Secretaría de Seguridad y Protección Ciudadana

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-0-36100-20-0089-2021

89-GB

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 2020 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	390,020.5
Muestra Auditada	194,817.3
Representatividad de la Muestra	50.0%

El universo seleccionado por 390,020.5 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal 2020; la muestra auditada está integrada por cinco contratos para prestar los servicios administrados del sistema automatizado de identificación de huellas dactilares, el procesamiento y almacenamiento para sistemas administrativos, así como el licenciamiento para el sistema de identificación biométrica automatizada, con pagos ejercidos por 194,817.3 miles de pesos, que representan el 49.9% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de las TIC en la Secretaría de Seguridad y Protección Ciudadana (SSPC) en 2020, relacionada con la Ciberseguridad, Continuidad de las Operaciones y Centro de Datos.

Antecedentes

En la fiscalización de la Cuenta Pública 2016, se practicó la auditoría número 12-GB "Auditoría de TIC" a la entonces Dirección General de Plataforma México, adscrita en aquel tiempo a la Secretaría de Gobernación. Se identificó en el desarrollo de soluciones tecnológicas que no se tenían implementados ambientes de desarrollo ni calidad para realizar pruebas con datos controlados a las actualizaciones del código de los sistemas; asimismo, se encontraron deficiencias en los controles para asegurar que los entregables fueron recibidos con la calidad requerida en los contratos de prestación de servicios.

El 30 de abril de 2019 se publicó en el Diario Oficial de la Federación el Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana, en el que se determina que ésta secretaría tiene a su cargo el ejercicio de las atribuciones en materia de seguridad pública y nacional, así como de protección civil y las que le asignen las leyes, reglamentos, decretos, acuerdos y órdenes del Presidente de los Estados Unidos Mexicanos; para tal efecto, el artículo tercero transitorio establece que a las unidades administrativas creadas conforme al citado Reglamento Interior, se les transferirán los recursos humanos, materiales, técnicos y financieros, para el desempeño adecuado de sus atribuciones, en los términos y condiciones que establezca la Unidad de Administración y Finanzas de la Secretaría de Seguridad y Protección Ciudadana, en coordinación con su homóloga de la Secretaría de Gobernación.

El 27 de mayo de 2019 se publicó en el Diario Oficial de la Federación la expedición de la Ley de la Guardia Nacional, instrumento normativo con el que se crea la Guardia Nacional como un Órgano Administrativo Desconcentrado adscrito a la Secretaría de Seguridad y Protección Ciudadana, dicha creación está basada en la transferencia de los recursos humanos, materiales y financieros correspondientes a las Divisiones y Unidades Administrativas provenientes de la Policía Federal, conforme a lo establecido en los transitorios de la ley en comento.

El 31 de mayo de 2019, se publicó en el Diario Oficial de la Federación el Reglamento Interior de la Secretaría de Gobernación en el que establece en su artículo Tercero Transitorio que se dará continuidad con la transferencia de los recursos humanos, materiales, técnicos y financieros a la Secretaría de Seguridad y Protección Ciudadana, en los términos y condiciones que establezcan las actas de transferencia que, para tal efecto, suscriban las unidades de Administración y Finanzas de las Secretarías de Gobernación, y de Seguridad y Protección Ciudadana.

Entre 2019 y 2020, se han erogado más de 701,443.6 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC – SSPC

(Miles de pesos)

Periodo del Gasto	2019	2020	Total
Monto por año	166,973.3	534,470.3	701,443.6

FUENTE: Elaborada con información proporcionada por la SSPC.

Con base 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 función de las TIC sujetas de revisión, así como determinar el alcance, naturaleza y muestra de la revisión, 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 2020, publicado en el Diario Oficial de la Federación el 11 de diciembre de 2019, se autorizó al Ramo Seguridad y Protección Ciudadana (36) un presupuesto de 60,150,695.9 miles de pesos, del cual se asignó a la Secretaría de Seguridad y Protección Ciudadana un presupuesto original de 1,378,031.6 miles de pesos.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2020, se concluyó que la SSPC (Sector Central) tuvo un presupuesto ejercido de 1,376,487.6 miles de pesos, de los cuales, 534,470.3 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 38.8% del presupuesto, como se muestra a continuación:

RECURSOS EJERCIDOS EN LA SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA (SECTOR CENTRAL) DURANTE 2020

(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recursos ejercidos en TIC
1000	Servicios personales	795,096.7	144,243.3
2000	Materiales y suministros	2,228.0	0.0
3000	Servicios generales	579,162.9	390,227.0
4000	Transferencias, asignaciones, subsidios y otras ayudas	0.0	0.0
	TOTAL	**1,376,487.6**	**534,470.3**

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

Los recursos ejercidos en materia de las TIC por 534,470.3 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2020 EN LA SSPC (SECTOR CENTRAL)
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**144,243.3**
3000		**SERVICIOS GENERALES**	**390,227.0**
	31401	Servicio telefónico convencional	375.8
	31602	Servicios de telecomunicaciones	115,983.3
	31701	Servicios de conducción de señales analógicas y digitales	38,413.6
	31904	Servicios integrales de infraestructura de cómputo	109,363.3
	32701	Patentes, derechos de autor, regalías y otros	48,672.7
	33301	Servicios de desarrollo de aplicaciones informáticas	990.7
	33304	Servicios de mantenimiento de aplicaciones informáticas	71,999.8
	33602	Otros servicios comerciales	4,427.8
		TOTAL	**534,470.3**

FUENTE: Elaborado con información proporcionada por la SSPC.

Las partidas específicas relacionadas con “Servicios Personales” (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 144,243.3 miles de pesos durante el ejercicio fiscal de 2020; considerando 638 plazas, el promedio anual percibido por persona fue de 226.1 miles de pesos.

Del universo seleccionado por 390,020.5 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC en 2020, se erogaron 194,817.3 miles de pesos en cinco contratos que representan el 49.9% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS EJERCIDOS DURANTE 2020

(Miles de pesos)

Procedimiento de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		
				Del	Al	Mínimo	Máximo	Ejercido
Adjudicación directa	SSPC/DGRMSOP/CT/12/2020 y convenio modificatorio	Idemia Identity & Security France, S.A.S	Servicio Administrado del Sistema Automatizado de Identificación de Huellas Dactilares (AFIS)	21/05/2020	31/12/2020	0.0	71,999.8	71,999.8
Adjudicación directa	SSPC/DGRMSOP/CT/22/2020, SSPC/DGRMSOP/CV/14/2020, SSPC/DGRMSOP/CV/05/2021 con 2 convenios modificatorios	Axtel, S.A.B. DE C.V.	Servicio de procesamiento y almacenamiento para sistemas administrativos	01/10/2020	27/07/2021	81,571.2	130,513.9	74,199.6
Adjudicación directa	SSPC/DGRMSOP/CT/33/2020	Biometría Aplicada, S.A de C.V.	Licenciamiento para el Sistema de Identificación Biométrica Automatizada ABIS-SSPC	01/12/2020	31/12/2020	0.0	48,617.9	48,617.9
Totales						**81,571.2**	**251,131.6**	**194,817.3**

FUENTE: Elaborado con información proporcionada por la SSPC.

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

2. Contrato número SSPC/DGRMSOP/CT/12/2020 “Servicio Administrado del Sistema Automatizado de Identificación de Huellas Dactilares (AFIS)”

Se analizó la información del contrato número SSPC/DGRMSOP/CT/12/2020 suscrito con el proveedor Idemia Identity & Security France, S.A.S., mediante el procedimiento de adjudicación directa, de conformidad con lo dispuesto en el artículo 134, de la Constitución Política de los Estados Unidos Mexicanos; 26, fracción III, 40, y 41, fracción I, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 71, 72, fracción II, de su Reglamento, vigente del 21 de mayo al 20 de noviembre de 2020, por un monto total de 59,999.8 miles de pesos, para prestar el “Servicio Administrado del Sistema Automatizado de Identificación de Huellas Dactilares (AFIS)”; el 20 de octubre de 2020 se suscribió el convenio modificatorio número SSCP/DGRMSOP/CV/01/2020, mediante el cual se amplió la vigencia del contrato al 31 de diciembre 2020 y el monto total en 20.0% y quedar en 71,999.8 miles de pesos, los cuales fueron erogados en su totalidad durante el ejercicio de 2020, y se determinó lo siguiente:

Antecedentes

El 30 de abril de 2018 la Secretaría de Gobernación (SEGOB) y la empresa Idemia Identity & Security France, S.A.S., suscribieron el contrato número SG/CPS/66/2018, y el 31 de diciembre de 2018 celebraron su convenio modificatorio número SG/CVS/01/2019, bajo el procedimiento de adjudicación directa, con vigencia del 1º de mayo de 2018 al 18 de febrero 2019, por un monto de 91,800.0 miles de pesos, con el objeto de prestar el "Servicio Administrado del Sistema Automatizado de Identificación de Huellas Dactilares (AFIS)", como administrador del contrato participó la Dirección de Monitoreo de Aplicaciones y Servicios de Telecomunicaciones de la Dirección General Plataforma México adscrita en aquel entonces a la SEGOB.

El 11 de julio 2019 se suscribió el Convenio Específico de Transferencia de Recursos Humanos, Materiales, Tecnológicos y Financieros entre la Secretaría de Gobernación (SEGOB) y la Secretaría de Seguridad y Protección Ciudadana (SSPC), con el objeto de formalizar la transferencia de Recursos Humanos, Materiales, Tecnológicos y Financieros de la SEGOB a la SSPC que se integraban al Sector Seguridad y sus Órganos Administrativos Desconcentrados, para dar cumplimiento a lo dispuesto en el Sexto Transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 30 de noviembre de 2018. Debido a lo anterior, sería responsabilidad de la SSPC contar con la infraestructura y/o contratos necesarios para la migración de los servicios, para su posterior operación y administración a partir del 1º de enero de 2020.

Alcance del servicio

Contar con la herramienta informática denominada "MetaMorpho", que se utiliza actualmente en la red nacional de Plataforma México, para la captura y consulta biométrica de registros de huellas dactilares, palmares de control y fragmentos de huellas latentes y con la infraestructura y mantenimiento de las terminales remotas, propiedad de la Secretaría. El sistema automatizado de identificación de huellas dactilares (AFIS) es un servicio de información crítico que se brinda a diferentes dependencias federales, estatales y municipales de seguridad pública del país, al mes de mayo de 2020 contaba con 2,900 usuarios y 390 terminales remotas conectadas en todo el país.

Los componentes del servicio son el almacenamiento, procesamiento y soporte técnico especializado para los registros de decadactilares, palmares y latentes, la ejecución de los cotejos concurrentes de los servicios, así como asegurar la operación de la red nacional mediante las terminales remotas, consultas rápidas y sistema de información criminal, incluyendo la reparación de los equipos con el suministro de refacciones.

Proceso de contratación

- La secretaría indicó que la empresa Idemia Identity & Security France S.A.S., era el único proveedor para dar el servicio, no obstante, existen más proveedores especializados según consta en sus sitios de internet como NEC, 3M y Neurotechnology, entre otros.
- No se cuenta con la documentación para verificar que se revisó la existencia de proveedores en el ámbito nacional o internacional con posibilidad de cumplir con las necesidades de la contratación.

- El grupo auditor realizó un comparativo con la propuesta económica remitida por la SEGOB relativa al contrato número SG/CPS/66/2018, el cual tiene el mismo proveedor, objeto y servicios que el contrato número SSPC/DGRMSOP/CT/12/2020 suscrito por la SSPC y se identificó que para el servicio "Soporte Técnico de Terminales Remotas de Consulta y/o Captura" se ofertó un precio mensual más alto por 436.6 miles de pesos; cabe señalar que el contrato de la SSPC consideró el soporte técnico sólo para 43 estaciones con un monto mensual de 799.9 miles de pesos, siendo que los equipos operativos en el contrato de la SEGOB fueron 121 con un monto mensual de 363.3 miles de pesos, esto es, la SSPC contempló 78 terminales (64.5%) menos que SEGOB.

- Es preciso señalar que para la prestación del servicio administrado a la SSPC se hizo uso de la misma infraestructura que utilizó la SEGOB, es decir, pese a que los equipos fueron diseñados tecnológicamente desde el año 2010, el proveedor no renovó las estaciones de trabajo, las cuales tienen riesgo de fallas o interrupciones por obsolescencia, no obstante, el incremento del proveedor en el precio del soporte técnico de las estaciones fue del 120.0%, mientras que la inflación acumulada de marzo de 2018 a marzo de 2020 (periodo en el que se presentaron los servicios) fue del 7.38% de acuerdo con el índice nacional de precios al consumidor del INEGI.

- Del incremento mencionado en el punto anterior, la secretaría argumentó que se trata de un servicio integral, por lo que no debe verse al soporte técnico de las estaciones por separado, sin embargo, la documentación contractual tiene segregados los precios del servicio al sitio central y a las estaciones de trabajo; asimismo, se informó que para el contrato del ejercicio 2021, se eliminó el concepto de "Soporte técnico a estaciones de consulta y/o captura", obteniendo una economía, sin dar a conocer la razón de no aplicar este ahorro desde el contrato del ejercicio 2020.

- Por lo anterior, se efectuaron pagos por 3,143.7 miles de pesos conformados por ocho pagos del "Soporte Técnico de Terminales Remotas de Consulta y/o Captura" del contrato número SSPC/DGRMSOP/CT/12/2020, los cuales tuvieron un precio más alto que la contratación precedente con el mismo objeto, proveedor, servicios y equipos a la cual se le dio continuidad operativa, aun cuando los servicios se

prestaron con 78 equipos menos (una disminución del 64.5% respecto al contrato previo), los cuales estaban obsoletos sin renovación tecnológica.

Lo anterior incumplió los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 1º, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 24, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el Macroproceso 4.2, de Contrataciones, numeral 4.2.1.1.10, "Realizar investigación de mercado" contenido en el Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público publicado en el Diario Oficial de la Federación el 9 de agosto de 2010, última reforma publicada el 03 de febrero de 2016.

Análisis de proveedores

En relación con las declaraciones anuales del proveedor proporcionadas por el Servicio de Administración Tributaria (SAT), se identificaron los ingresos siguientes: Ejercicio de 2018 por 197,227.8 miles de pesos, Ejercicio de 2019 por 153,245.9 miles de pesos y Ejercicio de 2020 por 212,899.4 miles de pesos. El proveedor se encuentra registrado en el SAT bajo el régimen de Sociedad por Acciones Simplificadas, por lo tanto, al tomar en cuenta sus ingresos, incumple con lo establecido en el artículo 260, de la Ley General de Sociedades Mercantiles, el cual establece que los ingresos totales anuales de este tipo de sociedades no podrán ser mayores a la suma aproximada de 5 millones de pesos. Lo anterior, dará lugar a la Promoción del Ejercicio de la Facultad de Comprobación Fiscal ante el SAT para su investigación y desahogo.

Revisión técnica, funcional y administrativa

Se analizó la documentación técnica (anexo técnico, entregables, solicitudes de servicio, reportes de fallas e incidentes, entre otros) proporcionada por la SSPC, así como la información relacionada con el contrato anterior de la SEGOB, y se identificó lo siguiente:

Entregables del Servicio

Se identificó que los entregables denominados "Plan de Preparación del sitio", "Especificaciones Funcionales y Técnicas", "Soporte y Gestión del Proyecto", "Procedimiento de Escalamiento", "Reportes de Disponibilidad del Servicio", "Reportes de las Fallas en la Funcionalidad del Servicio" y "Reporte de Incidentes", no tienen definida una fecha acordada para su entrega.

Servicio de Almacenamiento, Procesamiento y Soporte Técnico Especializado del Sitio Central

- De un universo de 147 servidores, el grupo auditor revisó 75 (51.0%) distribuidos en nueve módulos que forman parte de la infraestructura del servicio, de los cuales, no fue proporcionada la evidencia del mantenimiento preventivo.

- No fue posible validar las funcionalidades del Sistema de Información Criminal (CCH), debido a que se encuentra fuera de operación por una falla eléctrica que ocasionó que el equipo ya no prendiera por la afectación de diversos componentes, inclusive se encuentra fuera de la cobertura de soporte desde diciembre de 2017.

- Se identificó que el servicio opera con componentes e infraestructura obsoletos diseñados desde el año 2010, lo que podría afectar la integridad y disponibilidad de la información relacionada con la captura y consulta biométrica del Sistema Automatizado de Identificación de Huellas Dactilares.

Niveles de servicio

De un universo de 77 tickets, el grupo auditor revisó el 100.0% registrados de mayo a noviembre de 2020, e identificó tres tickets (3.9%) repetidos.

Por lo anterior, se concluye que existe el riesgo de interrupción de la infraestructura que podría afectar la continuidad operativa de la Plataforma México, para prestar sus servicios a los tres niveles de gobierno en las actividades de seguridad pública del país, debido a la obsolescencia de los equipos por la falta de actualización de sus componentes, sin el debido soporte y mantenimiento para atender las incidencias; asimismo, se efectuaron pagos por 3,143.7 miles de pesos del servicio “Soporte Técnico de Terminales Remotas de Consulta y/o Captura”, los cuales tuvieron un precio más caro que la contratación precedente que tenía el mismo objeto, proveedor, servicios e infraestructura, aun cuando los nuevos servicios se prestaron con un 64.5% menos equipos respecto al contrato previo con tecnología obsoleta sin renovación tecnológica, a pesar de que las terminales fueron diseñadas con tecnología del año 2010.

2020-0-36100-20-0089-01-001 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana implemente los programas y procedimientos para la evaluación y renovación de la infraestructura tecnológica que soporta la operación del Sistema Automatizado de Identificación de Huellas Dactilares; asimismo asegure el desempeño de la infraestructura tecnológica que soporta los sistemas de la Plataforma México, a fin de mitigar los efectos de la obsolescencia tecnológica que podría provocar fallas que afectan la disponibilidad, integridad, procesamiento y continuidad de los servicios que se prestan a diversos entes públicos federales, estatales y municipales para la seguridad pública del país.

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.

2020-5-06E00-20-0089-05-001 **Promoción del Ejercicio de la Facultad de Comprobación Fiscal**

Para que el Servicio de Administración Tributaria instruya a quien corresponda con el propósito de que audite a Idemia Identity & Security France, S.A.S. (Registro Federal de Contribuyentes MOR080729JZ9 y domicilio fiscal en Avenida Ejército Nacional número 350, Piso 4, Colonia Polanco, V Sección, Demarcación Territorial Miguel Hidalgo, Código Postal 11560, Ciudad de México), con la finalidad de constatar el cumplimiento de sus obligaciones fiscales, debido a que en sus declaraciones anuales se identificaron los ingresos siguientes: ejercicio 2018 por 197,227.8 miles de pesos, ejercicio 2019, por 153,245.9 miles de pesos, y ejercicio 2020, por 212,899.4 miles de pesos, y la empresa se encuentra registrada bajo el régimen de Sociedad por Acciones Simplificadas, que establece que los ingresos totales anuales de este tipo de sociedades no podrán ser mayores a la suma aproximada de 5 millones de pesos (5,000.0 miles de pesos), en incumplimiento del artículo 260 de la Ley General de Sociedades Mercantiles,, a fin de constatar el cumplimiento de sus obligaciones fiscales.

2020-0-36100-20-0089-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 3,143,684.70 pesos (tres millones ciento cuarenta y tres mil seiscientos ochenta y cuatro pesos 70/100 M.N.), por los pagos del servicio denominado "Soporte Técnico de Terminales Remotas de Consulta y/o Captura" del contrato número SSPC/DGRMSOP/CT/12/2020, los cuales tuvieron un precio más elevado que el contrato precedente número SG/CPS/66/2018 de la Secretaría de Gobernación, el cual tenía el mismo objeto, proveedor, servicios e infraestructura a la cual se le dio continuidad operativa, sin embargo, el precio fue más alto aun cuando los servicios se prestaron con 78 terminales menos (64.5% menos respecto al contrato previo), aunado a que los equipos estaban obsoletos sin renovación tecnológica a pesar de que fueron diseñados con tecnología del año 2010, más los rendimientos financieros generados desde la fecha de su pago hasta la de su total recuperación; en incumplimiento de la Constitución Política de los Estados Unidos Mexicanos, artículo 134; de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 24; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III y del Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público publicado en el Diario Oficial de la Federación el 9 de agosto de 2010, última reforma publicada el 03 de febrero de 2016, Macroproceso 4.2 Contratación, numeral 4.2.1.1.10 "Realizar investigación de mercado".

Causa Raíz Probable de la Irregularidad

Falta de monitoreo, supervisión y control en las investigaciones de mercado y contratación de los servicios.

3. Contrato número SSPC/DGRMSOP/CT/22/2020 "Servicio de Procesamiento y Almacenamiento para Sistemas Administrativos (Centro de Datos)"

Se analizó la información del contrato abierto número SSPC/DGRMSOP/CT/22/2020 suscrito con la empresa Axtel, S.A.B. de C.V., mediante adjudicación directa en términos de lo previsto en los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 26, fracción III, 28, fracción I, 40 y 41, fracción V, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 71 y 72, fracción V, de su Reglamento, con vigencia del 1º de octubre al 31 de diciembre de 2020, por un monto mínimo de 67,976.0 miles de pesos y un monto máximo de 108,761.6 miles de pesos, con el objeto del "Servicio de Procesamiento y Almacenamiento, para Sistemas Administrativos (Centro de Datos)"; mediante el convenio modificatorio número SSPC/DGRMSOP/CV/14/2020, se nombró un nuevo administrador del contrato y se amplió el plazo al 31 de marzo de 2021, posteriormente con el convenio modificatorio número SSPC/DGRMSOP/CV/05/2021, se amplió el monto mínimo a 81,571.2 miles de pesos y el monto máximo a 130,513.9 miles de pesos, así como el plazo del contrato al 27 de julio de 2021; los pagos ejercidos durante el ejercicio de 2020 fueron por 74,199.6 miles de pesos, y se determinó lo siguiente:

Alcance del servicio

Los servicios consisten en un centro de datos externo para el almacenamiento y procesamiento de los sistemas informáticos, con un enfoque de servicios integrados bajo demanda con los más altos estándares de seguridad, continuidad y disponibilidad, así como la migración, configuración y puesta a punto del servicio, el cual debe considerar los conceptos siguientes: Continuidad y Migración del Servicio; Servicio de Procesamiento RISC; Servicio de Procesamiento X86; Servicio de Hipervisor; Servicio de Almacenamiento en Disco; Servicio de Respaldo; Servicio de Administración de Base de Datos; Administración de Sistemas Operativos; Servicio de Operación de Cómputo; Mesa de Servicio; Servicio de Centro de Dato, y el Licenciamiento y Servicio de Seguridad.

Antecedentes

- El 13 de marzo de 2019, la Secretaría de Gobernación (SEGOB) y la empresa Axtel, S.A.B. de C.V., celebraron el contrato abierto número SG/CPS/06/2019 con vigencia del 29 de febrero de 2019 al 29 de febrero de 2020 y su convenio modificatorio número SG/CVS/05/2020 suscrito el 31 de diciembre de 2019 con vigencia al 29 de febrero de 2020, por un monto mínimo de 103,800.0 miles de pesos y un monto máximo de 180,599.4 miles de pesos, con el objeto de prestar el "Servicio de Cómputo Sobre Demanda 2019". Es importante mencionar que en esa fecha la SEGOB

se encontraba a cargo de los recursos humanos, materiales, tecnológicos y financieros de las unidades administrativas que después formaron parte de la Secretaría de Seguridad y Protección Ciudadana (SSPC), cabe señalar que el contrato mencionado incluía la infraestructura y soluciones tecnológicas que se prestaban a dichas unidades de la SSPC, para la operación de aplicativos como la nómina, sistema del centro nacional de prevención de desastres, sistema de recepción de llamadas (911), sistema de protección civil, sistema de control de gestión, sistema de búsqueda y reasignación de bienes, entre otros.

- El 11 de julio de 2019, se celebró el "Convenio Específico de Trasferencia de Recursos Humanos, Materiales, Tecnológicos y Financieros" que suscribieron la SEGOB y la SSPC, con el objeto de formalizar la trasferencia de recursos humanos, materiales, tecnológicos y financieros de la SEGOB a la SSPC, que integran al sector de seguridad y sus órganos administrativos desconcentrados, para dar cumplimiento al artículo Sexto Transitorio del decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, publicada en el Diario Oficial de la Federación el 30 de noviembre de 2018.

  De lo antes citado, fue establecido en la cláusula séptima del convenio "De los recursos tecnológicos", que la Secretaría de Gobernación mediante la Dirección General de Tecnologías y Comunicaciones prestará hasta el 31 de diciembre de 2019, los servicios de equipos de cómputo, servidores, sistemas de almacenamiento central, equipos de telecomunicaciones, licencias de software, así como asesoría técnica a las unidades administrativas del sector central de la SSPC.

- El 9 de octubre del 2019, se formalizó el acta de entrega/recepción de tecnologías de la información y comunicaciones consistente en la entrega de diversos sistemas, aplicativos y bases de datos sustantivas y administrativas de SEGOB a la SSPC, a fin de que esta última pueda llevar a cabo la operación de los servicios y a partir de la cual se responsabiliza por el uso y funcionamiento de los sistemas descritos en dicha acta.

  Asimismo, en común acuerdo con la Secretaría de Gobernación, los servicios descritos en el acta mencionada se encontrarían hospedados en el centro de datos de la SEGOB hasta la conclusión de la vigencia de su contrato y su convenio modificatorio (29 de febrero de 2020), periodo en el cual la SSPC debería realizar los trámites administrativos y financieros pertinentes para asegurar la continuidad de sus operaciones en materia de sistemas.

Proceso de contratación

- El 27 de enero de 2020, la SSPC envió las solicitudes de cotización a las empresas que dieron respuesta el 4 de febrero de 2020, con las cuales se realizó la investigación de mercado determinando que la empresa Axtel, S.A.B. de C.V., ofertó la cotización más

económica por un periodo de 10 meses con un monto mensual de 11,506.9 miles de pesos, asimismo, se contaba con el estudio de factibilidad de fecha 27 de febrero 2020, el cual había sido aprobado por la Coordinación de Estrategia Digital Nacional de Presidencia de la Republica para realizar la contratación; no obstante lo anterior, no se llevó a cabo la adjudicación porque la SSPC manifestó que no contó con la autorización presupuestal y administrativa para su realización.

- El 11 de marzo de 2020, el Director General Recursos Materiales, Servicios y Obra Pública suscribió el oficio número SSPC/UAF/DGRMSOP/00902/2020, por el cual solicitó al Director General de Programación y Presupuesto emitir la suficiencia presupuestaria para la contratación del "Servicio de Procesamiento y Almacenamiento para Sistemas Administrativos (Centro de Datos)" de la SSPC.

- El 26 de marzo de 2020, el Director General de Programación y Presupuesto suscribió el oficio número SSPC/UAF/DGPPR/00638/2020, donde informó que fueron autorizadas las solicitudes de adecuación presupuestal y las suficiencias presupuestarias a través del módulo de adecuaciones presupuestarias de la Secretaría de Hacienda y Crédito Público, de tal manera que se contaba con los recursos económicos suficientes para la celebración del contrato de la SSPC.

- El 27 de mayo de 2020, se suscribió el contrato número SG/CPS/24/2020 entre la SEGOB y Axtel, S.A.B. de C.V., con vigencia del 13 de mayo al 31 de diciembre de 2020, por un monto mínimo de 66,339.9 miles de pesos y monto máximo de 165,849.8 miles de pesos, para prestar el "Servicio de Cómputo sobre Demanda". Como resultado de la revisión al alcance de la infraestructura y soluciones tecnológicas, el grupo auditor identificó que se mantuvo el soporte a los mismos sistemas críticos de la SSPC que estaban incluidos en el contrato abierto número SG/CPS/06/2019, suscrito el 13 de marzo de 2019 entre la SEGOB y la empresa Axtel, S.A.B. de C.V.

- El 4 de septiembre de 2020, la SSPC envió una segunda petición de ofertas a las mismas empresas que participaron en la primera investigación de mercado, las que respondieron el 9 de septiembre de 2020, donde sólo la empresa Axtel, S.A.B. de C.V., manifestó su disposición para prestar el servicio con una propuesta por un monto mensual de 30,762.0 miles de pesos, las demás empresas informaron que no se encontraban en posibilidad para cumplir con los tiempos establecidos para el periodo de octubre a diciembre de 2020.

- El 30 de marzo de 2021, se suscribió el convenio modificatorio número SSPC/DGRMSOP/CV05/2021 entre la SSPC y Axtel, S.A.B. de C.V., con vigencia al 27 de julio de 2021 por un monto mensual de 8,166.5 miles de pesos (no incluye la migración de los servicios), del cual el grupo auditor identificó una reducción de precios del orden del 50.3%, los cuales son similares a la primera propuesta presentada por Axtel, S.A.B. de C.V., el 4 de febrero de 2020.

Revisión de la contratación

Como resultado de la revisión del proceso de contratación se identificó lo siguiente:

- El grupo auditor realizó un comparativo de los precios y servicios ofrecidos por Axtel, S.A.B. de C.V., entre las dos propuestas que presentó durante la investigación de mercado, las cuales tienen la misma cantidad de equipos y servicios, no obstante, se identificó un incremento de 19,255.1 miles de pesos mensuales (167.3%), entre la primera propuesta presentada en febrero de 2020 por un monto de 11,506.9 miles de pesos, y la segunda entregada en septiembre del mismo año por un monto de 30,762.0 miles de pesos.

- En respuesta a la notificación del incremento de precios por parte del grupo auditor, la SSPC argumentó que el periodo de tiempo con el cual fueron estimados los precios de las propuestas no es el mismo y por esa razón los precios son muy distintos, además, manifestó que no contaba con la autorización presupuestal y administrativa para la contratación del servicio en el mes de febrero de 2020, por lo que tuvo la necesidad de acotar el periodo de contratación del servicio a tres meses.

- Asimismo, el grupo auditor revisó los entregables de mayo a diciembre de 2020 del contrato número SG/CPS/24/2020 suscrito entre la SEGOB y Axtel, S.A.B. de C.V., los cuales fueron comparados con la memoria técnica del contrato número SSPC/DGRMSOP/CT/22/2020 celebrado por la SSPC. Como resultado se identificó infraestructura de cómputo de servidores que prestan servicio a la SSPC en el contrato suscrito por la SEGOB, los cuales permitieron la operación de aplicativos como la nómina, sistema del centro nacional de prevención de desastres, sistema de recepción de llamadas (911), sistema de protección civil, sistema de control de gestión, sistema de búsqueda y reasignación de bienes, entre otros, por lo tanto, se tienen evidencias de trabajos realizados mediante el contrato pagado por la SEGOB que fueron prestados a la SSPC en el periodo de mayo a septiembre de 2020, dichos servicios también fueron pagados por la SEGOB y proporcionados a la SSPC hasta el mes de diciembre de 2020, por otra parte, se detectaron actividades relativas a la migración de servicios de nómina cuando la SSPC no tenía un contrato firmado con Axtel, S.A.B. de C.V; por consiguiente, la SSPC no justificó llevar a cabo la contratación en el periodo de octubre a diciembre de 2020, puesto que propició el pago de servicios duplicados que le venía prestando la SEGOB, además no obtuvo las mejores condiciones económicas ya que en el convenio modificatorio número SSPC/DGRMSOP/CV05/2021 del 30 de marzo de 2021, se obtuvo una reducción de precios del orden del 50.3%, los cuales son similares a la primera propuesta presentada por Axtel, S.A.B. de C.V., el 4 de febrero de 2020.

- Por lo anterior, se efectuaron pagos por 41,015.2 miles de pesos correspondientes a los servicios de “Continuidad y Migración del Servicio”, “Servicios de Cómputo”, “Servicios de Seguridad” y “Servicios de Comunicaciones” del contrato número SSPC/DGRMSOP/CT/22/2020, con aumentos de precios por los tres meses del contrato que no se encuentran debidamente justificados, en razón de que el proveedor venía prestando y cobrando el mismo servicio con la SEGOB en los siete meses anteriores y durante los tres meses de vigencia del contrato de la SSPC, aun cuando el convenio firmado entre la SEGOB y la SSPC daba a esta última la responsabilidad de la operación de la infraestructura y soluciones tecnológicas a partir del 1º de enero de 2020, además del acuerdo entre ambas dependencias que el hospedaje de los servicios de cómputo y sistemas concluiría el 29 de febrero de 2020. Asimismo, se tienen evidencias de trabajos realizados mediante el contrato número SG/CPS/24/2020 suscrito por la SEGOB con Axtel, S.A.B. de C.V., que fueron prestados a la SSPC durante el periodo de mayo a septiembre de 2020, cuando ésta no tenía un contrato con dicho proveedor, los cuales también fueron prestados y pagados hasta el mes de diciembre de 2020, lo que propició la duplicidad de pago. Adicionalmente, la SSPC no obtuvo las mejores condiciones económicas en la contratación por tres meses, ya que en el convenio modificatorio número SSPC/DGRMSOP/CV05/2021 del 30 de marzo de 2021, se obtuvo una reducción de precios del orden del 50.3%, los cuales son similares a la primera propuesta presentada por Axtel, S.A.B. de C.V., el 4 de febrero de 2020, lo que pone de manifiesto la falta de planificación para la prestación y pago de los servicios.

  Lo anterior incumplió con los artículos 1º, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 29, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; con el Macroproceso 4.2 de Contrataciones, numeral 4.2.1.1.10, “Realizar investigación de mercado” del Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público; con el numeral 14, fracción I, de los Lineamientos en Materia de Austeridad Republicana de la Administración Pública Federal publicados en el Diario Oficial de la Federación el 18 de septiembre de 2020; y con el artículo 9, fracción II del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias.

Revisión técnica del contrato

Se revisó la información relativa a los entregables únicos, mensuales, planes de trabajo, certificaciones del proveedor, entre otros, proporcionados por la Secretaría de Seguridad y Protección Ciudadana, y se identificó lo siguiente:

Entregables del Servicio

- No fueron establecidos los criterios de aceptación para la validación de los servicios base ni incrementales, por lo tanto, los entregables fueron recibidos sin revisión de calidad por parte de la SSPC.

- En relación con el numeral 21 “Servicios Incrementales” del Anexo Técnico, se identificó la falta de las memorias técnicas digitales como parte de la prestación del servicio, por lo anterior, se presumen pagos por servicios no prestados por 5,191.2 miles de pesos, debido a que no se cuenta con la evidencia de las “Memorias Técnicas” señaladas en las actas de entrega-recepción, las cuales forman parte de los entregables de los Servicios Incrementales.

  Lo anterior incumplió los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 7, fracción VI, de la Ley General de Responsabilidades Administrativas; 1º, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 66, fracción I, III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; con el Contrato número SSPC/DGRMSOP/CT/22/2020, Cláusula décima segunda “obligaciones del proveedor”; y del Anexo técnico del contrato número SSPC/DGRMSOP/CT/22/2020, Numeral 21 “Servicios Incrementales”.

Plan de Trabajo

Se carece del reporte de avance del cumplimiento de las fechas pactadas del plan de trabajo que permita medir los avances y, en su caso, tomar acciones con los retrasos que pudieran afectar a la operación de la secretaría.

Mesa de Servicio

Como parte de las pruebas del grupo auditor se solicitó el reporte de los incidentes y requerimientos, sin embargo, durante el ejercicio de 2020 no se contó con este tipo de registros.

Plan de Capacidad de la Infraestructura Tecnológica

Se carece de un plan de capacidad para verificar las necesidades de infraestructura tecnológica y operativas para el centro de datos, por lo tanto, no se tiene la certeza que la infraestructura implementada sea la requerida para la demanda y requerimientos de la secretaría.

Pruebas de Cumplimiento del Contrato

De un universo de 13 servicios fueron seleccionados 4 (30.8%) para las pruebas del grupo auditor, los cuales fueron “Migración de Servicios de Nomina”, “Servicio de Almacenamiento

en Disco", "Administración de Base de Datos" y "Firewall de Base de Datos", y se identificó lo siguiente:

Migración de Servicios de Nómina

- En relación con el "Entregable Único" denominado "Memoria Técnica", no se establecieron los criterios de aceptación para verificar la calidad del entregable.

- La configuración de usuarios y grupos del software de Oracle se realizó a partir del 5 de enero de 2016, las instancias de los servicios fueron levantadas desde el 23 de agosto del 2019, y los preparativos del ambiente de base de datos de nómina comenzaron el 21 de julio de 2020; cabe señalar que dichos servicios fueron realizados antes de la vigencia del contrato.

Servicio de Almacenamiento en Disco

- No se ejecutan replicaciones síncronas ni asíncronas en ninguno de los sistemas, la secretaría señaló que la plataforma se encuentra preparada, sin embargo, no existe un sitio remoto para realizarlas; asimismo, tampoco forma parte del Plan de Recuperación ante Desastres.

- La función para realizar operaciones de copia y restauración de datos no se encuentra activa para la recuperación de los sistemas.

Servicio de Administración de Base de Datos

No se tienen evidencias de la operación de los servicios siguientes: Clonación de bases de datos; Aplicación de parches para motores de bases de datos (al menos dos veces al año); Carga de información en las bases de datos; Creación, modificación y depuración de objetos en las bases de datos, y Replicación de base de datos en el mismo sitio.

Con lo anterior, se constató que se carece de un plan de capacidad de la infraestructura tecnológica para verificar las necesidades operativas previo a la contratación de los servicios; no se cuenta con criterios de aceptación para la validación de los entregables ni con reportes de avance del cumplimiento de los planes de trabajo; se efectuaron pagos por 41,015.2 miles de pesos con aumentos de precios en los tres meses del contrato que no se encuentran debidamente justificados, en razón de que el proveedor venía prestando y cobrando el servicio con la SEGOB en los siete meses anteriores y durante los tres meses de vigencia del contrato de SSPC, lo que propició la duplicidad de pago, además no obtuvo las mejores condiciones económicas en la contratación por tres meses, ya que en el convenio modificatorio del ejercicio 2021 tuvo una reducción de precios del orden del 50.3%, lo que

pone de manifiesto la falta de planificación para la prestación y pago de los servicios y se presumen pagos por servicios no prestados por 5,191.2 miles de pesos, debido a la carencia de las “Memorias Técnicas” requeridas en las actas de entrega-recepción del contrato.

2020-0-36100-20-0089-01-002 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana fortalezca los procedimientos y controles para establecer los criterios de aceptación para la validación de los entregables, la implementación del reporte de avance del cumplimiento de los planes de trabajo, las verificaciones para asegurar el registro de los incidentes con los que opera la mesa de servicio, así como instrumentar un plan de capacidad de la infraestructura tecnológica; con la finalidad de efectuar revisiones de calidad a los entregables, asegurar la realización de los planes de trabajo con la medición de los avances, mejorar la gestión de incidentes para aumentar los niveles de servicio, así como garantizar que la infraestructura implementada es la requerida para satisfacer las necesidades operativas 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.

2020-0-36100-20-0089-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 41,015,153.39 pesos (cuarenta y un millones quince mil ciento cincuenta y tres pesos 39/100 M.N.), por pagos de los servicios de "Continuidad y Migración del Servicio", "Servicios de Cómputo", "Servicios de Seguridad" y "Servicios de Comunicaciones" del contrato número SSPC/DGRMSOP/CT/22/2020, con aumentos de precios por los tres meses del contrato que no se encuentran debidamente justificados, en razón de que Axtel, S.A.B. de C.V., venía prestando y cobrando el mismo servicio con la Secretaría de Gobernación (SEGOB) en los siete meses anteriores y durante los tres meses de vigencia del contrato de la Secretaría de Seguridad y Protección Ciudadana (SSPC). Asimismo, la SSPC no obtuvo las mejores condiciones económicas en la contratación por tres meses, ya que en el convenio modificatorio número SSPC/DGRMSOP/CV05/2021 del 30 de marzo de 2021, se obtuvo una reducción de precios del orden del 50.3% prestando el mismo servicio, los que son iguales a los cotizados en la primera propuesta presentada por Axtel, S.A.B. de C.V., el 4 de febrero de 2020, lo que pone de manifiesto la falta de planificación para la prestación y pago de los servicios, más los rendimientos financieros generados desde la fecha de su pago hasta la de su total recuperación, en incumplimiento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 29; del Acuerdo por el que se modifican las políticas y

disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, artículo 9, fracción II; del Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público publicado en el Diario Oficial de la Federación el 9 de agosto de 2010, última reforma publicada el 03 de febrero de 2016, Macroproceso 4.2 "Contratación", numeral 4.2.1.1.10 "Realizar investigación de mercado"; y de los Lineamientos en Materia de Austeridad Republicana de la Administración Pública Federal publicados en el Diario Oficial de la Federación el 18 de septiembre de 2020, numeral 14, fracción I.

Causa Raíz Probable de la Irregularidad

Falta de monitoreo, supervisión y control en las investigaciones de mercado y contratación de los servicios.

2020-0-36100-20-0089-06-003 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 5,191,174.00 pesos (cinco millones ciento noventa y un mil ciento setenta y cuatro pesos 00/100 M.N.), por pagos por servicios no prestados debido a que se carece de la evidencia de las "Memorias Técnicas" requeridas en las actas de entrega-recepción del contrato número SSPC/DGRMSOP/CT/22/2020, suscritas entre la secretaría y el proveedor, las cuales forman parte de los entregables de los servicios incrementales, más los rendimientos financieros generados desde la fecha de su pago hasta la de su total recuperación, en incumplimiento de la Constitución Política de los Estados Unidos Mexicanos, artículo 134; de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1; de la Ley General de Responsabilidades Administrativas, artículo 7, fracción VI; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I, y III; del Contrato número SSPC/DGRMSOP/CT/22/2020, cláusula décima segunda "obligaciones del proveedor", y del Anexo técnico del contrato número SSPC/DGRMSOP/CT/22/2020, numeral 21, "Servicios Incrementales".

Causa Raíz Probable de la Irregularidad

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

4. Contrato número SSPC/DGRMSOP/CT/33/2020 “Licenciamiento para el Sistema de Identificación Biométrica Automatizada ABIS-SSPC”

Se analizó la información del contrato número SSPC/DGRMSOP/CT/33/2020 suscrito con Biometría Aplicada, S.A de C.V., mediante el procedimiento de adjudicación directa con fundamento en los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos;

26, fracción III, 28, fracción I, 40, 41, fracción I, de la Ley de Adquisiciones, Arrendamientos y Servicios de Sector Público, y 71 y 72, fracción II, de su Reglamento, con vigencia del 1º al 31 de diciembre de 2020, por un monto de 48,617.9 miles de pesos, para la prestación del servicio de licenciamiento para el Sistema de Identificación Biométrica Automatizada ABIS-SSPC; con el presupuesto de 2020, se pagó la totalidad del monto del contrato, y se determinó lo siguiente:

Alcance del servicio

Contar con la suscripción del uso del licenciamiento que permita desarrollar el Sistema de Identificación Biométrica Automatizada, compatible con los algoritmos de Neurotechnology, con la finalidad de resolver las necesidades de información, procesamiento y cruce biométrico que a nivel nacional requieren los organismos de seguridad pública, así como garantizar la continuidad y mejora del servicio de identificación biométrica que se brinda a las diferentes instituciones de seguridad del país.

El Centro Nacional de Información Plataforma México cuenta con un motor que considera datos biométricos faciales (2.8 millones), voz (780 mil registros) y AFIS (huellas dactilares 9.5 millones; palmares 3.8 millones y latentes-activos 950 mil imágenes), lo anterior requiere el desarrollo de un nuevo sistema de procesamiento multibiométrico para actualizar las versiones obsoletas, reducir los tiempos de respuesta para los usuarios, correlacionar la información de las diversas identidades, así como permitir la interoperabilidad con otros sistemas biométricos.

Las licencias son a perpetuidad para el procesamiento en los servidores con el sistema operativo Linux y Megamatcher Accelerator, en el caso de las terminales remotas para el enrolamiento biométrico trabajan con el sistema operativo XP, Windows 7 y Windows 10; las terminales remotas requieren 4,675 licencias para los componentes de huellas, palmares, rostro, iris y voz; los servidores de producción requieren 33 licencias para los mismos componentes, y los servidores de desarrollo-pruebas requieren 57 licencias.

El grupo auditor identificó que los sistemas operativos Windows XP y 7 no tienen soporte del fabricante desde el 8 de abril de 2014 y 14 de enero de 2020, respectivamente.

Proceso de contratación

- En la investigación de mercado se dejó constancia de que la empresa Biometría Aplicada, S.A de C.V., era la autorizada para la distribución del licenciamiento Megamatcher, no obstante, existen otras soluciones en el mercado que ofrecen las mismas funcionalidades de correlación de datos biométricos, de las cuales no les fue solicitada la propuesta técnica y económica para su evaluación.

- La dependencia elaboró minutas en las que se acordó que la mejor opción para la secretaría era el desarrollo de un sistema biométrico propio, sin embargo, no se cuenta con evidencia que acredite el análisis costo-beneficio realizado, ni la fuente de información para la determinación de dicha conclusión, a fin de corroborar que el desarrollo propio era la mejor opción para la SSPC.

- Se identificó que el servicio de "Licenciamiento para el Sistema de Identificación Biométrica Automatizada ABIS-SSPC" no fue incluido en el Programa Anual Adquisiciones, Arrendamientos y Servicios de la SSPC.

Revisión Técnica, Funcional y Administrativa

El grupo auditor revisó la documentación técnica (entregables, planes de trabajo, entre otros) proporcionada por la SSPC, con base en el contrato y el anexo técnico del servicio para verificar los mecanismos de control implementados por el administrador del contrato y el aprovechamiento de las licencias adquiridas, y se identificó lo siguiente:

Entregables del Servicio

- Los entregables carecen de firmas que acrediten que fueron recibidos de conformidad por la administración del contrato, por lo tanto, no se tiene la certeza de que dichos productos hayan sido debidamente revisados y aprobados por la dependencia.

- Al término de la vigencia del contrato se emitió un acta de entrega/recepción donde se manifestó el cumplimiento del plazo de entrega y el contenido requerido, sin embargo, no se observan los criterios definidos y la validación realizada para la recepción de los entregables.

Servicio de Licenciamiento

- No se proporcionó la evidencia de los criterios analizados para la estimación del crecimiento de las licencias, con la finalidad de verificar que satisfacen las necesidades actuales y futuras de la secretaría.

<u>Licenciamiento para Servidores</u>

- En relación con el desarrollo del motor para las biometrías de huellas dactilares, se identificó que dicho motor aún se encuentra en proceso de desarrollo y evaluación de reglas de negocio para determinar la viabilidad de implementar la funcionalidad

de eliminación de registros, por lo que no fue posible la ejecución de pruebas de búsqueda y cotejo de huellas dactilares.

- Con relación al desarrollo de los motores para el resto de las biometrías pagadas en el licenciamiento (palmas, facial, iris y voz), se identificó que, pese a que se cuenta con el licenciamiento instalado en los servidores de desarrollo, aún no se inicia con la construcción de dichos motores, por lo que no se cuenta con un avance que permita corroborar el uso de dichas licencias.

- En la revisión efectuada por el grupo auditor, se detectó que de un universo de 90 licencias de servidores para todas las biometrías incluido el motor, sólo se usan para fines de desarrollo 19 (21.1%), que corresponden a huellas dactilares y latentes, así como al paquete de desarrollo.

Licenciamiento para Estaciones Remotas

- En la revisión y pruebas efectuadas por el grupo auditor, se identificó de un universo de 3,400 licencias para las biometrías de palmas, facial, iris y voz, que únicamente se usan con fines de desarrollo 120 (3.5%); asimismo, del universo de 1,275 licencias para biometría de huellas digitales, sólo se usan con fines de desarrollo 30 licencias (2.4%).
  Cabe señalar que la licencias en uso están instaladas sólo en el ambiente de pruebas del desarrollo del motor biométrico, ninguna licencia se encuentra operando en ambiente productivo, por lo tanto, no se ha cumplido con el objeto del contrato para *"…apoyar a los órganos de investigación policial y de otras actividades que requieren la identificación de personas, proporcionándoles la capacidad de procesar registros biométricos con comparaciones 1:N y 1:1, en menor tiempo y con mayor precisión..."*.

- La secretaría proporcionó un plan de trabajo para el desarrollo del motor biométrico que no forma parte del contrato ni anexo técnico, el cual inició el 10 de septiembre de 2020 y finalizará el 26 de agosto de 2022. Cabe destacar que dicho plan no se encuentra formalizado por las áreas involucradas en el desarrollo del motor biométrico, tampoco cuenta con todos los elementos de la planeación del proyecto, ni con los planes subsidiarios como son el Alcance, Cronograma, Costos, Calidad, Recursos, Comunicaciones, Riesgos, Adquisiciones e Interesados, desde su inicio hasta su cierre, también se carece de la actualización en tiempo y forma de los avances de proyecto.

- Es preciso señalar que para la compra de las licencias de estaciones remotas no fueron indicadas las etapas del desarrollo del motor biométrico, ni los objetivos e indicadores de resultado que se espera obtener para las mismas, lo que propició que el licenciamiento para dichas estaciones fuera adquirido anticipadamente, toda vez que el desarrollo del motor biométrico no está concluido para el aprovechamiento de

- dichas licencias; cabe señalar que sólo se usan con fines de desarrollo el 3.5% de las licencias adquiridas para las estaciones remotas.

Servicio de Soporte al Licenciamiento

- Se identificó que el administrador del contrato no cuenta con una herramienta automatizada para el control del licenciamiento adquirido, en consecuencia, la gestión de licencias se realiza mediante una hoja de cálculo de manera manual.

- Se carece de una póliza de servicio para asegurar la prestación del soporte al licenciamiento adquirido, que regule las características, tiempos y responsabilidades del proveedor para la prestación de dicho soporte.

Como resultado de la revisión del licenciamiento para el sistema de identificación biométrica automatizada, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la dependencia son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIA DE LOS CONTROLES PARA LA OPERACIÓN DEL LICENCIAMIENTO DEL SISTEMA DE IDENTIFICACIÓN BIOMÉTRICA AUTOMATIZADA

Factor crítico	Riesgo
Aprovechamiento del licenciamiento	La falta de uso del licenciamiento adquirido representa un riesgo en la disponibilidad de los servicios de identificación biométrica, debido a que dichas licencias pueden ser obsoletas para satisfacer las necesidades de la dependencia en el momento en que sean instaladas, propiciando que los recursos ejercidos no cumplan con los objetivos del contrato ni de la seguridad pública en los tres niveles de gobierno.
Soporte y actualización del licenciamiento	Debido a la carencia de una póliza de servicio para establecer las responsabilidades, tiempos y características del soporte para el licenciamiento, se tiene el riesgo de la falta de oportunidad y calidad necesaria para mantener la continuidad operativa del servicio de identificación biométrica que presta el servicio de inteligencia para los organismos de seguridad pública.
Planeación, implementación y operación del desarrollo del motor biométrico	La carencia de planes de trabajo formalizados por las áreas involucradas en el desarrollo del motor biométrico, así como reuniones de seguimiento entre el equipo de desarrollo, el proveedor de licenciamiento y las áreas usuarias del sistema, genera el riesgo de incumplimiento en la puesta en marcha de los servicios para satisfacer las necesidades de la dependencia, así como el incumplimiento de los requisitos funcionales del motor biométrico, propiciando la falta de soporte a las actividades sustantivas de los órganos de investigación policial.

FUENTE: Información proporcionada por la SSPC y las pruebas del grupo auditor.

De lo anterior, se identificaron deficiencias en el análisis costo-beneficio, planeación, construcción, implementación y operación del desarrollo del motor biométrico, las cuales se deben solventar para evitar la degradación de la plataforma que presta servicios a la

seguridad pública nacional en los tres niveles de gobierno. Asimismo, se carece de la planeación y definición de las etapas del desarrollo del motor biométrico y de los objetivos e indicadores de resultado que se espera obtener para las mismas, lo que propició que el licenciamiento para estaciones remotas fuera adquirido anticipadamente, toda vez que el desarrollo del motor biométrico no está concluido para el aprovechamiento de dichas licencias. Adicionalmente, se determinó que no se ha cumplido con los objetivos del contrato ya que los avances para el desarrollo del motor biométrico sólo reportan el uso con fines de desarrollo del 3.5% de las licencias a más de 10 meses de su contratación.

2020-0-36100-20-0089-01-003 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana fortalezca los procedimientos y controles para solicitar las propuestas técnicas y económicas de todos los participantes relevantes del mercado, a fin de incluirlos en el estudio que considere las características técnicas de cada uno de ellos junto al análisis costo-beneficio para determinar la mejor opción para la dependencia, con la finalidad de contar con una comparación objetiva entre bienes y servicios iguales o de la misma naturaleza, así como asegurar las mejores condiciones económicas y técnicas en beneficio 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.

2020-0-36100-20-0089-01-004 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana implemente los procedimientos para aprovechar el licenciamiento del sistema de identificación biométrica automatizada, así como elabore todos los elementos de la planeación del proyecto con sus planes subsidiarios como son el Alcance, Cronograma, Costos, Calidad, Recursos, Comunicaciones, Riesgos, Adquisiciones e Interesados, desde su inicio hasta su cierre, con la actualización en tiempo y forma de los avances del proyecto con sus informes periódicos a la alta dirección de la dependencia para su seguimiento.

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.

2020-9-36100-20-0089-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en la Secretaría de Seguridad y

Protección Ciudadana o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que, en su gestión, respecto del proceso de contratación y administración del contrato número SSPC/DGRMSOP/CT/33/2020 "Licenciamiento para el Sistema de Identificación Biométrica Automatizada ABIS-SSPC", no cumplieron con las disposiciones vigentes para la compra de las licencias de estaciones remotas, toda vez que no fueron indicadas las etapas del desarrollo del motor biométrico, ni los objetivos e indicadores de resultado que se espera obtener para las mismas, lo que ocasionó que dicho licenciamiento fuera adquirido anticipadamente ya que el desarrollo del motor biométrico no está concluido para el aprovechamiento de dichas licencias. Asimismo, no se cuenta con todos los elementos para la planeación del proyecto, ni con los planes subsidiarios como son el Alcance, Cronograma, Costos, Calidad, Recursos, Comunicaciones, Riesgos, Adquisiciones e Interesados, desde su inicio hasta su cierre, también se carece de la actualización en tiempo y forma de los avances de proyecto; cabe señalar que sólo se usan con fines de desarrollo el 3.5% de las licencias adquiridas para las estaciones remotas, en incumplimiento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 1, párrafo segundo; de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 24; de la Ley General de Responsabilidades Administrativas, artículo 7, fracciones I y V, y del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, última reforma publicada el 23 de julio de 2018, artículo 10, fracción II, segundo párrafo, así como el proceso III.A Administración de Proyectos (ADP), Reglas del Proceso, numeral 3, del Manual antes citado.

5. Ciberseguridad

Se revisó la información proporcionada por la Secretaría de Seguridad y Protección Ciudadana, relacionada con la administración y operación de los controles de Ciberseguridad, vinculados con la infraestructura y soluciones tecnológicas, de conformidad con los controles para la Ciberseguridad y sus mejores prácticas, y con base en las políticas y lineamientos de la dependencia en esta materia.

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

De la información y documentación remitida por la secretaría, se observó que no cuenta con una Unidad de Tecnologías de la Información y Comunicaciones (UTIC) que coordine e integre los esfuerzos de las áreas operativas en la definición, formalización e implementación de los mecanismos de control, lo que propicia que las actividades relacionadas con la seguridad de

la información no se encuentren debidamente asignadas entre las áreas operativas que tienen relación con dichos controles, en consecuencia, no se tienen establecidos ni formalizados los roles y responsabilidades de cada una de las áreas en sus respectivos tramos de control.

El alcance de la auditoría consideró 20 controles de seguridad críticos (CSC) que incluyen 149 actividades de control individuales para evaluar el diseño y la efectividad operativa con sus respectivos objetivos de cumplimiento. Para la evaluación de los controles fueron considerados tres niveles, los cuales se obtuvieron de conformidad con el porcentaje alcanzado en la evaluación de los subcontroles con los rangos siguientes: Aceptable (más del 67.0%), Requiere fortalecer el control (entre el 33.0% y 67.0%) o Carencia de control (menos del 33.0%) y se observó lo siguiente:

SEMÁFORO DE CUMPLIMIENTO DE LOS CONTROLES DE CIBERSEGURIDAD EN LA SSPC DURANTE 2020

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

FUENTE: Elaborado con información proporcionada por la Secretaría de Seguridad y Protección Ciudadana.

Indicador: 🟢 Cumplimiento aceptable 🟡 Requiere fortalecer el control 🔴 Carencia de control

El detalle de las observaciones y hallazgos de cada uno de los controles de seguridad críticos es el siguiente:

CSC Control 1: Inventario y control de activos de hardware

- El catálogo de infraestructuras críticas no indica el nivel de criticidad asignado a cada uno de los activos de información, tampoco se proporcionó evidencia que acredite el análisis y los criterios definidos para determinar dicho nivel de criticidad.

- No se cuenta con una herramienta de descubrimiento activo/pasivo que permita identificar de manera automática los dispositivos conectados a la red, ni para actualizar el inventario de activos de hardware.

- Para las actividades de registro y monitoreo de los dispositivos conectados a la red se utiliza el formato “Requerimiento de Servicio”, no obstante, dicho formato no se encuentra debidamente formalizado ni autorizado por las áreas solicitantes y técnicas.

- No se tienen implementados controles de acceso a nivel de puerto para controlar los dispositivos que puedan autenticarse en la red.

- No se proporcionó evidencia que acredite los escaneos realizados a la red, a fin de corroborar que no existan dispositivos desconocidos registrados y activos.

- Se carece de herramientas para obtener la dirección física (MAC) de los equipos de forma automatizada, en consecuencia, el registro es manual mediante la línea de comandos de los equipos.

Por lo anterior, no se cumple con el objeto de gestionar activamente todo dispositivo de hardware en la red (inventario, seguimiento y corrección), de tal manera que sólo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados ni gestionados sean detectados, para prevenir que obtengan acceso.

CSC Control 2: Inventario y control de activos de software

- No se tienen definidas listas blancas de scripts, librerías ni software en los servidores.

- Se carece de herramientas para la generación automática del inventario de software, tampoco se cuenta con políticas ni procedimientos definidos para la generación del inventario de manera periódica, a fin de depurar el software no autorizado.

- Los sistemas operativos de los servidores presentan obsolescencia tecnológica y se encuentran fuera del soporte del fabricante, situación que representa un riesgo para la continuidad operativa de los sistemas.

- La dependencia no tiene establecidos filtros para la instalación de software libre en los equipos, lo que podría poner en riesgo la continuidad operativa de los procesos y

- Se carece de una solución para el monitoreo y bloqueo del software no autorizado que se encuentre instalado en los equipos de cómputo y servidores.

- No se proporcionó evidencia de que se realizan escaneos de software y para corroborar que no existan aplicaciones o programas no autorizados en los equipos.

- Se carece de políticas y procedimientos que definan las actividades y tiempos para la desinstalación de software no autorizado.

Por lo antes señalado, no se cumple con el objeto de gestionar activamente todo el software en la red (inventario, seguimiento y corrección), con la finalidad de que sólo el software autorizado esté instalado y pueda ejecutarse, de tal manera que el software no autorizado ni gestionado sea encontrado, para prevenir su instalación y ejecución.

CSC Control 3: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

- No se tiene definida una política de endurecimiento para la configuración de los servidores.

- Se carece de una estrategia institucional para la configuración de las imágenes seguras para todos los sistemas y equipos.

- No se cuenta con herramientas para la gestión de la configuración de los sistemas, a fin de verificar que se cuente con todos los elementos de configuración, excepciones y alertas de cambios no autorizados.

- No se han aplicado actualizaciones de seguridad (parches) en la infraestructura tecnológica debido, entre otras causas, a la falta de un ambiente de pruebas, lo anterior, representa un alto riesgo para la seguridad de la información en los servidores y equipos de usuario final.

- Durante las pruebas del grupo auditor se identificó que existen sistemas operativos obsoletos, los cuales se encuentran fuera del soporte extendido del fabricante.

- Se carece de una herramienta que permita la detección y bloqueo de los cambios no autorizados en los servidores, asimismo, no se tienen evidencias que acrediten la realización de actividades para la detección de dichos cambios.

- No se tiene una herramienta que permita detectar y generar alertamientos sobre cambios en la configuración del registro del sistema (REGEDIT).

Por lo anterior, no se cumple con el objeto de establecer, implementar y gestionar activamente (rastrear, informar, corregir), la configuración de seguridad de computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

CSC Control 4: Evaluación continua de la vulnerabilidad y solución

- Se carece de un procedimiento documentado y formalizado donde queden establecidos los roles, responsabilidades y tiempos para la eliminación y/o mitigación de las vulnerabilidades identificadas.

- No se tienen identificados los roles, responsabilidades, tiempos y documentación que se debe generar para el análisis del código fuente de los sistemas.

Por lo antes señalado, no se cumple en su totalidad con el objeto de adquirir, evaluar y tomar medidas sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

CSC Control 5: Uso controlado de privilegios administrativos

- No se tiene una herramienta automatizada para obtener el inventario de las cuentas administrativas.

- Se carece de bitácoras de auditoria para las cuentas privilegiadas.

- No se tiene evidencia del cambio de contraseñas de fábrica para los servidores, dispositivos y equipos de usuario final.

- Se carece de una herramienta para el registro y alertamiento de los cambios en los grupos administrativos.

Por lo anterior, no se cumple con el objeto de implementar procesos y herramientas para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

CSC Control 6: Mantenimiento, monitoreo y análisis de bitácoras de auditoría

- Se identificó que la infraestructura tecnológica tiene el registro de las bitácoras activado.
- Durante el ejercicio 2020, se identificaron revisiones del tráfico de red, y se cuenta con el análisis de la actividad sospechosa en dicha red.
- Se identificó el documento "Recopilación de evidencias y análisis de actividades sospechosas", en donde fue registrada la evidencia de los eventos ocurridos.
- Se detectó que no se cuenta con una herramienta para el monitoreo y notificación de los inicios de sesión en los servidores.

Por lo antes señalado, se cumple con el objeto de reunir, administrar y analizar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

CSC Control 7: Protección de correo electrónico y navegador web

- Se identificó que no se tienen aplicados bloqueos de lenguajes de script en navegadores web y clientes de correo electrónico.

- No se tiene conocimiento de la cantidad de eventos e incidentes detectados durante el ejercicio de 2020.

- No se realizan pruebas de suplantación de identidad, asimismo, durante el ejercicio 2020, no se han emitido comunicados con las políticas y procedimientos de seguridad de la información para los usuarios.

Por lo anterior, no se cumple en su totalidad con el objeto de minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano mediante su interacción con navegadores web y sistemas de correo electrónico.

CSC Control 8: Defensa contra software malicioso (malware)

- No se cuenta con una solución antimalware instalada, actualizada y en operación, situación con una alta vulnerabilidad ante un ataque cibernético, debido a la carencia de herramientas que eliminen o mitiguen el impacto en las áreas operativas que hacen uso de los sistemas.

- Los servidores no cuentan con soluciones anti-exploits (programa que se aprovecha de una vulnerabilidad para provocar un comportamiento imprevisto) ni sandboxing (ambiente aislado donde los programas sospechosos se pueden ejecutar para estudiar su comportamiento sin poner en peligro la red).

- No se cuenta con mecanismos ni métricas para definir las actividades y el tiempo estimado para la eliminación/contención de ataques con código malicioso.

Por lo antes señalado, no se cumple en su totalidad con el objeto de controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de la automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

CSC Control 9: Limitación y control de puertos de red, protocolos y servicios

- Se tiene definida una política de seguridad informática en el Centro de Datos, con los lineamientos y controles para el aseguramiento de la red como son la autenticación, cifrado y controles de conexión de red, y para las conexiones de la red privada virtual (VPN).

- Se cuenta con políticas de configuración de los cortafuegos (firewall), donde se observó que todos los servidores se encuentran bajo las políticas de seguridad configuradas en dicho equipo.

- No se proporcionó evidencia que acredite que se realiza una validación del uso operacional de puertos, protocolos y servicios en los dispositivos de red.

Por lo anterior, se cumple con el objeto de administrar (rastrear, corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

CSC Control 10: Capacidad de recuperación de datos

- Se identificó que un 30.0% de los servidores críticos no se encuentran respaldados con un sistema completo.

- No se tiene evidencia que acredite que se realizan pruebas de integridad de los datos en las copias de respaldo de forma periódica.

- No se cuenta con herramientas que permitan el cifrado físico y lógico de las copias de seguridad generadas.

Por lo antes señalado, no se cumple en su totalidad con el objeto de verificar los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.

CSC Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

- El control de acceso a la red se realiza de manera manual con base en los formatos de solicitud, no obstante, se identificó que no se tiene una configuración de seguridad aprobada para los equipos de seguridad de red.

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

Por lo anterior, no se cumple en su totalidad con el objeto de establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes exploten servicios y configuraciones vulnerables.

CSC Control 12: Seguridad Perimetral

- Se identificó que las firmas de seguridad de los equipos que protegen a la red se encuentran desactualizadas, por lo tanto, se encuentran operando sin las últimas actualizaciones liberadas por el fabricante, con un alto riesgo de que sean vulnerables ante nuevas amenazas cibernéticas.
- Se carece de sistemas de detección de intrusos (IDS) que permitan detectar actividades irregulares, incorrectas o anómalas, desde el exterior o interior de la infraestructura de red.

Por lo antes señalado, no se cumple en su totalidad con el objeto de detectar, prevenir y corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.

CSC Control 13: Protección de datos

- No se cuenta con el inventario de la información sensible que es almacenada, procesada o transmitida por los sistemas.
- No se proporcionó la evidencia que acredite el cumplimiento del procedimiento de obsolescencia de datos y equipos, del cual se informó que el periodo máximo de utilidad es de cinco años.
- Se carece de un procedimiento de cifrado de disco duro en los servidores.
- Los servidores no cuentan con una solución de prevención de pérdida de datos (DLP) que permita el monitoreo de la transferencia de información sensible, así como el bloqueo de las transferencias no autorizadas al mismo tiempo que emite alertas al personal de seguridad de la información.

Por lo anterior, no se cumple con el objeto de gestionar los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.

CSC Control 14: Control de acceso basado en necesidad de conocimiento

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

- No se cuenta con evidencia documental de la implementación y operación de una solución para la prevención de pérdida de datos.

Por lo antes señalado, no se cumple totalmente con el objeto de gestionar los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el acceso seguro a activos críticos (información, recursos, sistemas, entre otros) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.

CSC Control 15: Control de acceso inalámbrico

- No se proporcionó evidencia que acredite la realización del escaneo de puertos a fin de identificar puntos de acceso no autorizados en la red.

- No se cuenta con políticas ni procedimientos definidos, formalizados e implementados para la conexión de dispositivos ajenos a la infraestructura tecnológica de la dependencia.

- Se carece de políticas y procedimientos definidos, formalizados e implementados para las conexiones inalámbricas del tipo Bluetooth (redes inalámbricas de área personal) y NFC (tecnología inalámbrica de corto alcance).

Por lo anterior, no se cumple con el objeto de gestionar los procesos y herramientas utilizadas para rastrear, controlar y corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

CSC Control 16: Supervisión y monitoreo de cuentas

- Se carece de una herramienta automatizada para obtener el inventario de las cuentas administrativas, incluyendo el dominio y cuentas locales para asegurarse de que sólo las personas autorizadas tienen privilegios elevados.

- El procedimiento para la desactivación de las cuentas de VPN se realiza con una herramienta obsoleta con el soporte extendido finalizado desde abril de 2018.

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

- No se proporcionó evidencia de revisiones a los registros de acceso a los sistemas mediante el uso de cuentas privilegiadas.

Por lo antes señalado, no se cumple con el objeto de gestionar activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.

CSC Control 17: Implementar un programa de concientización y entrenamiento de seguridad

- No se cuenta con un procedimiento para la elaboración del análisis de brechas de las habilidades del personal de seguridad de la información.

- No se han realizado ejercicios que permitan medir el nivel de concientización de los usuarios en seguridad de la información.

Por lo anterior, no se cumple en su totalidad con el objeto de gestionar todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la dependencia, así como desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar mediante políticas, planificación organizacional, capacitación y programas de concienciación.

CSC Control 18: Seguridad del Software de Aplicación

- Se carece de un proceso documentado con los roles, responsabilidades y tiempos para la eliminación/mitigación de las vulnerabilidades identificadas en los sistemas.

- No se tienen mecanismos de control para asegurarse que las aplicaciones se encuentren actualizadas y con soporte por parte del fabricante.

Por lo antes señalado, no se cumple en su totalidad con el objeto de gestionar el ciclo de vida de seguridad de todo el software interno desarrollado y adquirido para prevenir, detectar y corregir las debilidades de seguridad.

CSC Control 19: Respuesta y Manejo de Incidentes de Ciberseguridad

- El plan de gestión y respuesta a incidentes aún no está terminado ni autorizado por la Alta Dirección para su implementación.

- Se carece de evidencias de la clasificación y tratamiento de los incidentes cibernéticos, así como de los roles y responsabilidades del equipo de respuesta a incidentes de seguridad.

- El plan de gestión y respuesta a incidentes no contempla los flujos de los procesos y roles asignados de la mesa de servicios, la sustitución del personal de respuesta a incidentes cuando se retira de la dependencia, la actualización de los escenarios de pruebas para adaptarse a las nuevas situaciones detectadas durante el tratamiento de los incidentes, así como la generación de una base de datos de lecciones aprendidas.

De acuerdo con lo anterior, no se cumple con el objeto de proteger la información de la organización, y su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión, entre otros) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.

CSC Control 20: Pruebas de penetración y ejercicios de equipo rojo

- No se cuenta con un programa de pruebas de penetración que incluya una gama completa de ataques combinados, como la inalámbrica, basadas en cliente, y ataques a aplicaciones web.

- No se proporcionó evidencia que acredite la ejecución de pruebas de penetración sobre la infraestructura tecnológica y aplicativos sustantivos.

- No se cuenta con un equipo rojo que realice ejercicios de pruebas de penetración de manera proactiva.

Por lo antes señalado, no se cumple con el objeto de probar la fortaleza general de la defensa de la secretaría (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

Como resultado de la revisión de los controles y procedimientos para la ciberseguridad, los principales riesgos por la carencia de los controles y sus consecuencias potenciales para las operaciones y activos de información de la secretaría son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE CIBERSEGURIDAD

Factor Crítico	Riesgo
Inventario y control de activos de hardware	La carencia del inventario y control de activos de hardware genera el riesgo de no poder controlar que sólo los dispositivos autorizados obtengan acceso a las redes y sistemas, y que los dispositivos no autorizados ni gestionados sean detectados para bloquear su acceso.
Inventario y control de activos de software	La falta de un inventario de software autorizado y no autorizado favorece que en los dispositivos poco controlados se tienen más posibilidades de ejecutar software innecesario desde el punto de vista de la organización (introduciendo posibles fallas de seguridad) o de ejecutar software malicioso introducido por un atacante después de que un sistema se vea comprometido.
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	La falta de configuraciones seguras en los dispositivos de usuario final propicia el riesgo de no contar con configuraciones autorizadas y cambios verificados para evitar que los atacantes exploten servicios y configuraciones vulnerables.
Uso controlado de privilegios administrativos	Las deficiencias en el control de los privilegios administrativos, genera el riesgo de no poder rastrear, controlar, prevenir y corregir el uso, asignación y configuración de privilegios a los usuarios que lo requieran de conformidad con sus atribuciones y facultades.
Protección de datos	La falta de cumplimiento de las políticas y procedimientos para la protección de datos propicia el riesgo de dificultar la prevención y mitigación de la exfiltración de datos y no permite asegurar la privacidad e integridad de la información sensible.
Control de acceso inalámbrico	Las deficiencias en el control de acceso inalámbrico, genera el riesgo de no poder rastrear, controlar y corregir el uso seguro de las redes de área local inalámbricas, puntos de acceso y sistemas de clientes inalámbricos.
Supervisión y monitoreo de cuentas	La falta de gestión activa del ciclo de vida de las cuentas del sistema (creación, uso, latencia, eliminación) conlleva al incremento de oportunidades para cualquier ataque.
Respuesta y Manejo de Incidentes de Ciberseguridad	El no poder mitigar el impacto asociado a un incidente y vincularlo con el responsable para su atención, puede ocasionar la pérdida de la confidencialidad, integridad y disponibilidad de la información.
Pruebas de penetración y ejercicios de equipo rojo	La carencia de pruebas de penetración impide probar la fortaleza general de la ciberdefensa de la secretaría (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

FUENTE: Elaborado con información proporcionada por la SSPC y el resultado de las pruebas del grupo auditor.

De lo antes señalado, se tienen deficiencias en el inventario y control de activos de hardware y software; la configuración segura en equipos de usuario final y servidores; el control de privilegios administrativos en sistemas y aplicaciones; la protección de datos sensibles; la respuesta y manejo de incidentes de ciberseguridad, y en las pruebas de penetración a la infraestructura y soluciones tecnológicas; lo anterior, pone en riesgo el funcionamiento de los equipos, servidores, redes, sistemas y aplicativos sustantivos ante los efectos de un ataque cibernético que podría impactar en la operación de la secretaría, y en los órganos de investigación policial de los tres niveles de gobierno para el desempeño de sus actividades relacionadas con la seguridad pública nacional.

2020-0-36100-20-0089-01-005 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana fortalezca las políticas, procedimientos y controles para el inventario y control de activos de hardware y software; la configuración segura en dispositivos móviles, equipos de usuario final y servidores; el uso controlado de privilegios administrativos; la protección de datos; el control de acceso inalámbrico; la supervisión y monitoreo de cuentas; el manejo de incidentes de ciberseguridad, y para las pruebas de penetración a la infraestructura y soluciones tecnológicas, con la finalidad de que sólo los dispositivos y software autorizados obtengan acceso a las redes, se mejore la seguridad de los dispositivos para evitar que los atacantes exploten servicios y configuraciones vulnerables, se controlen los privilegios administrativos para el acceso a los equipos y aplicaciones, se proteja la información instrumentando una infraestructura de respuesta a incidentes; así como probar la fortaleza de la ciberdefensa de la dependencia, y mitigar los efectos de un ataque cibernético que podría impactar en la operación de la secretaría y en los órganos de investigación policial de los tres niveles de gobierno en el desempeño de sus actividades sustantivas.

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

6. Continuidad de las Operaciones y Centro de Datos

En el análisis de la información proporcionada por la Secretaría de Seguridad y Protección Ciudadana, relacionada con la administración de los controles para la continuidad de las operaciones de la infraestructura y soluciones tecnológicas, así como con la seguridad física y lógica del centro de datos denominado “Centro Nacional de Información Plataforma México”, con base en las disposiciones y mejores prácticas en la materia y de conformidad con las políticas y lineamientos de la dependencia, se observó lo siguiente:

Análisis de Impacto al Negocio

- Se carece de un análisis de impacto al negocio (BIA) como iniciativa estratégica de la Alta Dirección de la dependencia, por lo tanto, no se tienen identificados los procesos ni servicios sustantivos que podrían resultar afectados por la interrupción de uno o más servicios de TIC, incluyendo los recursos y dependencias para priorizar las actividades de recuperación y continuidad de las operaciones.

- No se cuenta con los criterios para definir el objetivo del tiempo de recuperación (RTO) de los procesos y servicios, ni el objetivo del punto de recuperación (RPO) de los datos, con la finalidad de alinear las iniciativas, actividades y resultados de los planes de continuidad y recuperación de desastres con el BIA, para contar con un

programa de continuidad que sea resiliente ante un desastre con mínimas afectaciones e interrupciones a la operación, finanzas y reputación de la secretaría.

Plan de Continuidad de Negocio

- Se carece de una estrategia para coordinar la interacción de las distintas iniciativas del plan de continuidad de negocio (BCP); asimismo, no se tiene evidencia de la difusión de los procedimientos del modelo de continuidad para la operación de los registros nacionales y bases de datos de seguridad pública.

- No se proporcionó el análisis efectuado por la secretaría para determinar el nivel de prioridad en el inventario de activos de información críticos; por otra parte, el plan de continuidad de negocio no describe los roles ni responsabilidades para la implementación de la estrategia y alcance del plan.

- En relación con los servicios de la Red Nacional de Telecomunicaciones (RNT) y la Red Nacional de Radiocomunicación (RNR), se informó que dichas redes no están soportadas por un sitio alterno debido a la tecnología propietaria para la distribución de claves de cifrado, por lo anterior, resulta prioritario establecer mecanismos para asegurar la continuidad del servicio de radiocomunicación.

- No se proporcionó evidencia de las pruebas, lecciones aprendidas ni plan de remediación de incidentes del BCP durante el ejercicio de 2020.

Plan de Recuperación de Desastres

- En el ejercicio de 2019, el centro de datos alterno tuvo una falla en el sistema de almacenamiento de las bases de datos y servidores virtuales que daban soporte redundante con replicación de datos en tiempo real al sitio principal, en consecuencia, actualmente para prestar el servicio se deben instalar las versiones más recientes de los programas y datos en el sitio alterno antes de poder reanudar su operación.

- Debido a la carencia del Análisis de Impacto al Negocio, no se puede asegurar que los procedimientos, actividades y componentes del Plan de Recuperación de Desastres (DRP) consideran la priorización y necesidades de la Alta Dirección de la secretaría, así como los tiempos de tolerancia para operar sin afectar la continuidad de los procesos críticos.

- No se proporcionó evidencia de pruebas ejecutadas al DRP durante el ejercicio de 2020.

Respaldos de Información

- No se proporcionaron los planes de pruebas y restauración de respaldos de los servidores instalados en el CNIPM, para verificar que se encuentran funcionando en caso de contingencias.

- La estrategia de respaldos para bases de datos vigente durante el ejercicio de 2020, no indica la capacidad mínima que debe estar disponible en el CNIPM, ni el análisis realizado para determinar la periodicidad del respaldo de cada uno de los servidores.

- Se carece de evidencia de las pruebas efectuadas a la herramienta de respaldo y recuperación, para corroborar el funcionamiento de los procedimientos de restauración de datos y asegurar su correcta operación.

Seguridad Física y Lógica del Centro de Datos denominado "Centro Nacional de Información Plataforma México"

En el centro de datos principal denominado "Centro Nacional de Información Plataforma México", la administración de la infraestructura de procesamiento, almacenamiento y comunicaciones de la dependencia está a cargo de la misma secretaría, por otra parte, el control de accesos, el sistema de videovigilancia, la seguridad contra incendios e inundaciones, el control de las condiciones ambientales y el sistema eléctrico se encuentra bajo la responsabilidad de la Guardia Nacional; cabe señalar que no se tiene ninguna certificación nacional o internacional que avale los niveles de disponibilidad del centro de datos, y que de las pruebas del grupo auditor se observó lo siguiente:

Diseño del Centro de Datos

- Se carece de espacios para el almacenamiento de equipos y medios magnéticos, en consecuencia, se detectó equipamiento almacenado dentro de la misma sala de cómputo que podría afectar la operación de la infraestructura crítica.

- Durante la inspección física, se observaron pisos y pasillos con deterioro en sus materiales, lo cual pone de manifestó la falta de mantenimiento a las instalaciones de la sala de cómputo.

Control de Acceso Físico

- El acceso a las salas del Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC) no se encuentra automatizado.

- Las alarmas visuales y audibles de las puertas del centro de datos no se encuentran en operación.

Sistema de Videovigilancia

- No se proporcionó evidencia del funcionamiento, capacidad de los equipos ni tiempos de almacenamiento del sistema de videovigilancia.

- Durante el ejercicio de 2020, no se brindó mantenimiento preventivo al sistema.

Salidas de Emergencia y Evacuación

- En las salidas de emergencia y evacuación no funcionan las alarmas visibles ni audibles, las cuales deben alertar en caso de un conato de incendio, sismo o evacuación de las instalaciones; lo anterior, podría poner en riesgo la integridad física de las personas que laboran en el centro de datos.

- La salida de emergencia de la sala de procesamiento no se encuentra libre de obstáculos, asimismo, y carece de dispositivos luminosos o señalizaciones.

Medidas de seguridad contra incendios

- Los sistemas de detección de humo por aspiración de alta sensibilidad, así como los detectores de humo y calor se encuentran fuera de operación desde el ejercicio de 2016.

- El sistema para la detección automática de extinción de incendios se encuentra fuera de operación desde el año de 2016, por obsolescencia de sus componentes y falta de mantenimiento.

Medidas de seguridad contra daños ocasionados por líquidos

Los sensores de detección de líquidos se encuentran fuera de operación.

Sistema de control de ambiente

El sistema de enfriamiento no cuenta con un contrato de soporte y mantenimiento vigente, lo que podría causar un impacto en las condiciones de operación de los equipos.

Sistema Eléctrico

- No se proporcionó la evidencia de la periodicidad y resultados de las pruebas a la planta de emergencia que soporta todo el sistema eléctrico para la operación del centro de datos.

- No se cuenta con un contrato de soporte y mantenimiento para el sistema eléctrico; asimismo, no se proporcionó evidencia del último mantenimiento realizado a los tableros de control, unidades de energía ininterrumpible y plantas de emergencia.

Infraestructura Tecnológica

Las soluciones de almacenamiento fueron adquiridas en el ejercicio de 2012, la falta de mantenimiento ha provocado intermitencia en la operación de los servidores virtualizados, inestabilidad en los registros nacionales y aplicativos auxiliares, y falta de espacio para soportar el crecimiento de los datos.

De lo anterior, se carece de un análisis de impacto al negocio para alinear los planes de continuidad y recuperación ante desastres con las necesidades y prioridades definidas por la Alta Dirección, para mantener la resiliencia operativa de los procesos sustantivos de la secretaría; asimismo, la operación del centro de datos se encuentra comprometida por la falta de un programa de mantenimiento a los sistemas principales para su operación, lo que también pone en riesgo la integridad física de las personas que laboran en el centro de datos denominado “Centro Nacional de Información Plataforma México”.

2020-0-36100-20-0089-01-006 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana implemente un proyecto institucional dirigido por la Alta Dirección, para la instrumentación del Análisis de Impacto al Negocio donde se consideren todos los procesos sustantivos para la operación de la secretaría, el cual contemple las funciones, actividades, áreas, servicios, punto objetivo de recuperación de la información, tiempo objetivo de recuperación de los procesos, pérdidas económicas, costos adicionales, daños reputacionales, incumplimiento de las disposiciones, riesgos para la seguridad del personal y capacidad operativa, entre otros, con la finalidad de mitigar los riesgos asociados a la interrupción de los procesos y asegurar la continuidad de las operaciones de la dependencia.

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.

2020-0-36100-20-0089-01-007 **Recomendación**

Para que la Secretaría de Seguridad y Protección Ciudadana implemente un programa de mantenimiento para los sistemas de detección y extinción de incendios, el sistema de prevención de inundaciones, los equipos de aire acondicionado y climatización, las puertas y alarmas sonoras, el circuito cerrado de televisión, así como los equipos de energía eléctrica y

plantas de emergencia, con la finalidad de evitar o mitigar el riesgo de que se presenten fallas o incidentes en los sistemas y equipos que puedan interrumpir la operación de los procesos críticos de la dependencia, y poner en riesgo la integridad física de las personas que laboran en el centro de datos.

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

2020-5-36H00-20-0089-01-001 **Recomendación**

Para que la Guardia Nacional implemente un programa de mantenimiento para los sistemas de detección y extinción de incendios, el sistema de prevención de inundaciones, los equipos de aire acondicionado y climatización, las puertas y alarmas sonoras, el circuito cerrado de televisión, así como los equipos de energía eléctrica y plantas de emergencia, con la finalidad de evitar o mitigar el riesgo de que se presenten fallas o incidentes en los sistemas y equipos que puedan interrumpir la operación de los procesos críticos de la dependencia, y poner en riesgo la integridad física de las personas que laboran en el centro de datos.

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

Montos por Aclarar

Se determinaron 49,350,012.09 pesos pendientes por aclarar.

Buen Gobierno

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

Resumen de Resultados, Observaciones y Acciones

Se determinaron 6 resultados, de los cuales, en uno no se detectó irregularidad y los 5 restantes generaron:

8 Recomendaciones, 1 Promoción del Ejercicio de la Facultad de Comprobación Fiscal, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 3 Pliegos de Observaciones.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe de auditoría se comunicarán a la entidad fiscalizada, en términos de los artículos 79 de la Constitución Política de los Estados Unidos Mexicanos y 39 de la Ley de Fiscalización y Rendición de Cuentas de la Federación, para que en un plazo de 30 días hábiles presente la información y realice las consideraciones que estime pertinentes.

En tal virtud, las recomendaciones y acciones que se presentan en este informe de auditoría se encuentran sujetas al proceso de seguimiento, por lo que, debido a la información y consideraciones que en su caso proporcione la entidad fiscalizada podrán atenderse o no, solventarse o generar la acción superveniente que corresponda de conformidad con el marco jurídico que regule la materia.

Dictamen

El presente se emite el día 15 de octubre de 2021, 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, la administración de riesgos, la seguridad de la información, la continuidad de las operaciones, la calidad de datos, el desarrollo de aplicaciones y el 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 Seguridad y Protección Ciudadana no cumplió con las disposiciones legales y normativas aplicables en la materia, entre cuyos aspectos observados destacan los siguientes:

- En relación con el contrato del sistema automatizado de identificación de huellas dactilares, se identificó el riesgo de interrupción de la infraestructura que podría afectar la continuidad operativa de la Plataforma México, para prestar sus servicios a los tres niveles de gobierno en las actividades de seguridad pública del país, debido a la obsolescencia de los equipos por la falta de actualización de sus componentes, sin el adecuado soporte y mantenimiento para atender las incidencias. Asimismo, se efectuaron pagos por 3,143.7 miles de pesos del servicio de terminales remotas, los cuales tuvieron un precio más caro que la contratación precedente que tenía el mismo objeto, servicios e infraestructura, aun cuando los nuevos servicios se prestaron con un 64.5% menos equipos respecto del contrato previo con tecnología obsoleta sin renovación tecnológica, a pesar de que las terminales fueron diseñadas con tecnología del año 2010.

- Respecto del contrato para el servicio de procesamiento y almacenamiento para sistemas administrativos (Centro de Datos), se carece de un plan de capacidad de la infraestructura tecnológica para verificar las necesidades operativas previo a la contratación de los servicios. Asimismo, se efectuaron pagos por 41,015.2 miles de pesos con aumentos de precios en los tres meses del contrato que no se encuentran debidamente justificados, en razón de que el proveedor venía prestando y cobrando el servicio con la SEGOB en los siete meses anteriores y durante los tres meses de vigencia del contrato de SSPC, lo que propició la duplicidad de pago, además no obtuvo las mejores condiciones económicas en la contratación por tres meses, ya que en el convenio modificatorio del ejercicio 2021 tuvo una reducción de precios del orden del 50.3%, lo que pone de manifiesto la falta de planificación para la prestación y pago de los servicios. Adicionalmente, se realizaron pagos por servicios no prestados por 5,191.2 miles de pesos debido a la carencia de las "Memorias Técnicas" requeridas en las actas de entrega-recepción del contrato.

- En la revisión del contrato para el licenciamiento del sistema de identificación biométrica automatizada, se identificaron deficiencias en el análisis costo-beneficio, planeación, construcción, implementación y operación del desarrollo del motor biométrico, las cuales podrían aumentar la degradación de la plataforma que presta servicios a la seguridad pública nacional en los tres niveles de gobierno. Asimismo, se carece de la planeación y definición de las etapas del desarrollo del motor biométrico y de los objetivos e indicadores de resultado que se espera obtener para las mismas, lo que propició que el licenciamiento para estaciones remotas fuera adquirido anticipadamente, toda vez que el desarrollo del motor biométrico no está concluido para el aprovechamiento de dichas licencias. Adicionalmente, se determinó que no se ha cumplido con los objetivos del contrato ya que los avances para el desarrollo del motor biométrico sólo reportan el uso con fines de desarrollo del 3.5% de las licencias a más de 10 meses de su contratación.

- En relación con la Ciberseguridad, se tienen deficiencias en el inventario y control de activos de hardware y software; la configuración segura en equipos de usuario final y servidores; el control de privilegios administrativos en sistemas y aplicaciones; la protección de datos sensibles; la respuesta y manejo de incidentes de ciberseguridad, y en las pruebas de penetración a la infraestructura y soluciones tecnológicas; lo anterior, pone en riesgo el funcionamiento de los equipos, servidores, redes, sistemas y aplicativos sustantivos ante los efectos de un ataque cibernético, que podría impactar en la operación de los órganos de investigación policial de los tres niveles de gobierno para sus actividades relacionadas con la seguridad pública nacional.

- Con respecto de la Continuidad de las Operaciones y Centro de Datos, se carece de un análisis de impacto al negocio institucional para alinear los planes de continuidad y recuperación ante desastres con las necesidades y prioridades definidas por la Alta Dirección, para mantener la resiliencia operativa de los procesos sustantivos de la secretaría. Asimismo, la operación del centro de datos se encuentra comprometida por la falta de un programa de mantenimiento a los sistemas principales para su operación, lo que también pone en riesgo la integridad física de las personas que laboran en el centro de datos.

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

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Genaro Héctor Serrano Martínez	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 las cifras reportadas en la Cuenta Pública corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables, y analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprende el análisis de las contrataciones vigentes, la determinación de la procedencia de su renovación, la pertinencia de realizar contrataciones consolidadas, 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, y verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permiten su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales, y verificar la entrega en tiempo y forma de los servicios, así como la pertinencia de su penalización o deductivas en caso de incumplimientos.

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

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de penetración a las redes y sistemas, entre otros.

7. Evaluar la gestión de los programas de continuidad de las operaciones en sus elementos como el análisis de impacto al negocio (BIA); el plan de continuidad del negocio (BCP); el plan de recuperación ante desastres (DRP); las políticas de respaldos; la replicación de datos; la planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros. Verificar la seguridad física y lógica del centro de datos en sus componentes como el control de acceso físico; el sistema de videovigilancia; la prevención y extinción de incendios; el sistema de detección de líquidos; el control de medio ambiente y el sistema eléctrico, por mencionar algunos.

Áreas Revisadas

El Centro Nacional de Información Plataforma México y la Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, adscritas a la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica, y la Dirección General de Recursos Materiales, Servicios y Obra Pública adscrita a la Unidad de Administración y Finanzas de la Secretaría de Seguridad y Protección Ciudadana.

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. Constitución Política de los Estados Unidos Mexicanos: artículo 134;

2. Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 1, párrafo segundo;

3. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 1,24, 26, primer párrafo y 40 segundo párrafo;

4. Ley General de Responsabilidades Administrativas: artículo 7, fracciones I ,V y VI;

5. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 28, fracciones II y III, 29, fracciones I y II, 30 y 72, fracción II;

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

7. Otras disposiciones de carácter general, específico, estatal o municipal: Ley General de Sociedades Mercantiles, artículo 260;

   Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana publicado el 30 de abril 2019, artículos 11, fracción IX y 13, fracción II;

   Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, artículos 9, fracción II y 13, fracciones I y VII, 16, fracción III, 18 fracción I;

   Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, última reforma publicada el 23 de julio de 2018; Proceso II.A. Administración de Servicios (ADS), Regla del proceso 2, Actividad ADS 3 Administrar la capacidad de la infraestructura de TIC, factor crítico 4; Proceso II.B. Administración de la Configuración (ACNF), ACNF1, Factor Crítico 1; Proceso III.B. Administración de Proveedores (APRO), Actividad APRO 2 Monitorear el avance y desempeño del proveedor, Factor Crítico 3, inciso a y b; Proceso II.C. Administración de la Seguridad de la Información (ASI), ASI 6, factor crítico 1, inciso a; Proceso III.C Administración de la Operación (AOP), AOP 1 Establecer el mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC, AOP 3 Monitorear la infraestructura de TIC en operación; Marco de referencia COBIT, Prácticas de gestión "DSS04.02 Mantener una estrategia de continuidad", "DSS04.07 Gestionar acuerdos de respaldos"; Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y en la Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, última reforma publicada el 23 de julio de 2018, Apartados 4.3.2, 5.2.2, 5.3, 8.2 y 8.5 de la Norma ISO 22301/2019 "Seguridad y Resiliencia" "Sistemas de Administración de la Continuidad del Negocio", incluidos en las metodologías, mejores prácticas nacionales e internacionales de la matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC, que se integran en el Apéndice IV.B de este Manual;

Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público publicado en el Diario Oficial de la Federación el 9 de agosto de 2010, última reforma publicada el 03 de febrero de 2016, Macroproceso 4.2 Contratación, numeral 4.2.1.1.10 "Realizar investigación de mercado";

Lineamientos en Materia de Austeridad Republicana de la Administración Pública Federal publicados en el Diario Oficial de la Federación el 18 de septiembre de 2020, numeral 14, fracción I;

Contrato número SSPC/DGRMSOP/CT/22/2020, cláusula décima segunda "obligaciones del proveedor";

Anexo Técnico del contrato número SSPC/DGRMSOP/CT/22/2020, numeral 5.10 "Servicio de Mesa de Servicio" y numeral 21, "Servicios Incrementales".

Lineamientos en Materia de Austeridad Republicana de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 18 de septiembre de 2020, numeral 14; Contrato número SSPC/DGRMSOP/CT/33/2020, cláusula primera "Objeto del Servicio"; Anexo técnico del contrato número SSPC/DGRMSOP/CT/33/2020, numeral 2.3 "Objetivos Específicos".

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.