Pemex Corporativo

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2019-6-90T9N-20-0413-2020

413-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 2019 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.

Consideraciones para el seguimiento

Los resultados, observaciones y acciones contenidos en el presente informe individual 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 individual de auditoría se encuentran sujetas al proceso de seguimiento, por lo que en razón de la información y consideraciones que en su caso proporcione la entidad fiscalizada, podrán confirmarse, solventarse, aclararse o modificarse.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	2,251,506.6
Muestra Auditada	658,351.6
Representatividad de la Muestra	29.2%

El universo seleccionado por 2,251,506.6 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal 2019; la muestra auditada se integra por tres contratos para prestar los servicios integrales de aprovisionamiento de cómputo y el servicio de comunicación segura para el acceso a internet, con pagos ejercidos por 658,351.6 miles de pesos, que representan el 29.2 % del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en Petróleos Mexicanos (PEMEX) en 2019, relacionada con la Ciberseguridad y Continuidad de las Operaciones.

Antecedentes

En la fiscalización de la Cuenta Pública 2018, se practicó la auditoría número 449-DE "Auditoría de TIC", y se determinaron las irregularidades siguientes: se detectaron pagos injustificados por 674.8 miles de pesos por la carencia de elementos técnicos para asegurar que el proveedor aplicó los cambios en el desarrollo del Sistema Institucional de Consolidación de Información Financiera; se identificaron deficiencias en la práctica del análisis de vulnerabilidades de los aplicativos antes de su puesta en producción y en el aseguramiento de la calidad de los sistemas; se careció de un programa de capacidad de la infraestructura tecnológica para determinar los recursos requeridos en los contratos; se detectó que el prestador de servicios de operaciones de seguridad a través de sus herramientas puede interceptar, extraer y almacenar información sensible; asimismo, se identificaron deficiencias en las configuraciones de seguridad de los dispositivos de comunicaciones, así como en el monitoreo y análisis de registros de auditoría, aunado a la carencia de un Análisis de Impacto al Negocio desde la perspectiva de la Alta Dirección de PEMEX; lo anterior, compromete la integridad, confiabilidad y disponibilidad de los activos de información de la Empresa.

Entre 2015 y 2019, PEMEX invirtió 11,545,579.1 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

Recursos invertidos en materia de TIC
(Miles de pesos)

PERIODO DE INVERSIÓN	2015	2016	2017	2018	2019	TOTALES
MONTO POR AÑO	2,389,759.8	2,153,647.3	2,202,145.4	2,548,520.0	2,251,506.6	**11,545,579.1**

Fuente: Elaborada con base en la información proporcionada por PEMEX.

Resultados

1. Análisis Presupuestal

En relación con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019, publicado en el Diario Oficial de la Federación el 28 de diciembre de 2018, se autorizó al Ramo "TYY" Petróleos Mexicanos un presupuesto de 464,601,648.7 miles de pesos, del cual se asignó a Pemex Corporativo "T9N" un presupuesto modificado de 45,570,866.4 miles de pesos.

Del análisis a la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2019, se concluyó que Pemex Corporativo "T9N" tuvo un presupuesto pagado de 45,449,105.9 miles de pesos, de los cuales 4,821,414.9 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 10.6% del presupuesto, como se muestra a continuación:

RECURSOS PAGADOS EN PEMEX CORPORATIVO DURANTE 2019
(Miles de pesos)

Capítulo	Descripción	Pemex Corporativo	TIC
1000	Servicios personales	24,754,675.7	2,753,448.6
2000	Materiales y suministros	2,129,197.7	19,377.2
3000	Servicios generales	5,770,427.5	1,870,457.8
4000	Transferencias, asignaciones, subsidios y otras ayudas	12,605,533.0	0.0
5000	Bienes muebles, inmuebles e intangibles	50,668.0	42,141.4
6000	Inversión pública	138,604.0	135,989.9
	TOTAL	**45,449,105.9**	**4,821,414.9**

Fuente: Elaborado con base en la información proporcionada por PEMEX.

Los recursos ejercidos en materia de TIC por 4,821,414.9 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2019 PEMEX CORPORATIVO
(Miles de pesos)

Capítulo	Posición Financiera	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**2,753,448.6**
2000		**MATERIALES Y SUMINISTROS**	**19,377.2**
3000		**SERVICIOS GENERALES**	**1,870,457.8**
	204310900	Reparación, conservación y mantenimiento de equipos e instalaciones de telecomunicaciones	184,908.1
	204311500	Reparación, conservación y mantenimiento de equipos de computación propios	102,446.5
	207320301	Honorarios por servicios profesionales	7.3
	209350200	Servicio de agua pagado a terceros	15.5
	212362103	Fletes y maniobras	38.3
	215380100	Arrendamiento de edificios y locales	110.5
	215380101	Arrendamiento de terrenos	1,422.7
	215381200	Arrendamiento de equipos y programas de cómputo (software)	388,582.5
	221390700	Pago de regalías por uso de programas de computo	345,687.9
	222401000	Pago de hospedaje a personal en servicio	796.9
	222401001	Pago de alimentación a personal en servicio	563.6
	222401005	Pago de gastos varios a personal en servicio	669.5
	222403000	Pago de viáticos por cuota fija	4854.1
	222405000	Adquisición de boletos de avión para viajes nacionales	-6.0
	222409900	Anticipos para gastos de viaje y viáticos	-220.0
	228460300	Pagos a terceros por servicio de radio	656.2
	228460400	Pagos a terceros por servicio de teléfono	5,745.3
	228460501	Pagos a terceros por servicio de telefonía celular	1,619.5
	228460600	Pagos a terceros por servicio de intercomunicación con bancos de datos	122,120.7
	235541400	Agua potable	1.1
	235543600	Gastos de Transporte-Menaje de Casa a Personal Movilizado (Clave 88)	442.5
	235543900	Gastos varios de administración	10.7
	235544600	Servicios de informática pagados a terceros con actividad empresarial	641,311.1
	242500800	Impuesto sobre nóminas	65,746.8
	244455001	Liquidaciones por indemnizaciones y sueldos y salarios caídos personal planta sindicalizado	253.0
	244455002	Liquidaciones por indemnizaciones y sueldos y salarios caídos personal planta confianza	2,673.8
5000		**BIENES MUEBLES, INMUEBLES E INTANGIBLES**	**42,141.4**
6000		**INVERSIÓN PÚBLICA**	**135,989.9**
		TOTAL	**4,821,414.9**

Fuente: Elaborado con base en la información proporcionada por PEMEX.
Nota: Diferencias por redondeo.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 2,753,448.6 miles de pesos durante el ejercicio fiscal 2019; considerando 2,512 plazas, el promedio anual de percepción por persona fue de 1,096.1 miles de pesos.

Del total pagado en 2019 por 2,251,506.6 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 658,351.6 miles de pesos en tres contratos que representan el 29.2 % del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS EJERCIDOS DURANTE 2019
(Miles de pesos)

Procedimiento de contratación	Contrato/Convenio	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2019
				Del	Al	Mínimo	Máximo	
Adjudicación Directa	4400141079	Soluciones Tecnológicas Especializadas, S.A. de C.V.	Servicio de Cómputo para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales para los años 2017-2019 (Servicio Integral de Aprovisionamiento de Cómputo)	01/01/2017	31/12/2019	0.0	275,564.5	25,040.5
	Modificatorio Número 1		Ampliar el monto en un 22.69% con respecto al monto original y el plazo a 366 días naturales originalmente establecidos, así como la modificación a las cláusulas 1, 4, 11, 16, 22 y 28, quedando la contratación vigente hasta el 31 de diciembre de 2020 y un monto de 62,527.4 miles de pesos, generando un total de 338,092.0 miles de pesos.	31/12/2019	31/12/2020	0.0	62,527.4	
			Subtotales			0.0	338,091.9	25,040.5
Concurso Abierto Internacional	4800030244	Soluciones Tecnológicas Especializadas, S.A. de C.V., en participación conjunta con Factoría de TI, S.A.P.I. de C.V. y Neixar Systems, S.A. de C.V.	Servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores.	10/11/2017	10/11/2020	1,234,479.6	1,928,080.6	416,395.7
Concurso Abierto Electrónico Nacional	4800030734	Tecnologías de Información América, S.A. de C.V, en participación conjunta con Operbes S.A. de C.V., Servicios Operbes, S.A. de C.V., Soluciones Integrales Saynet, S.A. de C.V. y Asesorías Integrales TI, S.C.	Servicio de comunicación segura para el acceso a internet para Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales.	10/07/2018	07/10/2021	714,139.3	804,512.1	216,915.4
		Totales				**1,948,618.9**	**3,070,684.6**	**658,351.6**

Fuente: Elaborado con base en la información proporcionada por PEMEX.

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

2. Contrato número 4400141079 "Servicio de Cómputo para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales para los años 2017-2019 (Servicio Integral de Aprovisionamiento de Cómputo)"

Se analizó la información del contrato número 4400141079 y su convenio modificatorio número 1, celebrados con Soluciones Tecnológicas Especializadas, S.A. de C.V., mediante adjudicación directa, de conformidad con los artículos 78, fracción VI, de la Ley de Petróleos Mexicanos, 50 de su reglamento y 11, fracción III, 29 y 30 de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, por un

monto de 275,564.5 miles de pesos, vigente a partir del 1 de enero de 2017 y hasta la conclusión del objeto, la cual no podrá exceder del 31 de diciembre de 2019, para prestar el "Servicio de Cómputo para Petróleos Mexicanos, sus Empresas Productivas Subsidiarias y en su caso, Empresas Filiales para los años 2017-2019 (Servicio Integral de Aprovisionamiento de Cómputo)"; a través del convenio modificatorio se amplió el monto en 62,527.4 miles de pesos para llegar a un acumulado de 338,092.0 miles de pesos, así como el plazo hasta el 31 de diciembre de 2020; con recursos del ejercicio 2019 se realizaron pagos por 25,040.5 miles de pesos, y se determinó lo siguiente:

Alcance de los servicios

Consolidación de la demanda para el servicio de cómputo para Petróleos Mexicanos, sus Empresas Productivas y Subsidiarias y en su caso, Empresas Filiales, el detalle es como sigue:

EQUIPOS DEL CONTRATO NÚMERO 4400141079

Partida	Descripción	Cantidad
1	Servicio de Aprovisionamiento de equipo de cómputo portátil tipo 1	706
2	Servicio de Aprovisionamiento de equipo de cómputo portátil tipo 2	1,851
3	Servicio de Aprovisionamiento de computadora de escritorio tipo 1	2,230
4	Servicio de Aprovisionamiento de computadora de escritorio tipo 2	21,112
5	Servicio de Aprovisionamiento de replicador de puertos	484
6	Servicio de Aprovisionamiento de monitor de computadora escritorio tipo 1	135
7	Servicio de Aprovisionamiento de monitor para replicador de puertos	41

Fuente: Elaborado con información proporcionada por PEMEX.

Análisis del Inventario de Equipos

Con la finalidad de verificar los controles y herramientas para el control del inventario y pago de los equipos correspondientes al Servicio Integral de Aprovisionamiento de Cómputo, de un universo de 26,461 equipos se seleccionó una muestra de 2,883 equipos (10.9%) para las pruebas, las cuales fueron realizadas con las fuentes de información siguientes:

- Inventario inicial (formato A-3).
- Bajas reportadas por PEMEX y por el prestador de servicios.
- Cartas responsivas de bienes informáticos.
- Revisión del inventario de equipos en las instalaciones de PEMEX.

- Validación del inventario, soporte y desincorporaciones reportadas por el proveedor.

Inventario inicial (formato A-3)

- En el comparativo realizado con los 2,883 equipos de la muestra seleccionada, no se encontraron 211 (7.3%).

- Se identificó que el formato A-3 no fue formalizado hasta el 16 de mayo de 2019.

Bajas reportadas por PEMEX y por el prestador de servicios

Del comparativo entre los reportes de conformidad de los equipos pagados y las bajas reportadas tanto por PEMEX como por el prestador de servicios, se tiene el detalle siguiente:

BAJAS DE EQUIPOS DEL CONTRATO NÚMERO 4400141079

Ejercicio	Equipos pagados		Diferencia de equipos mensual	Diferencia de equipos acumulada	Bajas Reportadas Pemex	Bajas Reportadas Proveedor
2017	Enero	26,559	-	27	30	26
	Febrero	26,555	4			
	Marzo	26,555	-			
	Abril	26,553	2			
	Mayo	26,552	1			
	Junio	26,544	8			
	Julio	26,542	2			
	Agosto	26,538	4			
	Septiembre	26,537	1			
	Octubre	26,535	2			
	Noviembre	26,533	2			
	Diciembre	26,532	1			
2018	Enero	26,529	3	50	68	66
	Febrero	26,528	1			
	Marzo	26,524	4			
	Abril	26,521	3			
	Mayo	26,513	8			
	Junio	26,511	2			
	Julio	26,510	1			
	Agosto	26,494	16			
	Septiembre	26,491	3			
	Octubre	26,488	3			
	Noviembre	26,487	1			
	Diciembre	26,482	5			
2019	Enero	23,305	3,177	4,821	1,662	83
	Febrero	23,300	5			
	Marzo	23,294	6			
	Abril	22,058	1,236			
	Mayo	22,054	4			
	Junio	22,048	6			
	Julio	22,048	-			
	Agosto	22,035	13			
	Septiembre	22,018	17			
	Octubre	21,667	351			
	Noviembre	21,665	2			
	Diciembre	21,661	4			
Totales			**4,898**	**1,760**	**175**	

Fuente: Elaborado con información proporcionada por PEMEX y el Prestador de Servicios.

- En el ejercicio 2017, se pagaron 27 equipos menos al prestador de servicios respecto al inventario inicial; en ese mismo periodo, PEMEX reportó 30 equipos como baja y el proveedor informó 26.

- Durante 2018, se dejaron de pagar 50 equipos; en ese periodo, PEMEX reportó 68 bajas y 66 fueron dados de baja por el proveedor.

- Para el ejercicio 2019, se pagaron 4,821 equipos menos, sin embargo, PEMEX sólo reportó 1,662 equipos dados de baja, y el proveedor, 83. Cabe señalar que las diferencias de los meses de enero (3,177), abril (1,236) y octubre (351) de 2019 no guardan proporción con las bajas reportadas por PEMEX ni con las informadas por el proveedor.

- PEMEX informó al grupo auditor qué mediante oficios del 14 de marzo y 27 de septiembre de 2019, solicitó al proveedor la desincorporación de 5,082 equipos; sin embargo, mediante oficio del 22 de enero de 2020, el prestador de servicios sólo entregó 1,020 certificados de borrado de equipos que fueron retirados de las instalaciones de Pemex.

Por lo anterior, se observó que existen discrepancias entre los reportes de conformidad y las bajas reportadas tanto por PEMEX como por el prestador de servicios.

Cartas responsivas de bienes informáticos

- De la muestra seleccionada de 2,883 equipos, fueron restados 211 no encontrados en el formato A-3, así como 7 equipos reportados en las bajas, obteniendo una nueva muestra de 2,665 equipos; como resultado de la búsqueda de los equipos de la muestra en los resguardos de Pemex no fueron encontradas 123 cartas; no obstante, éstas fueron entregadas por el prestador de servicios.

- Los servicios de aprovisionamiento de equipos tienen el respaldo de la carta de resguardo que firman los usuarios, la cual sirve como constancia de la entrega inicial del equipo, sin embargo, la carta responsiva por sí misma no confirma que el equipo se encuentra activo en el inventario de la empresa.
- Adicionalmente, PEMEX manifestó que el inventario inicial (formato A-3) contiene un universo de equipos que no necesariamente son los mismos con los que se está dando el servicio.

Revisión del inventario de equipos en las instalaciones de PEMEX

Se validó una submuestra de 448 equipos (16.8%), a través del Sistema Central de Administración de la Configuración (SCCM), el cual es la herramienta tecnológica para controlar el inventario de todos los equipos del contrato en revisión; el criterio para comprobar que los equipos se encontraban activos en el inventario fue tomar la fecha de última hora en línea del usuario en el SCCM, se encontró lo siguiente:

- Se localizaron 79 equipos (17.6%).

- No fueron localizados 369 equipos (82.4%).

Validación del inventario, soporte y desincorporaciones reportadas por el proveedor

Del análisis de la información entregada por el prestador de servicios, se obtuvieron los resultados siguientes:

- Los inventarios del proveedor son inconsistentes debido a que los equipos de la muestra (2,665) sólo fueron encontrados en algunos meses del año, siendo que de acuerdo con los reportes de conformidad con los que PEMEX realiza los pagos, los equipos aparecen mensualmente hasta su baja o desincorporación.

- En relación con los equipos de la muestra (2,665), se encontró que al menos 29 recibieron soporte técnico en la mesa de servicio durante 2019, lo cual resulta contradictorio debido a que en ese mismo año sólo fueron encontrados 5 equipos en el inventario proporcionado por el proveedor.

- Respecto a las solicitudes de PEMEX para la desincorporación de equipos, de conformidad con el numeral "1.9 Retiro de Equipos y borrado de información" del Anexo Técnico del Contrato, el proveedor "retira los equipos que se utilizaron para dar el servicio, previo borrado seguro de los datos que se encuentran en los mismos", para lo cual genera un reporte donde consta que se aplicó el borrado; en el comparativo de los 1,020 reportes de borrado de equipos entregados por el proveedor con respecto a la muestra seleccionada del grupo auditor, sólo fueron localizados 14.

Como resultado de los comparativos, de la muestra seleccionada por el grupo auditor de 2,665 equipos sólo fueron eliminados los 79 equipos encontrados durante la revisión del inventario, los 14 equipos desincorporados por el proveedor con reporte de borrado seguro, así como las 14 bajas reportadas en los tickets de la mesa de servicio. Por lo tanto, se determina que 2,558 equipos no fueron localizados en las diversas fuentes de información relacionadas con los inventarios; cabe señalar que se verificó que dichos equipos no fueron pagados con recursos de la Cuenta Pública 2019. Asimismo, PEMEX informó que se están realizando las actas circunstanciadas para la desincorporación de los equipos por concepto de "Daño por impericia, robo de partes y robo total de equipos" de conformidad con lo estipulado en el contrato.

Se concluye que no se llevó a cabo un adecuado control, manejo, evaluación, supervisión y validación del inventario de equipos, debido a las diferencias en el control de inventarios determinadas durante la auditoría y por la falta de evidencias del soporte documental que deje constancia de las revisiones o cambios para acreditar el detalle de los equipos pagados mensualmente.

2019-6-90T9N-20-0413-01-001 **Recomendación**

Para que Pemex Corporativo fortalezca los mecanismos de control, manejo, evaluación, supervisión y validación de la gestión de inventarios de equipos de cómputo, y verifique que se cuente con el soporte documental, las revisiones y validaciones que acrediten el detalle de los equipos pagados mensualmente, con la finalidad de optimizar y asegurar el adecuado ejercicio del presupuesto de la empresa en esta materia.

3. Contrato número 4800030244 "Servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores"

Se analizó el contrato número 4800030244 celebrado con Soluciones Tecnológicas Especializadas, S.A. de C.V., en participación conjunta con Factoría de TI, S.A.P.I. de C.V. y Neixar Systems, S.A. de C.V., mediante Concurso Abierto Electrónico Internacional bajo la cobertura de los Tratados de Libre Comercio, con fundamento en los artículos 77 de la Ley de Petróleos Mexicanos; 11, fracción I, de las Disposiciones Generales de Contratación para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, con vigencia del 10 de noviembre de 2017 al 10 de noviembre de 2020, por un monto mínimo de 1,234,479.6 miles de pesos y monto máximo de 1,928,080.6 miles de pesos, con objeto de proporcionar el "Servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores", durante el ejercicio 2019 se realizaron pagos por 416,395.7 miles de pesos, y se determinó lo siguiente:

Alcance de la contratación

La administración de equipos del servicio integral administrado incluye computadoras personales y portátiles, estaciones de trabajo y video proyectores; entre los accesorios que se manejan están monitores, replicadores de puertos y unidades ópticas.

En relación con los servicios del contrato se encuentran la gestión de los sistemas operativos, control de inventario y configuraciones, mesa de servicios y soporte especializado a plataformas Microsoft y BMC (Gestión de Servicios de TI), el detalle de los equipos es el siguiente:

Cantidad de Equipos Requeridos del Contrato número 4800030244

Subpartida	Perfil	Descripción	Cantidad mínima	Cantidad máxima
1	PC-1	PC Básica	6,066	9,047
2	PC-2	PC Intermedia	10,512	15,678
3	PC-3	PC Desarrollo	2,503	3,733
4	L-1	Laptop Ligera	467	696
5	L-2	Laptop Ligera Touch "2 en 1"	226	337
6	L-3	Laptop Completa	1,744	2,602
7	L-4	Laptop Uso Rudo	447	667
8	WS-1	Workstation Windows Básica	136	203
9	WS-2	Workstation Windows Avanzada	696	1,038
10	WS-3	Workstation Windows Avanzada (WS-2) y Workstation Linux (WS-3)	27	41
11	VP-P	Video Proyector Portátil	700	1,510
12	VP-F	Video Proyector Fijo	839	1,431
		Totales	**24,363**	**36,983**

Fuente: Elaborado con información proporcionada por Petróleos Mexicanos.

En relación con las actividades de monitoreo de equipos a través de la herramienta de Gestión de Servicios de TI (BMC), se revisó que el funcionamiento es razonable de conformidad con lo establecido en el Contrato y Anexo Técnico.

4. Contrato número 4800030734 "Servicio de Comunicación Segura para el Acceso a Internet de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales"

Se analizó el contrato número 4800030734 celebrado con Tecnologías de Información América, S.A. de C.V, en participación conjunta con Operbes S.A. de C.V., Servicios OPERBES, S.A. de C.V., Soluciones Integrales Saynet, S.A. de C.V., y Asesorías Integrales TI, 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 vigencia del 10 de julio de 2018 considerando 90 días naturales para la habilitación del servicio, más 36 meses de ejecución del servicio (o antes de este plazo si se agota el monto máximo susceptible de ejercer), por un monto mínimo de 714,139.3 miles de pesos y un monto máximo de 804,512.1 miles de pesos, con objeto de proporcionar el "Servicio de Comunicación Segura para el Acceso a Internet de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales", durante el ejercicio 2019 se realizaron pagos por 216,915.4 miles de pesos, y se determinó lo siguiente:

Alcance de la contratación

Proporcionar el Servicio de Comunicación Segura para el Acceso a Internet (SCSAI) para habilitar, proteger, monitorear, detectar, analizar, contener, mitigar y responder a las amenazas y actividades adversas relacionadas con la protección de información y comunicación hacia y desde Internet por los usuarios y servicios bajo alcance.

El SCSAI considera siete sitios con enlace a Internet, los cuales deben contar con las soluciones tecnológicas siguientes:

Alcance del Contrato número 4800030734

Sitio de Acceso a Internet	Soluciones Tecnológicas
Ciudad de México Villahermosa Ciudad del Carmen Minatitlán Poza Rica Zapopan Reynosa	Filtrado de Contenido Web Protección Antivirus en Red Inspección de Tráfico SSL/TLS Firewall de Siguiente Generación (NGFW) Sistema de Prevención de Intrusiones Detección y Prevención de Fugas de Información Protección y Contención de Amenazas Persistentes Avanzadas en Red Detección y Respuesta de Amenazas en Equipos de Cómputo Finales Protección de DNS perimetral[1] Acceso Remoto vía VPN[1]

Fuente: Elaborado con información proporcionada por Pemex.
Nota[1]: Estas soluciones tecnológicas se proporcionan en los sitios de Ciudad de México y Villahermosa.

Entregables por única vez

- De acuerdo con el acta de entrega-recepción se recibieron los entregables relacionados a los planes de operación del Centro de Operaciones de Seguridad (SOC), los cuales fueron aceptados por el Administrador del proyecto, y por el Administrador y Supervisor del contrato, sin embargo, se identificó que los entregables siguientes: Presentación del arranque del servicio, Programa de implementación del SCSAI en formato Project Microsoft, Documento con la estructura organizacional del SOC, Proceso de atención y respuesta de eventos e incidentes de seguridad del SOC, Documento con la arquitectura física y lógica del SCSAI elaborado con la aplicación Visio Microsoft y las Memorias técnicas de implementación de los componentes del Sistema de prevención de intrusos (IPS), Anti-APT (Amenaza Avanzada Persistente), Filtrado de contenido web, Prevención de pérdida de datos (DLP), Sistema de nombres de dominio (DNS), Detección y respuesta de punto final (EDR), Cortafuegos (Firewall) y Servicio de red privada virtual (VPN) no contienen la fecha de elaboración, el nombre y la firma del personal del proveedor, y no se observa la participación del personal de PEMEX en la revisión y aprobación de los documentos.

- Los entregables relativos al procedimiento de monitoreo de los componentes de IPS, Anti-APT, Filtrado de contenido web, DLP, DNS, EDR, Firewall, Servicio VPN Antivirus Red, Procedimiento de actualización de firmas, Reglas en los componentes de IPS, Proceso de parcheo, actualización y optimización de los componentes de IPS, Operación e integración de datos de la Gestión de Eventos e Información de Seguridad (SIEM) y el Documento con el plan de continuidad de los servicios del SCSAI no contienen los datos que permitan identificar quién los elaboró y autorizó por parte del proveedor ni del personal de PEMEX.

- Se observó que existen entregables que no contemplan los roles, responsabilidades, tiempos y actividades del personal involucrado, tal es el caso del Procedimiento de actualización de firmas, Reglas en los componentes de IPS, así como el Proceso de parcheo, actualización y optimización de los componentes de IPS, entre otros.

Entregables periódicos

Se identificó que los entregables denominados reporte de eventos e incidentes de seguridad; reporte de incidentes, requerimientos y cambios operativos; reporte de disponibilidad del servicio, así como las sábanas de tickets del proveedor, corresponden al registro de los incidentes y requerimientos que son utilizados para la medición de los niveles de servicio, de los cuales se determinó lo siguiente:

Reporte de eventos e incidentes de seguridad

En relación con los eventos e incidentes de seguridad con la finalidad de medir el nivel de servicio se definió lo siguiente:

Conceptos para los eventos e incidentes de seguridad del Contrato número 4800030734

Categoría	Descripción
Denegación de servicio	Ataque que inutiliza el uso autorizado de las redes de datos.
Código malicioso	Programa maligno (malware) y todas sus variantes (virus, gusano, troyano, entre otros) que infecta de manera exitosa un equipo anfitrión (host).
Acceso no autorizado	Persona que gana acceso físico o lógico de manera no autorizada a un sistema, red de datos, aplicación, datos u otro recurso de TI.
Exfiltración de información	Robo o extracción no autorizada de información o datos a través de redes de datos y sistemas.
Incidente reportado por PEMEX	Incidentes identificados por PEMEX y distintos a las categorías listadas arriba que por su nivel de afectación probable o probada deban ser atendidos.

Fuente: Elaborada con información proporcionada por PEMEX.

- En relación con la categoría “Código malicioso”, PEMEX informó que algunos tickets fueron categorizados erróneamente por el SOC, los cuales corresponden a la generación de reportes diarios, solicitudes de bloqueo de equipos y bloqueo de direcciones IP.

- Respecto a la categoría “Acceso no autorizado”, fueron identificadas inconsistencias al momento de integrar la información por parte del SOC, en la sábana de tickets del mes de diciembre 2019.

- El SOC cuantifica erróneamente algunos tickets al momento de presentar la información; lo anterior fue identificado en los reportes de incidentes, requerimientos y cambios operativos.

Por lo anterior, se observan inconsistencias en el control, supervisión y verificación de los entregables, debido a que se identificaron documentos que no cuentan con datos de elaboración, autorización, roles, responsabilidades y tiempos para su realización; asimismo, no se clasifican adecuadamente los tickets, lo que ocasiona inconsistencias en los tiempos de atención y solución de los eventos, así como una deficiente medición de los niveles de servicio.

2019-6-90T9N-20-0413-01-002 **Recomendación**

Para que Pemex Corporativo fortalezca los procedimientos en la revisión periódica de las actividades de los proveedores de tecnologías de información para la realización de sus obligaciones contractuales, cumpliendo cabalmente con lo requerido en los entregables con elementos tales como fechas de elaboración, responsables, autorizaciones, roles, tiempos y actividades que sirven de base para las operaciones; asimismo, establezca mecanismos para validar la correcta clasificación, documentación e integración de los tickets que sirven como insumo para la medición de los niveles de servicio con la finalidad de mejorar la calidad y atención de los niveles de servicio para asegurar que los entregables actuales y planificados sean prestados de acuerdo con los objetivos establecidos por la empresa.

5. Ciberseguridad y continuidad de las operaciones

Del análisis a la información proporcionada a la ASF por Petróleos Mexicanos relacionada con la administración y operación de los controles de Ciberseguridad, vinculados con la infraestructura y soluciones tecnológicas, se revisó de conformidad con los controles para la Ciberseguridad y sus mejores prácticas, así como en base a las políticas y lineamientos de la Empresa en esta materia, se observó lo siguiente:

Incidente de seguridad informática (ciberataque)

El 10 de noviembre de 2019, se presentó un incidente de seguridad informática que afectó inicialmente la plataforma de servidores Windows y posteriormente a los equipos de usuario final, que consistió en un programa maligno (malware) de rescate (también llamado ransomware), el cual cifró la información contenida en los equipos, mostrando en la pantalla un mensaje que señalaba que la red había sido penetrada y los archivos encriptados con un fuerte algoritmo.

Procedimientos y controles previos al ciberataque

- La empresa no proporcionó documentación para acreditar que, previamente al incidente, se contaba con un inventario de los sistemas, aplicativos, tipo de información y cantidad de archivos que contenían los servidores y equipos de cómputo, así como de los respaldos de información que se habían efectuado antes del incidente.

- Antes del incidente, no se utilizaban herramientas para proteger las aplicaciones y los datos de los servidores, como son los agentes ATP (Protección Avanzada contra Amenazas) y las soluciones DLP (Prevención de Pérdida de Datos); asimismo, se carece de evidencia de la revisión periódica del antivirus para asegurar que los servidores Windows se encontraban protegidos contra software malicioso.

- En relación con las actualizaciones de seguridad (parches) de los servidores con sistema operativo Windows, se informó que se registraban en el Sistema Central de Administración de la Configuración (SCCM), sin embargo, dicha herramienta fue comprometida en el incidente de seguridad, por lo que no existe evidencia de las actualizaciones de seguridad aplicadas.

- Se proporcionó un listado con 63 actualizaciones de seguridad, se realizó una búsqueda de ellas en la página del fabricante y se encontró que 56 corresponden a Excel 2013, Office 2013, Office 2010, Adobe Flash Player y .NET Framework; cabe señalar que no se informó el detalle de los servidores ni la fecha de las actualizaciones, y de los siete parches restantes no se encontraron resultados.

- No se proporcionó evidencia de la realización de pruebas de penetración a la infraestructura tecnológica, sistemas empresariales y aplicativos departamentales de la empresa.

Controles y procedimientos implementados durante el ciberataque

- La Gerencia de Seguridad de la Información solicitó el apoyo del Centro de Operaciones de Seguridad (SOC) para la atención del incidente; algunas de las acciones de contención fueron el cambio de contraseñas de las cuentas de administrador; cortar la salida a internet de las redes de servidores con afectación; instalar el agente de seguridad en los servidores Windows; ejecutar el escaneo de antivirus en los equipos y servidores afectados; difundir una campaña de comunicación hacia los usuarios sobre los riesgos de la amenaza, entre otras.

- La empresa informó que fueron afectados 1,182 servidores Windows de los cuales 203 (17.2%) tenían instalado el sistema operativo Windows 2003; 703 (59.5%) Windows 2008; 216 (18.3%) Windows 2012 y 60 (5.0%) Windows 2016; respecto a los servidores 166 (14.0%) son físicos y 1,016 (86.0%) son virtuales. Asimismo, se identificó que 1,138 (96.3%) de los servidores afectados corresponden al ambiente productivo; 9 (0.7%) al ambiente de calidad y 35 (3.0%) al ambiente de desarrollo.

- Dentro de las aplicaciones afectadas se encuentran la Configuración dinámica de equipos (DHCP); Gestión documental y trabajo en equipo (SharePoint); Infraestructura de datos (PI); Sistema integral de información comercial (SIIC); Respaldos históricos de usuarios; Controlador de dominio; Sistema de

posicionamiento (SIPOA); ERP Tesorería; ERP SIIF (Sistema integral de información financiera); CITRIX; Nómina y SCCM, entre otras; cabe señalar que algunas de estas aplicaciones soportan los procesos de negocio de la Empresa.

- En el caso de los servidores con sistema operativo Windows 2003, el fabricante dejó de dar soporte el 14 de julio de 2015, no obstante, no se tiene evidencia de acciones para migrarlos a una plataforma con soporte vigente. Esta situación aumenta los riesgos para la seguridad de la información, debido a que los servidores ya no cuentan con actualizaciones de seguridad y pueden ser vulnerables a los ciberataques. Es importante señalar que para los servidores con sistema operativo Windows 2008, el soporte del fabricante terminó el 14 de enero de 2020.

- En relación con los equipos de usuario final (portátiles y de escritorio), se identificó que PEMEX cuenta con alrededor de 56,393 equipos de cómputo, de los cuales 11,054 (19.6%) fueron afectados por el incidente de seguridad; dichos equipos tenían instalado el sistema operativo Windows 7, 8.1 y 10; cabe señalar que el soporte ampliado del fabricante para Windows 7 finalizó el 14 de enero de 2020.

- De los 11,054 equipos afectados se identificó que 9,242 (83.6%) contaban con el agente ATP (Protección Avanzada contra Amenazas) y 1,812 (16.4%) no lo tenían; para el caso del agente DLP (Prevención de Pérdida de Datos), se identificó que 8,021 (72.6%) lo tenían instalado y 3,033 (27.4%) no; cabe señalar que esta observación fue incluida en el Informe Individual de la auditoría número 449-DE correspondiente a la fiscalización de la Cuenta Pública 2018.

Controles y procedimientos implementados posterior al ciberataque

- Sobre la identificación de los vectores de ataque, se conoce que el atacante aprovechó la vulnerabilidad de un servidor Microsoft SharePoint que estaba expuesto a la web, dicha vulnerabilidad permitió la ejecución remota de código en SharePoint cuando el software no puede verificar el código fuente de un paquete de aplicación, por lo que el atacante pudo ejecutar código arbitrario en el contexto del grupo de aplicaciones y servidores de SharePoint.

- La vulnerabilidad que permitió el ataque de los equipos de la empresa fue clasificada como crítica por el fabricante, por lo que liberó actualizaciones de seguridad para Microsoft SharePoint 2010, 2013, 2016 y 2019, las cuales fueron publicadas el 12 de marzo y el 25 de abril de 2019, sin embargo, dichas actualizaciones no se encontraban instaladas en los servidores de PEMEX al momento del ataque, aun cuando habían pasado más de seis meses de su publicación.

- La empresa no proporcionó evidencia documental de la gestión de parches ni de actividades de análisis para determinar la viabilidad de la instalación de las actualizaciones de seguridad liberadas por los fabricantes, por lo que no se cuenta

con soporte documental que justifique la razón de no haber instalado los parches de seguridad para el producto Microsoft SharePoint; por lo tanto, se tuvo la oportunidad de solventar la vulnerabilidad con la actualización de seguridad liberada por el fabricante, no obstante, la actualización no fue instalada y por ende la vulnerabilidad no fue remediada.

Evaluaciones del riesgo

- En el procedimiento para la evaluación de los riesgos de seguridad, no se identifican las políticas que establecen que las evaluaciones para los riesgos de ciberseguridad deben realizarse de forma cualitativa bajo demanda, así como cuál es el flujo de actividades para su solicitud y la documentación que debe generarse para tal fin; en este sentido, dado que en el documento no se aborda el tema de ciberseguridad, no se tiene la certeza de que el procedimiento se encuentre conforme al contexto de riesgos en esta materia.

Gestión de la vulnerabilidad

- No se proporcionó evidencia que acredite que se llevan a cabo pruebas de penetración para la identificación de vulnerabilidades, sin embargo, la entidad señaló que se realizan pruebas técnicas manuales, no obstante, no se remitió el soporte documental en el que se precise en qué consisten dichas pruebas.

Respuesta a incidentes de seguridad

- No se tiene evidencia documental de que la notificación del incidente de seguridad y la comunicación subsecuente a niveles jerárquicos superiores (directores, gerentes, áreas de comunicación, etc.) se realizó conforme al “Proceso Gestión de Incidentes de Seguridad de la Información”, debido a que no se proporcionó la matriz de escalamiento para la atención y respuesta de incidentes, así como el subproceso de comunicación de incidentes de seguridad de la información, de acuerdo con lo señalado en las fases de preparación, contención, erradicación y recuperación del proceso de gestión de incidentes de seguridad de la información.

- En relación con la recuperación de las aplicaciones hospedadas en los servidores que se vieron afectados, la empresa mostró un tablero de control con el inventario de 462 aplicaciones, de las cuales 364 (78.8%) operan con normalidad, 80 (17.3%) no están operativas y 18 (3.9%) se encuentran en proceso de reincorporación. Cabe señalar que han pasado más de 10 meses desde el incidente de seguridad y existen aplicaciones que no se encuentran operables.

- Se observó que no fue sino hasta después del incidente de seguridad cuando comenzaron las campañas de comunicación relacionadas con temas de ciberseguridad y se generan eventos de formación (e-learning).

Investigaciones, retenciones legales y preservación

- Se desconocen las actividades realizadas para la preservación de las evidencias (personal que tuvo acceso a las evidencias, procedimientos para trabajar con la evidencia, procedimiento de cadena de custodia), por lo que no se puede emitir un pronunciamiento al respecto.

Revisión de equipos de usuario final y servidores afectados por el ciberataque

De los equipos de usuario final y servidores que se vieron comprometidos por el incidente de seguridad, se llevó a cabo la revisión actual e histórica del antivirus, actualizaciones de seguridad (parches), respaldos, así como el estado actual que guardan (en cuarentena, operativo, no operativo). Los resultados son los siguientes:

Equipos de usuario final afectados

- Del universo de 11,054 equipos afectados, se revisó una muestra de 50 equipos, con el 90.0% de nivel de confianza y 12.0% de nivel de error; se identificó que 43 (86.0%) tenían instalada y actualizada una solución de antivirus, 2 (4.0%) no contaban con el antivirus actualizado y en 5 (10.0%) no fue posible validarlos ya que no se encontraban en la herramienta (SCCM).

- Se detectó que 34 equipos (68.0%) contaban con la instalación de parches actualizados, 12 (24.0%) no estaban actualizados y en 4 (8.0%) no fue posible validarlos ya que no es encontraban en la herramienta (SCCM).

- Se identificó que 45 equipos (90.0%) se encuentran en estado operativo y en 5 (10.0%) no fue posible validarlos, debido a que no se encontraron en la herramienta (SCCM).

- Se informó que los 50 equipos de la muestra fueron formateados y se instaló una nueva imagen base, la recuperación de los datos quedó a cargo de los usuarios finales, conforme a lo establecido en las Políticas para Usuarios Finales de Tecnología de Información.

Servidores afectados

- Del universo de 1,182 servidores Windows, se revisó una muestra de 70 servidores con un nivel de confianza de 90.0% y 10.0% de nivel de error; se identificó que 22 (31.4%) se encuentran en la plataforma de virtualización VMware, 17 (24.3%) tienen instalado el sistema operativo Windows y 31 (44.3%) no pudieron ser validados por diversas causas, tales como no se tuvo acceso al servidor, se encontraban en proceso de reaprovisionamiento o el servidor estaba apagado.

- De los 17 servidores Windows, se identificó que un equipo no tenía actualizado el antivirus, dos servidores tenían desactualizado el parche de seguridad de Microsoft Windows y en un servidor no fue posible validar su última actualización porque en la evidencia no se mostraba esa información.

- En relación con los 22 servidores migrados a la plataforma de virtualización VMware, durante las pruebas no se mostraron actualizaciones de seguridad (parches).

- Se identificó que la herramienta de respaldos de servidores "MC Networker Management" no cuenta con licenciamiento vigente (su licencia expiró el 19 de junio de 2020), por lo que no fue posible comprobar que se realizan los respaldos de los servidores.

Análisis de brechas en la ciberseguridad

Como parte de los trabajos de auditoría se evaluaron las diferencias en los controles de ciberseguridad, entre las observaciones reportadas en el Informe Individual de Auditoría de la fiscalización de la Cuenta Pública 2018 y las evidencias relacionadas con los mismos controles entregadas por la empresa en 2019, y se observó lo siguiente:

Control CSC 1 - Inventario de los dispositivos autorizados y no autorizados

Este control mantuvo el cumplimiento con el objeto de gestionar activamente todos los dispositivos 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 o no gestionados sean detectados y rechazados.

Control CSC 2 - Inventario de software autorizados y no autorizados

- PEMEX cuenta con las herramientas SCCM y BCM para gestionar el inventario del software instalado en los equipos de las plataformas Windows, sin embargo, no se maneja de manera automatizada todo el inventario del software instalado en los equipos de usuario final y servidores, con la finalidad de facilitar su clasificación para tomar acciones en base al riesgo y propósito del programa.

Este control no tuvo avances para cumplir con el objeto de gestionar activamente todo el software en la red (inventario, seguimiento y corrección), de tal manera que sólo el software autorizado esté instalado y pueda ejecutarse, así como el software no autorizado y no gestionado sea encontrado para prevenir su instalación y ejecución.

Control CSC 3 - Configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores

- No se cuenta con una herramienta para la validación de las imágenes maestras que se instalan en los equipos.
- Para los sistemas legados no existen herramientas para la revisión de la integridad de los archivos, sólo se cuenta con procedimientos para la liberación y actualización de éstos.

El control no tuvo avances para cumplir con el objeto de contar con una herramienta para la verificación de manera continua o automatizada de las imágenes seguras, por lo tanto, se requiere que se verifiquen los cambios de configuración necesarios que conduzcan a un sistema de configuración segura, para integrarlo en el proceso de gestión de cambios de la entidad, incluyendo la documentación, justificación y aprobación, y que las desviaciones se revisen periódicamente para su adecuación permanente.

Control CSC 4 - Evaluación continua de la vulnerabilidad y Solución

- Los escaneos de vulnerabilidades son realizados de manera remota y sin requerir que los agentes se instalen localmente en cada sistema.

- Las comparaciones de los escaneos sólo se realizan con la aprobación de las áreas responsables de la atención de las vulnerabilidades.

- Los resultados del análisis de vulnerabilidades son canalizados a las áreas responsables de realizar las remediaciones.

El control cumple 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.

Control CSC 5- Uso controlado de privilegios administrativos

El control mantuvo el cumplimiento con el objeto de gestionar los procesos y herramientas utilizados para rastrear, controlar, prevenir corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

Control CSC 6 - Mantenimiento, supervisión y análisis de registros de auditoría

- Las pistas de auditoría son revisadas de manera diaria para las aplicaciones críticas, sin embargo, son enviadas a las unidades de negocio de manera mensual para su validación.

- No se cuenta con procedimientos para evitar la fuga de información de los sistemas, dado que las acciones que realiza el usuario dentro del aplicativo son competencia de la unidad de negocio.

El control mostró avances para cumplir con el objeto de reunir, administrar y analizar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

Control CSC 7 - Correo electrónico y Protección Web del navegador

El control mantuvo el cumplimiento 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.

Control CSC 8 - Defensas de malware

- En la mayoría de los equipos de usuario final se tienen los agentes ATP (Protección Avanzada contra Amenazas) y DLP (Prevención de Pérdida de Datos).

- La mayoría de los servidores y equipos de usuario final se encuentran configurados con la opción de actualización de antivirus.

- Se hace uso del sandbox como mecanismo de seguridad por excepción para el caso de soluciones empresariales, asimismo, se cuenta con ambientes de desarrollo y ambientes de calidad para la realización de pruebas, antes a su liberación en ambientes productivos.

El control mostró avances para cumplir con el objeto de controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de Pemex, al mismo tiempo de optimizar el uso de la automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

Control CSC 9 - Restricción y control de puertos de red, protocolos y servicios

- El instructivo operativo con las reglas de comunicación para el bloqueo de los puertos con base en las políticas de seguridad está en proceso de actualización.

El control mostró avances para cumplir 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.

Control CSC 10 - Capacidad de recuperación de datos

- PEMEX no respalda los equipos de cómputo asignados a los usuarios finales, esta actividad queda a cargo de los propios usuarios.

- No se cuenta con copias de seguridad para los servidores.
- El respaldo de los sistemas en operación y de los conjuntos de datos de los sistemas se ejecuta con base en las solicitudes de servicio.
- La mayoría de los conjuntos de datos de los sistemas no son respaldados.

El control mostró avances para cumplir con el objeto de gestionar los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.

Control CSC 11 - Configuraciones seguras para dispositivos de red tales como cortafuegos, ruteadores y conmutadores

- Se encuentra en ejecución una estrategia para contar con una arquitectura "Confianza Cero en Seguridad", que incluye control de acceso a nivel de puerto lógico y físico en la red, así como herramientas para generar microsegmentación y control de acceso a la red.

El control 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.

Control CSC 12 - Límites de defensa

Este control mantuvo el cumplimiento de detectar/prevenir/corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.

Control CSC 13 - Protección de datos

El control mantuvo el cumplimiento 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.

Control CSC 14 - Acceso controlado basado en la necesidad de saber

El control mantuvo el cumplimiento de gestionar los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) 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.

Control CSC 15 - Control de acceso inalámbrico

- Se cuenta con un inventario de puntos de acceso inalámbricos autorizados.
- En los últimos tres meses no se han descubierto puntos de acceso vulnerables.
- Los sistemas utilizados para detectar dispositivos inalámbricos no autorizados sólo admiten el acceso a dispositivo autorizados y de manera inmediata son rechazados los dispositivos no autorizados y estos son registrados en bitácoras.

El control cumplió con el objeto de gestionar los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

Control CSC 16 - Supervisión y monitoreo de cuentas

El control mantuvo el cumplimiento 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 de ataque.

Control CSC 17 - Evaluación de habilidades de seguridad y capacitación adecuada para evitar deficiencias

- Se han realizado pláticas de sensibilización por videoconferencia denominadas “Foro TI”, abordando temas como ciberseguridad en la oficina y en trabajo remoto, asimismo, se han realizado campañas de concientización distribuidas electrónicamente.
- Se están preparando cursos de ciberseguridad en la plataforma “E-Learning”, estos cuentan con un esquema de evaluación en cada uno de sus módulos, así como una evaluación final la cual emite un certificado que acredita la aprobación del curso.

El control mostró avances para cumplir con el objeto de asegurarse de que todos los roles funcionales de PEMEX (priorizando aquellos que son misionales y su seguridad) mejoren los conocimientos, habilidades y capacidades específicas para soportar la defensa de la empresa, 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.

Control CSC 18 - Aplicación de software de seguridad

- El análisis de vulnerabilidades de los desarrollos de sistemas se realiza en los ambientes de desarrollo y/o calidad, se solicita un segundo análisis para las vulnerabilidades altas y críticas. En el caso de que no se puedan atender las

vulnerabilidades se acuerda un control compensatorio en tanto se pueda solventar la vulnerabilidad de raíz.

- En relación con las aplicaciones legadas, el 64.0% tiene pendiente la ejecución del análisis de vulnerabilidades.

El control no tuvo avances para cumplir 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.

Control CSC 19 - Respuesta a incidentes y gestión

Este control mantuvo el cumplimiento con el objeto de proteger la información de la organización, desarrollando e implementando una infraestructura de respuesta a incidentes 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.

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

- No se realizan pruebas de penetración, únicamente se llevan a cabo pruebas técnicas manuales para identificar vulnerabilidades.

- No se cuenta con un marcador global de las pruebas con objeto de clasificar los resultados para remediar las vulnerabilidades con en base en el riesgo y prioridad de los procesos.

El control no tuvo avances para cumplir con el objeto de probar la fortaleza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

Semáforo de Cumplimiento del Análisis de Brechas de los Controles de Ciberseguridad en PEMEX

Control	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2018																				
2019																				

Mantuvo el cumplimiento del control
Mostró avances en el cumplimiento del control
No tuvo avances en el cumplimiento del control

Fuente: Elaborado con información proporcionada por Pemex.

Continuidad de las operaciones

- La Subdirección de Desempeño y Mejora Continua manifestó que el Director General de Petróleos Mexicanos instruyó a los Directores Corporativos y Directores Generales de las Empresas Productivas Subsidiarias (EPS) para atender la

recomendación número 2018-6-90T9N-20-0449-01-009, emitida en el Informe Individual de auditoría número 449-DE de la Fiscalización Superior de la Cuenta Pública 2018.

- Para el desarrollo del Plan de Continuidad del Negocio de PEMEX y sus EPS, se requiere llevar a cabo un Análisis de Impacto al Negocio a fin de determinar el efecto que tendrá una interrupción en las operaciones para clasificarlas por su repercusión e identificar sus interdependencias.

- Como insumo para realizar dicho análisis, se integró un diagnóstico sobre los planes para la continuidad de las operaciones de PEMEX y sus EPS, así como las metodologías que fueron usadas para su desarrollo y las actividades críticas de los Procesos y de las áreas de la empresa que aún no se encontraban alineadas al Modelo Operativo basado en Administración por Procesos (MOBAP).

- Se encuentra en proceso el análisis correspondiente a las actividades críticas, lo cual permitirá identificar las actividades indispensables en caso de contingencia operativa, así como la definición del punto de partida para el desarrollo del Análisis del Impacto al Negocio.

- PEMEX manifestó que los planes de continuidad existentes funcionan de manera local y bajo un enfoque funcional para escenarios de contingencia muy específicos. Los planes fueron desarrollados con base en metodologías internas, no homologadas y no cuentan con Análisis de Impacto al Negocio que los fundamenten de acuerdo con las mejores prácticas observadas por la Auditoría Superior de la Federación.

Conclusiones

- Antes del ciberataque, las aplicaciones y los datos de los servidores no estaban protegidos con agentes para la protección avanzada contra amenazas ni con soluciones para la prevención de pérdida de datos; asimismo, se carece de evidencia de la revisión periódica del antivirus para asegurar que los servidores estaban protegidos contra software malicioso. Cabe mencionar que posteriormente al incidente de seguridad informática se instaló la protección en los servidores.

- Se carece de evidencia de la realización de pruebas de penetración a la infraestructura tecnológica, sistemas empresariales y aplicativos departamentales de la empresa.

- Se detectaron servidores con sistema operativo que ya no tienen soporte con el fabricante, no obstante, no se tiene evidencia de acciones para migrarlos a una plataforma con soporte vigente. Esta situación aumenta los riesgos para la

seguridad de la información, debido a que los servidores ya no cuentan con actualizaciones de seguridad y se encuentran vulnerables a los ciberataques.

- Se conoce que el hacker aprovechó una vulnerabilidad de los servidores Microsoft SharePoint que estaban expuestos a la web, lo que permitió la ejecución remota de código para cifrar la información de los equipos que fueron secuestrados. La vulnerabilidad fue clasificada como crítica por el fabricante, por lo que publicó actualizaciones de seguridad el 12 de marzo y 25 de abril de 2019, sin embargo, las actualizaciones no fueron instaladas en los servidores de PEMEX antes del ataque, aun cuando habían pasado más de seis meses de su publicación.

- No se proporcionó evidencia documental de la gestión de parches ni de actividades para determinar la viabilidad de la instalación de las actualizaciones de seguridad, por lo tanto, no se justifica la razón de no haber instalado los parches de seguridad para remediar la vulnerabilidad que contribuyó para que los equipos de cómputo hayan sido encriptados, lo que derivó en la pérdida de activos de información en los servidores y equipos de usuario final, así como en la interrupción de los procesos de negocio de la empresa.

- En relación con la recuperación de las aplicaciones hospedadas en los servidores que se vieron afectados por el ciberataque, del universo de 462 aplicaciones, 364 (78.8%) operan con normalidad, 80 (17.3%) no están operativas y 18 (3.9%) se encuentran en proceso de reincorporación. Cabe señalar que han pasado más de 10 meses desde el incidente de seguridad y existen aplicaciones que no se encuentran operables.

- En relación con los controles de ciberseguridad, respecto al ejercicio 2018 no se registran avances en el inventario de software autorizado y no autorizado, en las configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores, en la aplicación de software de seguridad, así como en las pruebas de penetración y ejercicios de equipo rojo; lo anterior aumenta el riesgo de un incidente de seguridad informática que podría ocasionar un impacto negativo en los activos de información y procesos de negocio de la empresa.

2019-6-90T9N-20-0413-01-003 **Recomendación**

Para que Pemex Corporativo implemente procedimientos para la revisión, evaluación y gestión de parches para las actualizaciones de seguridad en los equipos y servidores de las plataformas Windows, VMware, Linux y demás utilizadas por la empresa; asimismo, realice la migración de las plataformas para las cuales haya terminado su periodo de soporte con la finalidad de que dichos equipos y servidores cuenten con actualizaciones de seguridad y antivirus actualizados, que permitan reducir el riesgo ante un ataque cibernético.

2019-6-90T9N-20-0413-01-004 **Recomendación**

Para que Pemex Corporativo fortalezca las políticas y procedimientos para la ejecución de pruebas de penetración a la infraestructura y sistemas de información de manera sistemática y periódica, que sirvan de insumo para la identificación, gestión, seguimiento y solución de las vulnerabilidades que se encuentren; y ejecute los respaldos de información para los servidores y equipos de usuario final prioritarios, con la finalidad de mitigar el impacto que podría ocasionar un incidente de seguridad informática en la infraestructura y soluciones tecnológicas de la empresa.

2019-6-90T9N-20-0413-01-005 **Recomendación**

Para que Pemex Corporativo fortalezca los procedimientos para el control del inventario de software autorizado y no autorizado; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; aplicación de software de seguridad, así como en las pruebas de penetración y ejercicios de equipo rojo con la finalidad de garantizar el cumplimiento de los objetivos de ciberseguridad para asegurar de manera adecuada la identificación, protección, detección, respuesta y recuperación de los incidentes cibernéticos.

2019-9-90T9N-20-0413-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que la Unidad de Responsabilidades en Petróleos Mexicanos 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 la seguridad de la información en la infraestructura y soluciones tecnológicas, omitieron llevar a cabo las actividades de supervisión, monitoreo, actualización y gestión de parches de los servidores, conforme a las recomendaciones y actualizaciones de seguridad liberadas por el fabricante de los sistemas y aplicaciones de la infraestructura tecnológica; tampoco realizaron la migración de las plataformas de las cuales los fabricantes han anunciado la terminación del soporte ampliado, lo cual contribuyó para que los sistemas hayan sido vulnerados, lo que derivó en la pérdida de activos de información en los servidores y equipos de usuario final, así como en la interrupción de los procesos de negocio de la empresa en incumplimiento de la Ley General de Responsabilidades Administrativas, publicada en el Diario Oficial de la Federación el 18 de julio de 2016, artículo 7, fracciones I y V; y del Estatuto Orgánico de Petróleos Mexicanos, publicado en el Diario Oficial de la Federación el 26 de julio de 2019; artículo 79, fracción VIII, 81, fracción VI, 82, fracción III, 83, fracciones IV y VI y 85, fracción IX.

2019-9-90T9N-20-0413-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que la Unidad de Responsabilidades en Petróleos Mexicanos 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 la ciberseguridad en la infraestructura y soluciones tecnológicas, omitieron atender la recomendación 2018-6-90T9N-20-0449-01-008, emitida en el Informe Individual de auditoría 449-DE de la Fiscalización Superior de la Cuenta Pública 2018, debido a que informaron que se encontraban realizando acciones durante el segundo semestre de 2019, a fin de fortalecer los controles y procedimientos de seguridad para la protección de los dispositivos, aplicativos y componentes de red, sin embargo, las deficiencias señaladas en la recomendación persisten en los controles asociados al inventario de software autorizado y no autorizado; configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores; aplicación de software de seguridad, así como en las pruebas de penetración y ejercicios de equipo rojo; lo anterior puede causar un impacto en la seguridad de los activos de información, así como en los procesos de negocio de la empresa en incumplimiento de la Ley General de Responsabilidades Administrativas, publicada en el Diario Oficial de la Federación el 18 de julio de 2016, artículo 7, fracciones I y V; y del Estatuto Orgánico de Petróleos Mexicanos, publicado en el Diario Oficial de la Federación el 26 de julio de 2019, artículo 81, fracción VI, 82, fracción III y 83, fracciones IV y VI.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Planificación estratégica y operativa y Controles internos.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 5 resultados, de los cuales, en 2 no se detectaron irregularidades y los 3 restantes generaron:

5 Recomendaciones y 2 Promociones de Responsabilidad Administrativa Sancionatoria.

Dictamen

El presente se emite el 12 de octubre de 2020, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue “fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar

que se realizaron conforme a las disposiciones jurídicas y normativas aplicables", y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, Pemex Corporativo cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- Se carece de un adecuado control, manejo, evaluación, supervisión y validación del inventario de equipos de cómputo, debido a las diferencias en el control de inventarios determinadas durante la auditoría y por la falta de evidencias del soporte documental que deje constancia de las revisiones o cambios para acreditar el detalle de los equipos pagados mensualmente.

- Se detectaron servidores y equipos de cómputo con sistemas operativos obsoletos que ya no cuentan con soporte por parte del fabricante, lo cual aumenta el riesgo para la seguridad de la información, debido a la falta de actualizaciones de seguridad para remediar vulnerabilidades que están 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.

- En relación con los controles de ciberseguridad, respecto al ejercicio 2018 no se registran avances en el Inventario de software autorizado y no autorizado, en las configuraciones seguras para hardware y software en los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores, en la aplicación de software de seguridad, así como en las pruebas de penetración y ejercicios de equipo rojo; lo anterior, aumenta el riesgo de un incidente de seguridad informática que podría ocasionar un impacto negativo en los activos de información y procesos de negocio de la empresa.

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

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Genaro Héctor Serrano Martínez	Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinados por la Auditoría Superior de la Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables. Analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

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

3. Verificar que el proceso de contratación, el cumplimiento de las especificaciones técnicas y la distribución del bien o servicio satisficieron 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, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de 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), 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 la Información adscrita a la Dirección Corporativa de Administración y Servicios.

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: art. 134;

2. Ley General de Responsabilidades Administrativas: publicada en el Diario Oficial de la Federación el 18 de julio de 2016; artículo 7, fracciones I y V;

3. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: publicado en el Diario Oficial de la Federación el 30 de marzo de 2016: art. 66, fracción III;

4. Otras disposiciones de carácter general, específico, estatal o municipal: Constitución Política de los Estados Unidos Mexicanos: art. 134; Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria publicado en el Diario Oficial de la Federación el 30 de marzo de 2016: art. 66, fracción III; Medidas para garantizar la integridad de las contrataciones de la Ley de Petróleos Mexicanos: art. 83, fracción I de la Sección Segunda; Manual de Organización Estructura Básica de Petróleos Mexicanos y sus Empresas Productivas Subsidiarias con fecha de registro 05 de septiembre de 2018: atribuciones XV, XVI, XVII y XVIII de los subdirectores, inciso b, numeral XII; Manual de Organización de la Subdirección de Soluciones y Servicios de Negocio con fecha de registro 25 de febrero de 2019: numeral 9 inciso VI; Estatuto Orgánico de Petróleos Mexicanos, publicado en el Diario Oficial de la Federación el 26 de julio de 2019: artículo 16 fracciones XVI, 70 fracciones I, IV, 78 fracción IV, 79, fracción VIII, 81 fracciones I, III, IV, VI, 82, fracción III, 83, fracciones I, II, IV, V y VI; 85 fracción IV, IX; Norma ISO 27032:2012 Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad: apartado 12.3 Protección del servidor, inciso b y e; Marco de Referencia NIST Publicación especial 800-53 Revisión 4: CA-8 Pruebas de penetración, CP-9 Respaldo del sistema de información; Requerimientos de Técnicas de seguridad - Sistemas de gestión de seguridad de la información ISO/IEC FDIS 27001:2013: apartados A.7, A.7.2, A.8, A.8.1, A.8.3, A.9, A.9.4, A.12, A.12.2, A.12.6, A.12.7, A.13, A.13.1; Contrato 4400141079: cláusulas 9 y 16; Anexo A del Contrato 4400141079: numerales 1.8, 1.15, 4 y 7; Contrato 4800030734: Cláusula 7, 16 y 28; Anexo A Especificaciones y Condiciones de la Ejecución de los Servicios, numeral 3.13;

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.