2. Operación del Servicios Integral de Telecomunicaciones (SINTEL)", numerales "II. NOC (Centro de Operaciones de la Red)" y "III. SOC (Centro de Operaciones de Seguridad)".

Contrato número DGRMSG-DCC-S-029-2022, Cláusulas Primera, Tercera y Décima Novena.

Anexo técnico del contrato número DGRMSG-DCC-S-029-2022, numerales "I. Objeto de la contratación", "4.2.2.2.5. Plataforma de contenedores" y "4.2.6.6 Servicio pruebas de penetración (caja gris y caja negra)".

Fundamento Jurídico de la ASF para Promover o Emitir Acciones y Recomendaciones

Las facultades de la Auditoría Superior de la Federación para promover o emitir las acciones y recomendaciones 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.