Secretaría de Educación Pública

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2021-0-11100-20-0257-2022

Modalidad: Por Medios Electrónicos

Núm. de Auditoría: 257

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

	EGRESOS
	Miles de Pesos
Universo Seleccionado	338,018.2
Muestra Auditada	222,715.0
Representatividad de la Muestra	65.9%

El universo seleccionado por 338,018.2 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal 2021; la muestra auditada está integrada por 3 contratos y 3 convenios modificatorios, relacionados con los servicios de centros de datos y de Seguridad Informática con pagos ejercidos por 222,715.0 miles de pesos, que representan el 65.9% del universo seleccionado.

Adicionalmente, la auditoría comprende el análisis presupuestal de la Cuenta Pública de 2021 de la Secretaría de Educación Pública (SEP) 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 SEP, así como Continuidad de las operaciones. 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 11 " Educación Pública".

Antecedentes

La Secretaría de Educación Pública (SEP) se creó el 3 de octubre de 1921 con el propósito esencial de crear condiciones que permitieran asegurar el acceso de las mexicanas y los mexicanos a una educación de excelencia con equidad, universalidad e integralidad, en el nivel y modalidad que la requieran y en el lugar donde la demanden.

La Direccion General de Tecnologías de la Información y Comunicaciones (DGTIC) tiene como objetivo mantener un Sistema de Gestión de la Calidad y de mejora continua; para ello debe:

- Fortalecer el desarrollo y uso de sistemas computarizados que permitan el eficaz desempeño de las funciones de la secretaría a través de la sistematización y automatización de los programas educativos y procesos administrativos, que soporten los procesos de planeación, ejecución y evaluación de las actividades de la dependencia.
- Asegurar la continuidad de los servicios informáticos y de comunicaciones de la secretaría a través del soporte oportuno y eficiente a los usuarios de las tecnologías de la información, así como la instrumentación de procesos automatizados de atención y administración de servicios.
- Dotar de la infraestructura informática y de comunicaciones a las áreas de la secretaría a través de la modernización y construcción de la infraestructura tecnológica que se soporte a los requerimientos de comunicación de voz, datos e imagen de la secretaría.

Como parte del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública de 2017, se realizó la auditoría 141-DS titulada “Auditoría de TIC”, en donde se validaron los servicios de seguridad, monitoreo, almacenamiento e infraestructura.

Con la información proporcionada por la entidad, se determinó que entre 2017 y 2021, la Secretaría de Educación Pública ha invertido 3,299,255.0 miles de pesos en materia de Tecnologías de la Información, como se muestra a continuación:

RECURSOS INVERTIDOS EN MATERIA DE TIC CUENTA PÚBLICA 2021
(Miles de Pesos)

Periodo de inversión	2017	2018	2019	2020	2021	Total
Cuenta Pública 2021	797,841.3	996,000.3	674,307.9	493,087.3	338,018.2	**3,299,255.0**

FUENTE: Elaborado con base en la información proporcionada por la SEP.
NOTA: Las cifras presentadas corresponden al Control Operativo TI a cargo de la DGTI.

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 de la 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 Educación Pública (SEP) se le aprobó un presupuesto de 337,851,440.8 miles de pesos, que después de ampliaciones y reducciones se modificó para quedar en 369,286,395.1 miles de pesos.

Respecto del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2021, la SEP tuvo un presupuesto ejercido de 17,290,367.3 miles de pesos en el capítulo 3000, de los cuales, 338,018.2 miles de pesos corresponden a recursos relacionados con las Tecnologías de Información y Comunicaciones (TIC), lo que representa el 2.0% del presupuesto ejercido, como se muestra a continuación:

RECURSOS EJERCIDOS EN CONTRATACIONES RELATIVAS A LAS TIC EN LA SEP DURANTE 2021
(Miles de pesos)

		A	B	C= B/A
Capítulo	**Descripción**	**Ejercido**	**Ejercido TIC**	**%**
3000	Servicios Generales	17,290,367.3	338,018.2	2.0
	TOTAL	**17,290,367.3**	**338,018.2**	**2.0**

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

Los recursos ejercidos en materia de TIC por 338,018.2 miles de pesos se integran de la manera siguiente:

INTEGRACIÓN DEL GASTO DE LAS CONTRATACIONES RELACIONADAS CON LAS TIC EN 2021 EN LA SEP
(Miles de pesos)

Capítulo / P. Presupuestaria	Subpartida	Descripción	Presupuesto Ejercido
3000		**Servicios Generales**	
3100		**Servicios básicos**	**262,262.8**
	31401	Servicio telefónico convencional	412.5
	31602	Servicios de telecomunicaciones	28,323.7
	31701	Servicios de conducción de señales analógicas y digitales	36,252.8
	31904	Servicios integrales de infraestructura de cómputo	197,273.8
3200		**Servicios de Arrendamiento**	**30,946.4**
	32301	Arrendamiento de equipo y bienes informáticos	30,946.4
3300		**Servicios profesionales, científicos, técnicos y otros servicios**	**44,809.0**
	33301	Servicios de desarrollo de aplicaciones informáticas	36,660.0
	33304	Servicios de mantenimiento de aplicaciones informáticas	8,149.0
		TOTAL	**338,018.2**

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

Del universo seleccionado en 2021 por 338,018.2 miles de pesos, que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 222,715.0 miles de pesos en 3 contratos y 3 convenios modificatorios que representan el 65.9% del universo seleccionado, el cual se integra de la manera siguiente:

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

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Ejercido
				De	Al	Mínimo	Máximo	
Licitación Pública	DGRMyS-DGTIC-LPN-001-2020	IQSEC, S.A. de C.V. en participación conjunta con VOSEDA NETWORKS, S.A. de C.V., y una persona física.	Servicio de Seguridad Informática.	25/11/2020	30/09/2022	96,785.9	241,964.7	
	Convenio Modificatorio al contrato DGRMyS-DGTIC-LPN-001-2020		Ampliación de la vigencia.	01/10/2022	31/12/2022	N/A	N/A	25,441.2
					Subtotal	**96,785.9**	**241,964.7**	**25,441.2**
Adjudicación Directa	DGRMyS-DGTIC-ADCA-003-2020	Metro Net, S.A.P.I. de C.V.	Centro de Datos SEP 2020.	01/04/2020	31/12/2020	108,673.1	271,682.8	
	Convenio Modificatorio al contrato abierto de prestación de servicios DGRMyS-DGTIC-ADCA-003-2020		Ampliación del monto y vigencia, así como modificación del Anexo de Ejecución en sus apartados I. Anexo Técnico y II. Propuesta Técnica y Económica del proveedor.	01/01/2021	31/03/2021	17,387.7	43,469.3	42,982.0
					Subtotal	**126,060.8**	**315,152.1**	**42,982.0**
Adjudicación Directa	DGRMyS-DGTIC-ADCA-001-2021	Sixsigma Networks México S.A. de C.V. (antes Metro Net, S.A.P.I. de C.V.)	Centro de Datos SEP 2021.	16/04/2021	31/12/2021	105,506.9	263,767.2	82,056.9
	Convenio Modificatorio al contrato abierto de prestación de servicios DGRMyS-DGTIC-ADCA-001-2021		Ampliación de la vigencia.	22/11/2021	31/03/2022	N/A	N/A	72,234.9
					Subtotal	**105,506.9**	**263,767.2**	**154,291.8**
					Total	**328,353.6**	**820,884.0**	**222,715.0**

FUENTE: Contratos y facturas proporcionadas por la SEP.

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

2. Contrato DGRMyS-DGTIC-LPN-001-2020 “Servicio de Seguridad Informática”

La Secretaría de Educación Pública formalizó el contrato número DGRMyS-DGTIC-LPN-001-2020 con la empresa IQSEC, S.A. de C.V., en participación conjunta con VOSEDA NETWORKS,

S.A. de C.V., y una persona física, mediante el procedimiento de licitación pública nacional, con fundamento en los artículos 26, fracción I, 26 Bis, fracción II, 28, fracción I, y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con vigencia del 25 de noviembre de 2020 al 30 de septiembre de 2022, por un monto mínimo de 96,785.9 miles de pesos y un máximo de 241,964.7 miles de pesos, con objeto de prestar el "Servicio de Seguridad Informática".

El 30 de septiembre de 2022 se suscribió el Primer Convenio Modificatorio para ampliar la vigencia del contrato al 31 de diciembre de 2022.

Alcance del Servicio

El contrato contempló la prestación de servicios de seguridad informática como son: Firewall, sistema de prevención de intrusos (IPS), red privada virtual (VPN), filtrado de contenidos, control de aplicaciones y antimalware; una solución de seguridad lineal, de seguridad proactiva, de prevención de ataques (DNS Interno y Externo); para el envío de información (paquetes) mediante una red digital; así como una solución de Centro de Operaciones de Seguridad (SOC).

Pagos

Durante el ejercicio 2021, se devengaron servicios por 25,441.2 miles de pesos que se pagaron con recursos de la Cuenta Pública de 2021.

Cumplimiento técnico y funcional de los servicios y entregables establecidos en el anexo técnico del contrato DGRMyS-DGTIC-LPN-001-2020

En la revisión del cumplimiento técnico del contrato número DGRMyS-DGTIC-LPN-001-2020, se identificó lo siguiente:

- La Dirección de Seguridad Informática y Prevención de Riesgos (DSIyPR) no elaboró una justificación técnica para modificar el alcance de la contratación para la inclusión de 2,500 agentes para la "Solución de Seguridad integral firewall, IPS, antimalware, filtrado de contenidos, control de aplicaciones y VPN", un sitio adicional para la "Solución de Seguridad Lineal" y tres sitios más para la "Solución de Seguridad Proactiva", siendo que en la convocatoria de licitación pública nacional se establecieron los mínimos y máximos de servicios. Tampoco realizó un dimensionamiento del crecimiento de los nuevos usuarios y la cantidad de agentes o sitios que requerirían ser incluidos en los servicios.
- No se implementaron políticas específicas para la identificación de los tipos de archivos que viajan en la red, ni de archivos ejecutables o malware dentro de archivos comprimidos como .rar o .zip.
- Los respaldos de las configuraciones del *firewall* que soporta el servicio de filtrado de contenidos, son realizados por los administradores de las herramientas sin notificarlos a la Dirección de Seguridad Informática y Prevención de Riesgos (DSIyPR), ni especificar el estado de su resguardo.

- A la fecha de la auditoría (octubre de 2022), no se han restringido los puertos USB en los equipos críticos que cuentan con el agente del servicio de seguridad lineal instalado, para reducir el riesgo de robo de información en equipos de operación relevante para la secretaría.
- Durante 2021, la DSIyPR no gestionó peticiones de configuraciones operativas o de reforzamiento a la seguridad en los *switches* que soportan el "Servicio de conmutación de paquetes core Alta densidad".
- No se cuenta con mecanismos de revisión por parte de la DSIyPR al cumplimiento de horarios operativos del personal del proveedor, ni para la retroalimentación a estos reportes.

Se concluye que existieron deficiencias en la revisión y seguimiento del contrato por parte del administrador del mismo, toda vez que no se configuraron las políticas relacionadas al bloqueo de puertos USB en equipos críticos, así como para la detección de *malware* dentro de archivos comprimidos; ni se cuenta con la justificación técnica para modificar el alcance de la contratación, en incumplimiento del III.B. Proceso de Administración de Proveedores (APRO), objetivo general, actividad APRO 2, Factores Críticos 1 y 3; actividad APRO 3, Factor Crítico 3; III.C. Proceso de Administración de la Operación (AOP), actividad AOP 3, factor crítico 3, del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI), publicado en el DOF el 8 de mayo de 2014 y sus reformas al 23 de julio de 2018; Objetivo general del puesto, funciones 4, 7 y 9 de la Dirección de Seguridad Informática y Prevención de Riesgos, del Manual de Organización General de la Dirección General de Tecnologías de Información y Comunicaciones formalizado el 26 de septiembre de 2018; Misión y función 10 del numeral 1.5.4, del Manual de Organización General de la Secretaría de Educación Pública publicado en el DOF el 10 de julio de 2018; Clausulas primera, décima segunda, del contrato número DGRMyS-DGTIC-LPN-001-2020; Partidas 1, 2, 4, 5, 8 y numeral 2.6 del Anexo de Ejecución del contrato número DGRMyS-DGTIC-LPN-001-2020.

Solución de Centro de Operaciones de Seguridad (SOC)

- No se realizaron actividades de depuración a las políticas de seguridad y configuraciones de las distintas herramientas que soportan el servicio.
- Durante 2021, el proveedor no realizó un análisis en búsqueda de posibles patrones o actividades anómalas en las diversas bitácoras generadas en las herramientas que soportan en el servicio.
- No se identificó el seguimiento llevado a cabo para las observaciones presentadas en los reportes del "Servicio de Protección Integral", a pesar de que algunos de estos hallazgos se identificaron como críticos.
- Los reportes del seguimiento para el uso indebido del nombre de la SEP en redes sociales limitan su alcance a Twitter, sin que se consideren otras redes sociales o plataformas de video.

- La DSIyPR no ejecutó actividades de atención, mitigación y seguimiento a los resultados y hallazgos presentados en los análisis de vulnerabilidades y pruebas de penetración proporcionados por el proveedor.
- El proveedor identifica y reporta los sitios fraudulentos en los entregables mensuales, sin que éste apoye y de soporte en las actividades de baja de estos sitios, conforme lo establecido en el anexo técnico del contrato.

Se concluye que la DSIyPR no supervisó que se mitigaran y se realizara el seguimiento a los hallazgos reportados por el proveedor, derivado de las actividades de investigación y análisis de vulnerabilidades en el Servicio de Protección Integral; no se depuraron las políticas de seguridad ni se realizó un análisis en búsqueda de actividades anómalas en las bitácoras de las herramientas utilizadas en el SOC. Lo anterior incumplió los artículos 3 y 27, fracción II, 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, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014 y sus reformas al 23 de julio de 2018; del III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; actividad APRO 3, Factor Crítico 3; del III.C. Proceso de Administración de la Operación (AOP), actividad AOP 3, Factor Crítico 3, del Manual Administrativo de Aplicación General en 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 al 23 de julio de 2018; Objetivo general del puesto, funciones 4 y 9 de la Dirección de Seguridad Informática y Prevención de Riesgos, del Manual de Organización General de la Dirección General de Tecnologías de Información y Comunicaciones formalizado el 26 de septiembre de 2018; Cláusulas Primera, Sexta, Décima segunda, del contrato número DGRMyS-DGTIC-LPN-001-2020; numerales 1.4, 2.4 y 2.5, la Sección Protección Integral, del Anexo de Ejecución del contrato número DGRMyS-DGTIC-LPN-001-2020.

2021-0-11100-20-0257-01-001 **Recomendación**

Para que la Secretaría de Educación Pública establezca actividades de atención y seguimiento a los hallazgos reportados como resultado del análisis de vulnerabilidades y pruebas de penetración, en donde se considere la definición de planes de trabajo y la documentación en los avances en la mitigación de cada una de las observaciones; lo que permitiría minimizar el riesgo de un ataque a la infraestructura que soporta los servicios críticos 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-002 **Recomendación**

Para que la Secretaría de Educación Pública implemente los mecanismos que le permitan garantizar la integridad de la información que se transmite en la red de la secretaría, definir políticas en las herramientas para el bloqueo de malware dentro de archivos comprimidos y restringir los puertos USB de los equipos cliente identificados como críticos. Asimismo, para que evalúe la pertinencia de solicitar a los proveedores de servicios de seguridad, apoyar en las tareas para dar de baja los sitios identificados como fraudulentos a nombre de la secretaría y ampliar el alcance del monitoreo en redes sociales, a los sitios con mayor concurrencia por parte del público.

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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

3. Contratos DGRMyS-DGTIC-ADCA-003-2020 “Centro de Datos SEP 2020” y DGRMyS-DGTIC-ADCA-001-2021 “Centro de Datos SEP 2021”

Durante 2021, estuvieron vigentes dos contratos abiertos con objeto de prestar el “Servicio de Centro de Datos” a la Secretaría de Educación Pública (SEP), los cuales se muestran a continuación:

CONTRATOS DEL SERVICIO DE CENTRO DE DATOS

Contrato	Prestador de servicios	Objetivo	Vigencia	Monto del contrato	Pagado 2021
				(Miles de pesos)	
DGRMyS-DGTIC-ADCA-003-2020	Metro Net, S.A.P.I. de C.V. (ahora Sixsigma Networks México, S.A. de C.V.)	Centro de Datos SEP 2020	Del 01/04/2020 al 31/03/2021	mínimo 126,060.8 máximo 315,152.1	42,982.0
DGRMyS-DGTIC-ADCA-001-2021	Sixsigma Networks México, S.A. de C.V.	Centro de Datos SEP 2021	Del 16/04/2021 al 30/03/2022	mínimo 105,506.9 máximo 263,767.2	154,291.8

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

Alcance del Servicio

El alcance de ambos contratos contempló lo siguiente:

- El licenciamiento usado en el servicio del Centro de Datos estará a cargo del proveedor y proporcionará los recursos humanos que den soporte y operación en un horario de 7x24.

- Espacio físico en el Centro de Datos incluyendo el suministro de infraestructura con facilidades propias de un centro de datos, necesarias para la coubicación de servidores en donde se almacenarán y ejecutarán los sistemas de información. El suministro de hardware dentro del Centro de Datos para la operación de aplicativos y bases de datos de los sistemas de información (Procesamiento, Licenciamiento y Almacenamiento).
- El proveedor deberá suministrar el equipamiento, racks y puesta a punto para recibir el enlace en las oficinas de la DGTIC, de la Subsecretaría de Planeación, Evaluación y Coordinación (SPEC) y de la Dirección General del Sistema de Administración de la Nómina Educativa Federalizada (DGSANEF).
- Administración y operación de la infraestructura de TIC y gestión de diversos servicios para la continuidad de las operaciones.
- Servicio de Análisis de Vulnerabilidades.

Los requerimientos de plataforma e infraestructura aplican para las Unidades Administrativas de la SEP siguientes:

- Dirección General de Planeación, Programación y Estadística Educativa (DGPPEE).
- Unidad del Sistema para la Carrera de las Maestras y los Maestros (USICAMM).
- Dirección General del Sistema de Administración de la Nómina Educativa Federalizada (DGSANEF).
- Subsecretaría de Educación Media Superior (SEMS).
- Dirección General de Televisión Educativa (DGTVE)/Coordinación General @prende.
- Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC).

Contrato DGRMyS-DGTIC-ADCA-003-2020 “Servicio de Centro de Datos SEP 2020”

Se formalizó el contrato número DGRMyS-DGTIC-ADCA-003-2020 con la empresa Metro Net, S.A.P.I. de C.V. (ahora Sixsigma Networks México, S.A. de C.V.), adjudicado directamente, con fundamento en los artículos 26, fracción III, 40, y 41, fracción III, y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), con vigencia del 1 de abril al 31 de diciembre de 2020, por un monto mínimo de 108,673.1 miles de pesos y un máximo de 271,682.8 miles de pesos, con objeto de prestar el “Servicio de Centro de Datos SEP 2020”.

El 31 de diciembre de 2020 se suscribió el Convenio Modificatorio para ampliar la vigencia al 31 de marzo de 2021, el monto mínimo a 126,060.8 miles de pesos y el máximo a 315,152.1 miles de pesos, así como para modificar el Anexo de Ejecución en sus apartados l. Anexo Técnico y II. Propuesta Técnica y Económica del proveedor.

Pagos

Con recursos de 2021 se realizaron pagos por 42,982.0 miles de pesos. En la revisión realizada, se observó lo siguiente:

- Se carece de los elementos que sustenten la cantidad de servicios considerados en las memorias de cálculo utilizadas para la elaboración de las 3 facturas que corresponden a requerimientos de plataforma e infraestructura de las unidades administrativas de la SEP que ascienden a 1,672.6 miles de pesos; asimismo, las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales no detallan la cantidad y tipo de servicios proporcionados por el proveedor, por lo que no se puede determinar que el monto pagado corresponda a servicios prestados por el mismo.

Contrato DGRMyS-DGTIC-ADCA-001-2021 "Servicio de Centro de Datos SEP 2021"

Se formalizó el contrato número DGRMyS-DGTIC-ADCA-001-2021 con la empresa Sixsigma Networks México, S.A. de C.V., adjudicado directamente, con fundamento en los artículos 26, fracción III, 40, y 41, fracción III, y 47, de la LAASSP, y en el artículo 85 del RLAASSP, con vigencia del 16 de abril al 31 de diciembre de 2021, por un monto mínimo de 105,506.9 miles de pesos y un máximo de 263,767.2 miles de pesos, con objeto de prestar el "Servicio de Centro de Datos SEP 2021".

El 22 de noviembre de 2021 se suscribió el Convenio Modificatorio al contrato abierto de prestación de servicios DGRMyS-DGTIC-ADCA-001-2021 para ampliar la vigencia al 31 de marzo de 2022 y actualizar la razón social del proveedor a Sixsigma Networks México, S.A. de C.V.

Proceso de Contratación

Se observaron discrepancias en el presupuesto asignado al proyecto en el estudio de factibilidad y no se justificó el cálculo realizado para la determinación de la suficiencia presupuestal.

Pagos

Con recursos de 2021 se realizaron pagos por 154,291.8 miles de pesos. En la revisión realizada, se observó lo siguiente:

- Se carece de elementos que sustenten la cantidad de servicios considerados en las memorias de cálculo utilizadas para la elaboración de las 10 facturas relacionadas con el servicio de soporte WSO2, que corresponden a requerimientos de plataforma e infraestructura de las unidades administrativas de la SEP que ascienden a 23,570.9 miles de pesos. Como resultado de la reunión de presentación de resultados finales y observaciones preliminares, la SEP presentó las cotizaciones realizadas por el proveedor, en las que estableció las unidades de servicio propuestas para esta actividad; sin embargo, al comparar dichas cotizaciones con los precios ofertados en el mercado por los fabricantes, se observó que las condiciones técnicas y económicas difieren con lo ofertado por los fabricantes de las soluciones tecnológicas utilizadas.

- Se estiman pagos en exceso por 71.5 miles de pesos, debido a que por el servicio mensual de enlaces de internet de julio de 2021, se pagaron 2,217.2 miles de pesos, a pesar de que el monto por los 21 días en que se ejecutó el servicio ascendía a 2,145.6 miles de pesos.
- Las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales, no detallan la cantidad y tipo de servicios proporcionados por el proveedor, por lo que no se puede determinar que el monto pagado corresponda a servicios prestados por el mismo.

Cumplimiento técnico y funcional de los servicios y entregables establecidos en los contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021

En la revisión del cumplimiento técnico de los contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021, se identificó lo siguiente:

- Con recursos de la Cuenta Pública de 2021 se pagaron 98,899.1 miles de pesos por el servicio recurrente del centro de datos; al ser un servicio integral con un costo mensual fijo, no fue posible identificar el pago por cada uno de los servicios implementados por el proveedor.
- No se cuenta con evidencia del seguimiento y remediación de los hallazgos identificados por el proveedor, como resultado del análisis de vulnerabilidades y amenazas informáticas.
- Para el servicio de cómputo en la nube, la secretaría no entregó evidencia del monitoreo de niveles de seguridad implementados por el proveedor.

Se concluye que existieron deficiencias en la revisión y seguimiento de los contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021, toda vez que se carece de la evidencia del seguimiento a las vulnerabilidades identificadas hasta su remediación; no se identificó el monitoreo a los niveles de servicio para cómputo en la nube; tampoco fue posible identificar en las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales la cantidad y tipo de servicios proporcionados por el proveedor, ni se contó con la documentación para determinar los montos a facturar del servicio mensual de unidades de administración y servicios para soporte y mantenimiento por el que se pagaron 1,672.6 miles de pesos para el contrato número DGRMyS-DGTIC-ADCA-003-2020 y por los servicios mensuales de actualización de licencia de WSO2 y de enlaces de internet por un monto de 23,642.4 miles de pesos para el contrato número DGRMyS-DGTIC-ADCA-001-2021. Lo anterior incumplió el artículo 3 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 publicado en el Diario Oficial de la Federación (DOF) el 8 de mayo de 2014 y sus reformas al 23 de julio de 2018; el III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 2, Factores Críticos 1 y 3; la actividad APRO 3, Factor Crítico 3, del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información (MAAGTICSI),

publicado en el DOF el 8 de mayo de 2014 y sus reformas al 23 de julio de 2018; el artículo 29, fracciones I, II, VI, VII, X, y XII, del Reglamento Interior de la Secretaría de Educación Pública publicado en el DOF el 15 de septiembre de 2020; las funciones 3, 4, 5, 7, 8, y 10 del apartado 7. Descripción de Puestos en el Manual de Organización de la Dirección General de Tecnologías de la Información y Comunicaciones; el numeral 2.1. Descripción del Proyecto, inciso a. Capacidad de cómputo en la nube, del Apartado Fase 2. Aspectos Técnicos del Proyecto del Anexo Técnico de los Contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021.

2021-0-11100-20-0257-01-003 **Recomendación**

Para que la Secretaría de Educación Pública fortalezca los controles de supervisión, seguimiento y validación por parte de los administradores de los contratos y del personal autorizado para la vigilancia y supervisión de los instrumentos jurídicos, que realicen revisiones independientes a las efectuadas por el proveedor sobre los servicios prestados y que documenten de manera formal dichas actividades para verificar el cumplimiento de las obligaciones derivadas de los contratos relacionados con servicios de Tecnologías de Información y Comunicaciones y se aseguren de que son proporcionados en su totalidad y que cumplen, en tiempo y forma, con los requerimientos 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-004 **Recomendación**

Para que la Secretaría de Educación Pública implemente medidas de control, adicionales a las realizadas por los proveedores, para la infraestructura de hardware, software y servicios; a fin de que supervise y garantice que los entregables, reportes, inventarios y actividades de los proveedores se lleven a cabo conforme lo establecido en los contratos, y esto sirva de apoyo para la aplicación de las deductivas y penalizaciones correspondientes.

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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 1,672,564.18 pesos (un millón seiscientos setenta y dos mil quinientos sesenta y cuatro pesos 18/100 M.N.), por los pagos realizados al amparo del contrato DGRMyS-DGTIC-ADCA-003-2020, celebrado con la empresa Metro Net, S.A.P.I. de C.V. (ahora Sixsigma Networks México, S.A. de C.V.), con vigencia del 1 de abril al 31 de marzo de 2021, para la prestación del Servicio de Centro de Datos SEP 2020, debido a que no se proporcionó la documentación soporte que sustente la cantidad de servicios que fueron considerados en las memorias de cálculo utilizadas para la elaboración de las 3 facturas de los requerimientos de plataforma e infraestructura de las unidades administrativas de la secretaría; adicionalmente, las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales no contienen el detalle de la cantidad y tipo de servicios proporcionados por el proveedor, por lo que no se puede determinar que el monto pagado corresponda a servicios prestados por el mismo, 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; y 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; Art. 13; del Manual Administrativo de Aplicación General en 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; y actividad APRO 3, Factor Crítico 3; del Reglamento Interior de la Secretaría de Educación Pública, Art. 29, Fracc. I, II, VI, VII, X y XII; y del Manual de Organización de la Dirección General de Tecnologías de la Información y Comunicaciones, Funciones 3, 4, 5, 7, 8, y 10 del apartado 7. Descripción de Puestos; del Contrato número DGRMyS-DGTIC-ADCA-003-2020, Cláusulas Décima Quinta. Derechos de Propiedad Intelectual y Décima Séptima. Transferencia de Derechos de Propiedad Intelectual; del Anexo Técnico de los Contrato número DGRMyS-DGTIC-ADCA-003-2020, numerales 2.1. Descripción del Proyecto, 2.3. Requerimientos Técnicos, Secciones Enlace de Comunicación Dedicados, Servicio de Internet, Solución para el Ambiente de Virtualización (AV), incisos a. Capacidad de cómputo en la nube; d. Solución de Gestión de Almacenamiento, y h. Servicio de Respaldos y Restauración de Datos y Bases de Datos de la Solución de Gestión de Almacenamiento, Respaldos y Restauración, Mesa de Servicios, Servicio de Monitoreo de los Servicios del Apartado Fase 2. Aspectos Técnicos del Proyecto.

Causa Raíz Probable de la Irregularidad

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

2021-0-11100-20-0257-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 23,642,450.31 pesos (veintitrés millones seiscientos cuarenta y dos mil cuatrocientos cincuenta pesos 31/100 M.N.), por los pagos realizados al amparo del contrato DGRMyS-DGTIC-ADCA-001-2021, celebrado con la empresa Sixsigma Networks México, S.A. de C.V., con vigencia del 16 de abril al 31 de diciembre de 2021, para la prestación del Servicio de Centro de Datos SEP 2021, debido a que no se proporcionó la documentación soporte que sustente la cantidad de servicios que fueron considerados en las memorias de cálculo utilizadas para la elaboración de las 10 facturas por un monto de 23,570,928.87 pesos, relacionadas con el servicio de soporte WSO2 para los requerimientos de plataforma e infraestructura de las unidades administrativas de la secretaría; ya que las condiciones técnicas y económicas propuestos por el proveedor para la prestación del servicio, difieren con lo ofertado por los fabricantes de las soluciones tecnológicas utilizadas; asimismo, para el servicio mensual de enlaces de internet de julio de 2021 que se prestó por 21 días, se observó que el prorrateo realizado por la SEP no consideró los 31 días del mes al ejecutar el cálculo para el pago, con base en lo cotizado por el proveedor, por lo que se estiman pagos en exceso por 71,521.44 pesos. Adicionalmente, las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales no contienen el detalle de la cantidad y tipo de servicios proporcionados por el proveedor, por lo que no se puede determinar que el monto pagado corresponda a servicios prestados por el mismo, 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; y 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; Art. 13; del Manual Administrativo de Aplicación General en 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; y actividad APRO 3, Factor Crítico 3; del Reglamento Interior de la Secretaría de Educación Pública, Art. 29, Fracc. I, II, VI, VII, X y XII; y del Manual de Organización de la Dirección General de Tecnologías de la Información y Comunicaciones, Funciones 3, 4, 5, 7, 8, y 10 del apartado 7. Descripción de Puestos; del Contrato número DGRMyS-DGTIC-ADCA-001-2021, Cláusulas Décima Quinta. Derechos de Propiedad Intelectual y Décima Séptima. Transferencia de Derechos de Propiedad Intelectual; y del Anexo Técnico de los Contrato número DGRMyS-DGTIC-ADCA-001-2021, numerales 2.1. Descripción del Proyecto, 2.3. Requerimientos Técnicos, Secciones Enlace de Comunicación Dedicados, Servicio de Internet, Solución para el Ambiente de Virtualización (AV), incisos a. Capacidad de cómputo en la nube; d. Solución de Gestión de Almacenamiento, y h. Servicio de Respaldos y Restauración de Datos y Bases de Datos de la Solución de Gestión de Almacenamiento, Respaldos y Restauración, Mesa de Servicios, Servicio de Monitoreo de los Servicios del Apartado Fase 2. Aspectos Técnicos del Proyecto.

Causa Raíz Probable de la Irregularidad

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

4. Ciberseguridad

Se revisó la información proporcionada por la Secretaría de Educación Pública 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 se requiere fortalecer 13 controles, 4 carecen de control y 3 cuentan con un nivel aceptable, como se muestra a continuación:

SEMÁFORO DE MADUREZ DE LOS CONTROLES DE CIBERSEGURIDAD EN LA SECRETARÍA DE EDUCACIÓN PÚBLICA 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 base en la información proporcionada por la SEP.
Indicador: 🟢 Cumplimiento aceptable 🟡 Requiere fortalecer el control 🔴 Carencia de control

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

Inventario y control de activos de *hardware*

- No se cuenta con mecanismos automatizados de gestión de direcciones IP de la infraestructura tecnológica que soporta los servicios de TIC.
- No se tiene un inventario que contemple la totalidad de activos de *hardware* de la secretaría (estén o no conectados a la red).
- 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.

Inventario y control de activos *software*

- La secretaría no cuenta con mecanismos que garanticen la eliminación del *software* no autorizado; tampoco ha definido un procedimiento en donde se especifiquen las acciones a seguir en caso de identificarse este tipo de *software*.

Configuración segura para *hardware* y *software*

- Existen oportunidades de mejora en los mecanismos de gestión de las configuraciones de *hardware* de la secretaría.

Evaluación continua de la vulnerabilidad y solución

- Existen oportunidades de mejora en los mecanismos implementados en la secretaría para la evaluación, ejecución, documentación y seguimiento para la gestión de las vulnerabilidades, así como para la actualización de sistemas operativos.

Uso controlado de privilegios administrativos

- 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 SEP.
- Se identificaron debilidades en la administración de privilegios.

Mantenimiento, monitoreo y análisis de bitácoras de auditoría

- 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 SEP.

Defensa contra *software* malicioso (*malware*)

- No se cuenta con mecanismos de restricción y bloqueo de medios extraíbles que se ejecuten de forma automática, cuando éstos se conectan a los equipos de cómputo o servidores.

Capacidad de recuperación de datos

- No se proporcionó la evidencia que acredite que se cuenta con mecanismos de resguardo, cifrado y control de acceso a los respaldos de información que se gestionan en el centro de datos tercerizado.

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

- Se identificaron áreas de oportunidad relacionadas con los mecanismos utilizados para la gestión de configuraciones en los equipos de red de la SEP.

Seguridad Perimetral

- Se detectaron deficiencias en la seguridad perimetral.

Protección de datos

- Se identificaron áreas de oportunidad en 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 y no se cuenta con un 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 de Ciberseguridad

- Se carece de la definición de un procedimiento de respuesta a incidentes de ciberseguridad, también existen áreas de mejora en los mecanismos utilizados para la gestión de estos incidentes.

- No se realizan pruebas de escenarios de incidentes de seguridad cibernética con los usuarios de la SEP, con la finalidad de validar que la estrategia de respuesta definida por la secretaría es adecuada y suficiente en caso de una contingencia.

Pruebas de penetración y ejercicios de equipo rojo

- Existen oportunidades de mejora en los mecanismos implementados en la secretaría para la evaluación y seguimiento para la gestión de las vulnerabilidades.

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 Educación Pública.

2021-0-11100-20-0257-01-005 **Recomendación**

Para que la Secretaría de Educación Pública 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-006 **Recomendación**

Para que la Secretaría de Educación Pública 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; para que implemente mecanismos con la finalidad de dar seguimiento a la corrección de vulnerabilidades y que defina y formalice procedimientos para la atención y evaluación de incidentes de seguridad que le permitan proteger la integridad, confidencialidad y disponibilidad de la información; para que implemente y realice el seguimiento a los programas de concienciación y entrenamiento en materia de seguridad informática, y para 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-007 **Recomendación**

Para que la Secretaría de Educación Pública 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-008 **Recomendación**

Para que la Secretaría de Educación Pública defina y formalice estándares de seguridad y configuraciones para los sistemas e implemente mecanismos para proteger dichas configuraciones y evitar modificaciones no autorizadas; para 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, para 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

5. Continuidad de las Operaciones

Como parte de los trabajos de auditoría, se verificaron las condiciones que la Secretaría de Educación Pública presenta en la administración de los controles para la continuidad de las operaciones de Tecnologías de la Información y Comunicaciones, vinculados con la infraestructura y soluciones tecnológicas. En el análisis realizado se observó lo siguiente:

- La secretaría no cuenta con un documento formalizado donde se establezcan las áreas y los puestos de los responsables de definir los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC.

- Se carece de un procedimiento para llevar a cabo la actualización del catálogo de servicios de TIC.

- No se cuenta con un análisis de impacto al negocio, ni con 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 existe una metodología para que la SEP realice 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 la 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.

- Se carece de un Plan de Continuidad del Negocio (BCP) en el que se identifiquen las estrategias, procedimientos y actividades a realizar para cada escenario de contingencia en la secretaría.

- No se cuenta con procedimientos, roles y responsabilidades del personal involucrado, 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.

- No se 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 y no se cuenta con un calendario de ejecución de pruebas de recuperación.

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 del 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; III.C. Proceso de Administración de la Operación (AOP), objetivos específicos 1 y 2, 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; de los artículos 42, 47, incisos a, c, d, 48, inciso a; 75, segundo párrafo, y 76, inciso g, 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.

Centro de Datos

Durante el 2021, la Secretaría de Educación Pública contó con el Servicio de centro de datos proporcionado por el proveedor Sixsigma Networks México S.A. de C.V., suscrito con el contrato número DGRMyS-DGTIC-ADCA-001-2021. En el análisis realizado, se observó lo siguiente:

- No se proporcionó la matriz de riesgos del centro de datos, ni los procedimientos utilizados para el control de acceso físico y lógico, así como para la atención de incidentes de ambiente físico.

- No se cuenta con la evidencia para verificar la infraestructura resistente al fuego, salidas de emergencia, alarmas y la señalización de seguridad del centro de datos.

- 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.

- Se carece de documentación que acredite la inspección realizada por la SEP al centro de datos del proveedor, con la finalidad de verificar sus controles implementados (acceso, vigilancia, sistemas de aire acondicionado, de prevención de daños por inundación e incendio, eléctricos, entre otros), así como las políticas y procedimientos definidos por el prestador de servicios.

- 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, ni de la antigüedad y la frecuencia para el cambio de los servidores y mainframes ubicados en el centro de datos, así como del responsable de la custodia de los respaldos.

- En relación con los respaldos de información de la secretaría, no se cuenta con cronogramas y medios de rotación, procedimientos de restauración, almacenamiento de información, manuales de contingencia, de operación de dispositivos para evitar, detectar o corregir los riesgos físicos, matriz de escalamiento de incidentes de ambiente físico y procedimiento de acceso para otorgar, limitar y revocar en caso de emergencia.

- 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.

- No se identificó el procedimiento establecido con el prestador de servicios para efectuar el retiro, transporte y almacenamiento de activos de TIC de forma segura, así como, para ingresar, instalar y configurar un dispositivo en el centro de datos y para ejecutar su mantenimiento.

- La secretaría no cuenta con una política para la clasificación de la información (seguridad nacional, seguridad pública, información reservada y confidencial).

- No se demostró la gestión y seguimiento realizado a los problemas, vulnerabilidades o riesgos materializados en el centro de datos.

- No se entregó evidencia respecto al plan de capacidad implementado para evitar la saturación del uso de los centros de datos, la gestión de bitácoras de monitoreo de los servidores físicos y virtuales, así como de respaldos; tampoco se indicaron los mecanismos de cifrado para los medios de almacenamiento de las bases de datos críticas de la SEP.

Por lo anterior, se concluye que existieron deficiencias en los controles de seguridad física y lógica del Centro de datos, en incumplimiento del 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, y 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.

2021-0-11100-20-0257-01-009 **Recomendación**

Para que la Secretaría de Educación Pública 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; para que verifique la capacidad y rendimientos de la infraestructura tecnológica para determinar si es suficiente para prestar los servicios de Tecnologías de la Información y Comunicaciones con los niveles acordados y para 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-010 **Recomendación**

Para que la Secretaría de Educación Pública 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); para 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; para 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, para 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 de las operaciones de la Secretaría de Educación Pública; finalmente, para 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-011 **Recomendación**

Para que la Secretaría de Educación Pública 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

2021-0-11100-20-0257-01-012 **Recomendación**

Para que la Secretaría de Educación Pública implemente controles y mecanismos en los centro de datos de la secretaría para contar con cifrado en los medios de almacenamiento, para que defina el listado de los operadores responsables de su resguardo y mantenimiento; para 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 Virtual de Presentación de Resultados Finales y Observaciones Preliminares derivada de los procesos de fiscalización superior por medios electrónicos en los términos de los artículos 17 Bis, 17 Ter y 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, así como los numerales 1.1.3, fracción XXIII, 2.2.9, 2.3.5, fracción VI, y 2.3.9, fracción II de las Reglas de Carácter General Aplicables a los Procesos de Fiscalización Superior por Medios Electrónicos.

Montos por Aclarar

Se determinaron 25,315,014.49 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 5 resultados, de los cuales, en uno no se detectó irregularidad y los 4 restantes generaron:

12 Recomendaciones y 2 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 31 de enero de 2023, 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 Educación Pública cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En la revisión de los contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021, cuyo objeto fue proporcionar el Servicio de Centro de Datos, celebrado con Metro Net, S.A.P.I. de C.V. (ahora Sixsigma Networks México, S.A. de C.V.), se determinó lo siguiente:
  - Se estima un probable daño o perjuicio por 25,315.0 miles de pesos debido a que las actas de entrega-recepción y los oficios de notificación de aceptación de los servicios mensuales no sustentan la cantidad y tipo de servicios prestados por el proveedor, por lo tanto, no se cuenta con la evidencia que acredite el número de

servicios considerados en las memorias de cálculo, utilizadas para la elaboración de las facturas y los pagos realizados.

- Se identificaron deficiencias en la administración y operación de los 20 controles de Ciberseguridad para la infraestructura de hardware y software de la secretaría, toda vez que se requiere fortalecer 13 controles, 4 carecen de control y 3 cuentan con un nivel aceptable; lo anterior podría afectar la integridad, disponibilidad y confidencialidad de la información, poniendo en riesgo la operación de la SEP.
- 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.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtra. 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 estén de conformidad con las disposiciones y normativas aplicables; analizar la integración del gasto ejercido en materia de TIC en los Capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprenda el análisis de las contrataciones vigentes; la determinación de la procedencia de su renovación; la pertinencia de realizar contrataciones consolidadas y; los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

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

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que 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, plan de recuperación de desastres, estándares).

Áreas Revisadas

La Unidad de Administración y Finanzas, la Dirección General de Presupuesto y Recursos Financieros, la Dirección General de Recursos Materiales y Servicios, la Dirección General de Tecnologías de la Información y Comunicaciones, la Dirección General Adjunta de Operaciones de Tecnologías de la Información y Comunicaciones, la Dirección de Seguridad Informática y Prevención de Riesgos, y la Dirección de Administración de Procesamiento y Almacenamiento, todas adscritas a la Secretaría de Educación Pública.

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; 11, fracción II; Art. 13, Frac. I; Art. 23; Art. 27, Frac. II; 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, inciso a, c y d; Art. 75, segundo párrafo; Art. 76, incisos c, d, e y f; Art. 76, inciso g; Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la 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; III.C. Proceso de Administración de la Operación (AOP), objetivos específicos 1 y 2; actividad AOP 3, factor crítico 3; actividad AOP 4; 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); .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; del Reglamento Interior de la Secretaría de Educación Pública, Art. 29, Fracc. I, II, VI, VII, X y XII; Manual de Organización General de la Dirección General de Tecnologías de Información y Comunicaciones, Objetivo general del puesto,

funciones 1, 3, 4, 5, 6, 7, 8, 9 y 10, del apartado 7.Descripción de Puestos de la Dirección de Seguridad Informática y Prevención de Riesgos; Manual de Organización General de la Secretaría de Educación Pública, Misión y función 10 del numeral 1.5.4; Contrato número DGRMyS-DGTIC-LPN-001-2020, Cláusulas Primera, Sexta, Décima segunda; Anexo de Ejecución del contrato número DGRMyS-DGTIC-LPN-001-2020, Partidas 1, 2, numerales 2.1, 2.2, 2.3, 2.4, 2.5; 3, 4, 5, 6, 7 y 8, numerales 2.2.1, 2.3.2, 2.5, 2.5.2, 2.6; Anexo Técnico de los Contratos números DGRMyS-DGTIC-ADCA-003-2020 y DGRMyS-DGTIC-ADCA-001-2021, numeral 2.1. Descripción del Proyecto, inciso a. Capacidad de cómputo en la nube, del Apartado Fase 2. Aspectos Técnicos del Proyecto; del Contrato número DGRMyS-DGTIC-ADCA-003-2020, Cláusulas Décima Quinta. Derechos de Propiedad Intelectual y Décima Séptima. Transferencia de Derechos de Propiedad Intelectual; del Anexo Técnico de los Contrato número DGRMyS-DGTIC-ADCA-003-2020, numerales 2.1. Descripción del Proyecto, 2.3. Requerimientos Técnicos, Secciones Enlace de Comunicación Dedicados, Servicio de Internet, Solución para el Ambiente de Virtualización (AV), inciso a. Capacidad de cómputo en la nube; incisos d. Solución de Gestión de Almacenamiento, h. Servicio de Respaldos y Restauración de Datos y Bases de Datos de la Solución de Gestión de Almacenamiento, Respaldos y Restauración, Mesa de Servicios, Servicio de Monitoreo de los Servicios del Apartado Fase 2. Aspectos Técnicos del Proyecto; del Contrato número DGRMyS-DGTIC-ADCA-001-2021, Cláusulas Décima Quinta. Derechos de Propiedad Intelectual y Décima Séptima. Transferencia de Derechos de Propiedad Intelectual; del Anexo Técnico de los Contrato número DGRMyS-DGTIC-ADCA-001-2021, numerales 2.1. Descripción del Proyecto, 2.3. Requerimientos Técnicos, Secciones Enlace de Comunicación Dedicados, Servicio de Internet, Solución para el Ambiente de Virtualización (AV), inciso a. Capacidad de cómputo en la nube; incisos d. Solución de Gestión de Almacenamiento, h. Servicio de Respaldos y Restauración de Datos y Bases de Datos de la Solución de Gestión de Almacenamiento, Respaldos y Restauración, Mesa de Servicios, Servicio de Monitoreo de los Servicios del Apartado Fase 2. Aspectos Técnicos del Proyecto;

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.