

Secretaría de Relaciones Exteriores**Auditoría de TIC**

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-0-05100-20-0013-2021

13-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	675,596.4
Muestra Auditada	199,877.4
Representatividad de la Muestra	29.6%

El universo seleccionado por 675,596.4 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 cuatro contratos, dos de ellos corresponden a la prestación del servicio para el desarrollo, actualización, mantenimiento y soporte de aplicaciones, otro tiene como objeto el servicio de estrategia de seguridad de la información y el último fue para los servicios integrales de transición del pasaporte en Estados Unidos de América y México, con pagos ejercidos por 199,877.4 miles de pesos, que representan el 29.6% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Secretaría de Relaciones Exteriores (SRE) en 2020, relacionada con la Ciberseguridad y Continuidad de las Operaciones.

Antecedentes

En la revisión de la Cuenta Pública 2015, se practicó la auditoría 31-GB “Auditoría de TIC” donde se detectaron irregularidades en el servicio para la concertación de citas y emisión del Pasaporte Mexicano en territorio nacional como penalizaciones no cobradas por incumplimiento de los niveles de servicio, falta de supervisión del proveedor para acreditar las horas de desarrollo de las actividades, imprecisiones en los cálculos de penalizaciones para la rotación de personal y, por último, no se había cumplido con el objetivo de modernizar la expedición del pasaporte debido a la falta de reducción de los tiempos del trámite porque el proceso tenía varias actividades manuales con el manejo de un alto volumen de papel.

Entre 2016 y 2020, se han erogado 1,061,142.4 miles de pesos en sistemas de información e infraestructuras tecnológicas, adicionalmente, las direcciones generales de Servicios Consulares y Delegaciones ejercieron 483,632.6 miles de pesos en la partida 33903 “Servicios Integrales” durante el ejercicio 2020, la cual corresponde a gastos de TIC, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC – SRE							
(Miles de Pesos)							
Periodo del Gasto	Unidad	2016	2017	2018	2019	2020	Total
	DGTII	189,888.4	181,534.8	194,879.5	272,771.3	222,068.4	1,061,142.4
Monto por año	DGSC-DGD					483,632.6	483,632.6

FUENTE: Elaborada con información proporcionada por la Secretaría de Relaciones Exteriores.

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, al Ramo Relaciones Exteriores (05) se le autorizó un presupuesto de 8,723,637.7 miles de pesos, del cual a la Secretaría de Relaciones Exteriores se le asignó un presupuesto original de 8,120,726.5 miles de pesos.

Respecto del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2020, se concluyó que la Secretaría de Relaciones Exteriores (Sector

Central) mediante ampliaciones y reducciones tuvo un presupuesto ejercido de 12,326,462.8 miles de pesos, de los cuales, 705,701.0 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 5.7% del presupuesto, como se muestra a continuación:

RECURSOS EJERCIDOS EN LA SECRETARÍA DE RELACIONES EXTERIORES (SECTOR CENTRAL) DURANTE 2020
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recursos ejercidos en TIC
1000	Servicios personales	5,001,681.1	30,104.6
2000	Materiales y suministros	9,852.7	0.0
3000	Servicios generales	5,340,179.2	675,596.4
4000	Transferencias, asignaciones, subsidios y otras ayudas	1,847,618.4	0.0
5000	Bienes muebles, inmuebles e intangibles	127,131.4	0.0
TOTAL		12,326,462.8	705,701.0

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

Los recursos ejercidos en materia de TIC por 705,701.0 miles de pesos se integran de la manera siguiente:

GASTOS TIC 2020 EN LA SRE
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
1000		SERVICIOS PERSONALES	30,104.6
3000		SERVICIOS GENERALES	675,596.4
	31401	Servicio telefónico convencional	616.3
	31501	Servicio de telefonía celular	282.8
	31601	Servicio de radiolocalización	234.3
	31701	Servicios de conducción de señales analógicas y digitales	281.0
	31904	Servicios integrales de infraestructura de cómputo	64,705.6
	32301	Arrendamiento de equipo y bienes informáticos	1,142.6
	33301	Servicios de informática	82,509.4
	33903	Servicios integrales ¹	525,466.5
	37106	Pasajes aéreos internacionales para servidores públicos en el desempeño de comisiones	131.5
	37602	Viáticos en el extranjero para servidores públicos en el desempeño de comisiones	226.5
TOTAL			705,701.0

FUENTE: Elaborado con información proporcionada por la SRE.

NOTA¹: Incluye recursos ejercidos por 483,632.6 miles de pesos de las Direcciones Generales de Servicios Consulares y Delegaciones. Diferencias por redondeo.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 30,104.6 miles de pesos durante el ejercicio fiscal 2020; considerando 63 plazas, el promedio anual percibido por persona fue de 477.9 miles de pesos.

Del universo seleccionado en 2020 por 675,596.4 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 199,877.4 miles de pesos en cuatro contratos que representan el 29.6% 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	Contratos	Proveedor	Objeto del Contrato	Vigencia		Monto		
				Del	Al	Mínimo	Máximo	Ejercido
Adjudicación Directa (Artículo 1º LAASSP)	SRE-DRM-AD-15/19 con 3 convenios y SRE/DRM/AD-034/2020	INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación	Prestación del servicio para el desarrollo, actualización, mantenimiento y soporte de aplicaciones	01/04/2019	31/12/2020	66,000.0	165,000.0	82,509.2
Adjudicación directa	SRE-DRM-AD-22/19	TIC Defense, S.A de C.V.	Servicio de Estrategia de Seguridad de la Información	16/08/2019	15/04/2022	0.0	57,750.0	18,289.0
Adjudicación directa	SRE/DRM/AD-043/2020 con un convenio	IECISA México, S.A. de C.V.	Servicios Integrales de Transición de Pasaporte en Estados Unidos de América y México	16/08/2020	31/03/2021	179,000.0	400,000.0	99,079.2
Totales						245,000.0	622,750.0	199,877.4

FUENTE: Elaborado con información proporcionada por la SRE.

Durante la integración de la muestra de contratos realizada por el grupo auditor, se identificó un pago por 1,010.6 miles de pesos efectuado a TIC Defense, S.A. de C.V., que no fue registrado a cargo de la Unidad Responsable que ejerció los recursos públicos.

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.

2020-0-05100-20-0013-01-001 **Recomendación**

Para que la Secretaría de Relaciones Exteriores fortalezca los mecanismos de clasificación y registro del gasto, con la finalidad de que el ejercicio del presupuesto se refleje a cargo de las unidades responsables que ejercieron los recursos públicos y con ello aumentar la calidad en el registro presupuestario 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.

2. Contratos números SRE-DRM-AD-15/19 y SRE/DRM/AD-034/2020 “Servicio para el desarrollo, actualización, mantenimiento y soporte de aplicaciones”

Se analizó la información del contrato número SRE-DRM-AD-15/19 celebrado con INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC), mediante el procedimiento de adjudicación directa, de conformidad con los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 1° de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 4° de su Reglamento, vigente del 1° de abril al 31 de diciembre de 2019, por un monto mínimo de 30,000.0 miles de pesos y máximo de 75,000.0 miles de pesos, con objeto de prestar el “Servicio para el desarrollo, actualización, mantenimiento y soporte de aplicaciones”; el 3 de julio de 2019, se celebró el primer convenio modificatorio al contrato, con objeto de modificar la cláusula décima sexta “Administración y Verificación”; el 4 de diciembre de 2019, se celebró un segundo convenio para ampliar la vigencia al 31 de marzo de 2020; el 27 de marzo de 2020, se celebró un tercer convenio modificatorio donde se amplió la vigencia al 15 de junio de 2020, así como el monto mínimo a 36,000.00 miles de pesos y máximo a 90,000.0 miles de pesos, por los servicios devengados de este contrato se efectuaron pagos por 34,414.0 miles de pesos durante 2020. También se analizó la información del contrato número SRE/DRM/AD-034/2020, con vigencia del 16 de junio al 31 de diciembre de 2020, por un monto mínimo de 30,000.00 miles de pesos y máximo de 75,000.0 miles de pesos, con el mismo objeto del contrato número SRE-DRM-AD-15/19, del cual durante 2020 se efectuaron pagos por 48,095.2 miles de pesos, y se determinó lo siguiente:

Alcance del servicio

La secretaría requiere el apoyo de un tercero a fin de estar en posibilidad de tener profesionistas calificados para el soporte, gestión y desarrollo en materia tecnológica y administrativa, para atender en promedio 65,000 solicitudes de atención de soporte técnico especializado, así como el desarrollo, soporte y mantenimiento de más de 45 sistemas administrativos en las oficinas centrales, 50 sistemas para trámites en las Representaciones en el Exterior y dos sistemas para las Delegaciones.

Revisión Administrativa de los Entregables

En el análisis de la documentación proporcionada por la dependencia, se observó lo siguiente:

- No se proporcionaron los entregables denominados “Relación de incidentes/solicitudes atendidas por el personal de soporte de primer nivel” y “Relación de incidentes/solicitudes atendidas por el personal de soporte de primer nivel” para el periodo de enero a diciembre de 2020, asimismo, se detectó que el

acta de entrega-recepción de la primera quincena de junio de 2020 corresponde a la segunda quincena de junio de 2020.

- No se presentaron las listas de asistencia para el periodo de marzo a diciembre de 2020 debido a la contingencia sanitaria, sin embargo, no fueron implementados controles compensatorios para verificar que las horas devengadas correspondieron a las efectivamente pagadas.
- Los entregables denominados “Plan general de trabajo”, “Plan de trabajo del requerimiento”, “Control de cambios del requerimiento y generación de casos de uso”, “Matriz de trazabilidad”, “Interfaz Gráfica”, “Plan de pruebas que incluye matriz de pruebas”, “Generación del código fuente modificado para atender requerimiento”, “Manual de usuario”, “Lista de revisión para la liberación del requerimiento” y “Acta de cierre de proyecto” no contienen las firmas de los usuarios finales que definieron los requerimientos durante el periodo de marzo a diciembre de 2020, con lo cual no se acredita que las funcionalidades fueron a satisfacción de dichos usuarios.
- En el Anexo Técnico de ambos contratos, no se estipuló la obligatoriedad de presentar todos los entregables establecidos en la metodología del desarrollo de sistemas de la dependencia, tampoco fueron considerados en las penalizaciones ni deductivas de dichos contratos.

Cumplimiento Técnico y Funcional de los Entregables

De un universo de 34 sistemas desarrollados en la gestión del contrato número SRE/DRM/AD-034/2020, el grupo auditor de la ASF seleccionó seis (17.6%) para su revisión técnica y funcional, para lo cual consideró su nivel de criticidad, riesgo e impacto operativo, los cuales fueron los siguientes:

MUESTRA PARA LA REVISIÓN TÉCNICA DE LOS SISTEMAS DESARROLLADOS EN EL CONTRATO NÚMERO SRE/DRM/AD-034/2020

(Miles de pesos)

Proyecto	Nombre	Objetivo	Fecha de desarrollo	Nivel de criticidad	Ubicación	Lenguaje	Responsable del uso del sistema	Número de usuarios	Estado actual	Costo
P2020-011	Sistema Integral de Permisos Artículo 27 Constitucional (SIPAC27)	Reingeniería con el objetivo de desfasar un software de pago utilizado para firmar electrónicamente los documentos emitidos por el sistema, así como la mejora de sus funcionalidades.	14/04/2020	Alta	Triangular	PHP	Dirección General de Asuntos Jurídicos	5000	En producción	3,101.3
P2019-038	Jóvenes Construyendo el Futuro (JCF)	Sistema que gestiona el registro de becarios y empresas (tutores) para el programa Jóvenes Construyendo el Futuro (JCF 1.0 El Salvador) en los países de El Salvador y Honduras, adicionalmente el sistema permitirá la entrega de beneficios a los inscritos. El proyecto incluye modificaciones a los sistemas Jóvenes Construyendo el Futuro Honduras (JCFH), Jóvenes Construyendo el Futuro 2.0 El Salvador (JCF 2.0), Jóvenes Construyendo el Futuro Honduras 2.0 (JCFH 2.0) y Jóvenes Construyendo el Futuro 2.1 Honduras y el Salvador (JCF 2.1).	18/12/2019	Alta	Triangular	PHP	Dirección Ejecutiva de la AMEXCID	7800	En producción ¹	12,005.2

FUENTE: Elaborado con información proporcionada por la Secretaría de Relaciones Exteriores.

NOTA¹: Los módulos JCF 2.1 y JCFH 2.0 aún se encuentran en pruebas de seguridad de acuerdo con las declaraciones realizadas por la SRE.*Sistema Integral de Permisos Artículo 27 Constitucional (SIPAC27)*

El sistema suspendió los trámites que se siguen ante la Dirección General de Asuntos Jurídicos, de conformidad con el “ACUERDO por el que se modifica por séptima ocasión el diverso por el que se dan a conocer los días en que se suspenderán los plazos y términos aplicables en los trámites y procedimientos administrativos sustanciados ante la Secretaría de Relaciones Exteriores, con motivo de la emergencia sanitaria generada por el virus SARS-CoV2 (COVID-19)” publicado el 29 de septiembre de 2020, en el Diario Oficial de la Federación; como resultado de las pruebas realizadas por el grupo auditor de la ASF en ambiente productivo, se detectó que la plataforma no cuenta con pistas de auditoría, en consecuencia, no se cuenta con controles que apoyen el análisis de las transacciones en caso de irregularidades.

Jóvenes Construyendo el Futuro (JCF)

En el análisis y pruebas realizadas a las características técnicas y funcionales descritas en los entregables (casos de uso, casos de prueba, instructivo de operación para la solución tecnológica, entre otros), se observó lo siguiente:

- En el Módulo de Registro, se identificó un error de descarga en el convenio de colaboración y ficha de tutor.
- En el Módulo de Vinculación, no se pudo ingresar con un usuario nuevo debido a que el sistema no aceptó nuevas solicitudes al no ser un periodo de validación.
- Se detectó que no se almacena el PAN (número de cuenta principal) de acuerdo con el requisito del inciso 3.4 "Convierta el PAN en ilegible en cualquier lugar donde se almacene" de las Normas de Seguridad de Datos de PCI versión 3.0.
- En los Controles de Entrada de Datos, se identificó que para el campo Registro ante Hacienda (RTN), el sistema no efectúa validaciones mediante expresiones regulares ni como apoyo en la validación de la estructura del número de registro, por lo no es posible asegurar la estructura del RTN con el objetivo de minimizar errores en la base de datos.
- En la Descarga de Documentos, se identificó que la plataforma no realiza la descarga de los "Lineamientos del Programa" en la página principal (versión 2.0).
- Respecto de la Seguridad en el desarrollo del sistema, no se identificó un "término de tiempo" de sesión ante la inactividad del usuario, con la finalidad de minimizar la oportunidad para que el atacante pueda acceder al equipo y reutilizar el identificador de sesión, en caso de que el usuario no hubiera cerrado dicha sesión, tampoco se presentó evidencia de roles definidos para el uso de los sistemas de información.

Gestión de los planes de trabajo

En la revisión de los planes de trabajo, se observó lo siguiente:

Sistema Integral de Permisos Artículo 27 Constitucional (SIPAC27)

Fueron modificadas las fechas de cierre del proyecto, originalmente se había liberado el 27 de agosto de 2020, de acuerdo con el plan general del 31 de agosto de 2020, sin embargo, en el plan general entregado el 30 de septiembre de 2020, se ajustó la fecha de liberación al 1o de septiembre de 2020, no obstante, no se proporcionó una justificación de estos cambios.

Jóvenes Construyendo el Futuro 2.0 El Salvador (JCF 2.0)

- Fueron ajustadas las fechas de entrega originales como sigue:
 - Pruebas de seguridad: se modificó la fecha de entrega del 26 de mayo al 19 de junio de 2020.
 - Pruebas con el usuario (QA): se modificó la fecha de entrega del 28 de mayo al 24 de junio de 2020.

- Implementación: se modificó la fecha de entrega del 29 de mayo al 25 de junio de 2020.
- Cierre: se modificó la fecha de entrega del 29 de mayo al 26 de junio de 2020.
- Se identificó un retraso de las pruebas de QA del 27 de mayo al 19 de junio de 2020.
- Se observó un retraso en las pruebas de seguridad del 26 de mayo al 9 de noviembre de 2020, lo que derivó en atrasos de las pruebas de usuario, implementación y cierre del sistema.
- Cabe señalar que las pruebas de QA y Seguridad son realizadas por áreas diferentes a la responsable del desarrollo del sistema y no forman parte de los entregables definidos con el prestador de servicios.

Jóvenes Construyendo el Futuro Honduras 2.0 (JCFH 2.0)

Se identificó que a la fecha de la auditoría (septiembre 2021) no se han concluido las fases de Pruebas de Seguridad (fecha de conclusión: 25/06/2020), Pruebas con el usuario (fecha de conclusión: 29/06/2020), Implantación (fecha de conclusión: 30/06/2020) y Cierre (fecha de conclusión: 30/06/2020).

Jóvenes Construyendo el Futuro 2.1 Honduras y el Salvador (JCF 2.1)

- El desarrollo del sistema empezó el 14 de julio de 2020 y, a la fecha de la auditoría, (septiembre 2021) no se ha concluido.
- Se modificó la fecha de entrega del análisis de requerimiento y diseño de la solución del 29 de julio al 11 de agosto de 2020.
- Los documentos denominados “Plan general de pruebas” e “Informe de avances” confirman que no se terminaron las actividades asociadas en el mes de agosto de 2020.
- Se tienen retrasos de las pruebas QA originalmente estipuladas para entrega del 21 de septiembre al 9 de octubre de 2020.
- Se identificó que a la fecha de la auditoría (septiembre 2021) no se han concluido las fases de Pruebas de Seguridad (fecha de conclusión: 08/10/2020), Pruebas con el usuario (fecha de conclusión: 13/10/2020), Implantación (fecha de conclusión: 14/10/2020) y Cierre (fecha de conclusión: 16/10/2020).

Por lo anterior, se presumen penas convencionales no aplicadas por un monto de 2,689.1 miles de pesos, derivadas de los retrasos presentados en el proyecto Jóvenes Construyendo el Futuro 2.1 Honduras y el Salvador (JCF 2.1), correspondientes a 35 días hábiles en la etapa

de construcción que tenía como fecha de compromiso el 10 de agosto de 2020 y fue entregada el 30 de septiembre del 2020.

Actividades de los funcionarios públicos

El grupo auditor identificó que durante la atención, tramitación y resolución de los asuntos relativos al contrato número SRE-DRM-AD-15/19, el Director de Área de la Dirección General de Tecnologías de Información e Innovación de la SRE se desempeñó previamente en el cargo de Administrador de Proyectos con el prestador de servicios (INFOTEC) hasta el mes de marzo 2020, conforme a los reportes de actividades. Posteriormente, el 16 de abril de 2020, fue contratado por la SRE en el cargo de Director de Área de la Dirección General de Tecnologías de Información e Innovación, como administrador del mismo contrato, así como del contrato número SRE/DRM/AD-034/2020 que tiene el mismo objeto que el primero mencionado, en donde se observó que recibió a entera satisfacción las actas de entrega-recepción de los servicios de los meses de julio a diciembre de 2020, las cuales forman parte del trámite de pago de los servicios.

Respecto de lo anterior, se concluye que el Director de Área de la Dirección General de Tecnologías de Información e Innovación de la SRE se ubicó bajo una posible actuación de conflicto de interés, en contravención del artículo 58 de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013; del numeral 8 “Compromisos con el servidor público”, inciso h, y del numeral 12 “Conflicto de Intereses”, del “Código de conducta del personal de la SRE 2020”.

Metodología para el Desarrollo de Soluciones Tecnológicas

El grupo auditor revisó el proceso de desarrollo de sistemas de conformidad con las políticas y metodología de la dependencia, y con base en las mejores prácticas en la materia, se observó lo siguiente:

- En relación con el “Dominio de la Metodología Ágil” se identificó que de 19 subprocesos se implementó uno (5.3%), cabe señalar que la secretaría manifestó que no cuenta con la implementación de la metodología ágil para los proyectos.
- No se cumplieron las especificaciones de diseño, codificación y seguridad definidas por la dependencia, ni se utilizaron metodologías para el análisis, diseño, programación y pruebas de software con el objetivo de lograr una mayor confiabilidad.
- No se contó con un procedimiento de lecciones aprendidas, ni encuestas de satisfacción de las áreas usuarias, asimismo, no se tiene documentada una política de desarrollo de software seguro para las áreas internas de la dependencia, ni para los prestadores de servicios.

Por lo anterior, se concluye que se tienen áreas de oportunidad en la aplicación de la metodología de desarrollo de soluciones tecnológicas, en las pistas de auditoría de los sistemas, en el desarrollo seguro de software, así como en la administración de proyectos.

2020-0-05100-20-0013-01-002 **Recomendación**

Para que la Secretaría de Relaciones Exteriores fortalezca los mecanismos de control, verificación y supervisión de los contratos, donde establezca con los proveedores la obligación de remitir todos los entregables definidos en la metodología de desarrollo de soluciones tecnológicas y tome en cuenta sus criterios de aceptación para la configuración de penalizaciones y deductivas, con la finalidad de asegurar la realización de los compromisos contractuales y mejorar la calidad de los entregables que recibe 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.

2020-0-05100-20-0013-01-003 **Recomendación**

Para que la Secretaría de Relaciones Exteriores fortalezca la metodología de desarrollo de sistemas con la definición, formalización e implementación de pistas de auditoría en los sistemas, desarrollo seguro de software, encuestas de satisfacción a los usuarios, lecciones aprendidas, así como en la administración de proyectos para asegurar el cumplimiento de los planes de trabajo, a fin de corregir desviaciones e implementar mejores prácticas para lograr las metas y objetivos de los proyectos de desarrollo de sistemas, así como evitar un impacto operativo por el retraso en la puesta en producción de los sistemas críticos de la secretaría.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión 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.

2020-9-05514-20-0013-16-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que la Dirección General de Investigación adscrita a la Auditoría Especial de Seguimiento, Informes e Investigación de la Auditoría Superior de la Federación realice las investigaciones pertinentes para esclarecer los hechos, y en su caso, determine la presunta responsabilidad administrativa correspondiente por las irregularidades de los servidores públicos que, en su gestión, se ubicaron bajo una posible actuación de conflicto de interés en la administración de los contratos números SRE-DRM-AD-15/19 y SRE/DRM/AD-034/2020, debido a que durante la atención, tramitación y resolución de los asuntos de los contratos referidos, el Director de Área de la Dirección General de Tecnologías de Información e

Innovación de la Secretaría de Relaciones Exteriores se desempeñó previamente en el cargo de Administrador de Proyectos con el prestador de servicios (INFOTEC) hasta el mes de marzo 2020. Posteriormente, el 16 de abril de 2020 fue contratado por la dependencia en el cargo de Director de Área de la Dirección General de Tecnologías de Información e Innovación, como administrador de los contratos mencionados, en donde se observó que recibió a entera satisfacción las actas de entrega-recepción de los servicios de los meses de julio a diciembre de 2020, las cuales forman parte del trámite de pago de los servicios, en incumplimiento de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013, artículo 58, y del Código de conducta del personal de la SRE 2020, numeral 8 "Compromisos con el servidor público", inciso h, y del numeral 12 "Conflicto de Intereses".

2020-0-05100-20-0013-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 2,689,057.65 pesos (dos millones seiscientos ochenta y nueve mil cincuenta y siete pesos 65/100 M.N.), por penas convencionales no aplicadas derivadas de los retrasos presentados en el proyecto Jóvenes Construyendo el Futuro 2.1 Honduras y el Salvador (JCF 2.1), correspondientes a 35 días hábiles de atraso en la etapa de construcción que tenía como fecha de compromiso el 10 de agosto de 2020 y fue entregada el 30 de septiembre del 2020, 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, segundo párrafo; de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículos 24 y 53; de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013, artículo 7, fracciones I y VI; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III, y del Anexo técnico del contrato número SRE/DRM/AD-034/2020, numeral 1.12, "Penas Convencionales y Deducciones al Pago", inciso "a".

Causa Raíz Probable de la Irregularidad

No existe monitoreo ni supervisión de los compromisos contractuales, tampoco de los lineamientos y disposiciones para el desarrollo de sistemas de información, aunado a una deficiente gestión de riesgos del organismo, lo que impidió que los servicios se prestaran en tiempo, forma y de acuerdo con el fin contratado.

3. Contrato número SRE-DRM-AD-22/19 "Servicio de Estrategia de Seguridad de la Información"

Se analizó la información del contrato número SRE-DRM-AD-22/19 suscrito con TIC Defense, S.A de C.V., mediante el procedimiento de adjudicación directa, de conformidad con los artículos 26, fracción III, 40, 41, fracción IV, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 71 y 72, fracción IV, de su Reglamento, con vigencia del 16 de agosto de 2019 al 15 de abril de 2022, por un monto de 57,750.0 miles de pesos, con objeto

de prestar los “Servicios de seguridad de la información”; el 30 de junio de 2020, se realizó un convenio modificatorio mediante el cual se canceló temporalmente el servicio de “Gobierno de la Seguridad de la Información”, se efectuaron pagos por 18,289.0 miles de pesos durante el ejercicio 2020, y se determinó lo siguiente:

Alcance del servicio

Contar con una solución que incluya el servicio de ciberseguridad integral, el cual tiene entre sus principales funciones el gobierno de seguridad de la información; la analítica de seguridad, correlación de eventos y gestión de bitácoras; los servicios de identificación y mitigación de vulnerabilidades informáticas; el análisis forense; el ciclo de vida de desarrollo seguro; el alertamiento ante riesgos y amenazas, y la concientización en seguridad de la información, así como el monitoreo de seguridad en el país y en cada una de las representaciones de México en el extranjero de los sitios que integran la red.

Investigación de Mercado

La dependencia cuenta con un comparativo de los costos ofertados por los proveedores que fueron convocados y de los servicios de ejercicios anteriores, sin embargo, no fue proporcionada evidencia que acredite que se realizó un análisis de las propuestas técnicas presentadas por los proveedores para la comparación objetiva entre servicios iguales o de la misma naturaleza.

Revisión Técnica, Funcional y Administrativa

El grupo auditor realizó el análisis y pruebas de los servicios con base en la documentación técnica (entregables, solicitudes de servicio, políticas, procedimientos, entre otros), para tal efecto de un universo de seis servicios fueron revisados dos (33.3%), considerando el riesgo e impacto en la operación de las unidades administrativas, los cuales fueron el Gobierno de Seguridad de la Información y el Servicio Integral de Ciberseguridad, se observó lo siguiente:

Servicio de Gobierno de Seguridad de la Información

En relación con la cancelación de este servicio mediante el convenio modificatorio, se concluyó que no afectaba directamente la operación de la seguridad cibernética de la secretaría, asimismo, en el periodo de agosto 2019 a junio 2020 se habían realizado diversas actividades con las cuales se podía continuar con la operación de los servicios.

Servicio Integral de Ciberseguridad

En relación con los Servicios de Identificación y Mitigación de Vulnerabilidades Informáticas, se identificó que el análisis de vulnerabilidades únicamente se ejecuta bajo solicitud del área responsable del aplicativo o sistema, la secretaría no cuenta con un plan que contemple la aplicación del análisis de vulnerabilidades para todos los sistemas.

Niveles de Servicio del Contrato

Fue revisada la aplicación de los criterios de calidad y oportunidad en la entrega de los servicios, se identificó lo siguiente:

- No se contó con evidencia del análisis y los criterios que fueron considerados para la definición de las métricas de los niveles de servicio, ni de los porcentajes a aplicar en caso de incumplimiento del proveedor.
- No se proporcionó evidencia para acreditar la medición, análisis y criterios para calificar al 100.0% el nivel de satisfacción reportado en los avances del cumplimiento de las obligaciones del proveedor.
- No se cuenta con procedimientos definidos, formalizados e implementados para efectuar la medición de los niveles de servicio, en los que se indiquen los insumos requeridos, tiempos, roles, responsabilidades y documentación de la evaluación, por mencionar algunos.

En relación con los reportes de seguridad de la información presentados de enero a diciembre de 2020, fueron identificados 270 tickets y se observó lo siguiente:

- Se detectaron 21 tickets (7.8%) en los que la hora de cierre del incidente es previa a la hora de inicio del mismo.
- En el archivo de incidentes no se muestra la validación y aprobación del cierre del ticket por parte del personal que reportó el incidente, lo que no da la certeza de que los incidentes hayan sido solucionados en los tiempos registrados.

Actividades de los funcionarios públicos

El grupo auditor identificó que el Director de Seguridad Tecnológica de la Dirección General de Tecnologías de Información e Innovación de la SRE, el cual entró en funciones a partir de agosto de 2020, y que también tiene el rol de administrador del contrato número SRE-DRM-AD-22/19, formó parte del equipo de trabajo de la empresa TIC Defense, S.A. de C.V., durante el periodo de agosto de 2019 a junio de 2020 con el cargo de “Especialista en Análisis de Vulnerabilidades, Pruebas de Penetración y Análisis Forense”; sin embargo, durante el periodo de agosto a diciembre de 2020, aprobó los entregables del mismo contrato que forman parte del trámite de pago de los servicios.

Respecto de lo anterior, se concluye que el Director de Seguridad Tecnológica de la Dirección General de Tecnologías de Información e Innovación de la SRE, se ubicó bajo una posible actuación de conflicto de interés, en contravención del artículo 58 de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013 y del Numeral 8 “Compromisos con el servidor público”,

inciso h, numeral 12 "Conflicto de Intereses" del "Código de conducta del personal de la SRE 2020".

De lo anterior, se concluye que se tienen áreas de oportunidad en la definición, análisis y medición de los niveles de servicio de los contratos, así como en el registro y verificación de la integridad de las bitácoras de la mesa de servicio.

2020-0-05100-20-0013-01-004 Recomendación

Para que la Secretaría de Relaciones Exteriores implemente procedimientos y controles para la definición, análisis y medición de los niveles de servicio de los contratos, el registro y verificación de la integridad de las bitácoras de la mesa de servicio y en la contratación de los funcionarios para evitar el conflicto de intereses, con la finalidad de mejorar la gestión de los servicios, así como la respuesta a los incidentes de seguridad que pueden comprometer a los activos de información críticos 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.

2020-9-05514-20-0013-16-002 Promoción de Responsabilidad Administrativa Sancionatoria

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que la Dirección General de Investigación adscrita a la Auditoría Especial de Seguimiento, Informes e Investigación de la Auditoría Superior de la Federación realice las investigaciones pertinentes para esclarecer los hechos, y en su caso, determine la presunta responsabilidad administrativa correspondiente por las irregularidades de los servidores públicos que, en su gestión, se ubicaron bajo una posible actuación de conflicto de interés, en la administración del contrato número SRE-DRM-AD-22/19, debido a que durante la atención, tramitación y resolución de los asuntos del contrato referido, el Director de Seguridad Tecnológica de la Dirección General de Tecnologías de Información e Innovación de la Secretaría de Relaciones Exteriores, el cual entró en funciones a partir de agosto de 2020, y que también tenía el rol de administrador del contrato número SRE-DRM-AD-22/19, formó parte del equipo de trabajo de la empresa TIC Defense, S.A. de C.V., durante el periodo de agosto de 2019 a junio de 2020 con el cargo de "Especialista en Análisis de Vulnerabilidades, Pruebas de Penetración y Análisis Forense"; sin embargo, durante el periodo de agosto a diciembre de 2020, aprobó los entregables del mismo contrato que forman parte del trámite de pago de los servicios, en incumplimiento de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013, artículo 58, y del Código de conducta del personal de la SRE 2020, numeral 8 "Compromisos con el servidor público", inciso h, y del numeral 12 "Conflicto de Intereses".

4. Contrato número SRE/DRM/AD-043/2020 "Servicios Integrales de Transición de Pasaporte en Estados Unidos de América y México"

Se analizó la información del contrato número SRE/DRM/AD-043/2020 celebrado con IECISA México, S.A. de C.V., mediante el procedimiento de adjudicación directa de conformidad en los artículos 26, fracción III, 41, fracción II, y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 85 de su Reglamento, vigente del 16 de agosto de 2020 al 31 de marzo de 2021, por un monto mínimo de 179,000.0 miles de pesos y máximo de 400,000.0 miles de pesos, con objeto de prestar los "Servicios Integrales de Transición del Pasaporte Mexicano en Estados Unidos de América y en México", a efecto de dar continuidad a la expedición de pasaportes de lectura mecánica, durante el periodo de transición hacia el pasaporte de lectura electrónica. El 30 de diciembre de 2020, se realizó un convenio modificatorio mediante el cual se amplió la vigencia del contrato y se hizo constar el cambio de denominación de IECISA México, S.A de C.V., a INETUM México, S.A. de C.V., por los servicios devengados durante 2020 se efectuaron pagos por 99,079.2 miles de pesos, y se determinó lo siguiente:

Antecedentes

El 29 de enero de 2019, la Secretaría de Relaciones Exteriores celebró el contrato número SRE-DRM-AD-01/19 y tres convenios modificatorios para la prestación del "Servicio para la Emisión del Pasaporte Mexicano en la Sección Consular de la Embajada, Consulados, Consulados sobre Ruedas y consulados Móviles de la Secretaría de Relaciones Exteriores en Estados Unidos de América y en las Delegaciones en Territorio Nacional", bajo el procedimiento de adjudicación directa, con vigencia del 15 de enero de 2019 al 15 de agosto de 2020.

El 28 de julio de 2020, la SRE suscribió el contrato abierto plurianual número SRE/DRM/LP-037/2020 para la prestación de los "Servicios Integrales de Apoyo para la Migración y Emisión del Pasaporte Mexicano Electrónico", con la empresa Grupo de Tecnología Cibernética, S.A. de C.V., en participación conjunta con otras ocho empresas, mediante la Licitación Pública Electrónica Internacional bajo la cobertura de Tratados de Libre Comercio No. LA-005000999-E14-2020, con vigencia del 14 de julio de 2020 al 13 de enero de 2026, por un monto máximo de 3,858,154.1 miles de pesos, para equipar todos los Puntos de Emisión de Pasaportes en México, Estados Unidos de América y el Resto del Mundo, emitiendo el pasaporte mexicano en sitio en Canadá, Reino Unido, España, Francia y Alemania, y se observó que durante el ejercicio 2020 no se efectuaron pagos.

Alcance de los servicios

El servicio se integró por cinco subpartidas las cuales son las siguientes:

- Subpartida 1. Servicio de emisión de pasaportes mexicanos: incluye el enrolamiento de datos biográficos, validación biométrica, verificación de identidad, digitalización del expediente, personalización de pasaportes y equipamiento (equipos de cómputo,

cámaras, escáner y lectores biométricos, impresoras, entre otros), en los puntos de emisión de pasaportes (PEP) de la Secretaría en México y en los Estados Unidos de América.

- Subpartida 2. Servicio de identificación de libretas mediante tecnología de radiofrecuencia (RFID): incluye el suministro de las etiquetas, así como el equipamiento para el grabado de datos en las etiquetas y dispositivos de lectura.
- Subpartida 3. Servicio de almacenamiento de datos local para los PEP: incluye el servicio local de archivos y su mantenimiento correctivo.
- Subpartida 4. Servicio de laminación de pasaportes: incluye el suministro de equipos de ensamble de lámina de seguridad y mantenimiento correctivo.
- Subpartida 5. Láminas de seguridad para pasaporte: consiste en el suministro de láminas de seguridad con las especificaciones y características requeridas por la secretaría.

Proceso de Contratación

En relación con el Estudio de Factibilidad, no se incluyeron los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad más adecuado para determinar la conveniencia de adquirir, arrendar o contratar servicios.

Revisión del cumplimiento técnico del contrato

La dependencia informó que para evitar duplicidades con el contrato número SRE/DRM/LP-037/2020, resultó necesario el apagado de los servicios de la subpartida 1 “Servicio de Emisión de Pasaportes Mexicanos” del contrato número SRE/DRM/AD-043/2020 a partir de octubre 2020, las subpartidas 2 a 5 continuaron prestando sus servicios debido a que no se duplicaban y permitían la emisión del pasaporte de lectura mecánica, el grupo auditor revisó la gestión de los servicios de la subpartida 1 y se observó lo siguiente:

Entregables del servicio

- No se establecieron los criterios ni formatos para el suministro de los entregables mensuales.
- En la revisión de los productos de agosto a noviembre de 2020, se identificó la falta del entregable “Informe donde se especifiquen por cada incidente, la causa, la solución aplicada, así como la duración de la misma” del Servicio de Enrolamiento de Datos Biográficos en los PEP en México; tampoco se suministró el entregable “Reporte de Trámites Redigitalizados” del Servicio de Enrolamiento y Validación Biométrica en los PEP en México.

- Respecto de los “Entregables del Equipamiento” de la subpartida 1, no se generó un entregable mensual que reporte los datos de identificación de cada equipo como número de serie, localización del equipo, altas, bajas, movimientos (sustitución de equipos) o cambios de lugar durante la prestación del servicio tanto para el territorio nacional como para los Estados Unidos de América; cabe señalar que para otras subpartidas si fueron generados los entregables del inventario de los equipos, como fue el caso del servidor local de archivos, así como para los equipos de ensamble en los PEP en México y los Estados Unidos de América.
- No se cuenta con un desglose de los precios unitarios de los componentes incluidos en las estaciones de enrolamiento biográfico y administración para el territorio nacional, por lo anterior, se desconoce el costo de cada equipo que conforma la estación de trabajo.
- No fueron generados los “Entregables del Equipamiento” para los consulados de los Estados Unidos de América, únicamente se entregaron para las oficinas en el territorio nacional.

Por lo anterior, se presume que se efectuaron pagos por servicios no prestados de los meses de agosto a diciembre de 2020, correspondientes a la subpartida 1 “Servicio de Emisión de Pasaportes Mexicanos” en los consulados de los Estados Unidos de América por 19,606.4 miles de pesos, debido a la carencia de los entregables descritos en el numeral C. “Equipamiento en los PEP de la Secretaría en México y en los Estados Unidos de América” y el Numeral J. “Entregable del equipamiento”, asimismo, tampoco se cuenta con un inventario mensual formalizado ni autorizado con los datos de identificación de cada equipo, en los PEP en Estados Unidos de América pagados por componente que sirva como constancia de la prestación de los servicios.

Gestión del inventario de equipos

Para la revisión del inventario de los equipos de la subpartida 1 en territorio nacional por parte del grupo auditor de la ASF, la dependencia entregó cuatro versiones distintas que no incluían todos los equipos, tenían números de serie duplicados o faltaban delegaciones, finalmente se entregó un inventario con un total 1,025 equipos de los cuales se revisó una muestra de 70 con el 90.0% de nivel de confianza y un margen de error del 10.0%, y se identificó lo siguiente:

- No se identificaron reemplazos de equipos en territorio nacional, tampoco se cuenta con evidencia del retiro de los equipos excepto la delegación Cuauhtémoc.
- No se proporcionaron los resguardos de los equipos en territorio nacional que provenían del contrato número SRE-DRM-AD-01/19 y se identificaron formatos de altas de equipos firmados por “el Consorcio”, sin embargo, el contrato número SRE/DRM/AD-043/2020 fue adjudicado a una sola empresa.

Por lo antes señalado, se identificaron áreas de oportunidad en el control de los inventarios de conformidad al numeral I. "Administración de los Equipos" del anexo técnico del contrato SRE/DRM/AD-043/2020, donde se estableció que el proveedor sería responsable del registro, control y resguardo de los equipos, incluyendo datos de identificación de cada equipo, localización, asignaciones, movimientos (reasignaciones) a partir de que se concluyera el proceso de instalación de los equipos.

Garantía de los equipos

- En relación con la garantía de 200 equipos de cómputo de escritorio modelo Prodesk 600 G1, se detectó que 192 (96.0%) estaban vencidas debido a que expiró entre el periodo 2017 a 2019.
- En el caso de las impresoras modelo M553DN, de un total de 121, equipos se identificó que 111 (91.7%) estaban vencidas debido a que la garantía expiró entre el periodo 2017 y los primeros meses de 2020.
- No se tienen evidencias de la validación previa a la contratación de la garantía de los equipos, cabe señalar que se desconoce si en las delegaciones existieron sustituciones de equipos, debido a que la secretaría no proporcionó información al respecto.

Pruebas de la infraestructura tecnológica

El grupo auditor revisó el cumplimiento de las características técnicas de los equipos y dispositivos de los contratos números SRE/DRM/AD-043/2020 y SRE/DRM/LP-037/2020, y se identificó lo siguiente:

Contrato número SRE/DRM/AD-043/2020

De un universo de 784 equipos, se seleccionó una muestra de 70 equipos con el 90% de nivel de confianza y un margen de error de 10%, que corresponden al total de equipos reportados para las delegaciones Tijuana, Cuauhtémoc y Estado de México, se constató mediante una verificación lo siguiente:

- No se realizaron las pruebas a los equipos de la muestra en las delegaciones Tijuana, Cuauhtémoc y Estado de México, debido a que la dependencia manifestó que fueron retirados del lugar y se procedió a la destrucción de los discos duros.
- Se carece de evidencia del acta de pase de salida de los equipos en Tijuana y el Estado de México, en el caso del Estado de México se proporcionó una relación de equipos que se iban a recolectar, en lo que respecta a Tijuana no se proporcionó documentación.

- Respecto a la delegación Cuauhtémoc, se proporcionó la relación de equipos que se iban a recolectar, así como el acta de pase de salida de los equipos, formalizada por “el Consorcio” en lugar de la empresa contratada en solitario.

Contrato número SRE/DRM/LP-037/2020

De un universo de 3,370 equipos, se seleccionó una muestra de 354 equipos con el 95% de nivel de confianza y margen de error de 5%, que corresponden a total de equipos que se reportaron para las delegaciones de Tijuana, Cuauhtémoc y Estado de México, se constató mediante una verificación lo siguiente:

- En cada una de las delegaciones de Tijuana, Cuauhtémoc y Estado de México se identificó una impresora térmica y una pantalla de turnos en sus cajas, que a la fecha no han sido instaladas aun cuando fueron entregadas desde noviembre de 2020.
- En la delegación Cuauhtémoc, se identificaron seis equipos backs y tres equipos de cómputo de escritorio empaquetados sin instalación.
- En la delegación Estado de México, se identificaron tres equipos backs empaquetados sin instalación, adicionalmente, se identificó un escáner de pasaporte con lectura electrónica que no estaba en operación.
- En las tres delegaciones se revisaron todas las cámaras, sin embargo, los números de serie no coincidieron con el inventario, de la misma manera, los números de serie de las impresoras de pasaportes P4000 SURYS tampoco coincidieron entre sí.
- En el inventario de equipos fueron identificados números de serie duplicados, asimismo, en la delegación Estado de México se detectó la sustitución de una computadora de escritorio que no se encontraba actualizada en dichos inventarios.

Software para realizar el monitoreo de los equipos y dispositivos de cómputo

El software para el monitoreo de la infraestructura tecnológica denominado “Aranda” no se encuentra en operación, el cual permitiría visualizar y configurar vía remota los componentes de los equipos y obtener varios reportes para el control del hardware, no se tiene definida una fecha para su puesta en marcha.

Mesa de Servicio

Se carece de encuestas de satisfacción a los usuarios, tal como lo establece el anexo técnico del contrato número SRE/DRM/AD-043/2020.

Borrado Seguro

- Se identificó que la secretaría no concluyó con el borrado seguro de los equipos de cómputo marca HP de los servicios de la subpartida 1, tanto en territorio nacional como en los Estados Unidos de América.
- Durante las pruebas del grupo auditor, se efectuó una consulta mediante una solución de monitoreo de seguridad a los equipos del contrato número SRE/DRM/AD-043/2020, como resultado se identificaron 38 equipos conectados aun cuando tenían que estar apagados desde octubre 2020 para evitar duplicidades con el contrato número SRE/DRM/LP-037/2020, dichos equipos no cuentan con el borrado seguro.

De lo anterior, se concluye que se tienen áreas de oportunidad en la gestión de inventarios y garantías de los equipos de cómputo y dispositivos que se usan para la emisión del pasaporte mexicano, así como en el borrado seguro de esos mismos equipos para proteger la confidencialidad de la información.

2020-0-05100-20-0013-01-005 Recomendación

Para que la Secretaría de Relaciones Exteriores fortalezca los mecanismos de control, manejo, evaluación, supervisión y validación de la gestión de inventarios de equipos de cómputo y dispositivos y verifique que se cuente con el soporte documental (entregables), garantías y movimientos (altas, bajas, cambios o retiro de equipos) que acrediten el detalle de los equipos pagados mensualmente, con la finalidad de mejorar la administración de la infraestructura tecnológica, así como optimizar el ejercicio del presupuesto de la secretaría en esta materia.

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.

2020-0-05100-20-0013-01-006 Recomendación

Para que la Secretaría de Relaciones Exteriores fortalezca los procedimientos y controles para la realización del borrado seguro en los equipos que son reemplazados, actualizados o retirados durante la gestión del inventario de la infraestructura tecnológica, con la finalidad de eliminar la información de manera segura para evitar su mal uso y que pone en riesgo la confidencialidad y privacidad de la información 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.

2020-0-05100-20-0013-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 19,606,422.50 pesos (diecinueve millones seiscientos seis mil cuatrocientos veintidós pesos 50/100 M.N.), por pagos efectuados por servicios no prestados de los meses de agosto a diciembre de 2020, correspondientes a la subpartida 1 "Servicio de Emisión de Pasaportes Mexicanos" en los consulados de los Estados Unidos de América, del anexo técnico del contrato número SRE/DRM/AD-043/2020, debido a la carencia de los entregables descritos en el numeral C. "Equipamiento en los PEP de la Secretaría en México y en los Estados Unidos de América" y el Numeral J. "Entregable del equipamiento", tampoco se cuenta con un inventario mensual formalizado ni autorizado con los datos de identificación de cada equipo, en los puntos de emisión de pasaportes en Estados Unidos de América pagados por componente que sirva como constancia de la prestación 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, segundo párrafo; de la Ley General de Responsabilidades Administrativas, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013, artículos 7, fracciones I y VI; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III, y del Anexo técnico del contrato número SRE/DRM/AD-043/2020, del numeral C. "Equipamiento en los PEP de la Secretaría en México y en los Estados Unidos de América" y del numeral J. "Entregable del Equipamiento".

Causa Raíz Probable de la Irregularidad

No existe monitoreo ni supervisión de los compromisos contractuales, tampoco de los lineamientos y disposiciones para el desarrollo de sistemas de información, aunado a una deficiente gestión de riesgos del organismo, lo que impidió que los servicios se prestaran en tiempo, forma y de acuerdo con el fin contratado.

5. Ciberseguridad

Se revisó la información proporcionada por la Secretaría de Relaciones Exteriores, 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.

El objetivo de la auditoría de seguridad cibernética es proporcionar a la dependencia una evaluación de la efectividad de la ciberdefensa, con un enfoque en las acciones fundamentales para asegurar el cumplimiento de los controles de seguridad críticos para una ciberdefensa eficaz de conformidad con las mejores prácticas. El programa de auditoría incluye los procesos de 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, relaciones con terceros y prácticas de gobernanza y gestión de las unidades administrativas y tecnologías de la información.

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 Falta de control (menos del 33.0%) y se observó lo siguiente:

SEMÁFORO DE CUMPLIMIENTO DE LOS CONTROLES DE CIBERSEGURIDAD EN LA SRE 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 Relaciones Exteriores.

INDICADOR: ● Aceptable ● Requiere fortalecer el control ● Falta de control

Las conclusiones de cada uno de los controles de seguridad críticos son las siguientes:

CSC Control 1: Inventario y control de activos de hardware

Se tienen áreas de oportunidad para cumplir con el objetivo 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 cumple con el objetivo de gestionar activamente todo el software en la red (inventario, seguimiento y corrección), con la finalidad de que sólo 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

Se tienen áreas de oportunidad para cumplir con el objetivo de establecer, implementar y gestionar activamente (rastrear, informar, corregir), la configuración de seguridad de dispositivos móviles, 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 cumple con el objetivo 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 cumple con el objetivo 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 cumple con el objetivo 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 cumple con el objetivo de minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.

CSC Control 8: Defensa contra software malicioso (malware)

Se cumple con el objetivo 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 cumple con el objetivo 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 cumple con el objetivo 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

Se tienen áreas de oportunidad para cumplir con el objetivo 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 cumple con el objetivo 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

Se tienen áreas de oportunidad para cumplir con el objetivo 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

No se cumple con el objetivo 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

Se cumple con el objetivo 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

No se cumple con el objetivo 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

Se cumple con el objetivo 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 a través de políticas, planificación organizacional, capacitación y programas de concientización.

CSC Control 18: Seguridad del Software de Aplicación

Se tienen áreas de oportunidad para cumplir con el objetivo 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

Se tienen áreas de oportunidad para cumplir con el objetivo de proteger la información de la organización, así como 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 cumple con el objetivo 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.

Se concluye que se tienen áreas de oportunidad para gestionar activamente todo el software en la red, en la configuración de privilegios administrativos en computadoras y aplicaciones, en el acceso a los activos críticos con base a una clasificación aprobada, en el monitoreo de cuentas, así como para probar la fortaleza general de la ciberdefensa de la dependencia.

2020-0-05100-20-0013-01-007 Recomendación

Para que la Secretaría de Relaciones Exteriores fortalezca las políticas y procedimientos para mejorar la gestión de la ciberseguridad en los controles de seguridad críticos siguientes: inventario y control de activos de software; uso controlado de privilegios administrativos; control de acceso basado en la necesidad de conocimiento; supervisión y monitoreo de

cuentas, así como en las pruebas de penetración a la infraestructura y soluciones tecnológicas; con la finalidad de gestionar activamente todo el software en la red, robustecer la configuración de privilegios administrativos en computadoras, redes y aplicaciones, asegurar el derecho a acceder a los activos críticos basado en una clasificación aprobada, minimizar las oportunidades de los atacantes con el monitoreo de cuentas, así como probar la fortaleza general de la ciberdefensa ante los ataques informáticos.

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

En el análisis de la información proporcionada por la Secretaría de Relaciones Exteriores, relacionada con la administración de los controles para la continuidad de las operaciones, vinculados con la infraestructura y soluciones tecnológicas, con base en las disposiciones y mejores prácticas en la materia, así como de conformidad con las políticas y lineamientos de la dependencia, se observó lo siguiente:

Gobierno y Gestión para la Continuidad de las Operaciones

- No se tienen procedimientos de activación/desactivación del plan de recuperación de desastres (DRP), para restablecer en forma inmediata las aplicaciones identificadas como críticas y en una segunda instancia, las aplicaciones de apoyo a la operación.
- No se cuenta con evidencia de las acciones del plan de recuperación de desastres, asimismo, se carece de los mecanismos de atención ante contingencias siguientes: procedimientos de respuesta y recuperación; tareas de resolución de un evento de interrupción; restablecimiento al estado anterior a la contingencia; mecanismos para resguardar el sitio alternativo (se carece de éste), y planes para la recuperación de los sistemas, así como el plan de concientización y capacitación para la ejecución del DRP.
- En relación con el Análisis de Impacto al Negocio (BIA) no se identificó la clasificación de los procesos por el posible impacto financiero, tampoco la definición del Punto de Recuperación Objetivo (RPO) para la pérdida tolerable de los datos.

Gestión de la capacidad de la infraestructura de TIC

- No se tiene un programa de capacidad, ni las métricas de seguimiento al mismo, que asegure la operación de los servicios de TIC conforme a los compromisos y niveles de servicio acordados durante su diseño.
- No se cuenta con procedimientos que regulen las actividades siguientes: monitoreo del rendimiento y la capacidad utilizada de la infraestructura de TIC; identificación y

análisis de los incidentes que se presentaron por falta de capacidad; verificación de tendencias de cargas de trabajo de los componentes de la infraestructura; acciones a realizar cuando la capacidad y rendimiento no estén en el nivel requerido; adicionar al plan de continuidad las características de capacidad y rendimiento de cada componente de la infraestructura de TIC.

- No se tiene la identificación de oportunidades para mejorar la capacidad de la arquitectura tecnológica en operación y realizar recomendaciones sobre los incidentes por falta de capacidad de la infraestructura de TIC.
- No se cuenta con un procedimiento para la definición, análisis, planificación, medición y mejoramiento de la disponibilidad de servicios de TIC.

Gestión de la continuidad de servicios de TIC

- No se identificó en el programa de continuidad que las situaciones de recuperación se encuentran alineadas con las necesidades prioritarias de la secretaría.
- No se tienen calendarios y resultados de las pruebas del Programa de Continuidad durante el ejercicio 2020.
- El análisis de riesgos no contempla las categorías de red de datos en sus escenarios (falla en dispositivos de seguridad, falla en la red de datos), ni la categoría de hardware en sus escenarios (falla en servidores, falla en NAS), por mencionar algunos.
- No se cuenta con evidencia para asegurar que los proveedores clave y socios externos cuentan con planes de continuidad alineados con las necesidades de la dependencia.
- No se tiene la asignación de roles y responsabilidades para la ejecución de las pruebas del plan de continuidad.

Habilidades y Competencias del Personal en la Continuidad de Operaciones

- No se cuenta con la definición de requisitos y planes de capacitación para las personas asociadas a la planeación de la continuidad, evaluaciones de impacto, evaluaciones de riesgo, así como para la comunicación y respuesta de incidentes.
- Se carece de evidencia del desarrollo de competencias basadas en capacitación práctica incluyendo la participación en ejercicios y pruebas.
- No se tiene retroalimentación para supervisar las habilidades y competencias del personal involucrado en la continuidad de operaciones.

Gestión de respaldos

El documento denominado “Procedimiento de respaldos” carece de elementos como carátula, objetivo, alcance, marco normativo, reglas Internas, glosario y definiciones.

Evaluaciones de la Continuidad de Operaciones

No se cuenta con la evaluación de la efectividad del plan de continuidad, ni el nivel de alineación entre el Plan de Continuidad de Negocio y el Plan de Recuperación de Desastres.

Se identificaron áreas de oportunidad en el diseño de las tareas para la recuperación de la operación; en el programa de capacidad de las soluciones e infraestructura tecnológica; en la gestión de la disponibilidad de los servicios, así como para fortalecer la ejecución de pruebas al plan de recuperación de desastres.

2020-0-05100-20-0013-01-008 Recomendación

Para que la Secretaría de Relaciones Exteriores fortalezca las políticas, procedimientos y controles para las actividades siguientes: atención ante contingencias; diseño de las tareas para la recuperación de la operación; operación del programa de capacidad de las soluciones e infraestructura tecnológica; análisis y medición de la disponibilidad de los servicios; asignación de roles y responsabilidades para la recuperación de los procesos, así como la ejecución de las pruebas al programa de continuidad de las operaciones, con la finalidad de asegurar la resiliencia operativa de los procesos críticos, aplicativos sustantivos e infraestructura tecnológica 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.

Montos por Aclarar

Se determinaron 22,295,480.15 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, 6 generaron:

8 Recomendaciones, 2 Promociones de Responsabilidad Administrativa Sancionatoria y 2 Pliegos de Observaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 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, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, la Secretaría de Relaciones Exteriores cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con el servicio para el desarrollo, actualización, mantenimiento y soporte de sistemas, se identificaron áreas de oportunidad para la aplicación de la metodología de desarrollo de soluciones tecnológicas y gestión de proyectos; asimismo, se presume que no fueron aplicadas penas convencionales por 2,689.1 miles de pesos derivadas de los retrasos del proyecto Jóvenes Construyendo el Futuro Honduras y el Salvador.
- En relación con los contratos para el desarrollo, actualización, mantenimiento y soporte de sistemas y, estrategia de seguridad de la información, se identificó que dos servidores públicos se ubicaron bajo una posible actuación de conflicto de interés, durante la aprobación de los entregables que forman parte del pago de los servicios.
- Respecto de los servicios integrales de transición de pasaporte en Estados Unidos de América y México, se tienen áreas de oportunidad para la gestión de inventarios y garantías de los equipos de cómputo que se usan para la emisión del pasaporte

mexicano, así como en el borrado seguro para eliminar datos con la finalidad de proteger la confidencialidad de la información; adicionalmente, fueron efectuados pagos por servicios no prestados de equipamiento (equipos de cómputo, cámaras, escáner y lectores biométricos, impresoras, entre otros), en los puntos de emisión del pasaporte en los Estados Unidos de América, debido a la falta de entregables e inventarios que sirven como constancia de la prestación de los servicios por 19,606.4 miles de pesos.

- En relación con los controles de ciberseguridad críticos, se detectaron áreas de oportunidad para gestionar activamente el software en la red, en la configuración de privilegios de los usuarios en computadoras y aplicaciones, en el acceso a los activos críticos con las debidas autorizaciones, así como para probar la fortaleza general de la ciberdefensa de la dependencia.
- Respecto de la continuidad de las operaciones, se debe fortalecer el diseño de las tareas para la recuperación de la operación; el programa de capacidad de las soluciones e infraestructura tecnológica; la gestión de la disponibilidad de los servicios, así como la ejecución de pruebas al plan de recuperación de desastres.

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; 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, 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 y 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) y las políticas de respaldos, replicación de datos, planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros.

Áreas Revisadas

Las direcciones generales de Tecnologías de Información e Innovación (DGTII) y Delegaciones (DGD, ahora Oficinas de Pasaportes), adscritas a la Unidad de Administración y Finanzas, así como la Dirección General de Servicios Consulares (DGSC), adscrita a la Jefatura de Unidad para América del Norte de la Secretaría de Relaciones Exteriores (SRE).

Disposiciones Jurídicas y Normativas Incumplidas

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

1. Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 1, segundo párrafo y artículo 45, quinto párrafo;
2. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 24 y 53;
3. Ley General de Responsabilidades Administrativas: última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2013, artículos 7, fracciones I, VI y IX, y 58;
4. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 23, fracción IV, artículo 28 y 66, fracciones I y III;
5. Otras disposiciones de carácter general, específico, estatal o municipal: 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 publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, artículo 13, fracción VII, 16, fracción III y 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, numeral 9 "Reglas generales", Proceso II.C Proceso de Administración de la Seguridad de la Información (ASI), Actividad ASI 6 "Integrar al SGSI los controles mínimos de seguridad de la información", Factor crítico 1, inciso e); Proceso II.A. Administración de Servicios (ADS), regla del proceso 2, Actividad ADS 2 "Diseñar los servicios de TIC", Factor

crítico 6, Actividad ADS 3 "Administrar la Capacidad de la Infraestructura de TIC", Factor crítico 1, inciso d), Factores críticos 4 y 6, Actividad ADS 4 "Administrar la continuidad de servicios de TIC", Factores críticos 3 y 4; Proceso II.B. Administración de la Configuración (ACNF), Actividad ACNF 1 "Establecer la cobertura y el alcance de la administración de la configuración", Factor crítico 1; Proceso III.B. Administración de Proveedores (APRO), Actividad APRO 1 "Generar lista de verificación de obligaciones", Factor crítico 2, Actividad APRO 2 "Monitorear el avance y desempeño del proveedor", Factor crítico 3, inciso a), Actividad APRO 3 "Apoyo para la verificación del cumplimiento de las obligaciones de los contratos", Factor crítico 1; III.C "Administración de la Operación" (AOP), Actividad AOP 1 "Establecer el mecanismo de operación y mantenimiento de los sistemas, aplicaciones, infraestructura y servicios de TIC", numerales 1 y 2 de los Objetivos Específicos y Factor crítico 3;

Estándar ISO 24762 "Directrices para los Servicios de Recuperación de Desastres de Tecnología de la Información y las Comunicaciones", Controles 5.8, 5.9 y 5.11;

Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT 2019), dominio "Entregar, dar Servicio y Soporte" (DSS), en sus prácticas DSS4.01 "Definir la política de continuidad del negocio, sus objetivos y alcance", actividades 3 y 4; DSS4.02 "Mantener la resiliencia del negocio", actividades 1, 6 y 7; DSS4.03 "Desarrollar e implementar una respuesta de continuidad del negocio", actividades 2, 4, 5, 6, 7 y 8; DSS4.04 "Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el "plan de respuesta ante desastres" (DRP), actividades 1, 2, 3, 4, 5 y 6; DSS4.06 "Realizar formación sobre el plan de continuidad", actividades 1, 2, 3 y 4; DSS4.07 "Administrar los acuerdos de respaldo", actividades 1 y 2; DSS4.08: "Realizar revisiones post-reanudación", actividades 1, 2 y 3;

Manual de Organización de la Dirección General de Tecnologías de Información e Innovación versión 4.0 con inicio de vigencia el 7 de septiembre de 2018, numeral 6 de la Subdirección de Presupuesto al Exterior, numeral 3 de la Dirección de Arquitectura de Sistemas, numeral 8, 10, de la Dirección de Ingeniería y Desarrollo de Aplicaciones, numeral 3 de la Dirección de Procesos de Aseguramiento de la Calidad;

Política General de Seguridad de la Información de la Secretaría de Relaciones Exteriores, numeral 6.9 Aspectos de seguridad de la información en la gestión de la continuidad del negocio, fracción II incisos 4, 5 y 6;

Proceso "ADS" Proceso de administración de servicios publicado por la Secretaría de Relaciones Exteriores el 01 de marzo de 2017, sección "Cronograma de Trabajo";

Código de conducta del personal de la SRE 2020, numeral 8 "Compromisos con el servidor público", inciso h, numeral 12 "Conflicto de Intereses";

Política de Borrado Seguro de la Secretaría de Relaciones Exteriores, Objetivo y numerales 4.1.1, 4.3.1, 4.3.2, 4.3.3, 4.3.4;

Contrato número SRE/DRM/AD-034/2020, cláusula Decima Sexta "Administración y Verificación";

Contrato número SRE-DRM-AD-22/19, cláusula Décima Primera "Penas convencionales y Deducciones al pago";

Anexo uno del contrato número SRE-DRM-AD-15/19, numeral "15. Entregables";

Anexo técnico del contrato número SRE/DRM/AD-034/2020, numeral "1.11 Entregables" y numeral 1.12, "Penas Convencionales y Deducciones al Pago", inciso "a";

Anexo técnico del contrato número SRE/DRM/AD-043/2020, numeral C. "Equipamiento en los PEP de la Secretaría en México y en los Estados Unidos de América", inciso d) Entregables del Servicio de Enrolamiento de Datos Biográficos en los PEP de la Secretaría en México, numeral 3 Entregables del Servicio de Enrolamiento Biométrico, numeral J. Entregables del equipamiento, numeral i. Reportes a Entregar por el Licitante Adjudicado;

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.