Caminos y Puentes Federales de Ingresos y Servicios Conexos

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-1-09J0U-20-1631-2021

1631-DE

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	158,281.3
Muestra Auditada	70,309.6
Representatividad de la Muestra	44.4%

El universo seleccionado por 158,281.3 miles de pesos corresponde al total de pagos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC), en el ejercicio fiscal de 2020; la muestra auditada está integrada por dos contratos para prestar los servicios de gestión de cobro del sistema de telepeaje en la red CAPUFE, con pagos por 70,309.6 miles de pesos, que representan el 44.4% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE) en 2020, relacionada con la ciberseguridad y continuidad de las operaciones.

Antecedentes

En la fiscalización de la Cuenta Pública de 2017, fueron identificadas inconsistencias en la gestión de los contratos y en el programa de continuidad de las operaciones, respecto de las cuales se promovieron y emitieron las acciones correspondientes, mismas que obran en el informe individual de la auditoría número 369-DE “Auditoría de TIC”.

Entre 2016 y 2020, CAPUFE ha erogado 1,038,518.6 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

RECURSOS EROGADOS EN MATERIA DE TIC EN LOS ÚLTIMOS CINCO AÑOS EN CAPUFE

(Miles de Pesos)

Periodo del gasto	2016	2017	2018	2019	2020	Total
Monto por año	197,338.3	280,136.9	276,673.0	121,093.0	163,277.3	1,038,518.6

FUENTE: Elaborado con información proporcionada por CAPUFE.

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 la función de las TIC sujetas de revisión y determinar el alcance, naturaleza y muestra de la revisión del cual, se obtuvieron los resultados que se presentan en este informe.

Resultados

1. Análisis Presupuestal

Mediante el oficio número 307-A.-3510 del 26 de diciembre de 2019, el subsecretario de egresos de la Secretaría de Hacienda y Crédito Público comunicó el presupuesto de egresos de la federación y calendarios para el ejercicio fiscal de 2020, a su vez, por medio del oficio circular número 5.1.103.-0057 del 30 de diciembre de 2019, el titular de la unidad de administración y finanzas de la Secretaría de Comunicaciones y Transportes comunicó a los responsables de la administración y finanzas de Caminos y Puentes Federales de Ingresos y Servicios Conexos la autorización para los capítulos 2000 y 3000 de un presupuesto por 975,448.3 miles de pesos.

En el análisis de la información presentada en el estado analítico del ejercicio del presupuesto de egresos del año 2020, se concluyó que CAPUFE tuvo un presupuesto pagado de 523,779.1 miles de pesos en los capítulos 2000 y 3000, asimismo, reportó un presupuesto por ejercer por 376,669.3 miles de pesos; en relación con el presupuesto pagado, los recursos relacionados con las TIC corresponden a 163,277.3 miles de pesos, lo que representa el 31.2% del presupuesto, como se muestra a continuación:

RECURSOS PAGADOS EN CAPUFE EN LOS CAPÍTULOS 2000 Y 3000 DURANTE 2020

(Miles de pesos)

Capítulo	Descripción	Presupuesto Pagado	Recursos pagados en TIC
2000	Materiales y suministros	20,128.3	1,875.6
3000	Servicios generales	503,650.8	161,401.7
	TOTAL	**523,779.1**	**163,277.3**

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

Los recursos pagados en materia de las TIC por 163,277.3 miles de pesos, se integran de la manera siguiente:

GASTOS EN TIC EN EL EJERCICIO DE 2020 EN CAPUFE
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Pagado
2000		**MATERIALES Y SUMINISTROS**	**1,875.6**
3000		**SERVICIOS GENERALES**	**161,401.7**
	31401	Servicio telefónico convencional	470.9
	31501	Servicio de telefonía celular	39.6
	31601	Servicio de radiolocalización	70.0
	31602	Servicios de telecomunicaciones	3,064.8
	31603	Servicios de internet	983.7
	31701	Servicios de conducción de señales analógicas y digitales	17,680.7
	31904	Servicios integrales de infraestructura de cómputo	18,369.1
	32301	Arrendamiento de equipo y bienes informáticos	6,026.6
	32701	Patentes, derechos de autor, regalías y otros	7,707.4
	33104	Otras asesorías para la operación de programas	1,633.6
	33606	Servicios de digitalización	245.0
	33903	Servicios integrales	70,740.1
	35301	Mantenimiento y conservación de bienes informáticos	34,370.2
		TOTAL	**163,277.3**

FUENTE: Elaborado con información proporcionada por CAPUFE.

Del universo seleccionado en 2020 por 158,281.3 miles de pesos que corresponden al total de pagos en contratos relacionados con las TIC, se erogaron 70,309.6 miles de pesos en dos contratos que representan el 44.4% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS PAGADOS DURANTE 2020

(Miles de pesos)

Procedimiento de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia Del	Vigencia Al	Monto Mínimo	Monto Máximo	Pagado
Adjudicación Directa	4500028970	Gestión Tecnológica de Autopistas, S.A. de C.V.	Servicios de gestión de cobro del Sistema de Telepeaje en la Red CAPUFE	19/09/2019	31/07/2020	14,974.0	78,103.3	51,384.2
	CM 5500009624		Incrementar el monto mínimo y máximo, así como la vigencia	19/09/2019	30/09/2020	2,873.8	15,019.90	
	Subtotal					17,817.80	93,123.20	51,384.2
Adjudicación Directa	4500030031	Gestión Tecnológica de Autopistas, S.A. de C.V.	Servicios de gestión de cobro del Sistema de Telepeaje en la Red CAPUFE	01/10/2020	21/12/2020	10,673.10	22,104.60	18,925.4
	Total sin impuestos ni retenciones					**28,490.9**	**115,227.8**	**70,309.6**

FUENTE: Elaborado con información proporcionada por CAPUFE.

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

2. Contratos números 4500028970 y 4500030031 "Servicios de gestión de cobro del sistema de telepeaje para la red propia de CAPUFE"

Se analizó la información del contrato número 4500028970 suscrito con Gestión Tecnológica de Autopistas, S.A. de C.V., mediante adjudicación directa con fundamento en los artículos 26, fracción III, 28, fracción I, 40, 41, fracciones II y V, y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, vigente del 19 de septiembre de 2019 al 31 de julio 2020, por un monto mínimo de 14,974.0 miles de pesos y máximo de 78,103.3 miles de pesos, con el objeto de prestar los "Servicios de gestión de cobro del sistema de telepeaje para la red propia de Caminos y Puentes Federales de Ingresos y Servicios Conexos", asimismo, se suscribió el convenio modificatorio número 5500009624 con el objeto de incrementar el monto mínimo en 2,873.8 miles de pesos y máximo por 15,019.9 miles de pesos, así como ampliar la vigencia al 30 de septiembre de 2020, con presupuesto del ejercicio 2020 se efectuaron pagos por 51,384.2 miles de pesos más los impuestos y retenciones correspondientes. Adicionalmente, se analizó el contrato número 4500030031 suscrito con el mismo proveedor y para el mismo objeto, vigente del 1º de octubre al 21 de diciembre de 2020, por un monto mínimo de 10,673.1 miles de pesos y máximo de 22,104.6 miles de pesos, durante el ejercicio de 2020 se pagaron 18,925.4 miles de pesos más los impuestos y retenciones correspondientes, y se determinó lo siguiente:

Alcance del servicio

La prestación del servicio de administración de la gestión de cobro del sistema de telepeaje que incluye la administración y gestión de listas, la facturación y cobranza, los informes de cierre, la contratación de usuarios para el sistema de telepeaje, la contratación de personal para la prestación de los servicios, la capacitación de su personal, así como la adquisición de los equipos, bienes o aplicativos que el proveedor requiera para la prestación de los servicios; adicionalmente, el suministro y distribución de TAG (etiqueta de peaje) con un costo de activación con cargo al usuario y en favor del proveedor.

Antecedentes

El 14 de mayo de 2014, se formalizó el contrato de prestación de servicios número 4500021486 CAPUFE, 4500021493 FNI Y CTO. GOLFO 008/14 GOLFO CENTRO al consorcio denominado Telepeaje Dinámico, S.A. de C.V. (TEDISA) con vigencia al 31 de julio de 2018. Como resultado del convenio marco de interoperabilidad para la gestión de autopistas y los convenios bilaterales de interoperabilidad emanados de éstos, se suscitaron diversos desacuerdos entre CAPUFE y TEDISA, por lo que el 31 de julio de 2015 CAPUFE solicitó a la Secretaría de la Función Pública (SFP) iniciar el procedimiento administrativo de conciliación con TEDISA radicado en el expediente número 189/2015 de la SFP.

Como resultado del procedimiento administrativo de conciliación, el 14 de junio de 2016, CAPUFE y TEDISA celebraron el primer convenio modificatorio con los números 5500007311 CAPUFE, 5500007312 FONADIN y CTO GOLFO 005-16 GOLFO CENTRO, cuyo objeto fue la modificación de diversas cláusulas, anexos del modelo de operación, contraprestación,

estándares de servicio, penalizaciones e interoperabilidad, posteriormente fueron firmados tres convenios modificatorios adicionales para la operación del servicio.

El 20 de junio de 2019 se celebró el contrato número 4500028789 con vigencia a partir del 7 de junio de 2019, mediante adjudicación directa a las empresas Impulsora de Servicios Terrestres, S.A. de C.V., y Gestión Tecnológica de Autopistas, S.A. de C.V. (la primera parte del grupo TEDISA), para tener un operador para la red propia de CAPUFE, asimismo, se celebró el primer convenio modificatorio para ampliar el monto máximo en un 5.5% así como un segundo convenio modificatorio para ampliar la vigencia del contrato al 18 de septiembre de 2019.

Proceso de Contratación

El grupo auditor revisó la documentación relacionada con el procedimiento de contratación e identificó lo siguiente:

Investigación de Mercado del Contrato número 4500030031

- La solicitud de cotización para participar en la investigación de mercado fue enviada a 12 empresas, de las cuales respondieron cinco y tres de ellas declinaron su participación, en el caso de la empresa Acciona Ingeniería y Desarrollo Empresarial, S.A. de C.V. (AIDE), manifestó que requería de un plazo de 30 días para llevar a cabo la transición del servicio, asimismo, señaló que no contaba con la acreditación de producción de bienes registrada en el Instituto Mexicano de la Propiedad Industrial, tampoco contaba con personal con discapacidad cuando menos al 5.0% de su planta de empleados, no tenía experiencia de operar algún sistema de telepeaje en otro país, ni la certificación de haber aplicado políticas de igualdad de género; la propuesta económica presentada por AIDE fue conforme a las condiciones solicitadas por CAPUFE.

- Por su parte, la empresa Gestión Tecnológica de Autopistas, S.A. de C.V. (GTA), indicó que el tiempo para iniciar con la prestación del servicio hacía materialmente imposible enfrentar el reto en las condiciones planteadas, asimismo, manifestó que no contaba con un certificado de calidad, no tenía experiencia de operar algún sistema de telepeaje en otro país, no tenía constancias de liberación de garantías de cumplimiento de contratos, tampoco contaba con personal con discapacidad cuando menos al 5.0% de su planta de empleados, ni con la certificación de haber aplicado políticas de igualdad de género; la propuesta económica presentada por GTA no cumplió con las condiciones solicitadas por CAPUFE.

- Por otra parte, en virtud de que el área encargada de la elaboración de la investigación de mercado no tuvo las condiciones para la comparación de las propuestas, efectuó un análisis con base en los precios establecidos en el contrato que se encontraba vigente, por lo anterior, no se realizó una comparativa objetiva debido a que los precios y conceptos que utilizó CAPUFE son distintos entre las empresas AIDE y GTA.

Estudio de factibilidad de los contratos números 4500028970 y 4500030031

Se carece del estudio de factibilidad aun cuando el Órgano Interno de Control en CAPUFE hizo la sugerencia de solicitar la aprobación del procedimiento a la Unidad de Gobierno Digital de la SFP.

Justificación del procedimiento de contratación de los contratos números 4500028970 y 4500030031

- A principios del año 2020, la Dirección General de CAPUFE, en conjunto con las direcciones de Administración y Finanzas y Operación, plantearon la estrategia de dividir el proyecto en dos partes, la primera consistía en la contraprestación de un nuevo operador para mantener la continuidad del sistema de telepeaje de la red propia, la segunda se trataba de convertir a CAPUFE en operador de Telepeaje.

- Como resultado de las investigaciones de mercado, se realizó una modificación al modelo de operación, *"con la intención de que los operadores de telepeaje que señalaron no podían cumplir con los requisitos planteados en la investigación de mercado pudieran participar"*, sin embargo, ningún ofertante podía cumplir con las condiciones establecidas.

- El grupo auditor identificó que no se respetaron las condiciones de la solicitud de cotización presentada por CAPUFE, por tal motivo realizó un comparativo entre las propuestas económicas del contrato precedente número 4500028970 con el nuevo contrato número 4500030031 adjudicado de manera directa a GTA, y se identificó que para los servicios de cobro del sistema de telepeaje en red CAPUFE la forma de pago fue diferente, siendo que en el contrato precedente se cobró de manera mensual por cada cruce en caseta de cobro, en contraste, el nuevo contrato estableció una cuota mensual fija de un cruce hasta 490,000 y, en caso de un mayor número de cruces se pagaría una contraprestación progresiva de manera adicional.

Por lo anterior, se pagaron en exceso 3,223.2 miles de pesos conformados por seis facturas y tres notas de crédito de la contraprestación de servicios de cobro del sistema de telepeaje en red CAPUFE del contrato número 4500030031, sin justificar el aumento por la prestación de los servicios que fueron realizados bajo las mismas condiciones técnicas y administrativas estipuladas en el contrato anterior número 4500028970, con el mismo proveedor y sin respetar las condiciones de la solicitud de cotización establecidas por CAPUFE.

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; 7, fracciones I y VI, de la Ley General de Responsabilidades Administrativas; 26, párrafo séptimo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 30, párrafo primero, y 81, fracción IV, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; y el Contrato número 4500030031, cláusula 16, párrafo segundo.

Revisión del cumplimiento técnico, funcional y administrativo

El grupo auditor revisó la información relativa al cumplimiento de los contratos y anexos correspondientes e identificó lo siguiente:

Actividades generales

- No se cuenta con el inventario del equipamiento instalado en las plazas y carriles de la red CAPUFE ni del equipo en el centro de operación de telepeaje.

- No se tiene la relación del personal que prestó el servicio con sus datos de oficina, teléfonos, celulares ni correos electrónicos.

- Respecto a los aplicativos de soporte para el funcionamiento del sistema de telepeaje, no se cuenta con registros de su uso ni se entregaron a la finalización de los contratos.

- No se tiene evidencia del cumplimiento del estándar "TIER III de Uptime Institute" por parte del centro de operación del proveedor, ni de las bitácoras de los servicios de mantenimiento prestados durante la vigencia del contrato.

- No se proporcionó evidencia de los respaldos de información ni de los controles para mitigar la fuga de información.

- No se cuenta con reportes de monitoreo de disponibilidad de las conexiones de las plazas de cobro a la central de telepeaje para confirmar su operación.

Interoperabilidad

- El proveedor no entregó el *back office* (gestión empresarial), el inventario de los equipos, las bitácoras del servicio ni las bases de datos para la continuidad de la operación.

- No se dieron a conocer a CAPUFE los términos del mantenimiento y administración de las cuentas de usuarios en interoperabilidad.

- No se cuenta con la herramienta de servicio al cliente, ni con los registros históricos de las solicitudes presentadas por los usuarios con información como cuenta, número de registro, solicitud presentada y resultado del trámite, entre otros.

- No se tiene evidencia del envío y recepción de las listas totales, listas incrementales ni transacciones.

- Se carece de los requisitos mínimos de comprobación de las cédulas de certificación de aforo interoperable con sus archivos de transacciones de interoperabilidad (cruces efectuados por usuarios de CAPUFE en autopistas a cargo de los operadores de interoperabilidad y viceversa).

- CAPUFE informó que, debido a la falta de información señalada en los puntos anteriores, no fue posible validar las conciliaciones del ejercicio de 2020, lo que pudiera tener afectación en los ingresos.

Actividades para el cierre del contrato

- No se rindió un informe en forma impresa y en medio electrónico con la integración de la cartera vencida por usuario y tramo carretero, de los fondos en garantía por usuario, de los saldos de prepago, de las aclaraciones en proceso de atención, de los depósitos de la cobranza pendientes de dispersar por tramo, así como de las facturas expedidas en el último mes para efectos de control.

- No se tiene evidencia de la entrega de las plazas de cobro con las claves de acceso y configuraciones, ni de la entrega de los procesos ejecutados en el *back office* tanto de la operación del sistema de telepeaje como del servicio de gestión de cobro.

- No se realizó la entrega formal de la migración de las bases de datos ni del borrado seguro de la información.

- El proveedor dejó un servidor sin claves de acceso, por lo que no fue posible verificar la información que se encuentra en éste.

- No se ha realizado el proceso de liberación y cancelación de las pólizas de fianza a favor de CAPUFE.

Aclaraciones de la entidad fiscalizada respecto a los resultados finales del grupo auditor

- El 14 de enero de 2022, el organismo remitió las "Cédula de Transacciones recibidas por Operador …" de los meses de enero a diciembre del ejercicio 2020, firmadas por el Director Técnico y de Operación de GTA, del cual no se establece su participación en el contrato, asimismo, las cédulas no se encuentran firmadas por los demás operadores de Telepeaje (I+D, PINFRA, CAMS, CEP-SICE y OHL) ni cuentan con el archivo electrónico con el detalle de cruces, lo anterior, no permite verificar que los aforos e ingresos en dichas cédulas fueron los operados durante el periodo reportado.

- Cabe señalar que la cláusula 12.1 "Pruebas o Verificación" de los contratos números 4500028970 y 4500030031, estipula que el organismo *"verificará que la prestación de los servicios se realice conforme a lo solicitado en el presente contrato y anexos que lo acompañan. Las verificaciones se realizarán de forma aleatoria, sin necesidad de establecer un programa previo o temporalidad determinado"*, no obstante, las cédulas entregadas no se acompañan de ninguna verificación por parte de CAPUFE.

- Adicionalmente, de conformidad con el Anexo 1.1 "Interoperabilidad", apartado "Facturación" de los contratos números 4500028970 y 4500030031, se establece lo siguiente:

" …

Cuando sea el caso, el Operador de Telepeaje deberá emitir y enviar a los operadores de Telepeaje en Interoperabilidad que suscriban el Convenio Marco de Interoperabilidad o los Convenios Bilaterales la factura correspondiente por los cruces correspondientes, la cual deberá cumplir con todos los requisitos fiscales y el soporte documental mínimo que se describe a continuación:

- Archivo en electrónico con el detalle de los cruces del período respectivo.

[…]

De igual forma, los Operadores de Telepeaje en interoperabilidad deberán emitir y enviar al Operador de Telepeaje la factura correspondiente por los cruces correspondientes, la cual deberá cumplir con todos los requisitos fiscales y el soporte documental mínimo que se describe a continuación:

-Factura firmada por el Director de Administración y Finanzas del Operador de Telepeaje o personal autorizado por el representante legal.

-Cédula de verificación del Operador de Telepeaje con el Operador de Telepeaje en interoperabilidad firmada por ambos operadores.

-Archivo en electrónico con el detalle de cruces del período respectivo.

…"

Por lo anterior, la entidad fiscalizada no contó con el soporte documental mínimo que permitiera verificar la cédula de certificación de aforo interoperable, por lo tanto, se efectuaron pagos de enero a diciembre de 2020 por 43,381.6 miles de pesos, correspondientes a la contraprestación de la gestión de cobro de telepeaje de los usuarios en las redes interoperables, lo que incluye caminos, puentes, tramos, vialidades urbanas y autopistas donde exista interoperabilidad del telepeaje, incluso aquellas realizadas en la red de autopistas concesionadas al Fondo Nacional de Infraestructura o la entidad que lo sustituya de los contratos números 4500028970 y 4500030031, sin que se comprobara que los servicios fueron prestados de conformidad con lo establecido en los contratos señalados y su Anexo 1.1 "Interoperabilidad", apartado "Facturación"; adicionalmente, no se realizó el cierre de las actividades del contrato para contar con toda la información de los trabajos realizados.

Lo anterior incumplió los artículos 1o, segundo párrafo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 7 fracciones I y VI de la Ley General de Responsabilidades Administrativas; 66, fracciones I y III del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria; 12.1 "Pruebas o Verificación" de los contratos números 4500028970 y 4500030031; los Anexos 1.1 "Interoperabilidad", apartado "Facturación" de los contratos números 4500028970 y 4500030031; la Cláusula 3.6 "Centro de operación de

Telepeaje", 4 inciso C de los contratos números 4500028970 y 4500030031; y el Anexo 1.5 "Procedimientos, información y documentación para el cierre del contrato" de los contratos números 4500028970 y 4500030031.

Se concluye que no se realizó una comparación objetiva de las propuestas de los proveedores debido a que los precios y conceptos utilizados en la investigación de mercado fueron distintos entre las empresas participantes; se pagaron en exceso 3,223.2 miles de pesos por servicios de cobro del sistema de telepeaje sin justificar el aumento de precio de los servicios realizados bajo las mismas condiciones técnicas y administrativas del contrato precedente, con el mismo proveedor y sin respetar las condiciones de la solicitud de cotización de CAPUFE; se efectuaron pagos por 43,381.6 miles de pesos por la gestión de cobro de telepeaje de los usuarios en las redes interoperables, sin cumplir con los requisitos mínimos para la comprobación de la cédula de certificación de aforo interoperable para constatar la prestación de los servicios; asimismo, no se realizó el cierre de las actividades del contrato para contar con toda la información de los trabajos realizados, comprobar que se cumplió con los planes de trabajo, así como liberar los recursos para emprender nuevos servicios.

2020-1-09J0U-20-1631-01-001 **Recomendación**

Para que Caminos y Puentes Federales de Ingresos y Servicios Conexos fortalezca los procedimientos, controles y verificaciones en las contrataciones con componentes relacionados con las tecnologías de información y comunicaciones, para mejorar la evaluación de las propuestas técnicas y económicas de los proveedores participantes, vigilar que se cumplan las condiciones establecidas para la operación y optimización de los contratos, así como supervisar que se ejecuten las actividades de cierre para la entrega de los servicios; con la finalidad de obtener las mejores condiciones económicas y técnicas para la prestación de los servicios, así como comprobar que los planes de trabajo se realizaron para la obtención de los beneficios esperados de los contratos en beneficio del organismo.

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.

2020-1-09J0U-20-1631-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal o al patrimonio de Caminos y Puentes Federales de Ingresos y Servicios Conexos por un monto de 3,223,159.67 pesos (tres millones doscientos veintitrés mil ciento cincuenta y nueve pesos 67/100 M.N.), por los pagos en exceso de la contraprestación de servicios de cobro del sistema de telepeaje en red CAPUFE del contrato número 4500030031, sin justificar el aumento de precios por la prestación de los servicios que se realizaron bajo las mismas condiciones técnicas y administrativas del contrato precedente número 4500028970 que tuvo el mismo objeto y proveedor, además de que no se respetaron las condiciones de la solicitud de cotización establecidas por el organismo público para la contratación, 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 26, párrafo séptimo; de la Ley General de Responsabilidades Administrativas, artículo 7, fracciones I y VI; del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículos 30, párrafo primero, y 81, fracción IV; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III; y del Contrato número 4500030031, cláusula 16, párrafo segundo.

Causa Raíz Probable de la Irregularidad

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

2020-1-09J0U-20-1631-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal o al patrimonio de Caminos y Puentes Federales de Ingresos y Servicios Conexos por un monto de 43,381,626.54 pesos (cuarenta y tres millones trescientos ochenta y un mil seiscientos veintiséis pesos 54/100 M.N.), por los pagos de la contraprestación de la gestión de cobro de telepeaje de los usuarios en las redes interoperables, lo que incluye caminos, puentes, tramos, vialidades urbanas y autopistas donde exista interoperabilidad del telepeaje, incluso aquellas realizadas en la red de autopistas concesionadas al Fondo Nacional de Infraestructura o la entidad que lo sustituya, correspondientes a los contratos números 4500028970 y 4500030031, los cuales se realizaron sin contar con el soporte documental mínimo comprobatorio para verificar la cédula de certificación de aforo interoperable y constatar que los servicios se prestaron de conformidad con lo establecido en los contratos y su anexo 1.1 "Interoperabilidad", apartado "Facturación", adicionalmente, no se realizó el cierre de las actividades del contrato para contar con toda la información de los trabajos realizados, 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, artículo 7, fracciones I y VI; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 66, fracciones I y III; de la Cláusula 12.1 "Pruebas o Verificación" de los contratos números 4500028970 y 4500030031; Anexos 1.1 "Interoperabilidad", apartado "Facturación" de los contratos números 4500028970 y 4500030031; de la Cláusula 3.6 "Centro de operación de Telepeaje", 4 inciso c) de los contratos números 4500028970 y 4500030031; y del Anexo 1.5 "Procedimientos, información y documentación para el cierre del contrato" de los contratos números 4500028970 y 4500030031.

Causa Raíz Probable de la Irregularidad

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

3. Ciberseguridad

Se revisó la información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos 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 del organismo público en esta materia.

La revisión tiene por objeto proporcionar al organismo público una evaluación de la efectividad de la ciberdefensa con referencia a los controles críticos del Centro de Seguridad de Internet (CIS), 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.

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, en el caso del nivel “Aceptable” (más del 67.0%) se encontraron dos, que “Requiere fortalecer el control” (entre el 33.0% y 67.0%) se identificaron siete, y los relacionados con “Carencia de control” (menos del 33.0%) fueron 11, de acuerdo con lo siguiente:

SEMÁFORO DE CUMPLIMIENTO DE LOS CONTROLES DE CIBERSEGURIDAD EN CAPUFE DURANTE EL EJERCICIO 2020

Control	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2020																				

Aceptable
Requiere fortalecer el control
Carencia de control

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

Los hallazgos más relevantes de cada uno de los controles de seguridad críticos son los siguientes:

CSC Control 1: Inventario y control de activos de hardware

EVALUACIÓN DEL CONTROL 1 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario y control de activos de hardware	8	5	2	1	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se cuenta con una herramienta que permita actualizar el inventario de activos de hardware para identificar de manera automática los dispositivos conectados.

- No se proporcionó evidencia de los escaneos realizados en las redes, a fin de corroborar el bloqueo de los dispositivos no autorizados.

- No se cuenta con herramientas para obtener la dirección MAC (Control de acceso a medios) de los equipos de forma automatizada, tampoco se proporcionó evidencia de la conciliación con el inventario de activos.

- Se carece de controles de acceso a nivel de puerto para que los dispositivos puedan autenticarse en la red, asimismo, no se cuenta con un procedimiento para detectar que los dispositivos tienen un acceso autorizado y vigente.

Por lo anterior, no se cumple en su totalidad 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

EVALUACIÓN DEL CONTROL 2 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Inventario y control de activos de software	**10**	5	4	1	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- El sistema de inventarios de los desarrollos de aplicativos no incluye los sistemas operativos de los servidores que soportan a la infraestructura tecnológica.

- No se proporcionó evidencia de la eliminación del software no autorizado, tampoco hay restricciones para la instalación de software libre en los equipos.

- Se carece de una solución para la detección y bloqueo del software no autorizado en los equipos de cómputo y servidores del organismo.

- No se tienen listas blancas de aplicaciones para asegurar que sólo se ejecuta software autorizado y que todo el software no autorizado está bloqueado.

- No se cuenta con políticas que definan las actividades y tiempos para la desinstalación del software no autorizado que se encuentre en la infraestructura tecnológica.

Por lo antes señalado, no se cumple en su totalidad 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

EVALUACIÓN DEL CONTROL 3 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	**5**	3	2	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se proporcionó evidencia de la implementación de estándares de configuración de seguridad del directorio activo para los sistemas operativos diferentes a Windows.

- Se carece de un catálogo de plantillas para bases de datos y aplicaciones de los servidores, estaciones de trabajo, equipos portátiles y dispositivos móviles.

- No se cuenta con una herramienta para la gestión de la configuración de los sistemas ni con un sistema de vigilancia SCAP (protocolo de automatización de contenido de seguridad) para los sistemas operativos, bases de datos y aplicaciones.

- No se proporcionó evidencia para corroborar que la infraestructura tecnológica que soporta a los aplicativos del organismo se encuentra parametrizada a partir de una configuración de seguridad base.

- Se identificaron 20 conmutadores de comunicaciones de acceso a las redes, sin actualizaciones debido a la falta de un contrato de mantenimiento.

- Se carece de un histórico de los cambios realizados en los sistemas operativos, bases de datos, equipos de cómputo y equipos de seguridad perimetral.

- No se cuenta con mecanismos de control para identificar y aislar el software con comportamiento anómalo de los equipos de cómputo y dispositivos móviles.

- En relación con los cambios en los registros del sistema (REGEDIT), no se cuenta con mecanismos de control para evitar actualizaciones de usuarios no autorizados.

Por lo anterior, no se cumple en su totalidad con el objeto 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

EVALUACIÓN DEL CONTROL 4 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Evaluación continua de la vulnerabilidad y solución	**7**	4	3	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- Se carece de la definición de los niveles de protección de la información y las conexiones permitidas para los dispositivos de los usuarios finales en la política para el acceso a la infraestructura mediante cuentas VPN (red virtual privada).

- No se cuenta con el procedimiento para establecer los roles, responsabilidades y tiempos para la eliminación o mitigación de las vulnerabilidades identificadas.

- No se cuenta con una herramienta automatizada para la gestión de actualizaciones de seguridad (parches), tampoco se tienen definidos los roles, responsables ni tiempos para el mantenimiento de dichas actualizaciones.

- Se tienen identificados parches críticos que no han sido actualizados debido a la falta de soporte por parte del proveedor, tampoco se cuenta con un plan para remediar los riesgos.

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

CSC Control 5: Uso controlado de privilegios administrativos

EVALUACIÓN DEL CONTROL 5 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Uso controlado de privilegios administrativos	**9**	8	1	0	

FUENTE**:** Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se cuenta con una herramienta automatizada para el inventario de las cuentas administrativas.

- No se tiene una herramienta de autenticación de múltiples factores para las cuentas de administrador en los sistemas operativos, base de datos y aplicaciones.

- No se proporcionó evidencia de las restricciones de acceso a las herramientas de scripting (secuencia de comandos) como powershell, python, entre otras.

- Las cuentas con privilegios de administración no utilizan un equipo dedicado, tampoco se tiene control sobre las bitácoras de auditoría para alertar sobre actividades sospechosas en el registro o los intentos fallidos de cuentas con altos privilegios.

- Se carece de una herramienta para registrar y alertar sobre los cambios en los grupos administrativos relacionados con el mantenimiento de las cuentas.

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

EVALUACIÓN DEL CONTROL 6 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Mantenimiento, monitoreo y análisis de bitácoras de auditoría	**8**	4	4	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se proporcionó evidencia del seguimiento y remediación de los eventos detectados por la herramienta de gestión de la información y eventos de seguridad durante el ejercicio de 2020.

- No se cuenta con una herramienta para el monitoreo y notificación de los inicios de sesión en los servidores de la red institucional.

- No se tienen reportes de las irregularidades detectadas en las bitácoras de los sistemas críticos.

Por lo antes señalado, no se cumple en su totalidad 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

EVALUACIÓN DEL CONTROL 7 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de correo electrónico y navegador web	**10**	-	6	4	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

Por lo anterior, se cumple con el objeto 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)

EVALUACIÓN DEL CONTROL 8 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Defensa contra software malicioso (malware)	**8**	4	3	1	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se cuenta con una administración centralizada de la herramienta antimalware.
- Los servidores con sistema operativo de código abierto no cuentan con herramientas de protección contra virus ni amenazas.
- Se carece de un catálogo institucional de código malicioso para prevenir su acceso a las redes.
- No se cuenta con herramientas sandboxing (para detectar ataques de malware y bloquearlos antes de que entren en la red), el análisis de las amenazas se ejecuta a través de los motores de seguridad de los fabricantes.

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

EVALUACIÓN DEL CONTROL 9 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Limitación y control de puertos de red, protocolos y servicios	**5**	1	-	4	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

Por lo anterior, se cumple con el objeto de administrar (rastrear, controlar, 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

EVALUACIÓN DEL CONTROL 10 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Capacidad de recuperación de datos	**5**	4	1	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se respalda la totalidad de los servidores críticos con el sistema completo, con el riesgo de perder información ante alguna contingencia.

- No se proporcionaron las evidencias de las actividades realizadas para asegurar la protección de seguridad de la rotación de los medios de almacenamiento, las copias de seguridad en sitio, remotas de sitios alternos y servicios en la nube, tampoco se tiene evidencia de la protección de los discos duros de la librería virtual.

- No se tiene evidencia de las pruebas de las copias de seguridad de todos los sistemas y bases de datos críticas del organismo durante el ejercicio 2020.

Por lo antes señalado, no se cumple 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 ésta.

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

EVALUACIÓN DEL CONTROL 11 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	**7**	6	1	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se cuenta con políticas para la configuración base de los dispositivos de seguridad perimetral.

- No se tienen herramientas automatizadas para verificar las configuraciones de los dispositivos ni la detección de cambios en los componentes de seguridad perimetral.

- Se identificó que el 30.0% de los conmutadores, equipos inalámbricos y enrutadores, no tienen las últimas actualizaciones de seguridad (parches) del sistema operativo, debido a que son modelos obsoletos que no tienen soporte del fabricante ni contrato de mantenimiento.

- No se cuenta con mecanismos de doble autenticación para los dispositivos de red.

Por lo anterior, no se cumple 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: Límites de Defensa

EVALUACIÓN DEL CONTROL 12 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Límites de Defensa	**12**	7	2	3	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se cuenta con los procedimientos autorizados para asegurar que sólo los paquetes permitidos pasan a través de los límites de red, así como para el tratamiento de los paquetes no autorizados (eliminados, cuarentena, entre otros) durante el ejercicio 2020.

- Se carece de autenticación de doble factor para verificar el origen de las configuraciones de los dispositivos principales de las redes.

- No se tiene evidencia del tiempo de respuesta máximo para bloquear el tráfico no autorizado.

Por lo anterior, 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

EVALUACIÓN DEL CONTROL 13 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Protección de datos	**9**	6	3	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se cuenta con un inventario de la información sensible que es almacenada, procesada o transmitida por los sistemas, incluyendo la que es administrada por proveedores y la que está ubicada en servicios administrados, tampoco con una clasificación de ésta.

- No se tiene evidencia de la aplicación de la metodología de clasificación de activos de información críticos.

- No se cuenta con un procedimiento para la obsolescencia de los datos.

- Se carece de un procedimiento de cifrado de discos duros que indique el tipo de equipo (servidores, equipos de usuario final, dispositivos móviles, entre otros).

- Se carece de un mecanismo de seguridad para la transferencia de información mediante dispositivos móviles.

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 la necesidad de conocer

EVALUACIÓN DEL CONTROL 14 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Control de acceso basado en la necesidad de conocer	**9**	8	-	1	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se proporcionó la configuración que demuestre la separación de equipos con información sensible de las demás áreas operativas del organismo.

- No se cuenta con solución de prevención de pérdida de datos (DLP).

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

Por lo antes señalado, no se cumple 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

EVALUACIÓN DEL CONTROL 15 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Control de acceso inalámbrico	**10**	7	3	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se proporcionó evidencia de un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.

- No se proporcionó la política ni el procedimiento autorizado para que los usuarios puedan conectar sus propios dispositivos a las redes institucionales.

- En caso de que un equipo de cómputo requiera el acceso a las redes, se informó que debe contar con las últimas actualizaciones de seguridad, así como con antivirus actualizado; no obstante, no se proporcionaron evidencias de la verificación de dicho procedimiento.

- Se carece de evidencia del flujo permitido para las conexiones de tipo Bluetooth (tecnología inalámbrica de corto alcance) y NFC (comunicación de campo cercano) dentro de las redes del organismo.

Por lo anterior, no se cumple con el objeto de gestionar los procesos y herramientas utilizadas para rastrear, controlar, prevenir 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

EVALUACIÓN DEL CONTROL 16 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Supervisión y monitoreo de cuentas	**13**	9	4	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- Se carece de herramientas automatizadas para el inventario de todas las cuentas administrativas, incluyendo dominio y las cuentas locales.

- Los lineamientos sobre el uso, protección y ciclo de vida de claves criptográficas no se encuentran formalizados ni autorizados.

- 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, ni para la suspensión después de un período de inactividad establecido.

- No se proporcionó el procedimiento para el monitoreo y atención de las cuentas en caso de que se identifiquen situaciones atípicas.

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 los atacantes.

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

EVALUACIÓN DEL CONTROL 17 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Implementar un programa de concientización y entrenamiento de seguridad	**9**	8	-	1	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- Se carece de un procedimiento formalizado para asegurar la actualización del programa de conciencia en materia de seguridad informática.

- 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 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 a través de políticas, planificación organizacional, capacitación y programas de concienciación.

CSC control 18: Seguridad del Software de Aplicación

EVALUACIÓN DEL CONTROL 18 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Seguridad del software de aplicación	**11**	8	3	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos

- No se cuenta con procedimientos para el análisis de la calidad del código de los sistemas previo a su liberación en ambiente productivo.

- En relación con el análisis de vulnerabilidades de los desarrollos de sistemas, no se cuenta con un procedimiento con los roles, responsabilidades y tiempos para la eliminación o mitigación de las vulnerabilidades identificadas.

- Se carece de procedimientos autorizados para probar la calidad y seguridad de las aplicaciones suministradas por los prestadores de servicios.

- No se tiene evidencia de la definición, autorización e implementación de políticas y lineamientos para los controles de cambio en los ambientes de desarrollo, calidad y producción, tampoco se tienen documentados dichos controles.

Por lo antes señalado, no se cumple 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

EVALUACIÓN DEL CONTROL 19 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Respuesta y manejo de incidentes de ciberseguridad	**8**	7	1	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- Se tiene un plan de gestión y respuesta a incidentes de ciberseguridad para el servicio del Centro de Operaciones de Seguridad (SOC), no obstante, no se cuenta con un plan integral que cubra los sistemas y aplicativos del organismo.

- No se cuenta con un plan de sensibilización para los empleados que participan en la gestión de incidentes.

- El plan de gestión y respuesta a incidentes no contempla 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, ni 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

EVALUACIÓN DEL CONTROL 20 DE CIBERSEGURIDAD EN CAPUFE

Control	Subcontroles evaluados	No cumple	Parcialmente	Cumple	Semáforo de cumplimiento
Pruebas de penetración y ejercicios de equipo rojo	**8**	7	1	-	

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- No se proporcionó evidencia documental que acredite la ejecución de las pruebas de penetración sobre la infraestructura tecnológica del organismo.

- Se carece de la formalización y autorización del documento de lecciones aprendidas y del plan de remediación, tampoco se identificó el periodo de las pruebas.

- La metodología para la realización del análisis de vulnerabilidades y las pruebas de penetración, no se encuentra formalizada ni autorizada por el organismo.

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

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

PRINCIPALES RIESGOS POR LA CARENCIA DE LOS CONTROLES DE CIBERSEGURIDAD

Factor Crítico	Riesgo
Uso controlado de privilegios administrativos	La carencia del control de los privilegios administrativos propicia 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.
Capacidad de recuperación de datos	La falta de pruebas de recuperación de datos podría implicar el riesgo de que los respaldos no sean funcionales en el momento de su restauración, o que la información respaldada no sea la requerida por el organismo para la continuidad de sus operaciones.
Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	La falta de restricción del uso de lenguajes de codificación en navegadores web, podría generar el riesgo de la explotación de configuraciones y servicios vulnerables por parte de los posibles atacantes.
Protección de datos	La falta de políticas y procedimientos para la protección de datos podría dificultar la prevención y mitigación de la exfiltración de información, además no permite asegurar la privacidad e integridad de la información sensible.
Control de acceso basado en la necesidad de conocer	La falta de gestión de los procesos y herramientas utilizados para rastrear, controlar y corregir el acceso seguro a activos críticos pone en riesgo no poder mantener la confidencialidad de la información.
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 del ciclo de vida de las cuentas del sistema y de aplicaciones, podría generar brechas en la seguridad de los sistemas y aumenta las oportunidades de los atacantes para que puedan explotarlas.
Implementar un programa de concientización y entrenamiento de seguridad	La carencia de un programa y entrenamiento en seguridad de la información pone en riesgo que los usuarios no cuenten con la capacidad de detectar, identificar y en su caso responder ante posibles ataques cibernéticos.
Seguridad del software de aplicación	Debido a la falta de mecanismos para prevenir, detectar y corregir las debilidades de seguridad en los sistemas desarrollados por el organismo, es posible que se tengan vulnerabilidades en el código de los sistemas que puedan ser explotadas por usuarios maliciosos.
Respuesta y manejo de incidentes de ciberseguridad	La carencia de implementación de planes para la mitigación de un incidente informático con los responsables de su atención, podría ocasionar la falta de detección y respuesta oportuna de dicho incidente.
Pruebas de penetración y ejercicios de equipo rojo	La carencia de pruebas de penetración podría ocasionar la falta de detección de vulnerabilidades que podrían poner en riesgo la confidencialidad, integridad y disponibilidad de la información.

FUENTE: Elaborado con información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos.

Por lo anterior, se concluye que el 55.0% de los controles de seguridad críticos muestran carencias que ponen en riesgo a los activos de información, por lo que resulta prioritario fortalecer los controles relacionados con los privilegios administrativos, la recuperación y protección de datos, el control de las redes inalámbricas, la seguridad de los sistemas y aplicativos, así como la respuesta y manejo de incidentes de ciberseguridad, con la finalidad de identificar, contener y mitigar un ataque cibernético.

2020-1-09J0U-20-1631-01-002 **Recomendación**

Para que Caminos y Puentes Federales de Ingresos y Servicios Conexos evalúe e implemente políticas y procedimientos para los subcontroles observados en la revisión de la ciberseguridad, los cuales están relacionados con el uso controlado de privilegios administrativos; la capacidad de recuperación de datos; la configuración segura de los

equipos de red; la protección de datos; el control de acceso basado en la necesidad de conocer; el control de acceso inalámbrico; la supervisión y monitoreo de cuentas; la implementación de un programa de concientización y entrenamiento de seguridad; la seguridad del software de aplicación; la respuesta y manejo de incidentes de ciberseguridad, así como en las pruebas de penetración y ejercicios de equipo rojo, con la finalidad de asegurar el cumplimiento de los objetivos de control de la ciberseguridad para la identificación, protección, detección, respuesta y recuperación de los incidentes cibernéticos.

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.

2020-9-09J0U-20-1631-08-001 **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 Caminos y Puentes Federales de Ingresos y Servicios Conexos 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 de establecer lineamientos e implantar esquemas de seguridad para la infraestructura de tecnologías de información y comunicaciones que permitan garantizar la conectividad e integridad de la información, omitieron implementar los controles para la protección de datos sensibles, administración de accesos de usuarios a los sistemas y navegación segura en internet, debido a la falta de cumplimiento de los subcontroles observados en la revisión de la ciberseguridad, los cuales están relacionados con la protección de datos, el uso controlado de privilegios administrativos y la configuración segura de los equipos de red, lo que pone en riesgo la integridad, confidencialidad y disponibilidad de la información, en incumplimiento del 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 8 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, del Objetivo General del Proceso II.C Administración de la Seguridad de la Información (ASI); del Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos publicado el 22 de julio de 2011 en el Diario Oficial de la Federación, del artículo 57, fracción IX; y del Manual de Organización General del Caminos y Puentes Federales de Ingresos y Servicios Conexos, función 9, del puesto Subdirección de Tecnologías de Información.

4. Continuidad de las Operaciones

En el análisis de la información proporcionada por Caminos y Puentes Federales de Ingresos y Servicios Conexos, 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 del organismo, se observó lo siguiente:

Programa de continuidad

- El programa de continuidad no articula las diferentes acciones que la entidad tiene que llevar a cabo para dar continuidad de los servicios de TIC.

- No se cuenta con la priorización de las funciones a restaurar para evitar la recuperación de servicios de menor impacto y asegurarse de que la respuesta y la recuperación se encuentren alineadas con las necesidades prioritarias del organismo.

- No se revisa con los ejecutores el contenido del programa de continuidad para que cada uno de ellos conozca las actividades que habrán de realizar en caso de requerirse la aplicación del programa.

- Se carece de un plan de continuidad de negocio (BCP) para el soporte y las pruebas de los diversos procesos sustantivos con la participación de los proveedores para garantizar que las políticas de continuidad se cumplen en tiempo y forma.

- No se cuenta con un procedimiento para la definición, análisis, planificación, medición y mejoramiento de la disponibilidad de servicios de tecnologías de información.

Análisis de impacto del negocio (BIA)

- Se carece del análisis de impacto al negocio, en el que se identifiquen las funciones, actividades, unidades administrativas, así como los servicios que proporciona el organismo que podrían resultar afectados por la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias.

- No se tienen identificadas las actividades prioritarias para el suministro de productos y servicios que podrían verse afectadas por interrupciones o desastres, tampoco sus dependencias ni recursos para su continuidad.

- No se cuenta con la definición del marco de tiempo dentro del cual el impacto de no reanudar las actividades sería inaceptable para la organización (RTO).

- No se tienen establecidas las pérdidas aceptables de datos antes de reanudar las actividades interrumpidas (RPO).

Plan de recuperación de desastres (DRP)

- De los 35 empleados que tienen actividades relacionadas con el DRP, actualmente sólo 12 (34.3%) continúan laborando para CAPUFE, por lo que no se tiene certeza de que el personal involucrado para la activación del plan conozca las acciones a seguir para la activación, ejecución y mantenimiento de dicho plan.

- No se cuenta con la planeación de pruebas calendarizadas como parte de los ejercicios del DRP, ni con la identificación de las aplicaciones y sistemas que puedan ser afectados en una contingencia.

- No se proporcionaron los procedimientos de respuesta y recuperación, activación del plan de acción, recuperación de los procesos críticos de negocio y restablecimiento del negocio al estado anterior de la contingencia o desastre.

- No se cuenta con los planes para la recuperación de todos los recursos de los sistemas, ni se proporcionó el plan de concientización y capacitación de las áreas involucradas en el mantenimiento y ejecución del DRP.

Administración de la capacidad de la infraestructura tecnológica

- No se cuenta con evidencia de las métricas para el seguimiento del programa de capacidad que asegure la operación de los servicios de TIC conforme a los compromisos y niveles de servicio acordados.

- No se proporcionaron los elementos para evaluar el monitoreo de los niveles de servicio, el análisis de los incidentes, la verificación de las tendencias de cargas de trabajo de la infraestructura y las acciones a realizar cuando la capacidad y el rendimiento no estén en el nivel requerido.

Respaldos de la información

- No se cuenta con lineamientos para la actualización de las políticas y procedimientos de respaldo de la información.

- Las pruebas de restauración de respaldos no forman parte de ejercicios programados o calendarizados para probar su funcionalidad.

Como resultado de la revisión del proceso de continuidad de las operaciones, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de organismo son los siguientes:

PRINCIPALES RIESGOS POR LAS INCONSISTENCIAS DEL PROGRAMA DE CONTINUIDAD DE LAS OPERACIONES

Factor Crítico	Riesgo
Programa de Continuidad de las Operaciones	No se cuenta con una política con objetivos, metas, procedimientos y controles necesarios para la continuidad de las operaciones, lo que podría generar el riesgo de no contar con los elementos necesarios para asegurar que la operación de los servicios y procesos críticos se restablezcan en el tiempo requerido por la entidad.
Análisis de Impacto al Negocio (BIA)	La carencia de un análisis de impacto al negocio genera el riesgo de la falta de identificación de los servicios, funciones, actividades y unidades administrativas relevantes para la continuidad de la operación del organismo, así como del impacto técnico, económico y reputacional que podría ser causado por la interrupción de uno o más servicios de TIC.
Planeación de la capacidad	La falta de métricas para el seguimiento del programa de capacidad que asegure la operación de los servicios de TIC, conforme a los compromisos y niveles de servicio, podría generar la falta de aprovechamiento al no poder prever la saturación de los recursos.
Políticas de recuperación y respaldo	No se tiene un procedimiento para la ejecución de pruebas de restauración de respaldos en los aplicativos de misión crítica, lo cual podría tener el riesgo de que los medios no funcionen adecuadamente en caso de que se necesite la información almacenada.

FUENTE: Elaborado con información proporcionada por CAPUFE.

Por lo anterior, se concluye que el organismo carece de los mecanismos de resiliencia para adaptarse a interrupciones e incidentes con el fin de mantener la continuidad de las operaciones y proteger los activos de la organización; tampoco se han desarrollado planes sobre el funcionamiento de las unidades claves durante un período de interrupción de los servicios de TIC.

2020-1-09J0U-20-1631-01-003 **Recomendación**

Para que Caminos y Puentes Federales de Ingresos y Servicios Conexos defina, elabore e implemente un Análisis de Impacto al Negocio conducido por la Alta Dirección del organismo, en el que se identifiquen las funciones, actividades, áreas y servicios críticos que podrían resultar afectados ante la interrupción de uno o más componentes de TIC, así como un Plan de Continuidad del Negocio que incluya las acciones diseñadas para asegurar la continuidad de las soluciones tecnológicas, la infraestructura, los procesos, herramientas y funciones que soportan los servicios indispensables para las áreas sustantivas, con la finalidad de contar con los mecanismos de resiliencia para adaptarse a la interrupción y reanudar las operaciones en el menor tiempo posible con el mínimo impacto para el organismo.

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.

2020-9-09J0U-20-1631-08-002 **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 Caminos y Puentes Federales de Ingresos y Servicios Conexos 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 de establecer los lineamientos del plan de contingencia que le permita al organismo asegurar la continuidad de los sistemas, omitieron implementar los planes relacionados con el impacto y la continuidad del negocio, debido a la carencia del Análisis de Impacto al Negocio y el Plan de Continuidad del Negocio, lo que propició la falta de definición de los controles requeridos para mantener la operación de los procesos, sistemas y actividades críticas, afectando el funcionamiento de las áreas sustantivas del organismo para prestar los servicios internos y a la población en general; en incumplimiento del 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 8 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, Proceso II.A Proceso de Administración de Servicios (ADS), Actividades ADS 3 "Administrar la Capacidad de la infraestructura de TIC" y ADS 4 "Administrar la continuidad de servicios de TIC"; del Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos, publicado el 22 de julio de 2011 en el Diario Oficial de la Federación, artículo 57, fracción X; y del Manual General de Organización de Caminos y Puentes Federales de Ingresos y Servicios Conexos, función 10, del puesto "Subdirección de Tecnologías de Información".

Montos por Aclarar

Se determinaron 46,604,786.21 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 4 resultados, de los cuales, en uno no se detectó irregularidad y los 3 restantes generaron:

3 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 31 de enero de 2022, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, 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, Caminos y Puentes Federales de Ingresos y Servicios Conexos no cumplió con las disposiciones legales y normativas aplicables en la materia, entre cuyos aspectos observados destacan los siguientes:

- En relación con los servicios de gestión de cobro del sistema de telepeaje para la red propia de CAPUFE, no se realizó una comparación objetiva de las propuestas de los proveedores debido a que los precios y conceptos utilizados fueron distintos entre las empresas participantes; se pagaron en exceso 3,223.2 miles de pesos por servicios de cobro del sistema de telepeaje sin justificar el aumento de precios por los trabajos realizados bajo las mismas condiciones técnicas y administrativas del contrato precedente, además no se respetaron las condiciones de la solicitud de cotización del organismo; se efectuaron pagos por 43,381.6 miles de pesos por la gestión de cobro de telepeaje de los usuarios en las redes interoperables, sin cumplir con los requisitos mínimos para la comprobación de la cédula de certificación de aforo interoperable para constatar la prestación de los servicios, adicionalmente, no se realizó el cierre de las actividades del contrato para contar con toda la información de los trabajos realizados.

- Respecto a la ciberseguridad, se identificó que el 55.0% de los controles de seguridad críticos muestran carencias que ponen en riesgo a los activos de información, por lo

anterior, se deben fortalecer los controles relacionados con los privilegios administrativos de las cuentas, la recuperación y protección de datos, la seguridad de los sistemas y aplicativos, así como la respuesta y manejo de incidentes para identificar, contener y mitigar los impactos de un ataque informático.

- Sobre la continuidad de las operaciones el organismo carece de los mecanismos de resiliencia para adaptarse a interrupciones e incidentes con el fin de mantener la continuidad de las operaciones y proteger los activos de la organización.

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, y los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

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

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

La Subdirección de Tecnologías de Información adscrita a la Dirección de Administración y Finanzas y la Dirección de Operación, ambas direcciones adscritas a la Dirección General de Caminos y Puentes Federales de Ingresos y Servicios Conexos.

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, segundo párrafo;

3. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículo 26, párrafo séptimo, y 48, fracción II;

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

5. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: artículos 30, párrafo primero, y 81, fracción IV

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: 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 de Aplicación General en dichas materias publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, artículo 18, fracción III;

   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 8 de mayo de 2014, con última reforma publicada el 23 de julio de 2018, numeral 9, de las "Reglas generales", así como los Objetivos Generales de los Procesos II.A Administración de Servicios (ADS), II.C Administración de la Seguridad de la Información (ASI) y III.D Operación de los Controles de Seguridad de la Información y del ERISC (OPEC), Proceso de Administración de Proveedores (APRO 2) "Monitorear el avance y desempeño del proveedor", Factor Crítico 3, inciso a y b, Proceso II.A Proceso de Administración de Servicios (ADS), Actividades ADS 4 "Administrar la continuidad de los servicios de TIC", ADS 3 "Administrar la Capacidad de la infraestructura de TIC" y ADS 4 "Administrar la continuidad de servicios de TIC";

   Norma ISO 222301/2019 "Seguridad y Resiliencia "Sistemas de Administración de la continuidad de Negocio", Apartado 4.3.2, 8.2 y 8.3;

   Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos, publicado el 22 de julio de 2011 en el Diario Oficial de la Federación, artículo 57, fracción X;

Manual General de Organización de Caminos y Puentes Federales de Ingresos y Servicios Conexos, función 9 y 10, del puesto "Subdirección de Tecnologías de Información".

Contrato número 4500030031, cláusula 16, párrafo segundo;

Cláusula 12.1 "Pruebas o Verificación" de los contratos números 4500028970 y 4500030031; Anexos 1.1 "Interoperabilidad", apartado "Facturación" de los contratos números 4500028970 y 4500030031; Cláusula 3.6 "Centro de operación de Telepeaje", 4 inciso C de los contratos números 4500028970 y 4500030031; Anexo 1.5 "Procedimientos, información y documentación para el cierre del contrato" de los contratos números 4500028970 y 4500030031.

Anexo Técnico del contrato número 4500030031, Numeral 5.10 "Servicio de Mesa de Servicio".

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.