Petróleos Mexicanos

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2018-6-90T9N-20-0449-2019

449-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 2018 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	1,610,794.8
Muestra Auditada	361,016.1
Representatividad de la Muestra	22.4%

El universo seleccionado por 1,610,794.8 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 2018; la muestra auditada se integra por tres contratos para prestar el servicio especializado para desarrollo, mantenimiento, configuración y migración de soluciones tecnológicas; servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores, así como el servicio de comunicación segura para el acceso a Internet para Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales, con pagos ejercidos por 361,016.1 miles de pesos, que representan el 22.4 % del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en Petróleos Mexicanos en 2018, relacionada con la Ciberseguridad.

Antecedentes

En la revisión de la Cuenta Pública 2012, se ejecutó la Auditoría DE-156 "Aprovechamiento de Infraestructura y Servicios de las TIC", donde se observó que el Sistema de Gestión por Procesos se encontraba suspendido y sin generar beneficios a la institución, asimismo, la evaluación de la implementación del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI) mostró un 47.1% de avance con respecto al 86.0% reportado por la entidad.

Durante la Cuenta Pública 2013, se desarrolló la Auditoría DE-188 "Aprovechamiento de Recursos, Infraestructura y Servicios de TIC", donde se determinó que no estuvo justificada la adquisición, operación y aprovechamiento del software para el monitoreo de las redes denominado "EyeNet", con pagos injustificados por 108,376.5 miles de pesos, lo cual derivó en un procedimiento resarcitorio. Asimismo, se identificaron deficiencias en el desempeño de las estaciones de servicio, debido a que no se verificaba el comportamiento habitual de las compras de combustible para evitar conductas irregulares.

Para la Cuenta Pública 2016, se realizó la Auditoría 444-DE "Auditoría de TIC", donde se identificó la carencia de una estrategia para el aprovechamiento de los recursos humanos, también se detectó un sobredimensionamiento en los servicios prestados por los centros de cómputo.

Entre 2014 y 2018, Petróleos Mexicanos (PEMEX) invirtió 11,051,765.5 miles de pesos, en sistemas de información e infraestructuras tecnológicas (Materiales y suministros, Servicios generales y Bienes muebles, inmuebles e intangibles), integrados de la manera siguiente:

Recursos invertidos en materia de TIC
(Miles de pesos)

PERIODO DE INVERSIÓN	2014	2015	2016	2017	2018	TOTALES
MONTO POR AÑO	1,757,693.0	2,389,759.8	2,153,647.3	2,202,145.4	2,548,520.0	**11,051,765.5**

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

Resultados

1. Análisis Presupuestal

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2018, se concluyó que PEMEX tuvo un presupuesto de 498,740,220.8 miles de pesos, de los cuales, 5,637,719.5 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 1.1% del total, como se muestra a continuación:

Recursos ejercidos en 2018
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Presupuesto Ejercido TIC
1000	Servicios personales	92,436,669.9	2,677,646.2
2000	Materiales y suministros	5,822,302.4	40,667.3
3000	Servicios generales	32,693,109.9	2,159,308.0
4000	Transferencias, asignaciones, subsidios y otras ayudas	57,471,241.4	300.1
5000	Bienes Muebles, Inmuebles e Intangibles	1,456,901.7	198,987.3
6000	Inversión pública	185,373,868.2	560,810.6
7000	Inversiones financieras y otras provisiones	1,429,616.9	0.0
9000	Deuda Pública	122,056,510.4	0.0
	TOTAL	**498,740,220.8**	**5,637,719.5**

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

Los recursos ejercidos en materia de TIC por 5,637,719.5 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2018 PEMEX
(Miles de pesos)

Capítulo	Posición Financiera	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**2,677,646.2**
2000		**MATERIALES Y SUMINISTROS**	**40,667.3**
3000		**SERVICIOS GENERALES**	**2,159,308.0**
	204310200	Reparación, conservación y mantenimiento de vehículos	15.1
	204310400	Reparación, conservación y mantenimiento de mobiliario	4.0
	204310900	Reparación, conservación y mantenimiento de equipos	234,175.0
	204311001	Reparación, conservación y mantenimiento de inmuebles	43.2
	204311300	Reparación, conservación y mantenimiento de maquinaria	4.9
	204311500	Reparación, conservación y mantenimiento de computadoras	51,718.7
	209350200	Servicio de agua pagado a terceros	33.6
	212362103	Fletes y maniobras	56.9
	215380100	Arrendamiento de edificios y locales	1,481.0
	215381200	Arrendamiento de equipos y programas de cómputo	334,042.3
	221390700	Regalías por uso de programas de computo	393,336.4
	222401000	Pago de hospedaje a personal en servicio	1,196.1
	222401001	Pago de alimentación a personal en servicio	214.7
	222401005	pago de gastos varios a personal en servicio	508.8
	222403000	pago de viáticos por cuota fija	4,694.3
	222405000	Adquisición de boletos de avión para viajes nacionales	298.0
	222405100	Adquisición de boletos de avión para viajes al extranjero	- 54.8
	222409900	Anticipos para gastos de viaje y viáticos	140.6
	223421900	Pago de deducibles de seguro por siniestros	1.2
	228460300	Pagos a terceros por servicio de radio	630.5
	228460400	Pagos a terceros por servicio de teléfono	9,621.8
	228460501	Pagos a terceros por servicio de telefonía celular	6,792.8
	228460600	Pagos a terceros por servicio de intercomunicación	237,322.9
	235540600	Servicios de mensajería	13.3
	235541200	Alimentación y hospedaje a trabajadores	13.1
	235541400	Servicio de agua potable pagado a terceros	7.9
	235541500	Servicios diversos pagados a terceros empresariales	64,271.7
	235542000	Servicios de impresión de formatos, catálogos, etc.	9.5
	235543900	Gastos varios de administración	31.6
	235544500	Servicios de capacitación pagados a terceros empresariales	15,242.7
	235544600	Servicios de informática pagados a terceros empresariales	711,477.9
	242500800	Impuesto sobre nóminas personal de operación	63,251.9
	235545000	Liquidaciones por indemnizaciones y por sueldos	28,710.3
4000		**TRANSFERENCIAS, ASIGNACIONES, SUBSIDIOS Y OTRAS**	**300.1**
5000		**BIENES MUEBLES, INMUEBLES E INTANGIBLES**	**198,987.3**
6000		**INVERSIÓN PÚBLICA**	**560,810.6**
		TOTAL	**5,637,719.5**

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 2,677,646.2 miles de pesos durante el ejercicio fiscal 2018; considerando 3,018 plazas, el promedio anual por persona fue de 887.2 miles de pesos.

Del total ejercido en 2018 por 1,610,794.8 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 361,016.1 miles de pesos en tres contratos que representan el 22.4 % del universo, el cual se integra de la manera siguiente:

Muestra de Contratos Ejercidos durante 2018
(Miles de pesos)

Procedimiento de contratación	Contrato/Convenio	Proveedor	Objeto del contrato	Vigencia		Monto		Ejercido 2018
				Del	Al	Mínimo	Máximo	
Concurso Abierto Nacional	PMX-2017-740-627	Capgemini México, S. de R.L. de C.V.	Servicio técnico especializado para desarrollo, mantenimiento, configuración, migración y/o actualización de soluciones en diversas plataformas tecnológicas	29/09/2017	31/12/2017	2,237.6	22,375.5	
	Convenio modificatorio 1		Ampliación del plazo	01/01/2018	07/07/2018			17,557.0
		Subtotal				2,237.6	22,375.5	17,557.0
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	278,116.7
Concurso Abierto Nacional	PMX-2018-294-281	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 de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales	10/07/2018	10/07/2021	714,139.3	804,512.1	65,342.4
					Total	**1,950,856.5**	**2,754,968.3**	**361,016.1**

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

Los pagos fueron reconocidos en las partidas presupuestarias correspondientes; además, el análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

2. Contrato PMX-2017-740-627 "Servicio Técnico Especializado para Desarrollo, Mantenimiento, Configuración, Migración y/o Actualización de Soluciones en Diversas Plataformas Tecnológicas".

Se analizó la información del contrato PMX-2017-740-627 con procedimiento 4800030243 celebrado con Capgemini México, S. de R.L. de C.V, mediante un Concurso Abierto Electrónico Nacional, con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 75 y 77, párrafos primero, segundo y tercero, de la Ley de Petróleos Mexicanos y 11, fracción I, 17, 19, 20 y 25 de las Disposiciones Generales de Contrataciones para Petróleos Mexicanos y sus Empresas Productivas Subsidiarias, vigente del 29 de septiembre al 31 de diciembre de 2017, por un monto mínimo de 2,237.6 miles de pesos y monto máximo de 22,375.5 miles de pesos, con el objeto de incorporar servicios técnicos especializados de programación y/o configuración para agilizar la implementación de nuevas soluciones, así como proporcionar el mantenimiento, configuración, migración y/o evolución de las soluciones legadas, soluciones industriales y empresariales que permitan soportar integralmente los servicios del negocio; además el 29 de diciembre de 2017, se suscribió el Convenio Modificatorio No. 1 para ampliar el plazo del 01 de enero al 07 de julio de 2018, por lo que durante el ejercicio 2018 se realizaron pagos por 17,557.0 miles de pesos. Al respecto, se determinó lo siguiente:

Alcance de los Servicios

La prestación de los servicios se gestionó a través de las "Solicitudes de órdenes de trabajo a compañías" mediante las modalidades siguientes:

- Modalidad por Asignación: Se refiere a la solicitud del servicio a través de la asignación de especialistas técnicos en sitio, según la relación de perfiles estipulados contractualmente para atender requerimientos de desarrollo, mantenimiento, configuración, migración y/o actualización de soluciones en cualquiera de las plataformas tecnológicas de acuerdo con las necesidades de Pemex. Cabe mencionar que el contrato y anexo de "Especificaciones y condiciones de la ejecución del Servicio" no establece el método de estimación utilizado para determinar la cantidad de perfiles y horas que estará asignado el personal, por lo tanto, no se asegura un adecuado dimensionamiento de los perfiles, actividades y horas cobradas.

- Modalidad por requerimiento: Se relaciona con la solicitud del servicio a través de un requerimiento y la descripción detallada de los trabajos por realizar, que es enviada por Pemex al proveedor; al respecto, se recibe una propuesta de servicios, la cual deberá estar realizada a través del modelo de estimación puntos de función. Cabe mencionar que para cada uno de los perfiles técnicos solicitados durante el plazo del contrato se estableció la tarifa día-hombre (jornadas de 8 horas en días hábiles).

Cumplimiento Contractual

Se revisaron los servicios pagados en 2018, y se identificaron 56 solicitudes de órdenes de trabajo a compañías que fueron atendidas por el proveedor; además, se determinó una muestra (12 órdenes de trabajo) con el 80.0% de nivel de confianza y 15.0% de error para verificar el cumplimiento contractual y técnico; cabe mencionar que por cada Orden de Trabajo pueden estar asociadas una o más Solicitudes de Cambios (CRQ) que son registradas en una Herramienta para la gestión del proceso de solicitud, construcción, pruebas y puesta en producción de cada cambio, el detalle de la muestra es el siguiente:

Muestra de solicitudes de órdenes de trabajo a compañías del procedimiento 4800030243

(Miles de pesos)

Núm.	Orden de Trabajo	Modalidad	Alcance	Monto	CRQ relacionados
1	CAPG-27	Asignación	Indicadores de desempeño estratégicos y operativos	941.3	10518, 3100, 8017 y 8702
2	CAPG-35	Asignación	Soportes y nuevos desarrollos ABAP para las soluciones de los Procesos en PEMEX Y EPS	841.1	8435, 8436 y 9228
3	CAPG-36	Requerimiento	Aplicación de Ingesta a Expediente Electrónico del Proceso de Procura	1,071.9	5207
4	CAPG-39	Asignación	Mantenimiento Sistema Integral de Información Comercial (SIIC)	151.6	8061 y 8143
5	CAPG-54	Asignación	Mantenimientos SIIC - módulos Clientes, Precios y Facturación	121.3	8061
6	CAPG-56	Asignación	Mantenimiento SIIC - Módulos	100.1	9343 y 9545
7	CAPG-57	Asignación	Soporte y nuevos desarrollos ABAP para las Soluciones de los Procesos en PEMEX y EPS	630.8	9271, 9409 y 9815
8	CAPG-58	Asignación	Continuación con el proyecto de Indicadores de Desempeño Estratégico y Operativos	592.4	10518, 8192, 3630, 10629 y 3482
9	CAPG-66	Asignación	Sistema Integral de Información Comercial (SIIC)	145.6	9943
10	CAPG-67	Asignación	Sistema Integral de Información Comercial (SIIC)	145.6	9343
11	CAPG-73	Asignación	Soporte y nuevos desarrollos ABAP para las Soluciones de los Procesos en PEMEX y EPS	490.6	7009, 8436, 8273 y 10427
12	CAPG-74	Asignación	Continuar con el proyecto de Indicaciones de Desempeño Estratégicos y Operativos	369.5	3630, 8192 y 10518
			TOTAL	**5,601.8**	

Fuente: Elaborada por la ASF con información proporcionada por PEMEX.

Modalidad por Asignación

Se verificó el cumplimiento contractual de las once solicitudes de órdenes de trabajo a compañías bajo la modalidad por asignación y se identificaron incumplimientos en el 100.0% de las mismas, las observaciones son las siguientes:

- La entrega de las solicitudes de servicio y del acuse de recibido por el proveedor no se realizó mediante correo electrónico, en incumplimiento del Anexo del contrato.

- Por cada servicio realizado, el proveedor no entregó una carta-garantía que ampare los servicios de cada orden por un periodo de 30 días naturales.

Evaluación de Perfiles Técnicos

De acuerdo con lo establecido en el Anexo "Perfiles Técnicos", se determinó revisar 16 de éstos relacionados con 12 solicitudes de órdenes de trabajo a compañías, el detalle es el siguiente:

Perfiles técnicos del procedimiento 4800030243

Orden de Trabajo	Perfil
CAPG-27	23.- Especialista en plataforma en Microsoft (Collaboration & Business Intelligence) 24.- Especialista en Arquitectura de Datos 26.- Especialista en Analítica Avanzada
CAPG-35	1.- Especialista en plataforma ABAP
CAPG-39	14.- Especialista en plataformas 4GL (Informix 4GL, Oracle Forms, Centura, Cold Fusion, Genexus)
CAPG-54	14.- Especialista en plataformas 4GL (Informix 4GL, Oracle Forms, Centura, Cold Fusion, Genexus)
CAPG-56	14.- Especialista en plataformas 4GL (Informix 4GL, Oracle Forms, Centura, Cold Fusion, Genexus)
CAPG-57	1.- Especialista en plataforma ABAP
CAPG-58	23.- Especialista en plataforma en Microsoft (Collaboration & Business Intelligence) 24.- Especialista en Arquitectura de Datos 26.- Especialista en Analítica Avanzada
CAPG-66	14.- Especialista en plataformas 4GL (Informix 4GL, Oracle Forms, Centura, Cold Fusion, Genexus)
CAPG-67	14.- Especialista en plataformas 4GL (Informix 4GL, Oracle Forms, Centura, Cold Fusion, Genexus)
CAPG-73	1.- Especialista en plataforma ABAP
CAPG-74	26.- Especialista en Analítica Avanzada 24.- Especialista en Arquitectura de Datos

Fuente: Elaborada por la ASF con información proporcionada por PEMEX.

- De los 16 perfiles revisados, se desprendió que se carece de evidencia documental que acredite la especialidad, en infracción del Anexo "Perfiles Técnicos".

Pruebas Unitarias e Integrales

Fueron proporcionados los formatos de aceptación de las pruebas; no obstante, no se encuentran acompañados de la documentación soporte para verificar los resultados, de acuerdo con los numerales 8.4 (Pruebas Unitarias) y 8.6 (Pruebas Integrales) de la Metodología de Desarrollo y Mantenimiento de Sistemas de Información, las observaciones son las siguientes:

- Pruebas Unitarias: En la revisión de los 23 CRQ relacionados a las 12 órdenes de trabajo, se identificó que en 9 de 23 (39.1%) no se generó evidencia documental para garantizar que la construcción de la solución se encuentra completa, cumpla con la funcionalidad solicitada y que en todos los casos las pruebas hayan tenido éxito.

- Pruebas Integrales: Se identificó que para 18 de 23 CRQ revisados (78.3%) no se generó evidencia documental para garantizar que se probaron todos los requerimientos de negocio y que los resultados fueron exitosos.

Verificación de las Funcionalidades

Con la revisión de un total de 23 CRQ que fueron revisados y se encuentran relacionados con 12 solicitudes de órdenes de trabajo a compañías, se verificó la funcionalidad en 7 de 23 (30.4%), de las cuales se tienen las observaciones siguientes:

Funcionalidades revisadas del procedimiento 4800030243

Orden de Trabajo	Funcionalidad	Cumple / No cumple
CAPG-36	**CRQ 5207** - Aplicación que será la base para toda la ingesta y consulta de documentos dentro del Expediente Electrónico del Proceso de Procura.	Cumple
CAPG-27	**CRQ 8702** - Generación de tableros automatizados de balances en sistemas de transporte y terminales de almacenamiento.	Cumple
CAPG-35	**CRQ 8435** - Habilitar interfaz de envío de datos de órdenes de SAP => SIACOPERT a la sociedad PFER Pemex Fertilizantes. **CRQ 9228** - Modificar el encabezado del reporte por Gerencia de Financiamiento e Inversiones para generar hojas, oficios y reporte de programa, en Generación de oficio modificar formato y calcular correctamente el campo POR que viene especificado en el oficio.	Cumple
CAPG-57	**CRQ 9271** - Configuración del proceso de venta de activos improductivos en el ERP del Corporativo.	No cumple
CAPG-58	**CRQ 3482** - Actualización de la Herramienta Tecnológica para el Sistema Institucional de Consolidación de Información Financiera.	No cumple
CAPG-73	**CRQ 8436** - Adecuar función para insertar registros en la tabla del COIR (nuevas cuentas con valor alfanumérico).	Cumple

Fuente: Elaborada por la ASF con información proporcionada por PEMEX.

- En relación con la Solicitud para la Actualización de la Herramienta Tecnológica para el Sistema Institucional de Consolidación de Información Financiera, se identificó que el BPC (Business Planning and Consolidation) es un software comercial de consolidación de información financiera de SAP, usado comúnmente en el mercado de estas aplicaciones; y que no se cuenta con el detalle de los requerimientos ni con el diseño de la solución, tampoco con el soporte técnico que garantice que el proveedor realizó alguna configuración, adecuación o desarrollo relacionado con la funcionalidad solicitada, el detalle de los pagos es el siguiente:

Pagos realizados por la Solicitud de la Orden de Trabajo a Compañías CAPG-58

(Miles de pesos)

			A	B	C=A*B	D	E=C+D
Alcance	**Periodo de los servicios**	**Id del Perfil**	**Cantidad (Días hombre)**	**Precio unitario**	**Subtotal**	**IVA**	**Total**
Proyecto de Indicadores de Desempeño Estratégicos y Operativos con la explotación, extracción y análisis estadístico y avanzado de la información	12/03/2018 al 04/05/2018	Perfil 23	17	3.5	60.1	9.6	69.7
		Perfil 26	17	4.3	73.9	11.8	85.7
		Perfil 24	33	4.3	143.4	23.0	166.4
		Perfil 23	16	3.5	56.6	9.0	65.6
		Perfil 26	19	4.3	82.6	13.2	95.8
		Perfil 24	38	4.3	165.2	26.4	191.6
						TOTAL	**674.8**

Fuente: Elaborada por la ASF con información proporcionada por PEMEX.

Nota. Diferencias por redondeo.

Por lo anterior, se presumen pagos injustificados por 674.8 miles de pesos por la carencia de elementos técnicos para garantizar que el proveedor atendió la solicitud de cambio, relacionada con la Actualización de la Herramienta Tecnológica para el Sistema Institucional de Consolidación de Información Financiera.

- El desarrollo del módulo de Notas de Crédito/Débito relacionado con el proceso de venta de activos improductivos en el ERP del Corporativo, no ha sido utilizado por el usuario final desde hace más de 10 meses, por lo que se desconoce si cumplirá con el fin contratado.

Cumplimiento a la Disposición Operativa para la Gestión de Cambios y Liberaciones

Con la finalidad de verificar el cumplimiento de los puntos de control establecidos en la Disposición Operativa para la Gestión de Cambios y Liberaciones, se revisaron las 12 solicitudes de las órdenes de trabajo a compañías, en relación con las actividades y

documentación soporte generada para 20 de 23 CRQ (solicitudes de cambio) clasificados como Cambios Normales, al respecto se identificó lo siguiente:

- En cuatro solicitudes de cambio no se tiene el plan de liberación ni plan de regreso.

- En dieciséis solicitudes de cambio se carece del correo electrónico en donde el normativo acepta como exitosos los criterios de validación y aceptación en operación controlada.

- En cinco solicitudes de cambio no se cuenta con el correo electrónico que el usuario del negocio enviaría al coordinador de cambio para aceptar el resultado exitoso de cada uno de los criterios de validación y aceptación post implantación.

Metodología de Desarrollo y Mantenimiento de Sistemas de Información

Se revisó la metodología implementada para el desarrollo de soluciones tecnológicas de TIC, así como la Disposición Operativa para la Gestión de Cambios y Liberaciones de acuerdo con las mejores prácticas relacionadas, considerando la especificación de los requerimientos, el diseño, el desarrollo, la verificación, validación e integración de los componentes o productos necesarios para su entrega, así como las características de integridad, confiabilidad y disponibilidad de los datos contenidos en dichas soluciones, y se identificó lo siguiente:

- Análisis de Vulnerabilidades: La metodología y las disposiciones operativas relacionadas no especifican su tratamiento, antes del inicio de la puesta en operación de nuevos desarrollos o mantenimientos de acuerdo con los tipos de cambio, así como los procedimientos, autorizaciones, excepciones y documentación soporte, entre otros.

- Aseguramiento de la Calidad: No se tiene implementado un procedimiento formalizado de revisión de la calidad del código de los desarrollos de software; se carece de controles técnicos de verificación para las revisiones de calidad que se efectúan a los componentes y productos.

- Pase a Producción y Gestión del Código Fuente: No se tiene una herramienta de apoyo a la metodología de desarrollo para el control de versiones y establecimiento de líneas base; asimismo, tampoco mecanismos para asegurar que las bibliotecas de los desarrollos son actualizadas con la versión del componente de la solución que está siendo transferido a producción, que se archive la versión existente y su documentación soporte.

- Migraciones o Despliegues en ambientes previos y productivos: No se identifica un punto de control relacionado con la gestión de los despliegues o migraciones realizadas en los ambientes de pruebas y productivos (bitácoras), que permita identificar la trazabilidad de los cambios y asegurar que éstos han sido probados en ambientes previos.

- Controles de Seguridad: Se carece de controles y procedimientos formales que protejan al código del Sistema, sus componentes y productos, para garantizar que no se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.

Los principales riesgos debido a la carencia o inconsistencia de los controles para el desarrollo de soluciones tecnológicas son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIAS EN LOS CONTROLES PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS

Factor crítico	Riesgo
Análisis de Vulnerabilidades de los aplicativos antes de su puesta en producción	La carencia del análisis de vulnerabilidades a las solicitudes de desarrollo de software o mantenimientos previos a su puesta a producción, representa un probable riesgo en la disponibilidad de las funcionalidades de la aplicación, debido a que no se están protegiendo los recursos que forman parte del sistema a nivel hardware, software y datos, lo que podría causar afectaciones en la operación, impactar tiempos, actividades y propiciar pérdidas financieras para la Empresa.
Seguridad del código de los sistemas	Debido a la falta de controles de seguridad para la protección del código de los sistemas, se tiene un probable riesgo para el Sistema, sus componentes, productos y demás elementos relacionados, ya que no existen procedimientos que impidan que se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.
Aseguramiento de la Calidad de los Sistemas	La carencia de procedimientos para la revisión de los resultados y productos que se deben entregar dentro de cada etapa y la confirmación del cumplimiento con los requerimientos, no asegura la calidad del proyecto, debido a que no se está midiendo el grado en el que el personal del proyecto se adhiere a la metodología y las desviaciones. Lo anterior se observa, con la finalidad de proponer recomendaciones para mejorar los procesos o para contar con mejores puntos de control cuando las desviaciones se presenten.
Gestión del Código Fuente	La falta de procedimientos para el control de versiones impide gestionar los cambios en el código fuente de los programas y poder revertirlos, lo que repercute en probables riesgos tales como la falta de ordenamiento para el almacenamiento de las versiones de código fuente que se tienen que gestionar; la imposibilidad de realizar cambios sobre los elementos almacenados de código fuente; la falta de un registro histórico de las acciones realizadas con cada versión de código fuente para construir las líneas base, entre otros.

FUENTE: Elaborada por la ASF con información proporcionada por PEMEX y los recorridos de pruebas.

No se acreditó la especialidad ni experiencia de los perfiles técnicos que participaron en el desarrollo de las soluciones; se detectaron pagos injustificados por 674.8 miles de pesos por la carencia de elementos técnicos que aseguren que el proveedor atendió la solicitud de cambio relacionada con la actualización de la herramienta tecnológica para el Sistema Institucional de Consolidación de Información Financiera. Asimismo, se detectaron desarrollos que no han sido utilizados por el usuario final desde hace más de 10 meses, aunado a que se identificaron deficiencias para la práctica del análisis de vulnerabilidades de los aplicativos previo a su puesta en producción y en el aseguramiento de la calidad de los sistemas.

2018-6-90T9N-20-0449-01-001 **Recomendación**

Para que Petróleos Mexicanos fortalezca la metodología de estimación de costos para el ciclo de vida del desarrollo de sistemas, que permita identificar el esfuerzo, costo y tiempo de las actividades que se realizan en los proyectos, con la finalidad de obtener métricas para calcular el costo del levantamiento de requerimientos, análisis, desarrollo, pruebas, implementación, puesta en marcha y mantenimiento de los sistemas, seleccionando el modelo de costos más apropiado de acuerdo con la etapa del proyecto, al lenguaje de programación utilizado y la documentación requerida, para asegurar las mejores condiciones para la Empresa.

2018-6-90T9N-20-0449-01-002 **Recomendación**

Para que Petróleos Mexicanos fortalezca los controles y procedimientos para que la prestación de los servicios de desarrollo y mantenimiento de soluciones tecnológicas cumpla con los criterios de aceptación de cada orden de trabajo y sea solicitada, prestada y recibida acorde a lo estipulado contractualmente; además, se asegure de que el personal responsable de atender los requerimientos cumpla con las competencias técnicas, y éstos tengan trazabilidad con los diseños funcionales y técnicos de las soluciones, con la finalidad de asegurar que sean atendidos y aprovechados conforme a las necesidades de las unidades de negocio asimismo, contar con prestadores de servicios competentes profesionalmente para realizar de manera adecuada los desarrollos y mantenimientos a los aplicativos.

2018-6-90T9N-20-0449-01-003 **Recomendación**

Para que Petróleos Mexicanos fortalezca los procedimientos de la metodología de desarrollo y mantenimiento de sistemas de información, en lo que se refiere al Análisis de vulnerabilidades de los aplicativos previo a su puesta en producción; Seguridad del código de los sistemas; Aseguramiento de la calidad y Gestión del código fuente, con la finalidad de verificar que los componentes y productos de las soluciones tecnológicas adquiridas o en desarrollo cumplan con los requerimientos definidos y cuenten con el nivel adecuado de seguridad de la información y calidad en el desarrollo de soluciones tecnológicas, a su vez salvaguarden la privacidad de los datos y se asegure el funcionamiento de las aplicaciones de la Empresa.

2018-9-90T9N-20-0449-08-001 **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 del Contrato PMX-2017-740-627 Servicio Técnico Especializado para Desarrollo, Mantenimiento, Configuración, Migración y/o Actualización de Soluciones en Diversas Plataformas Tecnológicas, solicitaron la implementación del módulo de Notas de Crédito/Débito relacionado al Proceso de Venta de Activos Improductivos en el ERP del

Corporativo y no ha sido utilizado por el usuario final desde su liberación realizada el 03 de julio de 2018, por lo que se desconoce si cumplirá con el fin contratado y justificará los recursos federales gastados en su desarrollo en incumplimiento de la Constitución Política de los Estados Unidos Mexicanos, Art. 134; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Art. 66, fracciones I y III; Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, y su reforma publicada el 23 de julio de 2018: Proceso de Administración de Proyectos (ADP), Apéndice IV.B Matriz de Metodologías, Normas y Mejores Prácticas aplicables a la Gestión de las TIC: Guía de los Fundamentos para la Dirección de Proyectos (PMBOK) - Gestión de los Costos del Proyecto - Estimar los Costos, Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software (CMMI-DEV); Estatuto Orgánico de Petróleos Mexicanos publicado en el Diario Oficial de la Federación el 05 de diciembre de 2017: Art. 18 fracciones VII y XXI; Art. 105 fracciones III, V y VII; Contrato PMX-2017-740-627: Cláusulas 5 y 16; Anexo B-1 Especificaciones Técnicas para el Servicio del contrato PMX-2017-740-627; Primer párrafo del apartado Modalidad por asignación y Cuarto párrafo del apartado Condiciones de ejecución y criterios técnicos de aceptación; Anexo Perfiles Técnicos; Metodología de Desarrollo y Mantenimiento de Sistemas de Información de Petróleos Mexicanos: numeral 8; y la Disposición Operativa para la Gestión de Cambios y Liberaciones (DCTI-CS-CL-GCO-0001): numeral 6

2018-6-90T9N-20-0449-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 674,848.04 pesos (seiscientos setenta y cuatro mil ochocientos cuarenta y ocho pesos 04/100 M.N.), por que no se tiene el detalle de los requerimientos ni el diseño de la solución para la Solicitud de Cambio 3482 de la Orden de Trabajo CAPG-58 correspondiente al procedimiento 4800030243, tampoco se cuenta con el soporte técnico que acredite que el proveedor realizó alguna configuración, adecuación o desarrollo relacionado con la funcionalidad mencionada, debido a la carencia de elementos técnicos que garanticen que el proveedor atendió dicha solicitud de cambio, la cual está relacionada con la Actualización de la Herramienta Tecnológica para el Sistema Institucional de Consolidación de Información Financiera, en incumplimiento de la Constitución Política de los Estados Unidos Mexicanos, Art. 134; del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, Art. 66, fracciones I y III; Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, y su reforma publicada el 23 de julio de 2018: Proceso de Administración de Proyectos (ADP), Apéndice IV.B Matriz de Metodologías, Normas y Mejores Prácticas aplicables a la Gestión de las TIC: Guía de los Fundamentos para la Dirección de Proyectos (PMBOK) - Gestión de los Costos del Proyecto - Estimar los Costos, Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software (CMMI-DEV); Estatuto Orgánico de Petróleos Mexicanos publicado en el Diario Oficial de la Federación el 05 de diciembre de 2017: Art. 18 fracciones VII y XXI; Art. 105 fracciones III, V y VII; Contrato PMX-2017-740-627: Cláusulas 5 y 16; Anexo B-1 Especificaciones Técnicas para el Servicio del contrato PMX-2017-

740-627; Primer párrafo del apartado Modalidad por asignación y Cuarto párrafo del apartado Condiciones de ejecución y criterios técnicos de aceptación; Anexo Perfiles Técnicos; Metodología de Desarrollo y Mantenimiento de Sistemas de Información de Petróleos Mexicanos: numeral 8; y la Disposición Operativa para la Gestión de Cambios y Liberaciones (DCTI-CS-CL-GCO-0001): numeral 6

Causa Raíz Probable de la Irregularidad

No existe monitoreo y supervisión al cumplimiento contractual y a los lineamientos, con respecto al servicio proporcionado por el proveedor.

3. Contrato 4800030244 para la prestación del "Servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores"

Se analizó el contrato 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 el Concurso Abierto Electrónico Internacional bajo la cobertura de los Tratados de Libre Comercio No. 2017-682-PMX_DOPA_PC_GCSSS-SA-CA-T-S, de acuerdo con los artículos 77 de la Ley de Petróleos Mexicanos y 11, fracción I, de las Disposiciones Generales de Contratación para Petróleos Mexicanos (Pemex) y sus Empresas Productivas Subsidiarias, con vigencia del 10 de noviembre de 2017 al 10 de noviembre de 2020, con un monto mínimo de 1,234,479.6 miles de pesos y monto máximo de 1,928,080.6 miles de pesos, con el objeto de prestar el servicio integral administrado de equipo de cómputo de escritorio, portátil, replicadores de puertos y monitores; en donde se efectuaron pagos por 278,116.7 miles de pesos por los servicios devengados en 2018, y se determinó lo siguiente:

Alcance de la contratación

La administración de equipos del servicio integral 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 Subservicios 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).

En 2012, este tipo de servicios se contrató a través de dos contratos abiertos y plurianuales con los proveedores Hewlett-Packard México, S. de R.L. de C.V. (HP), y OfiStore, S.A. de C.V. (OfiStore). Posteriormente se realizó una adjudicación directa para la contratación del "Servicio Integral de Aprovisionamiento de Equipo de Cómputo" con Soluciones Tecnológicas Especializadas, S.A de C.V., quien adquirió los 21,112 equipos propiedad de HP y los 5,447 propiedad de OfiStore.

Al 06 de diciembre de 2016, Pemex contaba con 77,044 equipos de cómputo de los cuales solo requerían 67,399 a partir de 2017, de acuerdo con la redistribución de equipos de cómputo realizada acorde a las funciones desarrolladas por los trabajadores. A partir de 2017,

la estrategia determinada fue la contratación del "Servicio Integral de Aprovisionamiento de Equipo de Cómputo" y "Servicio Integral Administrado de Equipo de Cómputo", el detalle de los servicios se muestra en la tabla siguiente:

Estrategia de contratación de equipos de cómputo para el periodo 2017 - 2019

Servicio Integral	Servicio para equipos	Servicio para accesorios	Total de servicios
Aprovisionamiento de Equipo Cómputo	25,899	660	26,559
Administrado de Equipo de Cómputo	41,500	22,835	64,335

FUENTE: Elaborada con información proporcionada por Pemex.

Revisión de Equipos y Control de Inventario

Se realizó una revisión en las instalaciones del Centro Administrativo Pemex (CAP) que cuenta con 3,122 equipos instalados en la Ciudad de México, y de una muestra aleatoria del 95.0% de confianza y 5.0% de error, se obtuvo un resultado de 376 equipos por revisar, para tal efecto, se tomó el Inventario de Equipos con corte a diciembre 2018 extraído de la Herramienta BMC Client Management, la revisión consistió en lo siguiente:

- Ejecución de script para conocer la marca, modelo y número de serie.
- Revisión de equipo periférico (Candado, Bocinas, Teclado y Mouse).
- Solicitud de carta de resguardo (proporcionadas en sitio por el personal de TI).
- Verificación de la ubicación, área y usuario asignado.

De los resultados de la revisión, se obtuvo un 77.4% (291 de 376 equipos) de cumplimiento, presentando observaciones, el 11.2% de los equipos (42 de 376), cabe mencionar que no fue posible revisar 43 equipos (11.4%) debido a que no se localizó al personal por diversas causas (reuniones, vacaciones, incapacidad, comisiones, foráneo, jubilación, por cambio de turno, personal sindicalizado, etc.), el detalle de la revisión de acuerdo con el tipo de perfil es el siguiente:

Muestra revisada de equipos del Contrato 4800030244

Perfil	Descripción	Total de equipos revisados	Cumple	No Cumple	Equipos no revisados
PC-1	PC Básica	88	63	17	8
PC-2	PC Intermedia	160	137	12	11
PC-3	PC Desarrollo	62	52	6	4
L-1	Laptop Ligera	9	5	1	3
L-2	Laptop Ligera Touch (2en1)	7	5	0	2
L-3	Laptop Completa	43	26	3	14
L-4	Laptop Uso Rudo	1	-	1	-
WS-1	Workstation Windows Básica	3	2	1	-
WS-2	Workstation Windows Avanzada	3	1	1	1
	TOTAL	376	291	42	43

FUENTE: Elaborado por la ASF con información proporcionada por PEMEX.

- Se identificaron usuarios que estaban utilizando un equipo que no correspondía a las características indicadas en las Cartas de Resguardo e Inventario de Equipos.

- No se proporcionó el soporte documental correspondiente a la reubicación de equipos o accesorios, puesta en operación de los equipos, así como el control de inventario.

- Se encontraron equipos cuya ubicación física (piso y/o edificio) no coincide con la registrada en el Inventario de Equipos.

- Se detectaron equipos sin bocinas ni candado.

2018-6-90T9N-20-0449-01-004 **Recomendación**

Para que Petróleos Mexicanos fortalezca los controles y procedimientos para identificar con oportunidad los cambios de asignación de equipos y accesorios en las herramientas BMC (gestión de servicios de TI) y CMDB (gestión de las configuraciones de los componentes tecnológicos), y contar con todos los elementos para conocer la trazabilidad de las actividades de instalación de los equipos en relación con los planes de trabajo y su registro adecuado en la CMDB con la finalidad de que se administren correctamente los equipos que son utilizados para las operaciones de los procesos.

4. Contrato PMX-2018-294-281 procedimiento 4800030734 "Servicio de comunicación segura para el acceso a internet de Petróleos Mexicanos, Empresas Productivas Subsidiarias y Filiales"

Se analizó el contrato de servicios PMX-2018-294-281 procedimiento 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. (en adelante TI América), mediante el procedimiento de Concurso Abierto Electrónico Nacional, con vigencia del 10 de julio de 2018 al 10 de julio de 2021, por un monto mínimo de 714,139.3 miles de pesos y monto máximo de 804,512.1 miles de pesos, con el objetivo de contar con el "Servicio de Comunicación Segura para el Acceso a Internet (en adelante 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", durante el ejercicio 2018 se realizaron pagos por 65,342.4 miles de pesos; al respecto, se determinó lo siguiente:

Alcance de la Contratación

La cobertura del servicio es para siete sitios con enlace a Internet, los cuales contarán con las soluciones tecnológicas siguientes:

Alcance del contrato PMX-2018-294-281

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 Protección de DNS perimetral[1] Acceso Remoto vía VPN[1] Detección y Respuesta de Amenazas en Equipos de Cómputo Finales

Fuente: Elaborado por la ASF con información proporcionada por PEMEX.
Nota [1]: Soluciones consideradas únicamente para los sitios de Ciudad de México y Villahermosa.

- El análisis de mercado no consideró la justificación relacionada con la cantidad de equipos de usuarios finales que debían ser protegidos, cabe mencionar que en las Bases de la Convocatoria únicamente se describe la cantidad mínima (43,000) y máxima (60,000) de equipos, sin detalles adicionales.

- Se confirmó que no existió un análisis basado en las necesidades de la entidad, antes de la elaboración de dichas Bases, por lo que se concluye que PEMEX no realizó un dimensionamiento para determinar la capacidad de los recursos requeridos en el contrato.

Eventos de Seguridad

Durante diciembre de 2018, se presentaron 443,240 eventos de seguridad que fueron detectados por las herramientas de prevención de intrusos y antimalware de PEMEX, y se bloquearon para evitar una afectación a los usuarios de la red; además, en el mes de febrero de 2019 se presentaron 323,793; el detalle es el siguiente:

Eventos de seguridad detectados por el contrato PMX-2018-294-281

Eventos	diciembre 2018	febrero 2019
Sistema de Prevención de Intrusiones (IPS)	250,000	190,900
Protección y Contención de Amenazas Persistentes Avanzadas en Red	190,000	127,700
Detección y Respuesta de Amenazas en Equipos de Cómputo Finales	3,240	5,193
Denegación de los servicios (servicio o recurso bloqueado)	0	0
TOTAL	**443,240**	**323,793**

FUENTE: Elaborada por la ASF con información proporcionada por Pemex.

Durante el ejercicio 2018, no se identificaron incidentes de seguridad que infringieran las políticas de seguridad informática de PEMEX.

Revisión del Centro de Operaciones de Seguridad (SOC)

En la verificación del cumplimiento contractual y técnico del SOC que es operado por el proveedor, se identificaron los servicios siguientes:

Herramientas utilizadas para gestión y monitoreo de los servicios del contrato PMX-2018-294-28

Servicio	Breve descripción del Servicio
Filtrado de Contenido Web	Controla y restringe el acceso a internet de acuerdo a una línea base (sitios web, aplicaciones, contenido no deseado, descargas, etc.)
Protección Antivirus en Red	Detecta y previene el software malicioso (virus, gusanos, troyanos, etc.) que pudiera instalarse en los servidores y en las estaciones de trabajo que conforman la red de PEMEX.
Inspección de Tráfico SSL/TLS	Monitorea la información enviada y recibida de la web, y garantiza que la comunicación sea segura y privada, cifrando los datos que se transmiten.
Firewall de Siguiente Generación (NGFW)	Detecta y bloquea ataques, brinda la protección integral contra amenazas.
Sistema de Prevención de Intrusiones (IPS)	Detecta y bloquea cualquier intento de intrusión, transmisión de código malicioso, ataques o amenazas a través de la red hacia los servidores.
Detección y Prevención de Fugas de Información (DLP)	Previene la pérdida o ex filtración de datos protegiendo la información, evitando que una persona ajena a PEMEX o no autorizada (interna) tenga acceso a la información confidencial y sensible.
Protección y Contención de Amenazas Persistentes Avanzadas en Red (ATP Red)	Protege y evita la materialización de ataques sofisticados a la red de PEMEX cuya finalidad es acceder a la información sensible sin ser detectado.
Detección y Respuesta de Amenazas en Equipos de Cómputo Finales (ATP Endpoint)	Detecta y remedia de forma proactiva y oportuna las amenazas (los intentos de acceso a la información, ejecutar programas maliciosos, vulnerar el equipo, etc.) sin interrumpir la operación de los usuarios finales.
Protección de DNS perimetral	Evita la ex filtración de datos y/o ataques de Denegación del Servicio (servicio o recurso bloqueado, sin acceso). Bloquea el acceso a sitios maliciosos, para prevenir el acceso no autorizado a la red de PEMEX o que se descarguen archivos maliciosos en los equipos.
Acceso Remoto vía VPN	Establece un canal, conexión y transmisión de datos segura a la red de PEMEX a través de internet.

Fuente: Elaborada por la ASF con información proporcionada por PEMEX.

- En relación con el Filtrado de Contenido Web se identificó que PEMEX no cuenta con una línea base debidamente formalizada y autorizada de los criterios establecidos para dicho filtrado.

- Sobre los servicios de Protección y Contención de Amenazas Persistentes Avanzadas en Red, Detección y Prevención de Fugas de Información, así como el servicio de Detección y Respuesta de Amenazas en Equipos de Cómputo Finales, se detectó que el proveedor que administra y monitorea los servicios de Comunicación Segura para el acceso a internet, a través de sus herramientas puede interceptar, extraer y almacenar información sensible, también tiene conocimiento del origen y destino de los datos, así como del remitente y destinatario. No obstante, no se identificaron mecanismos de control que alerten a PEMEX para evitar posibles fugas de información por parte del prestador de servicios.

Equipos de Usuarios Finales Protegidos en su Navegación en Internet

A través de las herramientas de administración de equipos de PEMEX se identificó una población de 56,162 usuarios; al respecto, se verificó la instalación y funcionamiento de las soluciones que protegen la navegación en Internet, en una muestra de 200 equipos de usuarios finales, determinada con un nivel de confianza del 90% y margen de error del 5%, se encontró lo siguiente:

- Equipos de cómputo finales en los cuales no se instaló la solución de Detección y Respuesta de Amenazas.

- Equipos sin la solución de Detección y Prevención de Fugas de Información.

- Equipos en los cuales no se instaló ninguna de las dos soluciones mencionadas.

No se llevó a cabo un análisis basado en las necesidades de PEMEX, antes de la elaboración de las bases de contratación, para determinar la capacidad de los recursos requeridos en el contrato; asimismo, se detectó que el prestador de servicios, a través de sus herramientas, puede interceptar, extraer y almacenar información sensible, no obstante, no se identificaron mecanismos de control que alerten a PEMEX para evitar posibles fugas de información.

2018-6-90T9N-20-0449-01-005 **Recomendación**

Para que Petróleos Mexicanos fortalezca los procedimientos en la prestación de los servicios para contar con planes que aseguren que la capacidad de la infraestructura tecnológica corresponde con las necesidades de la organización de una forma efectiva en términos de unidades, costos y tiempo, con la finalidad de que las contrataciones consideren los resultados de los programas de capacidad para soportar los servicios de manera alineada con la evolución de la demanda, aunado a obtener las mejores condiciones en términos de economía y calidad en beneficio de la Empresa.

2018-6-90T9N-20-0449-01-006 **Recomendación**

Para que Petróleos Mexicanos fortalezca los controles preventivos, detectivos y correctivos para el manejo de la información sensible a la que tienen acceso los proveedores, tales como el bloqueo de puertos físicos y lógicos, borrado seguro aleatorio de equipos, monitoreo de las bitácoras de actividades de los analistas, entre otros, con la finalidad de evitar la fuga de información sensible y asegurar la privacidad de la información que es gestionada por los prestadores de servicios.

2018-6-90T9N-20-0449-01-007 **Recomendación**

Para que Petróleos Mexicanos fortalezca los mecanismos de revisión periódica del cumplimiento contractual de las actividades, calidad de los productos generados y niveles de servicio establecidos con los prestadores de servicios, y se asegure del aprovisionamiento de los servicios de acuerdo con los requerimientos establecidos en los contratos, con la finalidad de prevenir incidentes de seguridad que pongan en riesgo la integridad, confidencialidad y disponibilidad de los activos de información de la Empresa.

5. Ciberseguridad

Se analizó la información proporcionada por Petróleos Mexicanos, relacionada con la administración y operación de los controles de Ciberseguridad, además se revisaron las políticas, marcos rectores y herramientas informáticas en esta materia, y se observó lo siguiente:

Inventario de Software Autorizado y no Autorizado

- La identificación de la instalación de software no autorizado en equipos de usuarios finales se realiza mediante una directiva, a través de la cual se impide cualquier intento de instalación de software que no esté registrado en la lista blanca; en el caso de los servidores la identificación se realiza con una inspección manual, cabe mencionar que la lista blanca no se encuentra formalizada.

- En relación con la lista de software autorizado, no existe un procedimiento que defina el medio para solicitar cambios, el personal que puede hacerlo y los aprobadores.

Configuraciones de Imágenes Seguras para Hardware y Software en los Dispositivos Móviles, Ordenadores Portátiles, Estaciones de Trabajo y Servidores

- PEMEX realiza una verificación manual de las imágenes maestras; sin embargo, no lo hace de manera continua ni automatizada, debido a que no cuenta con herramientas de verificación para estas tareas.

Evaluación Continua de la Vulnerabilidad y Solución

- No se tiene definido el tratamiento del análisis de vulnerabilidades antes de la puesta en operación de nuevos desarrollos de sistemas, ni los procedimientos, autorizaciones, excepciones, atención y monitoreo que son requeridos, tampoco los criterios para el involucramiento del Grupo Operativo de Liberaciones (GOL) y el Grupo Asesor de Cambios (GAC).

Mantenimiento, Supervisión y Análisis de Registros de Auditoría

- No se realiza una revisión periódica de las pistas de auditoría y las bitácoras de los aplicativos sustantivos, sus bases de datos y sistemas operativos, con la finalidad de identificar transacciones no autorizadas, posible fuga de información o vulnerabilidades relacionadas con la seguridad de los sistemas.

Correo Electrónico y Protección Web del Navegador

- En relación con el filtrado de contenido web no se cuenta con una línea base debidamente formalizada y autorizada de los criterios establecidos para dicho filtrado.

Protección de Datos y Defensas de Malware

- Se identificó que el proveedor que administra y monitorea estos servicios, a través de sus herramientas puede interceptar, extraer y almacenar información sensible, no obstante, no se identificaron mecanismos de control que alerten a PEMEX para evitar la posible fuga de información por parte del prestador de servicios.

- En relación con la protección de equipos de usuario final, se identificó que algunos no se encontraban protegidos, lo que los hace vulnerables a los ataques cibernéticos.

Restricción y Control de Puertos de Red, Protocolos y Servicios

- No se cuenta con herramientas de escaneo de puertos para verificar si existieron cambios en los servicios de la infraestructura tecnológica, así como en los sistemas sustantivos y adjetivos, con la finalidad de advertir oportunamente al personal de seguridad informática para tomar las acciones pertinentes.

Configuraciones Seguras para Dispositivos de Red tales como Cortafuegos, Enrutadores e Interruptores

- No se gestiona activamente ni se actualizan las reglas de configuración de seguridad de los dispositivos de infraestructura de red, tampoco se cuenta con un proceso formal relacionado con dicha actividad.

Capacitación Adecuada para Evitar Deficiencias

- Se tienen programas de comunicación, concientización y formación de seguridad para los usuarios finales, no obstante, no se evalúan los resultados de los programas aplicados, para identificar si el conocimiento en temas de seguridad informática es suficiente o necesita reforzarse.

Seguridad del Software de Aplicaciones

- Se carece de un procedimiento formalizado para la revisión de la calidad y seguridad del código de los desarrollos de software; así como de controles técnicos de verificación y validación para las revisiones de los componentes y productos construidos.

- No se tienen controles ni procedimientos formales que protejan el código de los sistemas, sus componentes y productos, para garantizar que no se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.

Pruebas de Penetración

- Durante 2018, no se realizaron pruebas de penetración externa o interna para identificar vulnerabilidades y vectores de ataque.

Continuidad de las Operaciones de TIC

- Durante 2018, se realizaron pruebas al Plan de Recuperación en caso de Desastre sobre 16 aplicativos críticos; no obstante, no fue posible verificar que dichas pruebas se encuentran alineadas con el Plan de Continuidad del Negocio ni al Análisis de Impacto del Negocio debido a que no fueron identificados ni proporcionados por PEMEX, en consecuencia, no se puede asegurar que el tipo de pruebas aplicadas y su cobertura considera la priorización, criticidad y necesidades de la Alta Dirección de la Empresa, así como los tiempos de tolerancia para operar sin afectar la continuidad del negocio.

Con la revisión de los controles y procedimientos para la Ciberseguridad, se comprobó que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de PEMEX, son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIAS EN LOS CONTROLES DE CIBERSEGURIDAD

Factor crítico	Riesgo
Configuraciones de seguridad en dispositivos de comunicaciones	La falta de revisión continua de la línea base de los dispositivos de comunicaciones, favorece la labor del atacante y retarda el fortalecimiento de los mecanismos de seguridad para contener los incidentes en las redes, lo que puede impactar a los procesos y servicios de la Empresa.
Análisis de Vulnerabilidades previo a la puesta en marcha de los aplicativos	La carencia del análisis de vulnerabilidades a las solicitudes de desarrollo de sistemas o mantenimientos previos a su puesta en producción, representa un riesgo en la disponibilidad de las funcionalidades de los aplicativos, debido a que no se aseguran de la protección de los recursos que forman parte del sistema en todas las capas que lo componen.
Mantenimiento, monitoreo y análisis de registros de auditoría	Las bitácoras no se revisan de manera periódica, lo que puede dar oportunidad a los usuarios maliciosos para ejecutar transacciones no autorizadas que comprometan la integridad de los activos de información.
Protección de Datos y Defensas de malware	El proveedor que administra y monitorea los servicios de seguridad, a través de sus herramientas puede interceptar, extraer y almacenar información sensible, así como conocer el origen y destino de los datos, lo que podría propiciar la fuga de información.
Restricción y Control de puertos de red, protocolos y servicios	Se carece del monitoreo de los puertos de red, lo que aumenta el riesgo en caso de que existan vulnerabilidades y que éstas puedan ser aprovechadas por los atacantes para acceder a la red y tomar información que comprometa los activos de la Empresa.
Pruebas de Penetración	La carencia de pruebas de penetración externa e interna puede poner en riesgo a la empresa al no identificar las vulnerabilidades y vectores de ataque a la infraestructura tecnológica y aplicativos sustantivos.
Análisis de Impacto al Negocio	La falta de un Análisis de Impacto al Negocio, ocasiona que no se tengan identificadas las funciones, actividades, unidades administrativas, ni los servicios sustantivos que podrían resultar afectados por la interrupción de los servicios de TIC, tampoco la estimación del impacto técnico, económico y reputacional desde la perspectiva de la Alta Dirección de la Empresa.

FUENTE: Elaborado por la ASF con la información proporcionada por PEMEX y los recorridos de pruebas.

Las deficiencias en las configuraciones de seguridad en los dispositivos de comunicaciones, la falta de análisis de vulnerabilidades previo a la puesta en marcha de los sistemas, la carencia de alertas para prevenir la fuga de información por parte de los prestadores de servicios y la falta de un Análisis de Impacto al Negocio desde la perspectiva de la Alta Dirección de PEMEX, representan un probable riesgo para la operación de los procesos y servicios, aunado a que comprometen la integridad, confiabilidad y disponibilidad de los activos de la Empresa.

2018-6-90T9N-20-0449-01-008 **Recomendación**

Para que Petróleos Mexicanos fortalezca los controles y procedimientos para las configuraciones de seguridad en dispositivos, análisis de vulnerabilidades previo a la puesta en marcha de los aplicativos, restricción y control de puertos de red, así como las pruebas de penetración a las redes y sistemas al menos semestralmente, con la finalidad de asegurar que toda la infraestructura empresarial (redes, aplicaciones y dispositivos móviles) cumpla con los objetivos de la seguridad informática, para fortalecer la capacidad de respuesta y protección de las redes ante los ataques.

2018-6-90T9N-20-0449-01-009 **Recomendación**

Para que Petróleos Mexicanos implemente un Análisis de Impacto al Negocio donde se consideren todos los procesos sustantivos para la operación de la empresa, el cual contemple las funciones, actividades, áreas, servicios, punto objetivo de recuperación de la información, tiempo objetivo de recuperación de los procesos, pérdidas económicas, costos adicionales, daños reputacionales, incumplimiento de las disposiciones, riesgos para la seguridad del personal y capacidad operativa, entre otros, con la finalidad de mitigar los riesgos asociados con el funcionamiento de los procesos para asegurar la continuidad de las operaciones de la Empresa.

Montos por Aclarar

Se determinaron 674,848.04 pesos pendientes por aclarar.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Controles internos y Aseguramiento de calidad.

Resumen de Observaciones y Acciones

Se determinaron 4 observaciones las cuales generaron: 9 Recomendaciones, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 1 Pliego de Observaciones.

Dictamen

El presente dictamen se emite el 12 de junio de 2019, 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, 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, Petróleos Mexicanos cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- No se acreditó la especialidad y experiencia de los perfiles técnicos que participaron en el desarrollo de los sistemas; se detectaron pagos injustificados por 674.8 miles de pesos por la carencia de elementos técnicos que aseguren que el proveedor atendió la solicitud de cambio relacionada con la actualización de la herramienta tecnológica para el Sistema Institucional de Consolidación de Información Financiera.

- Se detectaron desarrollos de sistemas que no han sido utilizados por el usuario final desde hace más de 10 meses, aunado a que se identificaron deficiencias para 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 carece de un programa de capacidad de la infraestructura tecnológica para determinar los recursos requeridos en los contratos; asimismo, se detectó que el prestador de servicios de operaciones de seguridad a través de sus herramientas puede interceptar, extraer y almacenar información sensible; no obstante, no se identificaron mecanismos de control que alerten a PEMEX para evitar la fuga de información por parte del proveedor.

- Se identificaron deficiencias en las configuraciones de seguridad de los dispositivos de comunicaciones, falta de mantenimiento, monitoreo y análisis de registros de auditoría, así como 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 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 correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; analizar el gasto ejercido en materia de TIC en los capítulos contables de la Cuenta Pública fiscalizada.

2. Validar que el estudio de factibilidad comprenda 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 el estudio de mercado.

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; analizar la documentación de las contrataciones para descartar asociaciones indebidas, subcontrataciones en exceso, adjudicaciones sin fundamento, transferencia de obligaciones, suscripción de los contratos (facultades para la suscripción, cumplimiento de las obligaciones fiscales, fianzas), entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permitan su fiscalización, correspondan 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 en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados, telecomunicaciones y demás relacionados con las TIC para verificar: los antecedentes; la investigación de mercado; la adjudicación; los beneficios esperados; el análisis de entregables (términos, vigencia, entrega, resguardo, operación, penalizaciones y garantías); las pruebas de cumplimiento y sustantivas, la implementación y post-implementación; además, verificar que el plan de mitigación de riesgos, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad fueron atendidos.

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; análisis y pruebas de vulnerabilidades, entre otros. Verificar los procedimientos que permitan disminuir el impacto que puede sufrir la entidad a causa de eventos adversos o desastres que atenten contra la continuidad de las operaciones.

Áreas Revisadas

La Dirección Corporativa de Tecnologías de la Información (DCTI) y la Dirección Corporativa de Administración y Servicios 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. Constitución Política de los Estados Unidos Mexicanos: Art. 134

2. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: Art. 66, fracciones I y III

3. Otras disposiciones de carácter general, específico, estatal o municipal: Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, y su reforma publicada el 23 de julio de 2018: Proceso de Administración de la Seguridad de la Información (ASI); Proceso de Administración de Proyectos (ADP), Apéndice IV.B Matriz de Metodologías, Normas y Mejores Prácticas aplicables a la Gestión de las TIC: Guía de los Fundamentos para la Dirección de Proyectos (PMBOK) - Gestión de los Costos del Proyecto - Estimar los Costos, Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software (CMMI-DEV), Norma ISO 20000 apartado de la Gestión de la Capacidad, Norma ISO 27032 Gestión de la Ciberseguridad; Estatuto Orgánico de Petróleos Mexicanos publicado en el Diario Oficial de la Federación el 05 de diciembre de 2017: Art. 18 fracciones VII y XXI; Art. 105 fracciones III, V y VII; Contrato PMX-2017-740-627: Cláusulas 5 y 16; Contrato No. PMX-2018-294-281: Cláusula 16; Anexo B-1 Especificaciones Técnicas para el Servicio del contrato PMX-2017-740-627; Primer párrafo del apartado Modalidad por asignación y Cuarto párrafo del apartado Condiciones de ejecución y criterios técnicos de aceptación; Anexo B-1 Especificaciones técnicas del contrato No. 4800030244: numerales 2.6, 2.7, 4.4 y 4.6; Anexo B-1 Especificaciones técnicas del contrato No. PMX-2018-294-281: Numeral 2 puntos 17, 20, 21; Subnumerales 3.9, 3.11 punto 1 y 2; Anexo Perfiles Técnicos; Metodología de Desarrollo y Mantenimiento de Sistemas de Información de

Petróleos Mexicanos: numeral 8;y la Disposición Operativa para la Gestión de Cambios y Liberaciones (DCTI-CS-CL-GCO-0001): numeral 6.

Fundamento Jurídico de la ASF para Promover Acciones

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.