

Pemex Corporativo**Auditoría de TIC**

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-6-90T9N-20-0208-2023

Modalidad: Presencial

Núm. de Auditoría: 208

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 2022 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	508,605.6
Muestra Auditada	450,140.7
Representatividad de la Muestra	88.5%

El universo seleccionado por 508,605.6 miles de pesos corresponde al total de pagos de los contratos relacionados con los servicios de ciberseguridad en el ejercicio fiscal de 2022; la muestra auditada está integrada por cuatro contratos y dos convenios para prestar los servicios de comunicación segura para el acceso a internet, las suscripciones para la protección del sistema de nombres de dominio y el análisis de comportamiento de red, así como el servicio para la protección y monitoreo de la ciberseguridad perimetral con pagos por 450,140.7 miles de pesos que representan el 88.5% del universo seleccionado.

Los recursos objeto de revisión en esta auditoría se encuentran reportados en la Cuenta de la Hacienda Pública Federal del ejercicio de 2022, Tomo VII, apartado Información Presupuestaria en el “Estado Analítico del Ejercicio del Presupuesto de Egresos en Clasificación Económica y por Objeto del Gasto”, correspondiente al Ramo “Empresas Productivas del Estado”.

Antecedentes

En la fiscalización de la Cuenta Pública de 2019, se detectaron servidores y equipos de cómputo con sistemas operativos obsoletos que ya no contaban con soporte por parte del fabricante, lo cual aumentó el riesgo para la seguridad de la información, debido a la falta de actualizaciones de seguridad para remediar vulnerabilidades que estaban expuestas a ataques cibernéticos. La vulnerabilidad de los servidores Microsoft SharePoint que estaban expuestos a la web, la cual fue explotada por el hacker en el incidente de seguridad informática del 10 de noviembre de 2019, había sido corregida por el fabricante seis meses antes del ataque, sin embargo, debido a la falta de gestión de actualizaciones de seguridad (parches), entre otros controles, la vulnerabilidad no fue remediada por Pemex, lo que contribuyó para que los equipos de cómputo hayan sido secuestrados, ocasionando la pérdida de activos de información en los servidores y equipos de usuario final, así como la interrupción de los procesos de negocio de la empresa. De estas observaciones se promovieron y emitieron las acciones correspondientes, que obran en el informe individual de la auditoría número 413-DE "Auditoría de TIC".

Entre 2018 y 2022, Pemex Corporativo erogó 10,727,583.3 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
(Miles de pesos)

	2018	2019	2020	2021	2022	Totales
Monto por año	2,399,678.4	1,931,976.4	2,046,585.7	2,221,955.9	2,127,386.9	10,727,583.3

FUENTE: Información proporcionada por Pemex Corporativo.

Con base en el análisis 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 de TIC, así como para determinar el alcance, naturaleza y muestra de la revisión con las cuales 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 2022, publicado en el Diario Oficial de la Federación el 29 de noviembre de 2021, se aprobó a Pemex Corporativo en los capítulos 2000, 3000 y 5000 un presupuesto de 12,438,192.6 miles de pesos, con las ampliaciones y reducciones autorizadas obtuvo un presupuesto modificado de 16,306,910.4 miles de pesos en dichos capítulos.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2022, se concluyó que el presupuesto pagado en los capítulos 2000, 3000 y 5000 fue el mismo que el presupuesto modificado para esos capítulos, del cual 2,127,386.9 miles de pesos corresponden a recursos relacionados con las TIC, que representan el 13.1% del presupuesto en los capítulos señalados, como se muestra a continuación:

RECURSOS PAGADOS EN TIC DURANTE EL EJERCICIO DE 2022

(Miles de pesos)

Capítulo	Concepto	Pagado	Pagado en TIC	%
2000	Materiales y suministros	6,078,133.9	11,995.3	0.2
3000	Servicios generales	9,922,538.1	1,820,062.4	18.3
5000	Bienes Muebles, Inmuebles e Intangibles	306,238.4	295,329.2	96.4
TOTAL		16,306,910.4	2,127,386.9	13.1

FUENTE: Información proporcionada por Pemex Corporativo.

Los recursos pagados en materia de las TIC por 2,127,386.9 miles de pesos se integran como se muestra a continuación:

GASTOS DE TIC EN PEMEX CORPORATIVO DURANTE EL EJERCICIO DE 2022

(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Pagado
2000	MATERIALES Y SUMINISTROS		11,995.3
	23901	Otros productos adquiridos como materia prima.	7.6
	24601	Material eléctrico y electrónico.	672.8
	24901	Otros materiales y artículos de construcción y reparación.	19.4
	27101	Vestuario y uniformes.	6,703.8
	27201	Prendas de protección personal.	4,569.6
	29801	Refacciones y accesorios menores de maquinaria y otros equipos.	22.1
3000	SERVICIOS GENERALES		1,820,062.4
	31401	Servicio telefónico convencional.	8,975.1
	31501	Servicio de telefonía celular.	59.9
	31602	Servicio de telecomunicaciones.	19.1
	31701	Servicios de conducción de señales analógicas y digitales.	100,103.1
	32301	Arrendamiento de equipo y bienes informáticos.	355,179.8
	32701	Patentes, derechos de autor, regalías y otros.	655,912.7
	33104	Otras asesorías para la operación de programas.	104.0
	33301	Servicios de desarrollo de aplicaciones informáticas.	395,539.4
	33401	Servicios para capacitación a servidores públicos.	2,335.1
	33604	Impresión y elaboración de material informativo derivado de la operación y administración.	10.2
	35301	Mantenimiento y conservación de bienes informáticos.	22,701.2
	35701	Mantenimiento y conservación de maquinaria y equipo.	205,135.4
	37104	Pasajes aéreos nacionales para servidores públicos de mando.	2.7
	37504	Viáticos nacionales para servidores públicos en el desempeño de funciones oficiales.	8,151.8
	37701	Instalación del personal federal.	39.2
	39801	Impuestos sobre nóminas.	65,793.7
5000	BIENES MUEBLES, INMUEBLES E INTANGIBLES		295,329.2
	51501	Bienes informáticos.	137,012.3
	56601	Maquinaria y equipo eléctrico y electrónico.	158,316.9
TOTAL			2,127,386.9

FUENTE: Información proporcionada por Pemex Corporativo.

Del universo seleccionado en el ejercicio de 2022 por 508,605.6 miles de pesos que corresponde al total de pagos de los contratos relacionados con servicios de ciberseguridad, se erogaron 450,140.7 miles de pesos en cuatro contratos y dos convenios que representan el 88.5% del universo seleccionado, y que son los siguientes:

MUESTRA DE CONTRATOS Y CONVENIOS DE TIC PAGADOS EN EL EJERCICIO DE 2022
(Miles de pesos y de dólares)

Tipo Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto MXN/USD	Pagado MXN
				Del	Al		
Concurso Abierto Electrónico Nacional excluido de las disposiciones de los Títulos o Capítulos de compras del Tratado de Libre Comercio de América del Norte	PMX-2018-294-281 (4800030734)	Tecnologías de Información de América, S.A. de C.V., en propuesta conjunta con Operbes, S.A. de C.V., Servicios Operbes, S.A. de C.V., Soluciones Integrales SYNET, S.A. de C.V., y Asesorías Integrales T.I., S.C.	Servicios de Comunicación Segura para el Acceso a Internet de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales	08/10/2018	07/10/2021	868,041.9 ¹	322,326.9
	Convenio Modificatorio No. 1		Incremento para la protección de la navegación a Internet de 80 portales propios de la empresa	08/06/2022	31/08/2022		
Concurso Abierto No. 2020-589-PMX_SA_PC_GCSS-SASSO-CA-I-S	PMX-2021-589-22 (4400147372)	Tecnologías de Información de América, S.A. de C.V.	Suscripción de Licenciamiento para la Protección DNS (Partida 1 y 2)	11/02/2021	10/02/2024	9,716.7 ²	63,450.4
Concurso Abierto Electrónico No. 2020-495-PMX_SA_PC_GCSS-SASSO-CA-N-S	PMX-2021-495-32 (4400146884)	Tecnologías de Información de América, S.A. de C.V.	Suscripción de licenciamiento de software para el análisis del comportamiento de red	06/04/2021	11/04/2024	4,548.1 ²	27,898.7
Adjudicación Directa	PMX-2022-178-128 (4800031698)	SCITUM, S.A. de C.V.	Servicios de Protección y Monitoreo de Ciberseguridad perimetral para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales	01/09/2022	31/08/2025	851,552.3 ¹	36,464.7
Total						450,140.7	

FUENTE: Información proporcionada por Pemex Corporativo.

NOTA¹: Monto en pesos.

NOTA²: Monto en dólares.

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. Servicios de comunicación segura para el acceso a internet

Se analizó el contrato número 4800030734 suscrito con Tecnologías de Información América, S.A. de C.V., en propuesta conjunta con Operbes, S.A. de C.V., Servicios Operbes, S.A. de C.V., Soluciones Integrales SYNET, S.A. de C.V., y Asesorías Integrales T.I., S.C., mediante Concurso Abierto Electrónico Nacional con fundamento en los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 77, de la Ley de Petróleos Mexicanos; y 11, fracción I, de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, con una vigencia del 8 de octubre de 2018 al 7 de octubre de 2021, por un monto mínimo de 714,139.3 miles de pesos y máximo de 868,041.9 miles de pesos, con el objeto de prestar el “Servicio de comunicación segura para el acceso a internet de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales”. El 30 de junio de 2020, se celebró un convenio modificatorio con objeto de incrementar los servicios de protección para la navegación a internet de 80 portales propios de Pemex, con una ampliación del monto del contrato del 7.9%. El 7 de junio de 2022, se formalizó un convenio de transacción entre Pemex y el consorcio de proveedores en el cual se reconoció un adeudo por 168,746.3 miles de pesos que sería pagado en 3 parcialidades, por otra parte, el consorcio se obligó a dar continuidad a los trabajos mediante un convenio modificatorio con la ampliación del plazo al 31 de agosto de 2022 y un monto adicional de 90,480.0 miles de pesos. Se efectuaron pagos por 322,326.9 miles de pesos por servicios con cargo al presupuesto de 2022, de cuya revisión se determinó lo siguiente:

Alcance del servicio

Los componentes principales del servicio fueron el filtrado de contenido web, la protección antivirus en red, la inspección del cifrado del tráfico de datos entre un navegador y un sitio web, la protección del sistema de nombres de dominio perimetral, el cortafuegos de siguiente generación, el sistema de prevención de intrusiones, el acceso remoto vía las redes privadas virtuales, la detección y prevención de fuga de información, la protección contra amenazas persistentes avanzadas en red, la detección y respuesta de amenazas en equipos de cómputo finales y el centro de operaciones de seguridad; los servicios anteriores dieron cobertura a los sitios de la Ciudad de México, Villahermosa, Ciudad del Carmen, Minatitlán, Poza Rica, Zapopan y Reynosa.

Proceso de contratación

En el análisis del expediente de contratación se identificó la carencia de un instrumento contractual para establecer la entrega y los requisitos de aceptación de los servicios de comunicación segura del 8 de octubre de 2021 al 6 de junio de 2022.

Revisión técnica, funcional y administrativa

Se revisó la documentación técnica (entregables, ordenes de surtimiento, notificaciones de recepciones de bienes-servicios, reportes de conformidad, anexos técnicos, entre otros), de la cual se constató el cumplimiento de los requisitos del contrato.

En conclusión, se identificó la carencia de un instrumento contractual durante ocho meses para establecer los requisitos de aceptación de los servicios.

2022-6-90T9N-20-0208-01-001 Recomendación

Para que Pemex Corporativo fortalezca las políticas, los procedimientos y los controles para establecer las condiciones para formalizar los convenios modificatorios que aseguren las mejores condiciones, características y alcances de los servicios, con la finalidad de garantizar el suministro, la economía y la calidad de los entregables en beneficio de la empresa.

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.

3. Suscripción de licenciamiento para la protección del sistema de nombres de dominio

Se analizó el contrato número 4400147372 suscrito con Tecnologías de Información América, S.A. de C.V., mediante concurso abierto con fundamento en los artículos 75, y 77, de la Ley de Petróleos Mexicanos; 13, 19, y 20, de las Disposiciones de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, con vigencia del 11 de febrero de 2021 al 10 de febrero de 2024, por un monto de 9,716.7 miles de dólares con el objeto de prestar los servicios de la “Suscripción de licenciamiento para la protección DNS”. Se efectuaron pagos por 63,450.4 miles de pesos correspondientes a los servicios devengados durante el ejercicio de 2022, y se determinó lo siguiente:

Alcance del servicio

Fortalecer la ciberseguridad del sistema de nombres de dominio (DNS) asociado a los portales web de Pemex con el objetivo de identificar y controlar de manera anticipada las amenazas relacionadas con el servicio de resolución de nombres de dominio, así como mitigar los riesgos ante la materialización de ataques cibernéticos con la finalidad de evitar interrupciones en los portales web principalmente los que están relacionados con las actividades sustantivas de Pemex Corporativo. Los servicios están integrados por la suscripción de licencias para la protección de DNS externos (un dominio y 20 zonas DNS), así como para la protección de DNS internos (50,000 licencias).

Proceso de contratación

En la revisión del expediente de contratación se encontró lo siguiente:

- Se identificó que sólo se utilizó una fuente de consulta para la investigación de mercado, en contravención de los lineamientos de Pemex que establecen consultar al menos tres fuentes de información.
- No se tuvo evidencia de la validación del registro extendido de los proveedores para confirmar el desempeño, los aspectos financieros, la calidad de sus servicios, los estándares de salud, la seguridad y las políticas de responsabilidad social, entre otros.

Revisión técnica, funcional y administrativa

En el análisis de la revisión técnica (entregables, reportes, niveles de servicio, actas de aceptación, anexos, entre otros), se encontró lo siguiente:

Niveles de servicio

- Se careció de un apartado específico para la descripción, las métricas, los cálculos y los tiempos de evaluación de los niveles de servicio, por lo tanto, no fue posible aplicar penalizaciones por cada día de atraso como lo establece el contrato.
- En el análisis de 34 eventos ocurridos del 28 de febrero al 12 de diciembre de 2022 se observó que el promedio de atención fue entre 8 y 12 días naturales.

Pruebas del servicio

Protección de DNS Externos

- Se verificó que la plataforma de IBM proporciona el servicio de protección del sistema de nombres de dominio externo con características de alta disponibilidad, monitoreo continuo y reportes para resolver problemas en la infraestructura tecnológica.
- Se validó un registro de amenazas para la protección contra ataques de denegación de servicios (DoS), así como para la detección de múltiples ataques (DDoS).
- Se constató la protección de los DNS con una prueba en tiempo real en el entorno mundial, así como los mecanismos de ciberseguridad antes de llegar al perímetro de la red corporativa.

Protección de DNS Internos

- Se verificó que la plataforma de Cisco provee el servicio de protección interna con características como la alta disponibilidad, el bloqueo de enlaces maliciosos, así como los reportes de las contenciones realizadas.
- Se validó el monitoreo de la infraestructura tecnológica, la respuesta del servicio de protección, así como el listado para remediar las vulnerabilidades detectadas.
- Se comprobó la protección de los DNS con una prueba en tiempo real de las peticiones generadas en la red interna hacia los sitios de internet maliciosos.

De lo anterior, sólo se utilizó una fuente de consulta para la investigación de mercado; asimismo, se careció de un apartado específico en el contrato para la descripción, los cálculos y los tiempos de evaluación de los niveles de servicio.

2022-6-90T9N-20-0208-01-002 **Recomendación**

Para que Pemex Corporativo fortalezca las políticas, los procedimientos y los controles en la elaboración de la investigación de mercado para que incluya al menos tres fuentes de información, así como la verificación de los aspectos técnicos, financieros, de calidad, de seguridad y de responsabilidad social de los proveedores, con la finalidad de robustecer las ofertas técnicas y económicas para asegurar las mejores condiciones de economía, eficacia y eficiencia en las contrataciones.

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.

2022-6-90T9N-20-0208-01-003 **Recomendación**

Para que Pemex Corporativo fortalezca las políticas, los procedimientos y los controles para definir los niveles de servicio en las contrataciones con el alcance, los cálculos y los tiempos para la evaluación de su cumplimiento, con la finalidad de asegurar que los servicios operen dentro de los parámetros aceptables con calidad y seguridad en beneficio de la empresa.

4. Suscripción de licenciamiento de software para el análisis del comportamiento de red

Se analizó el contrato número 4400146884 suscrito con Tecnologías de Información América, S.A. de C.V., mediante un concurso abierto electrónico con fundamento en los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 75 y 77, de la Ley de Petróleos Mexicanos y 36, 37 y 38, de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, con vigencia del 6 de abril de 2021 al 11 de abril de 2024, por un monto de 4,548.1 miles de dólares americanos con el objeto de la “Suscripción de licenciamiento de software para el análisis de comportamiento de red”. Se

efectuaron pagos por 27,898.7 miles de pesos correspondientes a los servicios devengados durante el ejercicio de 2022, y se determinó lo siguiente:

Alcance del servicio

La solución consistió en el licenciamiento de software para el análisis del comportamiento de red para 300,000 flujos de tráfico por segundo con la finalidad de incrementar la capacidad de detección en tiempo real de amenazas avanzadas en la red de datos institucional, así como para controlar de manera anticipada las amenazas cibernéticas que ponen en riesgo la disponibilidad, integridad y confidencialidad de la información.

Revisión técnica, funcional y administrativa

En el análisis de la revisión técnica (entregables, reportes, niveles de servicio, actas de aceptación, anexos, entre otros), se encontró lo siguiente:

Niveles de servicio

- Se careció de un apartado específico para la descripción, cálculos y tiempos de evaluación de los niveles de servicio aplicables al contrato, por lo anterior, no fue posible aplicar penalizaciones por cada día de atraso en caso de incumplimiento.
- En el análisis de 64 tickets levantados durante el ejercicio de 2022, se observó que sólo cuentan con la fecha y hora de creación sin las fechas de atención del ticket; en consecuencia, no se advierte ninguna medición para evaluar el cumplimiento de las solicitudes de servicio.

Debido a estas observaciones se promovió una recomendación en el resultado 3 del presente informe, para definir los niveles de servicio en las contrataciones con el alcance, los cálculos y los tiempos para la evaluación de su cumplimiento.

Pruebas del servicio

- Se verificó la operación en tiempo real de las funcionalidades en la red externa, como el análisis, detección y contención de malware, la detección de movimiento lateral y exfiltración de datos, el análisis de tráfico entre las redes externas e internas, así como las capacidades de inteligencia de amenazas con grupos de reconocimiento mundial, entre otras.
- Se identificó que las funcionalidades y los datos que se recolectan de ellas no trabajan de manera automática con otras plataformas, debido a que los resultados son procesados de manera manual bajo el criterio de los operadores de las soluciones.
- Por otra parte, las soluciones para la gestión de eventos e información de seguridad no se encuentran integradas entre todas las plataformas, por lo que se carece de interacción

entre ellas para identificar patrones y comportamientos anómalos que permitan la toma de decisiones integral en la estrategia de ciberdefensa de la empresa.

Finalmente, las funcionalidades y los datos recolectados del análisis del comportamiento de red no trabajan de manera automática con otras plataformas debido a que son procesadas de manera manual; asimismo, la gestión de eventos de seguridad de los diversos sistemas opera de forma aislada sin identificar comportamientos anómalos de forma integral para la ciberdefensa de la empresa.

2022-6-90T9N-20-0208-01-004 **Recomendación**

Para que Pemex Corporativo fortalezca las políticas, los procedimientos y los controles para automatizar la evaluación de los datos y resultados del análisis del comportamiento de la red institucional, así como unificar la información sobre seguridad y gestión de eventos de todos los sistemas de seguridad de la información que operan en la infraestructura tecnológica, con la finalidad de identificar, proteger, detectar y mitigar las amenazas cibernéticas de forma integral en la ciberdefensa de la empresa.

5. Servicios de protección y monitoreo de ciberseguridad perimetral

Se analizó el contrato número 4800031698 suscrito con SCITUM, S.A. de C.V. (SCITUM), mediante adjudicación directa con fundamento en los artículos 134, de la Constitución Política de los Estados Unidos Mexicanos; 78, fracción II, de la Ley de Petróleos Mexicanos y 26, fracción III, de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, con vigencia del 1 de septiembre de 2022 al 31 de agosto de 2025 por un monto de 851,552.3 miles de pesos, con el objeto de prestar los “Servicios de protección y monitoreo de ciberseguridad perimetral para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales”. Se efectuaron pagos por 36,464.7 miles de pesos por los servicios devengados durante el ejercicio de 2022, y se determinó lo siguiente:

Alcance del servicio

Los servicios están conformados por tres rubros distribuidos en partidas y subpartidas, el primero consiste en los servicios de seguridad con las partidas de protección perimetral, publicación y navegación, así como parte del centro de operaciones de seguridad. El segundo rubro contiene los nuevos servicios para las amenazas cibernéticas con el complemento del centro de operaciones de seguridad, con las subpartidas del correlacionador de eventos de seguridad, el ciberpatrullaje, los señuelos de red y la validación continua del perímetro de seguridad. Por último, se tienen disponibles servicios de ciberseguridad bajo demanda con las partidas de las pruebas de penetración, la respuesta a incidentes y el análisis forense. Los servicios cubren los sitios de Ciudad de México, Villahermosa, Ciudad del Carmen, Minatitlán, Poza Rica, Zapopan y Reynosa.

Pagos del contrato

Se realizó la conciliación de los documentos denominados “Codificación de Pagos y Descuentos” (COPADES) registrados en el ejercicio de 2022, de la cual se obtuvieron pagos por 36,464.7 miles de pesos con cargo al presupuesto de 2022.

Revisión técnica, funcional y administrativa

Se revisó la documentación técnica (entregables, reportes, actas de aceptación de entregables, entre otros); asimismo, se realizaron pruebas con los responsables del centro de operaciones de seguridad de Pemex y se encontró lo siguiente:

Pruebas del servicio

Subpartida de Acceso Remoto vía VPN (Red privada virtual)

En relación con el cliente de VPN no se comprobó la verificación de la dirección del control de acceso a medios del equipo para permitir o negar la conexión remota.

Servicios no prestados por SCITUM

Se realizaron pruebas a las funcionalidades para la protección del sistema de nombres de dominio (DNS) en participación conjunta con Tecnologías de Información América, S.A. de C.V. (TECNOLOGÍAS), y SCITUM, de las cuales se identificó que los servicios no son prestados por SCITUM como se muestra a continuación:

- Se realizaron tres simulaciones de envío de tráfico (válido, malicioso y no válido), en el caso del tráfico válido el paquete de consultas fue atendido en tiempo real por la plataforma del contrato de TECNOLOGÍAS. En un ambiente de equipos controlados y mediante una dirección de internet con características maliciosas se generaron consultas que fueron bloqueadas por el contrato de TECNOLOGÍAS. Por último, se realizó la prueba de tráfico no válido la cual fue interceptada por la solución del contrato de TECNOLOGÍAS.
- Cabe destacar que en todas las pruebas la consola del contrato de SCITUM no registró ninguna acción de contención a los paquetes de datos al ser atendidos previamente por el contrato de TECNOLOGÍAS.
- Como parte de las aclaraciones finales y observaciones preliminares de la auditoría, se efectuaron pruebas adicionales a eventos proporcionados por Pemex, como resultado se advirtió que dichos eventos no estaban relacionados con la protección del sistema de nombres de dominio; adicionalmente, no se identificó ninguna acción complementaria para la protección del sistema de nombres de dominio entre ambos proveedores.

Por lo anterior, se realizaron pagos por 231.8 miles de pesos por funcionalidades no prestadas para la protección del sistema de nombres de dominio incluidas en las partidas "1.1 Firewall de Siguiete Generación (Prevención de ataques de negación de servicio)", "1.3 Sistema de prevención de intrusiones (Bloqueo de tráfico basado en un servicio de reputación en la nube que incluye direcciones IP y entradas de DNS de los sitios conocidos como peligrosos)" y "1.5 Detección y contención de amenazas persistentes en red (Detección del tráfico de red malicioso como consultas de DNS)", las cuales son resueltas mediante los servicios del contrato de TECNOLOGÍAS.

Lo anterior incumplió los artículos 40 y 43, de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias; el numeral 13, apartado "Subdirección de Tecnologías de la Información", función VIII, del Manual de Organización de la Subdirección de Tecnologías de la Información de Petróleos Mexicanos; las cláusulas 9, 23 y 31, fracción VI, inciso e, del contrato número 4800031698 y el apartado "3. Especificaciones y Características Técnicas de los Servicios" del Anexo A "Aspectos Técnicos de la contratación y sus anexos" del contrato número 4800031698.

En resumen, en la conexión de acceso remoto no se comprobó la verificación de la dirección del control de acceso a medios del equipo; asimismo, se realizaron pagos por 231.8 miles de pesos por funcionalidades no prestadas para la protección del sistema de nombres de dominio, las cuales son resueltas mediante otro contrato.

2022-6-90T9N-20-0208-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal y al patrimonio de Petróleos Mexicanos por un monto de 231,817.26 pesos (doscientos treinta y un mil ochocientos diecisiete pesos 26/100 M.N.), por funcionalidades no prestadas del sistema de nombres de dominio incluidas en las partidas "1.1 Firewall de Siguiete Generación (Prevención de ataques de negación de servicio)", "1.3 Sistema de prevención de intrusiones (Bloqueo de tráfico basado en un servicio de reputación en la nube que incluye direcciones IP y entradas de DNS de los sitios conocidos como peligrosos)" y "1.5 Detección y contención de amenazas persistentes en red (Detección del tráfico de red malicioso como consultas de DNS)" del contrato número 4800031698 "Servicios de protección y monitoreo de ciberseguridad perimetral para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales", las cuales son resueltas mediante los servicios del contrato número 4400147372 "Suscripción de licenciamiento para la protección DNS"; más los rendimientos financieros generados desde la fecha de su pago hasta la de su recuperación, en incumplimiento de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias de fecha 21 de septiembre de 2021, artículos 40 y 43; del Manual de Organización de la Subdirección de Tecnologías de la Información vigente a partir del 6 de febrero de 2020, numeral 13, apartado "Subdirección de Tecnologías de la Información", función VIII; del contrato número 4800031698, cláusulas 9, 23 y 31, fracción VI, inciso e y del Anexo A "Aspectos Técnicos de la contratación y sus anexos" del contrato número 4800031698, apartado "3. Especificaciones y Características Técnicas de los Servicios".

Causa Raíz Probable de la Irregularidad

Falta de monitoreo, supervisión y control en la contratación de los servicios.

Montos por Aclarar

Se determinaron 231,817.26 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 5 resultados, de los cuales, en uno no se detectó irregularidad y los 4 restantes generaron:

4 Recomendaciones y 1 Pliego de Observaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 6 de febrero de 2024, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con 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 esto se realizó 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, Pemex Corporativo cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con los servicios de comunicación segura para el acceso a internet no se contó durante ocho meses con un instrumento contractual para establecer los requisitos de aceptación de los servicios.
- De la suscripción de licenciamiento para la protección del sistema de nombres de dominio sólo se utilizó una fuente de consulta para la investigación de mercado; por otra parte, el contrato carece de las métricas para la evaluación de los niveles de servicio.
- Sobre la suscripción de licenciamiento de software para el análisis del comportamiento de red se identificó que los resultados de las funcionalidades son procesados de forma manual en un entorno automatizado; asimismo, la gestión de los eventos de seguridad de la información no opera de forma integral para la ciberdefensa de la empresa.
- En cuanto a los servicios de protección y monitoreo de ciberseguridad perimetral se realizaron pagos por 231.8 miles de pesos por funcionalidades no prestadas para la protección del sistema de nombres de dominio, las cuales son resueltas mediante los servicios de otro contrato.

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 se corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables y analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.
2. Validar que el estudio de factibilidad comprende el análisis de las contrataciones vigentes, la determinación de la procedencia de su renovación, la pertinencia de realizar contrataciones consolidadas, y los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.
3. Verificar el procedimiento de contratación, el 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 estuvieron debidamente soportados, que contaron con controles que permitieron su fiscalización, y que correspondieron a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; asimismo, 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.

Áreas Revisadas

La Gerencia de Procesos de Tesorería adscrita a la Subdirección de Tesorería de la Dirección Corporativa de Finanzas; la Gerencia de Seguridad de la Información adscrita a la

Coordinación de Servicios de Tecnologías de la Información y la Coordinación de Planeación y Proyectos, ambas Coordinaciones adscritas a la Subdirección de Tecnologías de Información de la Dirección Corporativa de Administración y Servicios, ambas Direcciones adscritas a la Dirección General de Petróleos Mexicanos.

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. Otras disposiciones de carácter general, específico, estatal o municipal: la Ley de Petróleos Mexicanos, artículo 6; las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, artículos 11, fracción XIII, 40, 41 y 43; el Manual de Organización de la Subdirección de Tecnologías de Información de Petróleos Mexicanos publicado el 6 de febrero de 2020, numeral 13, apartado "Coordinación de Planeación de Proyectos", funciones I, IV, VIII y XVII; el Estatuto Orgánico de Petróleos Mexicanos, artículo 28, fracción X; las Políticas y Lineamientos para el Abastecimiento de Petróleos Mexicanos del 8 de noviembre de 2019, numerales IV.10, IV.10.1, IV.10.2, IV.10.3 y IV.11; el Contrato número 4800030734, Cláusulas 18, 28, apartado III "Deducciones por Incumplimiento Parcial o Deficiente Respecto a la Disposición de los Servicios", Inciso f, "Atención de Incidentes Operacionales", Inciso g, "Atención de requerimientos operacionales o cambios"; el contrato número 4400147372, cláusula 21, fracción I; el contrato número 4400146884, cláusula 13, "Supervisión y verificación de los servicios"; el contrato número 4800031698, cláusulas 9, 23 y 31, fracción VI, inciso e; y el Anexo A "Aspectos Técnicos de la contratación y sus anexos" del contrato número 4800031698, apartado "3. Especificaciones y Características Técnicas de los Servicios".

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.