CFE Corporativo

Auditoría de Ciberseguridad del Sector Energía

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-6-90UJB-20-0466-2021

466-DE

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2020 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

Fiscalizar los controles de ciberseguridad de los sistemas relacionados con la distribución de energía eléctrica, así como gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	746,142.4
Muestra Auditada	31,339.5
Representatividad de la Muestra	4.2%

El universo seleccionado por 746,142.4 miles de pesos corresponde al total ejercido en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2020; la muestra auditada está integrada de dos contratos relacionados con la prestación de los Servicios de Análisis de Vulnerabilidades, Cumplimiento y Gestión Continua del Riesgo Tecnológico en la Infraestructura de Cómputo; y el de Adquisición de SCADA SAS IEC61850, con pagos ejercidos por 31,339.5 miles de pesos, que representan el 4.2% del universo seleccionado. Cabe señalar que el alcance de la auditoría es la evaluación de la ciberseguridad en CFE y a la Empresa Productiva Subsidiaria CFE Transmisión (EPS CFE Transmisión) y la muestra está integrada por dos contratos relacionados con dicho tema, contenidos en el tomo VIII de la Cuenta Pública 2020.

Antecedentes

La energía es fundamental en todos los países, una interrupción del suministro eléctrico puede impactar en servicios fundamentales.

La ciberseguridad es un elemento imprescindible en el sector energético debido a la trascendencia de las infraestructuras críticas para los servicios públicos, el alto valor de los activos empresariales a proteger y, por la necesidad de defenderse ante los crecientes ciberataques que tiene este sector.

Algunos de los ataques a nivel mundial que se han presentado en este sector son los siguientes:

- 2003, EE. UU., planta de energía nuclear, malware Slammer. [1]
- 2008, Irán, instalaciones nucleares, gusano Stuxnest. [2]
- 2012, EE. UU, generación de energía, error humano y botnet mariposa. [3]
- 2012, Países Bajos, telecomunicaciones, hackeo.
- 2013-2015, EE. UU. y Canadá, generación de energía, hackeo.
- 2015, Corea del Sur, planta de energía nuclear, hackeo.
- 2016, Israel, red eléctrica, malware[4] y errores humanos.
- 2016, Ucrania, Kiev, red eléctrica, malware Industroyer. [5]
- 2019, EE. UU, sistemas eléctricos, Denegación de Servicio Distribuido (DDoS).

Como se puede apreciar en la lista anterior, el sector energético, al ser uno de los sectores más importantes, está expuesto a ciberataques de todo tipo, desde malware, ataques de DDoS y patrones estándar de ataques APT[6] hasta verse envueltos en ataques patrocinados por países.

Incidente del 28 de diciembre de 2020 en el Sistema Interconectado Nacional

El evento suscitado el 28 de diciembre de 2020 en el Sistema Interconectado Nacional, no fue derivado de un incidente de ciberseguridad de acuerdo con la información proporcionada por la CFE, en este incidente se presentaron fallas en las líneas de transmisión que forman parte

[1] Gusano informático que provoca una Denegación de servicio.
[2] Gusano informático que afecta a equipos con Windows, permite la ejecución de código malicioso alojado dentro de dispositivos USB sin la necesidad de utilizar un archivo autorun.
[3] Conjunto de dispositivos conectados a Internet (ordenadores personales, servidores, dispositivos móviles, dispositivos IoT, etc.) infectados y controlados por un malware.
[4] Cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario. Es un gusano informático que provoca una Denegación de servicio.
[5] Malware que es capaz de controlar directamente los conmutadores y los interruptores de las subestaciones eléctricas.
[6] Amenaza avanzada persistente (por sus siglas en inglés APT), utiliza técnicas de hackeo continuas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado y potencialmente destructivo.

de la interconexión eléctrica entre la Zona Metropolitana de Monterrey, Nuevo León y el polo energético e industrial de Altamira, Tamaulipas. Este incidente afectó el suministro eléctrico a 10 millones de clientes en 29 estados del país. La interrupción del servicio eléctrico duró aproximadamente una hora y 44 minutos. Los factores críticos que lo causaron fueron, entre otros: La falla en uno de los tres conductores de línea, como resultado de la ionización del aire debido a la quema de basura y arbustos en el derecho de vía; Instalación y puesta en servicio de nuevos tableros de protección, control y medición que fueron puestos en servicio sin haberse probado completamente y que afectaron el proceso operativo, el desempeño de diversas unidades de centrales eléctricas estaban fuera de lo establecido en el Código de Red; previo al incidente se estaban realizando trabajos en las subestaciones de la línea afectada, situación que no fue prevista por parte de los operadores de la CFE y el Centro Nacional de Control de Energía (CENACE).

Sistema Eléctrico Nacional

De conformidad con lo que establece la Ley de la Industria Eléctrica (LIE), el Estado ejerce el control operativo del Sistema Eléctrico Nacional (SEN) a través del CENACE. Mientras que la EPS CFE Transmisión, tiene por objeto realizar las actividades necesarias para prestar el servicio público de transmisión de energía eléctrica nacional, así como para llevar a cabo, entre otras actividades, el financiamiento, instalación, mantenimiento, gestión, operación y ampliación de la infraestructura necesaria para prestar el servicio público de transmisión y algunas de sus funciones son las siguientes:

- Prestar el Servicio Público de Transmisión de Energía Eléctrica.
- Operar la Red Nacional de Transmisión conforme a las instrucciones del CENACE.
- Cumplir con las obligaciones de Calidad, Confiabilidad, Continuidad y Seguridad que emita la Comisión Reguladora de Energía (CRE).
- Llevar a cabo los proyectos de ampliación y modernización de la Red Nacional de Transmisión que se incluyan en los programas correspondientes, previa instrucción de la SENER.
- Participar en el desarrollo de los programas de ampliación y modernización para la Red Nacional de Transmisión.
- Interconectar a sus redes las Centrales Eléctricas cuyos representantes lo soliciten, y conectar a sus redes los Centros de Carga cuyos representantes lo soliciten, en condiciones no indebidamente discriminatorias, cuando ello sea técnicamente factible.
- Llevar a cabo las demás operaciones y el mantenimiento de la Red Nacional de Transmisión de conformidad con los artículos 15 y 26 de la LIE.

.El SEN está integrado por:

- La Red Nacional de Transmisión (RNT).
- Las Redes Generales de Distribución (RGD).
- Las Centrales Eléctricas que entregan energía eléctrica a la RNT o a las RGD.
- Los equipos e instalaciones del CENACE utilizados para llevar a cabo el control operativo del SEN.
- Los demás elementos que determine la SENER.

La infraestructura de transmisión y distribución del SEN hace posible la transformación, transmisión, distribución y comercialización de energía eléctrica a lo largo de todo el país. Esta infraestructura es operada por gerencias de control que mantienen la confiabilidad e integridad del sistema. Las áreas supervisan, a su vez, que la demanda y la oferta de energía eléctrica estén balanceadas en cualquier instante.

Términos relacionados con la auditoría

Sistemas SCADA

El SCADA (Supervisory Control And Data Acquisition) es una herramienta que permite la Supervisión, Control y Adquisición de Datos compuesto por una o más estaciones maestras, ubicadas en un centro de control, conectadas por un sistema de comunicaciones a un número de unidades terminales remotas, que están ubicadas en diferentes instalaciones, que permite controlar y supervisar el sistema eléctrico, facilitando retroalimentación en tiempo real sobre mediciones y el estado de los equipos en campo, y permitiendo control sobre los mismos. Actualmente los sistemas SCADA son usados en la industria eléctrica en funciones como: Generación, Transmisión y Distribución.

Tecnología de Operación (TO)

La Tecnología de Operación (TO) es el uso de hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura. Los sistemas de tecnologías de Operación se encuentran en una amplia gama de sectores con alta utilización de activos, realizando una gran variedad de tareas que van desde el monitoreo de Infraestructura crítica hasta el control de robots en una planta de fabricación. Este tipo de tecnología es ampliamente utilizado en la industria de generación, transmisión y distribución de energía eléctrica.

Tecnología de Información (TI)

Todo equipo o sistema interconectado o subsistema de equipo que se utilice en la adquisición, almacenamiento, manipulación, gestión, movimiento, control, visualización, conmutación, intercambio, transmisión o recepción automática de datos o información. El término tecnología de la información incluye computadoras, equipos auxiliares, software, firmware y

procedimientos, servicios similares (incluidos los servicios de soporte) y recursos relacionados. [7]

Sistemas de Control Industrial

Sistemas utilizados para el control, monitorización y supervisión de los procesos industriales. Están conectados a los elementos que intervienen en el proceso (sensores y actuadores) y pueden interactuar con ellos enviando órdenes o recibiendo datos. [8]

La Tecnología de Operación (TO) incluye a todos los dispositivos y Sistemas de Control Industrial (ICS, por sus siglas en inglés) que permiten la automatización de procesos industriales de producción y de generación de servicios, por ejemplo, dispositivos para el control de válvulas, turbinas, motores para la apertura y cierre de compuertas, entre muchos otros. Los ICS, como por ejemplo los sistemas SCADA, constituyen una parte fundamental de la infraestructura crítica de las empresas del sector energético. Las empresas del sector energético confían en los ICS para generar, distribuir y transmitir energía. Actualmente existe una amplia variedad de activos electrónicos que apoyan en la generación, distribución y transmisión de energía eléctrica, por lo que resulta esencial proteger estos dispositivos para mantener la continuidad de las operaciones. Estos activos deben monitorearse continuamente y administrarse para reducir el riesgo de un ataque cibernético.

Actualmente, los sistemas TI y TO están más integrados, son más complejos y presentan vulnerabilidades. Cuando las instalaciones de generación y distribución transfieren el control de sus equipos desde sus infraestructuras internas a sistemas SCADA, los cuales tienen acceso a través de internet, están introduciendo ciber vulnerabilidades.

Comisión Federal Electricidad (CFE)

La Comisión Federal de Electricidad (CFE) es una Empresa Productiva del Estado, propiedad exclusiva del Gobierno Federal, con personalidad jurídica y patrimonio propio, que goza de autonomía técnica, operativa y de gestión, conforme a lo dispuesto en la Ley de la Comisión Federal de Electricidad.

Tiene como misión suministrar insumos y bienes energéticos requeridos para el desarrollo productivo y social del país de forma eficiente, sustentable, económica e incluyente, mediante una política que priorice la seguridad y la soberanía energética nacional y fortalezca el servicio público de electricidad

En enero de 2016 se publicaron los términos para la estricta separación legal de la CFE, estableciendo que la empresa realizaría sus actividades de manera independiente, bajo

[7] Definición de acuerdo con el NIST Special Publication 800-53.

[8] Definición de acuerdo con la publicación Estado de preparación en ciberseguridad del sector eléctrico en América Latina.

condiciones de estricta separación legal y a través de empresas productivas subsidiarias (EPS), empresas filiales (EF) o cualquier modelo de asociación previsto por la Ley de la CFE.

En este sentido, en abril de 2017 se publicó en el Diario Oficial de la Federación (DOF) el Estatuto Orgánico de la CFE que establece la estructura orgánica básica, integrada por un Consejo de Administración como órgano supremo de administración, un Director General, una Auditoría Interna dependiente del Consejo de Administración, cuatro comités técnicos de apoyo, seis direcciones corporativas, nueve Empresas Productivas Subsidiarias y cuatro empresas filiales, además de cuatro unidades de negocio.

Las EPS son Empresas Productivas del Estado, con personalidad jurídica y patrimonio propio, para realizar, de manera independiente y bajo condiciones de estricta separación legal de la CFE, cualquiera de las actividades siguientes: Generación, Transmisión, Distribución, Suministro básico, Suministro calificado, Suministro de último recurso, la proveeduría de insumos primarios para la industria eléctrica, así como las actividades auxiliares y conexas de la misma (Manual de Organización General de la CFE de fecha 25 de abril de 2018) .

EPS CFE Transmisión

La EPS CFE Transmisión es una Empresa Productiva Subsidiaria de la CFE, con personalidad jurídica y patrimonio propio, sujeta a la conducción central, dirección estratégica y coordinación de la CFE, de conformidad con lo establecido en la Ley de la CFE publicada en el DOF el 11 de agosto de 2014 y su Reglamento con última reforma publicada en el mismo medio el 9 de febrero de 2015, que tiene como finalidad generar valor económico y rentabilidad para el Estado Mexicano.

Coordinación de Servicios Tecnológicos

La Coordinación de Servicios Tecnológicos (CST), adscrita a la Dirección Corporativa de Administración, de acuerdo con el artículo 47 del Estatuto Orgánico de la CFE publicado en el DOF el 12 de abril de 2017, tiene como función coordinar la administración de tecnologías de información, transformación digital y comunicaciones, así como proponer las políticas y lineamientos en estas materias; promover la elaboración de convenios con instituciones para el intercambio de información, apoyos técnicos, tecnológicos y científicos; evaluar técnica y presupuestalmente las adquisiciones de tecnologías de la información de la CFE y sus empresas productivas subsidiarias; proponer y ejecutar mecanismos de evaluación y mejora de la calidad de los servicios tecnológicos y proponer la estrategia del programa de capacitación de los recursos humanos en materia de tecnologías de la información en la CFE.

Entre 2016 y 2020, en la CFE se han invertido 3,458,339.1 miles de pesos en equipo de cómputo / telecomunicaciones, arrendamiento de bienes, mantenimiento, servicio de desarrollo de aplicaciones, servicios de conducción de señales, servicios generales que incluye bienes informáticos y software, entre otros, integrados de la manera siguiente:

Tabla 1. Recursos erogados en materia de TIC en la CFE

(Miles de pesos)

PERIODO DE EROGACIÓN	2016	2017	2018	2019	2020	Total
MONTO POR AÑO	541,355.9	551,014.1	679,414.7	782,319.9	904,234.5	**3,458,339.1**

FUENTE: Elaborado por la ASF con base en la información proporcionada por la CFE.

Con base en el análisis de la gestión de las TIC, efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados, con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones y función de las TIC sujetas de revisión, y determinar el alcance, naturaleza y muestra de la revisión, se obtuvieron los resultados que se presentan en este informe.

Resultados

1. Cuenta Pública y Presentación en Estados Financieros

Análisis presupuestal

De acuerdo con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal de 2020, publicado en el Diario Oficial de la Federación el 11 de diciembre de 2019, a la CFE se le aprobó un presupuesto de 456,437,051.3 miles de pesos. De lo reportado en la Cuenta de la Hacienda Pública Federal 2020, la CFE tuvo un presupuesto pagado por 215,935,675.3 miles de pesos, y la EPS CFE Transmisión tuvo un presupuesto pagado por 54,650,690.9 miles de pesos.

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC), por la CFE corresponden a 746,142.4 miles de pesos como se muestra a continuación:

Tabla 2. Gastos de TIC en 2020

(Miles de pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
3000		**Servicios Generales**	**657,483.9**
	31701	Servicios de conducción de señales analógicas y digitales	247,607.6
	33104	Otras asesorías para la operación de programas	6.1
	33301	Servicios de desarrollo de aplicaciones informáticas	385,599.7
	35301	Mantenimiento y conservación de bienes informáticos	9,535.5
	35701	Mantenimiento y conservación de maquinaria y equipo	14,735.0
5000		**Bienes Muebles, Inmuebles e Intangibles**	**88,658.5**
	51501	Bienes informáticos	27,984.7
	56501	Equipos y aparatos de comunicaciones y telecomunicaciones	8,086.9
	59101	Software	52,586.9
		TOTAL	**746,142.4**

FUENTE: Elaborado con base en la información proporcionada por la CFE Corporativo.

NOTA: La GTI no indicó el monto correspondiente a Gastos de TIC para cada EPS.

Las partidas específicas relacionadas con Servicios Personales (Capítulo 1000), para la CFE, corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 158,066.5 miles de pesos durante el ejercicio fiscal 2020; considerando 171 plazas: 66 de confianza y 105 sindicalizados, el promedio anual percibido por persona fue de 924.4 miles de pesos.

Del total ejercido en 2020 en materia de TIC por 746,142.4 miles de pesos, se seleccionó una muestra de dos contratos relacionados con la ciberseguridad, cuya evaluación es el objeto de esta auditoría, por los que se realizaron pagos de 31,339.5 miles de pesos que representan el 4.2% del total ejercido, los cuales se integran de la manera siguiente:

Tabla 3. Muestra de contratos ejercidos durante 2020 por la CFE

(Miles de pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto	Ejercido 2020
				De	Al		
Concurso Abierto Nacional con fundamento en el Artículo 79 de la Ley de Comisión Federal de Electricidad, en las disposiciones 22 fracción I, inciso a) 24, 26, fracciones III y XI, 30 fracción I de las Disposiciones Generales en Materia de adquisiciones, arrendamientos, contratación de servicios y ejecución de obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias	800938585	Tecniman, S.A. de C.V.	Servicios de Análisis de Vulnerabilidades, Cumplimiento y Gestión Continua del Riesgo Tecnológico en la Infraestructura de Cómputo	17/08/2020	30/11/2020	17,927.7	17,927.7
Concurso Abierto Internacional bajo la cobertura de los Tratados de Libre Comercio con fundamento en el Artículo 79 de la Ley de Comisión Federal de Electricidad, en las disposiciones 22 fracción I, inciso a) 24, 26, fracciones III y XI, 30 fracción I de las Disposiciones Generales en Materia de adquisiciones, arrendamientos, contratación de servicios y ejecución de obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias	700511947	Siemens, S.A de C.V.	Adquisición de SCADA SAS IEC61850	07/09/2020	31/12/2020	13,411.8	13,411.8
FUENTE: Contratos y facturas proporcionadas por la CFE.					**Subtotal**	13,411.8	13,411.8
					Total	31,339.5	31,339.5

Al solicitar a la Gerencia de Tecnologías de Información (GTI) la integración de los pagos de los contratos por 31,339.5 miles de pesos por pagos de TIC, proporcionó información global y no específica, por lo que no fue posible identificar el pago de los contratos, durante la auditoría se solicitó la aclaración sin obtener respuesta.

Normativa

En el organigrama de la CFE se observó que la Gerencia de Tecnologías de Información se encuentra adscrita a la Coordinación de Servicios Tecnológicos; sin embargo, no cuenta con funciones definidas y formalizadas, toda vez que en el Estatuto Orgánico publicado en el DOF el 12 de abril de 2017 y en el Manual de Organización General (MOG) de la CFE del 25 de abril de 2018 no mencionan a esta Gerencia.

El Manual de Organización de la Gerencia de Tecnologías de Información de la CFE, no se ha actualizado desde 2012 e invocan el cumplimiento del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), lo cual, a la fecha de la auditoría (julio de 2021), ya no le aplica a la CFE, ni a sus EPS y tampoco a las EF.

2020-6-90UJB-20-0466-01-001 **Recomendación**

Para que la CFE Corporativo actualice el Manual de Organización de la Gerencia de Tecnologías de Información de la Comisión Federal de Electricidad, a fin de que se encuentre acorde con la estructura definida en su organigrama, que esté alineado a la Dirección Corporativa de Administración y a la Coordinación de Servicios Tecnológicos, con el fin de asegurar la gobernanza corporativa de las Tecnologías de Información y Comunicaciones en la Comisión Federal de Electricidad, sus Empresas Productivas Subsidiarias y Empresas Filiales.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-6-90UJB-20-0466-01-002 **Recomendación**

Para que la CFE Corporativo y la CFE Transmisión afecten las partidas del gasto correspondientes y verifiquen cómo se validan los pagos con las partidas relacionadas con las contrataciones en materia de Tecnologías de la Información y Comunicaciones.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2. Contrato número 800938585, celebrado con Tecniman, S.A. de C.V.

Se revisó el contrato número 800938585, celebrado con Tecniman, S.A. de C.V., mediante procedimiento de Concurso Abierto Nacional, con fundamento en el artículo 79 de la Ley de la Comisión Federal de Electricidad; en las disposiciones 22, fracción I, inciso a), 24, 26, fracciones III y XI, 30, fracción I, de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias, con objeto de prestar el "Servicio de Análisis de Vulnerabilidades, Cumplimiento y Gestión Continua del Riesgo Tecnológico en la Infraestructura de Cómputo de la CFE", con vigencia del 17 de agosto al 30 de noviembre de 2020, por un monto de 17,927.7 miles de pesos, con pagos realizados en 2020 por 17,927.7 miles de pesos, se determinó lo siguiente:

Objetivo

Implementar un proceso de análisis de vulnerabilidades, identificación de cumplimiento y gestión continua del riesgo tecnológico en la infraestructura de cómputo de la CFE, mediante:

- Una plataforma para la gestión de la solución, así como equipamiento para la operación de las consolas de análisis de vulnerabilidades, cumplimiento y gestión continua del riesgo tecnológico.

- Soporte técnico, licenciamiento, atención y seguimiento de incidentes.

Alcance

La solución permite de forma proactiva detectar las vulnerabilidades y riesgos de los activos de TIC de la CFE y su Empresas Productivas Subsidiarias (EPS). La solución consideró activos de Tecnologías de Información (TI).

El proveedor debería de cumplir con lo siguiente:

- Ofertar una infraestructura que incluya hardware, software, licenciamiento, suscripciones, equipamiento y soporte técnico para implementar la solución de análisis de vulnerabilidades.

- Considerar una base de 10,000 activos de cómputo y al menos 1,000 aplicativos webs.

- Proporcionar el software, licenciamiento, suscripciones, equipamiento y soporte técnico de la solución de análisis de vulnerabilidades, cumplimiento y gestión continua del riesgo tecnológico en la infraestructura de cómputo de la CFE.

- Proveer infraestructura nueva, con soporte y garantía durante 12 meses a partir de la implementación y puesta en operación de las componentes de la solución.

- Respaldar su oferta técnica con documentación oficial de la solución ofertada donde se especifiquen puntualmente las funcionalidades solicitadas y en donde se puedan verificar los requerimientos técnicos solicitados.

- Las licencias y póliza de soporte técnico tendrían una vigencia de 12 meses a partir de la implementación y puesta en operación de los componentes de la solución.

Investigación de mercado

- No se presentó evidencia de los criterios bajo los cuales se escogieron a los posibles proveedores.

- Se invitaron a 12 posibles proveedores para presentar la cotización en respuesta a la solicitud recibida por la CFE, sin embargo, sólo fueron 4 los que presentaron una cotización, cómo se muestra a continuación:

Tabla 4. Cotizaciones de Proveedores

(Miles de Pesos)

UNIDAD DE MEDIDA	PLAZO	SERVICIO	COTIZACIONES			
			BG2 SERVICES	CYBOLT	SCITUM	CYCSAS
1 servicio	12 meses	Implementación de software, licenciamiento, y suscripciones	7,148.1	236.9	7,731.7	4,062.5
		10,000 dispositivos y 1,000 aplicativos	8,240.3	17,096.4	9,130.6	12,442.4
		Total	15,388.4	17,333.3	16,862.3	16,504.9

FUENTE: Elaboración propia con información proporcionada por CFE.

- Del resultado de la Investigación de las Condiciones de Mercado, se observa que la empresa BG2 Services, S.A de C.V., es la que presenta menor precio y se identificó que se dedica a brindar el servicio de seguridad informática, sin embargo, este proveedor no participó en la evaluación de las propuestas técnicas y económicas dentro del Proceso de Contratación.

Pliego de requisitos

- Se carece de evidencia que de certeza que la información de todos los concursantes fue presentada en el Micrositio de Concursos de la CFE, lo que incumplió lo indicado en el numeral III.2 “Calendario de las etapas del procedimiento” del Pliego de Requisitos.

- No se proporcionó evidencia de que los recursos humanos del proveedor Tecniman, S.A. de C.V., plasmados en su oferta técnica se encuentren adscritos a su plantilla.

- El documento “Evaluación Económica” no cuenta con las firmas autógrafas del Jefe de Departamento de Concursos y Subgerente de Adquisiciones del Área Contratante en el apartado de Elaboró y Dictaminó.

- A la fecha de la auditoría (julio de 2021), la normativa de la CFE relacionada con las contrataciones (pliego de requisitos) no considera que el proveedor adjudicado demuestre tener experiencia en los servicios solicitados.

Análisis del proveedor

- El objeto social del proveedor ganador, Tecniman, S.A. de C.V., es de naturaleza distinta de los servicios requeridos por la CFE, tal como se especifica en su página https://www.tecniman.mx/ siendo sus principales actividades económicas el comercio al por mayor de equipo y material eléctrico, instalaciones eléctricas en construcciones y reparación y mantenimiento de maquinaria y equipo industrial. No obstante, el resultado de la evaluación técnica de los proveedores realizada por la CFE determinó que la oferta técnica de Tecniman, S.A. de C.V., cumplió con lo requerido en las especificaciones técnicas del Pliego de Requisitos.

- La ASF identificó que el proveedor Tecniman, S.A. de C.V., solo actuó como intermediario, ya que no acreditó con información justificativa y comprobatoria su participación en los servicios proporcionados a la CFE, toda vez que no contaba con la capacidad técnica y humana para realizarlos, la única actividad identificada por este ente fiscalizador fue haber participado en el proceso de licitación.

- Para proporcionar el servicio requerido por la CFE, el proveedor realizó la subcontratación de las empresas Silent4business, S.A. de C.V., y Adistec México, S.A. de C.V., para proporcionar el servicio de implementación, puesta en punto de la infraestructura solicitada y de la herramienta Tenable Vulnerability Management, sus licencias y soporte, respectivamente, que corresponde al 100.0% de los servicios contratados por la CFE.

- La ASF realizó la validación de los distribuidores y revendedores de los productos y servicios de marca Tenable en México en su página oficial, y se verificó que Tecniman, S.A de C.V., no figura como distribuidor ni revendedor oficial a pesar de que se le expidió una carta de licenciamiento por parte de Tenable.

- La CFE indicó no tener conocimiento de que el proveedor Tecniman, S.A. de C.V., realizaría una subcontratación, toda vez que en el Pliego de Requisitos no manifestó dicha posibilidad y que en dado caso de que el proveedor hubiera presentado una petición para realizar la subcontratación, se hubiera rechazado. La CFE manifiesta que, al no tener conocimiento de esta acción, se deslinda de toda actividad que haya realizado el proveedor respecto a la subcontratación.

- El proveedor incumplió con la disposición 45 del pliego de requisitos que establece que sólo cuando la CFE lo especifique el proveedor o contratista podrá subcontratar y en su caso no podrá rebasar el 49% del importe total del Contrato.

- Se constató que el pago realizado al proveedor Tecniman S.A de C.V., ascendió a 17,927.6 miles de pesos, el cual, para llevar a cabo los servicios subcontrató el 100.0% de éstos con las empresas Silent4business, S.A. de C.V., y Adistec México, S.A de C.V., con un costo total de 12,517.5 miles de pesos, por lo que no se justificó el beneficio económico obtenido por Tecniman S.A, de C.V de 5,410.1 miles de pesos, entre lo

cobrado a CFE y lo pagado por la subcontratación al 100.0%, al no haber participado en la ejecución de los servicios contratados, en incumplimiento a lo establecido en los artículos 93, fracción I, y 102, párrafo II, de la Ley de la Comisión Federal de Electricidad publicada en el Diario Oficial de la Federación el 11 de agosto de 2014; de la Disposición 3, fracciones I y II, 5, fracciones I y XII, 25, fracción III, y 45 de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias publicadas el 23 de junio de 2015 y su última reforma publicada en el Diario Oficial de la Federación el 29 de noviembre de 2019; en el artículo 47 del Estatuto Orgánico de la Comisión Federal de Electricidad publicado en el Diario Oficial de la Federación el 12 de abril de 2017; el numeral 5 Estructura Orgánica, inciso 1.4.0.3 Coordinación de Servicios Tecnológicos, objetivo, funciones 4, 9, y 11 del Manual de Organización General de la Comisión Federal de Electricidad publicado el 25 de abril de 2018 y el numeral 1.3.0.1.2.3.0.0.3. Unidad de Proyectos, funciones, párrafo cuarto y quinto del Manual de Organización de la Gerencia de Tecnologías de Información, publicado en la normateca interna de la CFE el 27 de agosto de 2012.

Características técnicas del servicio

En la revisión de las especificaciones requeridas por la Coordinación de Servicios Tecnológicos de la CFE, se identificó:

Instalación de la solución

Los 16 recursos que realizaron el despliegue e instalación de los sensores en las 18 ubicaciones de la CFE en la República Mexicana no formaron parte de la plantilla del personal de Tecniman, S.A. de C.V., corresponden al personal del proveedor Silent4Bussiness, S.A. de C.V.

Licenciamiento

El licenciamiento proporcionado tiene vigencia de un año, el cual finaliza el 16 de octubre de 2021. La CFE consideró licenciamiento para 10,000 dispositivos y 1,000 aplicativos de cualquiera de los procesos de Generación, Distribución, Transmisión, Suministro Básico. Los 10,000 activos representan para la CFE un 20.0% de sus activos de TIC y corresponde a equipos de cómputo personal (escritorio y laptops), servidores y aplicativos web, a la fecha de la auditoría (julio de 2021) se identificó:

- El licenciamiento es una suscripción, la cual no está a nombre de la CFE por lo que no se tiene certeza que la CFE sea dueña de dicho licenciamiento.

- Los activos incluidos bajo el alcance de la solución no están clasificados homogéneamente.

- La CFE no cuenta con los cálculos y métricas consideradas para dimensionar el tamaño de la solución que requería para cubrir sus necesidades.

- Del total de las 10,000 licencias no han sido utilizadas el 45.8%.

- Solo han sido analizados 6 aplicativos web de los 1,000 considerados en el alcance, solo ha sido utilizado el 0.6% de la capacidad estimada.

Funcionamiento de la solución

- A la fecha de la auditoría (julio de 2021), los sensores de Veracruz y Villahermosa, Tabasco, se encontraban fuera de línea debido a un corte de energía por tormenta y no se contaba con un plan de trabajo o acciones de remediación.

- El personal de la Coordinación de Servicios Tecnológicos no cuenta con el conocimiento para realizar la configuración de la solución.

- Para realizar la evaluación del riesgo, la herramienta realiza una comparación por sector; sin embargo, se tiene configurada a la CFE en el giro de Administración Pública y no en el de Energía por lo que dicha medición no permite identificar el grado de exposición al riesgo de acuerdo con el giro correspondiente.

- La CFE no ha realizado acciones para utilizar la información proporcionada en los escaneos y en su caso mitigar vulnerabilidades detectadas.

- La CFE solicitó que la herramienta realizara auditorías de configuraciones para diversos sistemas; a la fecha de la auditoría (julio de 2021), no se han llevado a cabo.

- La CFE solicitó que la solución contara con un conector específico para el servicio de Amazon Web Services, Azure y Google, relacionados con la construcción, administración y despliegue de aplicaciones y servicios en la nube; no obstante que se proporcionó, esta funcionalidad no se ha utilizado a la fecha de la auditoría (julio 2021).

- La solución cuenta con capacidades para efectuar análisis de vulnerabilidades basadas en mejores prácticas y marcos de referencia, tales como las emitidas por el Centro de Seguridad de Internet (CIS, por sus siglas en inglés), la Agencia de Sistemas de Información de Defensa (DISA, por sus siglas en inglés) y las Guías de Implementación Técnica de Seguridad (STIG, por sus siglas en inglés); sin embargo, el personal de la CFE no cuenta con los conocimientos para realizar este tipo de análisis.

Capacitación y acompañamiento

- No se presentó evidencia que acredite que se brindó el soporte en sitio durante el mes solicitado.

- Tecniman, S.A. de C.V., no ha proporcionado capacitación en la configuración de la herramienta.

Soporte técnico

No se tiene evidencia del uso de la base de conocimientos de la herramienta, ni que se hayan efectuado revisiones a las configuraciones por parte del proveedor.

Mesa de servicios

Para este servicio no se acreditó lo siguiente:

- La estructura organizacional de la mesa de ayuda que atiende los reportes.

- Documentación de la alineación de la mesa de servicios al estándar de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL, por sus siglas en inglés) y fungir como el único punto de contacto para reportar incidencias.

- La CST cuenta con acceso a la herramienta para registro de tickets (Remedy), sin embargo, no ha sido utilizado, ya que las solicitudes se hacen mediante correo electrónico, y no por una herramienta de registro de tickets.

- La definición de tiempos máximos de atención y planes de respuesta formalizados.

Por lo anterior, se determinó que la Gerencia de Abastecimiento y la Coordinación de Servicios Tecnológicos (CST) no optaron por las mejores condiciones para el estado al no haber seleccionado a distribuidores autorizados por el fabricante y que contara con la experiencia para implementar los servicios.

Respecto de la solución Tenable, ésta se encuentra instalada y es funcional en la CFE; no obstante, no se ha explotado todas las características y funcionalidades con las que cuenta.

2020-6-90UJB-20-0466-01-003 **Recomendación**

Para que la CFE Corporativo realice las modificaciones pertinentes en la normativa aplicable al proceso de contratación, en el cual se incluya que los posibles proveedores demuestren tener experiencia en las actividades a desarrollar y con los requerimientos solicitados, y que sea un factor en la evaluación técnica efectuada por la Coordinación de Servicios Tecnológicos.

Los términos de esta recomendación y los mecanismos para su atención fueron acordados con la entidad fiscalizada.

2020-6-90UJB-20-0466-01-004 **Recomendación**

Para que la CFE Corporativo programe ventanas de escaneo de vulnerabilidades a los activos críticos que se encuentren en el alcance de la solución y no sólo los solicitados a petición de las áreas usuarias (Empresas Productivas Subsidiarias de los procesos de Generación, Distribución, Transmisión, Suministro Básico y filiales), y que se configure la herramienta para que pueda comparar con vulnerabilidades del sector energético, utilizar las funcionalidades provistas por la solución y brindar capacitación especializada a los operadores de la herramienta que le permitan explotar al máximo sus capacidades de detección.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-9-90TVV-20-0466-08-001 **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 CFE Consolidado 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, no verificaron que la estructura organizacional presentada en la propuesta técnica por el proveedor no cumplió con lo establecido en el pliego de requisitos y contrataron al proveedor Tecniman S.A. de C.V, sin que contara con la capacidad técnica, humana y operativa para llevar a cabo la implementación de los servicios solicitados, ya que se detectó que subcontrató el 100.0% de dichos servicios por lo que no se garantizaron las mejores condiciones para el Estado en dicha contratación, en incumplimiento de lo establecido en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, párrafo tercero; los artículos 93, fracción I, y 102, párrafo II, de la Ley de la Comisión Federal de Electricidad publicada en el Diario Oficial el 11 de agosto de 2014; los artículos 7, fracciones I y VI, 69 y 70 de la Ley General de Responsabilidades Administrativas de los Servidores Públicos, publicada en el Diario Oficial de la Federación el 18 de julio de 2016; el artículo 47, fracción III, del Estatuto Orgánico de la Comisión Federal de Electricidad publicado en el Diario Oficial de la Federación el 12 de abril de 2017; el numeral 5 'Estructura Orgánica', el inciso 1.4.0.3, Coordinación de Servicios Tecnológicos, objetivo, funciones 4, 9 y 11 del Manual de Organización General de la Comisión Federal de Electricidad publicado en la normateca interna de CFE el 25 de abril de 2018; el numeral 1.3.0.1.2.3.0.0.3., Unidad de Proyectos, funciones, párrafos cuarto y quinto, del Manual de Organización de la Gerencia de Tecnologías de Información, publicado en la normateca interna de la CFE el 27 de agosto de 2012 y las Disposiciones 3, 5, fracciones I, X y XII, 25, fracción III, y 45 de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la CFE y sus EPS

publicadas en el Diario Oficial de la Federación el 23 de junio de 2015 y su última reforma publicada en el mismo medio el 29 de noviembre de 2019.

2020-6-90UJB-20-0466-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 5,410,133.01 pesos (cinco millones cuatrocientos diez mil ciento treinta y tres pesos 01/100 M.N.), por concepto derivado del pago que la CFE realizó del contrato número 800938585 'Servicio de Análisis de Vulnerabilidades, Cumplimiento y Gestión Continua del Riesgo Tecnológico en la Infraestructura de Cómputo de la CFE', que corresponden al beneficio económico no justificado que obtuvo el proveedor Tecniman, S.A. de C.V., por la diferencia entre el pago que recibió por parte de la CFE de 17,927,674.95 pesos (diecisiete millones novecientos veintisiete mil seiscientos setenta y cuatro pesos 95/100) y el costo que Tecniman, S.A. de C.V., pagó por 12,517.541.94 pesos (doce millones quinientos diecisiete mil quinientos cuarenta y uno pesos 94/100 M.M) a los proveedores Silent4business, S.A. de C.V., y Adistec México, S.A de C.V., con quienes subcontrató el servicio y los cuales lo ejecutaron al 100.0%; adicionalmente, incumplió al no informar en su propuesta que el servicio ofertado a la CFE se realizaría mediante esta subcontratación. La ASF identificó que el proveedor Tecniman, S.A. de C.V., sólo actuó como intermediario, ya que no acreditó con información justificativa y comprobatoria su participación en los servicios proporcionados a la CFE, toda vez que no contaba con la capacidad técnica y humana para realizarlos; la única actividad identificada por este ente fiscalizador fue haber participado en el proceso de licitación, por lo que no se contrató en las mejores condiciones para el estado, en incumplimiento de lo establecido en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, párrafo tercero; en los artículos 1, párrafo segundo, 5, último párrafo, y 51, párrafo tercero, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, publicada el 30 de marzo de 2006, en el Diario Oficial de la Federación y su última reforma publicada en el mismo medio el 19 de noviembre de 2019; de los artículos 7, fracciones I y VI, 69 y 70 de la Ley General de Responsabilidades Administrativas de los Servidores Públicos, publicada en el Diario Oficial de la Federación el 18 de julio de 2016; de los artículos 93, fracción I, y 102, párrafo II, de la Ley de la Comisión Federal de Electricidad, publicada en el Diario Oficial de la Federación el 11 de agosto de 2014; del artículo 47 del Estatuto Orgánico de la Comisión Federal de Electricidad publicado en el Diario Oficial de la Federación el 12 de abril de 2017; del numeral 5 Estructura Orgánica, inciso 1.4.0.3, Coordinación de Servicios Tecnológicos, objetivo, funciones 4, 9 y 11 del Manual de Organización General de la Comisión Federal de Electricidad publicado el 25 de abril de 2018, del numeral 1.3.0.1.2.3.0.0.3., Unidad de Proyectos, funciones, párrafos cuarto y quinto, del Manual de Organización de la Gerencia de Tecnologías de Información, publicado en la normateca interna de la CFE el 27 de agosto de 2012 y de la Disposición 3, fracciones I y II, 5, fracciones I y XII, 25, fracción III, y 45 de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias publicadas el 23 de junio de 2015 y su última reforma publicada en el Diario Oficial de la Federación el 29 de noviembre de 2019.

Causa Raíz Probable de la Irregularidad

Falta de supervisión a los servicios.

3. Contrato número 700511947 "Adquisición de SCADA SAS IEC61850 para la Comisión Federal de Electricidad Transmisión"

Se revisó el contrato número 700511947, celebrado con Siemens, S.A. de C.V., mediante un procedimiento de Concurso Abierto Internacional, con fundamento en el artículo 79 de la Ley de Comisión Federal de Electricidad, numerales 22, fracción I, inciso a), 24, 26, fracciones III y XI, 30, fracción I, de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias, con objeto de llevar a cabo la "Adquisición de SCADA SAS IEC 61850 para la Comisión Federal de Electricidad Transmisión", con vigencia del 7 de septiembre al 31 de diciembre de 2020, por un monto de 13,411.8 miles de pesos. Durante el ejercicio 2020, se realizaron pagos por 13,411.8 miles de pesos, se determinó lo siguiente:

Antecedentes

En el contrato se plasmó que debido a que la Red Nacional de Transmisión de la Comisión Federal de Electricidad requiere de una alta disponibilidad y confiabilidad operativa, la EPS CFE Transmisión, en aras de proporcionar un servicio con eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad, de acuerdo con el apartado 2 del artículo 4 de la Ley de la Industria Eléctrica requirió contratar estos servicios con el objetivo de evitar daños al personal de mantenimiento y a las instalaciones de la Red Nacional de Transmisión que ocasionen interrupciones a los usuarios de los servicios eléctricos.

Alcance

Se consideraron las siguientes actividades:

- Elaboración de la ingeniería del proyecto
- Suministro del equipamiento requerido
- Configuración
- Pruebas FAT (de fábrica)
- Capacitación

El proyecto consistió en el aprovisionamiento del sistema de Automatización de Subestaciones (SAS) IEC61850 así como de la infraestructura que lo soporta. Dicho sistema tiene la función de integrar todas las señales y parámetros eléctricos del equipo eléctrico primario y los dispositivos inteligentes electrónicos (DEI´s), de la subestación para ser enviados a los centros de control para su monitoreo y análisis. Asimismo, el sistema tiene la

funcionalidad de control en la Red Eléctrica de forma local o remota mediante su control supervisorio.

Pagos

Se identificaron deficiencias en el proceso de pago, dado que en la documentación se carecía de las firmas o sellos de validación de las facturas correspondientes a los pagos de los servicios adquiridos y los oficios de solicitud y trámite de pago.

Características técnicas del servicio

En la revisión de las especificaciones requeridas por la EPS CFE Transmisión, se identificó lo siguiente:

- El equipamiento fue entregado por el proveedor Siemens, S.A. de C.V., en diciembre de 2020, de un universo de 208 elementos que conforman el inventario, se eligió una muestra de 130, de los cuales, se identificó que, a la fecha de la auditoría (julio de 2021), sólo 24 elementos (18.5%) se encontraban instalados y energizados en los centros de datos de la Zona de Transmisión Yucatán y los 106 elementos restantes, es decir, un 81.5% se encontraban en almacén.

- El equipamiento no ha sido instalado en su totalidad, ya que la EPS CFE Transmisión se encuentra en espera de la conclusión de la obra civil que será la base para instalar las unidades de control de bahía y los tableros. Dado que no ha sido instalado, la entidad no ha podido realizar las pruebas solicitadas ni validar las características y configuraciones requeridas en el anexo 1 del contrato.

Supervisión

- El programa para la puesta de servicio no se encuentra formalizado y no muestra el inicio y fin de cada una de las actividades, incluidas las de la obra civil, por lo que no se tiene una fecha compromiso para la puesta en servicio de la totalidad de los elementos adquiridos.

- El Programa de puesta en servicio contiene 20 actividades con el avance planeado; sin embargo, carece del avance real de las mismas; este plan considera que, en marzo de 2022, se inicie la obra civil, la puesta en servicio sería a finales de abril y la entrega en operación incluyendo pruebas operativas sería a finales de noviembre de 2022.

- El Laboratorio de Pruebas de Equipos y Materiales (LAPEM), quien se encarga de realizar pruebas eléctricas o de cumplimiento de seguridad, no certificó la infraestructura solicitada en este contrato.

-

- La CFE solicitó que la infraestructura contara con al menos 2 años de garantía por escrito, a partir de la entrega de los equipos en almacén. A la fecha de la auditoría (julio de 2021) han transcurrido siete meses de la garantía del fabricante, sin que los equipos estén instalados.

Por lo anterior, se observa que existen deficiencias en la planeación, administración y supervisión para la implementación en la infraestructura adquirida, ya que lleva 7 meses en almacén y no ha sido instalada ni probada; así mismo, el programa para la puesta de servicio, no se encontraba formalizado y carece del avance real de las actividades por lo que no se tiene la certeza de la fecha en la cual se pondrá en marcha la infraestructura adquirida.

2020-6-90UIW-20-0466-01-001 **Recomendación**

Para que la CFE Transmisión fortalezca los mecanismos de supervisión relacionados con el proceso de pagos a los proveedores, y establezca mecanismos de control que permitan verificar o supervisar que las facturas sean recibidas mediante sello y firma e incluyan la fecha en la que fueron entregadas.

Los términos de esta recomendación y los mecanismos para su atención fueron acordados con la entidad fiscalizada.

2020-6-90UIW-20-0466-01-002 **Recomendación**

Para que la CFE Transmisión actualice el programa de Puesta en Servicio, conforme al avance real, dé seguimiento puntual a la obra civil requerida y se implemente toda la infraestructura adquirida en el contrato número 700511947, celebrado con Siemens, S.A. de C.V., antes de que se termine la garantía del proveedor.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

4. Gobierno de TIC

La Coordinación de Servicios Tecnológicos (CST) de la Comisión Federal de Electricidad (CFE) es el área responsable de asegurar la gobernanza corporativa de las Tecnologías de Información y Comunicaciones (TIC) en la CFE y sus Empresas Productivas Subsidiarias (EPS), del portafolio de iniciativas y proyectos estratégicos desde su planeación y presupuestación hasta su implementación, definir la arquitectura de los sistemas informáticos y tecnologías de la información, establecer la planeación, estándares, requerimientos y normativa en la materia, incluida la seguridad de la información, así como realizar la evaluación que garantice y promueva la mejora de la calidad de los servicios tecnológicos.

Entre sus funciones se encuentran:

- Diseñar, proponer y evaluar el plan estratégico en materia de tecnologías de información y comunicaciones de corto, mediano y largo plazos de la CFE y sus EPS, para asegurar la gobernanza corporativa.

- Definir y coordinar los estándares, arquitectura y requerimientos tecnológicos, normatividad y lineamientos corporativos en materia de gobierno de datos, comunicaciones, portales y TIC, entre otros, para contar con una infraestructura homologada e interoperable en la CFE y EPS.

- Ejercer la gobernanza corporativa de las TIC en la CFE y sus EPS, a través de las políticas en la materia, sus lineamientos y normatividad específica aplicable, para garantizar el adecuado uso y aprovechamiento de las TIC.

- Definir y diseñar las políticas, lineamientos y normatividad en materia de seguridad tecnológica para la CFE y sus EPS, que permitan garantizar la seguridad de los sistemas, datos e información.

En la CFE y en las EPS existen 2 conceptos respecto a la operación de las Tecnologías de Información:

- Tecnología de Información (TI), es aquella que da servicios e infraestructura a las actividades administrativas en la CFE, esta es supervisada y cuenta con lineamientos de gestión emitidos por la CST.

- Tecnología de Operación (TO), es aquella tecnología e infraestructura que soporta la operación de los servicios operativos de las EPS, relacionados con las actividades de Generación, Transmisión y Distribución de los servicios eléctricos, pueden variar de acuerdo con el ámbito de operación tal es el caso de tecnología nuclear, hidroeléctrica, energías limpias.

Para efectos de la revisión del proceso de gobierno, el grupo auditor tomó como base lo establecido en las Políticas Generales relativas a las Tecnologías de Información y Comunicaciones de la CFE y sus EPS y Filiales, que cuenta con una clasificación de procesos basados en los establecidos en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, por cada proceso se identificó lo siguiente:

Proceso de Gobierno de TIC

- La CST no considera en su planeación estratégica proyectos de ciberseguridad; se limita a servicios de TI de la CST excluyendo a las EPS y filiales.

Proceso de Administración del Presupuesto

- La CST no supervisa ni monitorea el presupuesto ejercido en los proyectos de TIC de otras áreas o EPS y Filiales; se carece de políticas y procedimientos específicos para la autorización de presupuesto de TI de áreas internas de la CFE, las EPS y filiales.

Proceso de Administración de las Contrataciones

- En caso de contrataciones de TI, la CST tiene un papel de asesor, sólo a petición de áreas administrativas y EPS. No se tiene un proceso definido para el seguimiento de las áreas de oportunidad de los proyectos estratégicos.

Proceso de Administración de Servicios

- La CST no realiza actividades de dimensionamiento a la de capacidad de su infraestructura.

Proceso de Administración de la Configuración

- La CST no cuenta con un procedimiento homologado para documentar las actividades relacionadas con el control de cambios para el de desarrollo de software e infraestructura.

Proceso de Administración de la Seguridad

- La CST, en sus procesos de gestión de riesgos de TIC, clasificación de infraestructura y monitoreo no considera a las EPS y filiales.

- No ha dado seguimiento y continuidad a sus actividades de reforzamiento de ciberseguridad.

Proceso de Operación de Controles de Seguridad de la Información

- La CST no ha realizado evaluaciones del nivel de madurez de su Sistema de Gestión de Seguridad de la Información.

- La CFE no ha definido, mediante políticas, la definición de que es la TO, su alcance y quien debe de realizar su administración y monitoreo, no ha definido ni formalizado controles de ciberseguridad en la infraestructura de TO.

Proceso de Administración de la Operación

- La CST no monitorea la infraestructura de otras direcciones corporativas, aun cuando les da alojamiento en el centro de datos de la Gerencia de Tecnologías de la Información.

Las Políticas Generales relativas a las Tecnologías de Información y Comunicaciones de la CFE y sus EPS y Filiales, no han sido actualizadas desde hace 6 años, ni cuentan con los criterios para realizar la clasificación de TI y TO.

La CST presenta informes anuales al Consejo Consultivo Técnico de la Dirección Corporativa de Administración, respecto a los servicios de TI que administra bajo contrataciones a su cargo.

Gobierno y administración del Proyecto Red Eléctrica Inteligente (REI)

Desde abril de 2018, la EPS CFE Transmisión está implementando el proyecto Red Eléctrica Inteligente (REI), el cual tiene como objetivo coadyuvar a incrementar la confiabilidad y calidad de sus sistemas críticos, que a su vez le permita realizar la interconexión de sistemas de energías renovables, reducir costos y disminuir el impacto al medio ambiente.

Planeación Estratégica (PE) del Proyecto REI

El proyecto se encuentra integrado en el Plan Estratégico de TIC de la CFE, identificado como proyecto estratégico, debido a su relevancia en cuanto al cumplimiento de la normativa aplicable para la CFE, plantea beneficios como: eficiencia de la red, penetración de energía renovable distribuida, reducción de pérdidas, reducción de costos, retorno de inversión. Se definió que se llevarían a cabo evaluaciones de riesgos continuas durante toda la implementación y ejecución del proyecto; sin embargo, se carecen de Índices de Desempeño Clave (KPI por sus siglas en inglés) y métricas para evaluar el cumplimiento de dichos beneficios, así como de la evaluación continua de los riesgos.

Se observó una discrepancia en el alcance oficial, el cual indica 1,615 subestaciones y el reportado en cuanto al número de Subestaciones a dotar de infraestructura, teniendo una diferencia de 65 subestaciones menos, es decir, 1,550, sin que se proporcionará una justificación.

Los responsables por parte de la EPS CFE Transmisión realizan informes de avance semestrales que no reflejan un avance real, debido a que solo contempla a las Tecnologías de Información (TI) y no el alcance general que incluye también componentes de Tecnologías de Operación (TO).

Administración del Presupuesto (APT) del Proyecto REI

El análisis financiero que fue autorizado para el proyecto REI fue elaborado en el 2017, mismo que a la fecha de la auditoría (julio de 2021) no había sido actualizado respecto a la implementación de acuerdo con su alcance, costos, riesgos y cronograma de trabajo, por lo que no es posible validar si el proyecto REI sigue siendo viable financieramente y si cumplirá con los beneficios esperados y con la implementación en la fecha establecida el 31 de diciembre de 2023.

El proyecto REI es un proyecto de inversión con recursos de la CFE que contempló inicialmente un presupuesto de 4,895,191.0 miles de pesos y que se subdivide en 6 familias de contratos para su implementación.

Administración de Proyectos (ADP) del Proyecto REI

Para la administración del proyecto, la EPS CFE Transmisión utilizó un enfoque Waterfall o de cascada (tradicional) contemplando las fases de ejecución siguientes: proceso licitatorio, entrega de bienes, instalación electromecánica y puesta en servicio, para su revisión contra mejores prácticas en administración de proyectos, la ASF utilizó como referencia la Guía PMBOK del Project Management Institute (PMI), que contempla 5 grupos de procesos esenciales para la administración de proyectos los cuales son: Grupo de Procesos de Inicio, Grupo de Procesos de Planificación, Grupo de Procesos de Ejecución, Grupo de Procesos de Monitoreo y Control y finalmente el Grupo de Procesos de Cierre, como resultado de la revisión se observó lo siguiente:

Grupo de procesos de INICIO

No se establecieron ni formalizaron los criterios específicos de conclusión de éxito o fracaso del Proyecto; se presume que el Acta de Constitución del Proyecto no se realizó en tiempo y forma, ya que se identificaron datos que difieren con la iniciativa original y firmas que no corresponden a las instancias que debieron autorizar el Proyecto.

Grupo de procesos de PLANIFICACION

Líneas base del proyecto.

La EPS CFE Transmisión no presentó evidencia con la que se pudiera validar el alcance y los entregables de cada fase (línea base de alcance), se carecía de evidencia para identificar el trabajo que se ha requerido para realizar la implementación y la puesta en operación de los equipos y servicios derivados del proyecto REI.

La EPS CFE Transmisión no presentó un cronograma de trabajo (línea base de tiempo) en donde se muestre el detalle de las actividades, sus fechas de ejecución y los responsables de cada actividad; no se especificó si existieron retrasos en las actividades que pudieran impactar al calendario planificado. No presentó documentación que valide el seguimiento y control de las fechas establecidas para el proyecto.

No fue posible identificar las bases de las estimaciones que sustentan el presupuesto requerido (línea base de costos) así como el detalle de los montos estimados de las adquisiciones y los riesgos de no adquirir los recursos necesarios para la ejecución del proyecto. Asimismo, no se cuenta con evidencia que sustente cómo se definieron y establecieron los montos por año.

Riesgos

Los riesgos se identificaron en la etapa inicial del proyecto y no se han actualizado, así mismo, no se han identificado y documentado riesgos adicionales a lo largo de la ejecución del proyecto.

Adquisiciones

No fue posible identificar el análisis realizado antes de las contrataciones, ni la logística de compra, por lo que se presume que no se realizó una planeación con antelación a la adquisición de los bienes toda vez que el 67.0% de los mismos se encuentran en almacén, sin que hayan tenido una utilidad a 7 meses de haberse adquirido.

El Laboratorio de Pruebas de Equipos y Materiales (LAPEM) sólo fue requerido para brindar apoyo en 28 de los contratos del proyecto REI, es decir, sólo participó en el 13.0% del total de contratos para la emisión del dictamen técnico sobre el cumplimiento de las características técnicas del equipamiento, para verificar el cumplimiento de las funciones electromecánicas del equipo primario de transmisión y distribución, no se justificó porqué en el resto de los contratos no participó.

Grupo de procesos de EJECUCIÓN

Adquisición de equipamiento

La relación de contratos del proyecto REI se integra por 6 familias, cada una de ellas cuenta con un porcentaje de instalación de los bienes adquiridos, contando con un total de 33% de instalación al momento de la auditoría (julio 2021).

Tabla 5. Estatus de contratos por familia

Familia	Cantidad Solicitada de bienes	Cantidad Recibida de bienes	Porcentaje de avance	Bienes en almacén	Porcentaje de bienes Instalados
SCADA REI	383,726.39	352,967.09	65%	352,967.09	1%
CONECTIVIDAD DE FIBRA OPTICA (Metros)	15,910,000	12,950,000	81.40%	12,233,099	11%
CONECTIVIDAD DE FIBRA OPTICA (Piezas)	216,084	162,008	74.97%	150612	15%
RED DE DATOS OPERATIVA	8,472	6,347	74.92%	4,411	44%
COMUNICAICONES UNIFICADAS	11013	10596	96.21%	6417	37%
RADIOCOMUNICACIONES (Metros)	10007.7	9417.7	94.10%	8492.7	19%
RADIOCOMUNICACIONES (Piezas)	3902	3742	95.90%	2706	37%
EMS/SCADA	66	66	100%	66	100%
				Total	**33%**

FUENTE: Información elaborada por ASF con información proporcionada por la CFE

No existe un cronograma de trabajo detallado para realizar la validación de la adquisición y entrega de equipamiento por año real contra lo planeado.

Grupo de procesos de monitoreo y control

Se carece de documentación de controles de cambios generados en la infraestructura para la implementación del proyecto REI.

En el informe de rendimiento operativo presentado por la EPS CFE Transmisión, mediante su Gerencia de Comunicaciones y Control en mayo 2021, se reportó el porcentaje de avance de 10.0% con una erogación de costos que ascendieron a 1,674,390.0 miles de pesos, sin embargo, no se identificó evidencia que acredite el porcentaje y monto de avance.

La EPS CFE Transmisión indicó que la terminación real del Proyecto REI será a finales del año 2024, por lo que posiblemente no se cumplirá con los tiempos establecidos en Manual de Requerimientos de TIC para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista (noviembre 2022).

Evaluación de la ciberseguridad durante la ejecución del proyecto REI

La EPS CFE Transmisión formalizó, el 01 de octubre de 2020, el proyecto estratégico denominado “Soluciones de Ciberseguridad para la protección de activos e infraestructura de la Red Eléctrica Inteligente”, con el Instituto Nacional de Electricidad y Energías Limpias (INEEL) y el Consejo Nacional de Ciencia y Tecnología (CONACYT), con el objetivo de diseñar y desarrollar soluciones de ciberseguridad para la estandarización, la evaluación, la implementación y el fortalecimiento de la infraestructura de ciberseguridad de la Red Eléctrica Inteligente Nacional. Con la finalidad de apoyar a la preservación de la disponibilidad, la integridad y la confidencialidad de la información, mediante la adopción de estándares y mejores prácticas internacionales en materia de seguridad de la información; estas actividades se tienen planeadas para concluir a finales del año 2024.

La CST es la responsable de emitir las políticas mediante las cuales las EPS y filiales deben de regirse en materia de Tecnologías de información, sin embargo, se observó que no ha participado en el proceso de desarrollo de esta iniciativa, por lo que se podrían estar duplicando esfuerzos para realizar actividades o iniciativas en materias de ciberseguridad.

La EPS CFE Transmisión envía el avance físico y financiero al Grupo Técnico Especializado (GTE), que tiene dentro de sus funciones conocer el avance de los "Proyectos y Programas de Inversión de Gran Magnitud" en su etapa de ejecución o construcción, como es el caso del Proyecto REI; sin embargo, no se presentó evidencia de la retroalimentación que haya dado este grupo.

De igual manera, el primer trimestre de cada año se entrega a la Comisión Reguladora de Energía (CRE) un informe pormenorizado de los avances en las obras de ampliación y modernización de la Red Eléctrica Inteligente, de acuerdo con lo establecido en el artículo 8

del Reglamento de la Ley de la Industria Eléctrica; sin embargo, a la fecha de la auditoría (julio 2021), la EPS CFE Transmisión no presentó evidencia en la que haya tenido respuesta de la CRE.

Por lo anterior, se identificó que la EPS CFE transmisión ha tenido deficiencias en la gestión, administración y supervisión para la implementación del proyecto REI, dado que no se tienen documentados Índices de Desempeño Clave (KPI, por sus siglas en inglés) para medir los beneficios esperados de la implementación de la Red Eléctrica Inteligente, no se han actualizado la situación financiera y los riesgos durante el proyecto; asimismo, del equipamiento que se ha adquirido solo se ha instalado el 33.0%, el resto se encuentra en almacén con el riesgo de que las garantías podrían expirar antes de su instalación; no está definida la responsabilidad de supervisión de las Tecnologías de Operación y Tecnologías de Información, la infraestructura que soporta a la infraestructura SCADA y el resto de sus procesos no ha sido evaluada contra las mejores prácticas de ciberseguridad de la industria; asimismo, debido a los retrasos identificados en la implementación, se tiene el riesgo de que no se cumpla con los tiempos establecidos en el Manual de Requerimientos de TIC para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista (noviembre 2022) y que no se lleguen a obtener los beneficios esperados.

2020-6-90UIW-20-0466-01-003 **Recomendación**

Para que la CFE Transmisión actualice la documentación de las líneas base del Proyecto Red Eléctrica Inteligente así como del presupuesto erogado; implemente mecanismos para robustecer y agilizar la respuesta a riesgos, asegurando su mitigación y, en caso de materialización, poder identificar y reducir el impacto; implementar un análisis antes de las contrataciones que contenga la logística de compra y adquisición, para evitar que los bienes obtenidos permanezcan en un almacén durante meses sin ser aprovechados; implementar un proceso para que la Coordinación de Servicios Tecnológicos realice evaluaciones para verificar el cumplimento de las especificaciones técnicas de las contrataciones en materia de Tecnologías de la Información, considerando la ciberseguridad, y desarrolle Índices de Desempeño Clave (KPI) para medir los beneficios esperados. Asimismo, para que se actualice el plan de trabajo y se realicen las actividades necesarias para cumplir con la fecha establecida en el Manual de Requerimientos de TIC para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista (noviembre 2022).

Los términos de esta recomendación y los mecanismos para su atención fueron acordados con la entidad fiscalizada.

2020-6-90UIW-20-0466-01-004 **Recomendación**

Para que la CFE Transmisión implemente estándares, marcos de referencia, mejores prácticas para la administración y seguimiento de proyectos relacionados con las Tecnologías de Información y Comunicaciones; así también, aplique los controles de ciberseguridad establecidos por la Coordinación de Servicios Tecnológicos relacionados para la Tecnología de Operación, que dependa de servicios de TIC.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-6-90UJB-20-0466-01-005 **Recomendación**

Para que la CFE Corporativo realice las acciones que permitan mejorar sus procesos de gobierno como la evaluación al impacto de proyectos de ciberseguridad; crear indicadores que permitan medir el éxito y los beneficios esperados; establecer en una política o procedimiento que todas las áreas administrativas y Empresas Productivas Subsidiarias que celebran contrataciones de TIC se les brinde asesoría por parte de las áreas de tecnologías pertinentes; gestionar las actividades de evaluación a la capacidad de los centros de datos; realizar actualizaciones al catálogo de software; reforzar los mecanismos de control de cambios; mitigar los problemas de obsolescencia tecnológica en la infraestructura de cómputo; llevar a cabo el seguimiento de las actividades del grupo estratégico de seguridad de la información y dar retroalimentación a los involucrados, y evaluar la madurez de dicho proceso; y establecer mecanismos de seguimiento de riesgos, con alcance a las Empresas Productivas Subsidiarias y empresas filiales, con el fin de garantizar la confiabilidad y correcta operación de los servicios de TI.

Los términos de esta recomendación y los mecanismos para su atención fueron acordados con la entidad fiscalizada.

2020-6-90UJB-20-0466-01-006 **Recomendación**

Para que la CFE Corporativo establezca las definiciones de Tecnología de Información y Tecnología de operación, sus alcances y los responsables de administrar, operar y configurar dichas tecnologías; asimismo, que la Coordinación de Servicios Tecnológicos, en su carácter de responsable del aseguramiento de la gobernanza corporativa de las Tecnologías de Información y Comunicaciones TIC (Tecnología de Información y Tecnología de Operación) en la CFE y sus Empresas Productivas Subsidiarias, realice la planeación, definición de estándares/requerimientos e implementación de políticas de administración de servicios de TO y de ciberseguridad, que incluya de manera enunciativa, mas no limitativa, procesos de gestión de activos, de actividades de mantenimiento, gestión de riesgos, mecanismos de monitoreo y gestión a incidentes; e incluya mecanismos de seguimiento y evaluación al cumplimiento de estas políticas.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-9-90TVV-20-0466-08-002 **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 CFE Consolidado 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, no han promovido las acciones pertinentes para la actualización de las políticas, lineamientos y normativa en materia de seguridad tecnológica y ciberseguridad, así como de gobernanza en materia de TIC, que garanticen la protección de la información de la Comisión Federal de Electricidad, las Empresas Productivas Subsidiarias y las Filiales; que no han promovido el desarrollo de normativa de administración interna para la gestión de activos informáticos que soporten a infraestructura de TO ni su definición, ni han realizado actividades de apoyo en la supervisión a dicha infraestructura, las cuales son críticas para la provisión de servicios de transmisión eléctrica, en incumplimiento de lo establecido en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, párrafo tercero; en el artículo 7, fracción I, de la Ley General de Responsabilidades Administrativas de los Servidores Públicos publicada en el Diario Oficial de la Federación el 18 de julio de 2016; en las fracciones I y II del artículo 47 del Estatuto Orgánico de la Comisión Federal de Electricidad, publicado en el Diario Oficial de la Federación el 12 de abril de 2017; en el Objetivo y funciones 1, 3, 4, 6 y 13 del numeral 1.4.0.3 del Manual de Organización General de la Comisión Federal de Electricidad del 25 de abril de 2018; en los artículos 3, 24 y 27 de las Políticas Generales relativas a las tecnologías de información y comunicaciones de la Comisión Federal de Electricidad y sus empresas productivas subsidiarias y filiales, del 10 de diciembre de 2015..

5. Seguridad de la información

Para evaluar la seguridad de la información de la Comisión Federal de Electricidad, la ASF utilizó el marco CIS (Controles Críticos de Seguridad del Centro de Seguridad de Internet, por sus siglas en inglés) para la infraestructura crítica de TIC (Centro de Datos, Telecomunicaciones, Seguridad Perimetral, Ambientes de Desarrollo y Controles de Acceso).

Los controles de seguridad de la información de la CFE están a cargo de la Coordinación de Servicios Tecnológicos (CST); la Jefatura de Unidad de Proyectos adscrita a la CST es la responsable de la implementación de las políticas generales de seguridad de la información en la CFE, y en sus empresas productivas subsidiarias (EPS) y filiales.

La CST se rige por los Lineamientos en Materia de Seguridad de la Información de la CFE y sus Empresas Productivas Subsidiarias, Filiales y Terceros, los cuales tienen como objetivo establecer los criterios en materia de seguridad de la información que observarán los usuarios para la protección de la información, uso racional de los recursos y sistemas informáticos de la CFE y sus EPS y filiales.

Evaluación de Ciberseguridad basada en CIS

El alcance de la auditoría consideró 18 controles de seguridad críticos (CSC) que incluyen 109 actividades de control individuales para evaluar el diseño y la efectividad operativa con sus respectivos objetivos de cumplimiento.

El alcance de la evaluación consideró equipos de cómputo, laptops, servidores del centro de datos, infraestructura de telecomunicaciones, Firewall a lo largo del país y herramientas Web Aplication Firewall.

Medición

Para la evaluación de los controles fueron considerados tres niveles de cumplimiento, los cuales fueron obtenidos con los rangos siguientes: Aceptable (más del 80.0%), Requiere Fortalecer el Control (entre el 40.0% y 79.0%) y Carencia de Control (menos del 30.0%), de dicha evaluación se observó lo siguiente:

- 2 controles obtuvieron un nivel aceptable.
- 8 controles obtuvieron un nivel que se requiere fortalecer.
- 8 se determinaron con una carencia de control.

2020-6-90UJB-20-0466-01-007 **Recomendación**

Para que la CFE Corporativo, por medio de la Coordinación de Servicios Tecnológicos, realice las acciones necesarias para mitigar las observaciones identificadas por el grupo auditor en la evaluación de Seguridad de la Información, por medio de controles del Centro de Seguridad de Internet (CIS, por sus siglas en inglés), tomando como prioridad aquellas evaluadas como carencia de control.

Los términos de esta recomendación y los mecanismos para su atención fueron acordados con la entidad fiscalizada.

6. Ciberseguridad en la EPS CFE Transmisión

Antecedentes

A raíz de la reforma eléctrica, en enero de 2016 se estableció que la empresa realizaría sus actividades de manera independiente, bajo condiciones de estricta separación legal y a través de empresas productivas subsidiarias (EPS), empresas filiales (EF) o cualquier modelo de asociación previsto por la Ley de CFE. El CENACE es el responsable del control del Sistema Eléctrico Nacional y son los encargados del despacho de energía y de vigilar la estabilidad del sistema, siendo el primero y segundo nivel operativo, y la EPS CFE Transmisión el tercer nivel.

Las nuevas responsabilidades de la EPS CFE Transmisión son las siguientes:

- Mantenimiento y Operación Física de la Red Nacional de Transmisión (Tensiones eléctricas desde 69 kV a 400 kV). [9]

- Ampliar y Modernizar la Red Nacional de Transmisión. [10]

- Contratos de Interconexión con Generadores y Contratos de Conexión con Centros de Carga. [11] .

- Medición para liquidaciones para el Mercado Eléctrico Mayorista y emitir Facturación al CENACE de acuerdo con la tarifa regulada. [12]

La EPS CFE Transmisión recibió por parte del CENACE 31 zonas de operación para hacer el control físico. A la fecha de la auditoría (julio 2021), la Red Nacional de Transmisión (RNT) se compone de esas 31 zonas, de las cuales 24 cuentan con su sistema de administración energética (EMS, por sus siglas en inglés) propia y 7 el servicio para la operación física lo proporciona CENACE. Cada zona de operación atiende una región del país y agrupa una cantidad de subestaciones mediante los sistemas SCADA y EMS.

Normas, estándares y marcos de Referencia relacionados con ciberseguridad en el sector de Energía

Las principales normas, estándares y marcos de referencia en el sector energía se presentan en la tabla siguiente:

9 Ley de la Industria Eléctrica Artículo 26, Términos para la estricta separación legal de la Comisión Federal de Electricidad, Capítulo 3.

10 Ley de la Industria Eléctrica Artículo 29.

11 Ley de la Industria Eléctrica Artículo 33.

12 Ley de la Industria Eléctrica Artículo 37, 38.

Tabla 6. Normas, estándares y marcos de referencia relacionados con ciberseguridad en el sector de Energía

<table>
<tr><th colspan="2">Normativa en materia del Sector Energético</th></tr>
<tr><td>NERC CIP - Conjunto de estándares de la Corporación Norteamericana de Confiabilidad Eléctrica (NERC, por sus siglas en inglés) para la Protección de las Infraestructuras Críticas (CIP, por sus siglas en inglés)

El conjunto de estándares del NERC para la Protección de las Infraestructuras Críticas (CIP) definen los requisitos de confiabilidad para planificar y operar el sistema de energía a granel de América del Norte y se desarrollaron utilizando un enfoque basado en resultados que se centra en el desempeño, la gestión de riesgos y las capacidades de la entidad. El modelo de confiabilidad define las funciones que deben realizarse para garantizar que el sistema eléctrico a granel opere de manera confiable y es la base de los estándares de confiabilidad orientados a proteger las redes de distribución de energía eléctrica frente a ciberataques o incidentes de seguridad que comprometan la disponibilidad del servicio energético en los Estados Unidos de América.</td><td>NIST 1800-7 “Conciencia situacional para las empresas eléctricas

Publicación especial del NIST que provee un conjunto de controles para mejorar la seguridad de la Tecnología Operativa (TO) a través del conocimiento de la situación de las empresas eléctricas.</td></tr>
<tr><td>NIST SP 800-53 “Controles de seguridad y privacidad para organizaciones y sistemas de información”.

Publicación especial del NIST que provee un conjunto de controles para la protección frente a diversas amenazas, incluyendo ataques hostiles, desastres naturales, fallos estructurales, errores humanos y riesgos de privacidad.</td><td>Acuerdo por el que se emite el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista publicado en el Diario Oficial de la Federación el 04 de diciembre de 2017

Establece los principios, reglas, directrices, ejemplos y procedimientos a seguir en el uso de las Tecnologías de la Información, para que el Centro Nacional de Control de Energía, los Transportistas, los Distribuidores, las Centrales Eléctricas y los Centros de Carga cuenten con los medios de comunicación para transferencia de voz y datos, con calidad de la información, requeridos para cumplir con la Telemetría en Tiempo real en forma directa para el Control Operativo del Sistema Eléctrico Nacional y con la operación del Mercado Eléctrico Mayorista, incluida la medición para liquidaciones</td></tr>
<tr><td colspan="2">Código de Red con acuerdos publicados en el Diario Oficial de la Federación el 08 de abril de 2016

Dicta los Criterios de eficiencia, Calidad, Confiabilidad, Continuidad, seguridad y sustentabilidad incluidos en este documento, tienen como objetivo permitir e incentivar que el SEN se desarrolle, mantenga, opere, amplíe y modernice de manera coordinada con base en requerimientos técnicos-operativos, y de la manera más eficiente y económica. Lo anterior bajo los principios de acceso abierto y trato no indebidamente discriminatorio. Asimismo, el Código de Red debe ser entendido como el documento que establece los requerimientos técnicos mínimos que los Integrantes de la Industria Eléctrica están obligados a cumplir con relación a las actividades de planeación y operación del SEN, así como establecer las reglas para la medición, el control, el acceso y uso de la infraestructura eléctrica. El Código de Red es de cumplimiento obligatorio para los Integrantes de la Industria Eléctrica y corresponderá a la CRE su interpretación y vigilancia</td></tr>
</table>

Normativa en materia del Sector Energético	
Políticas Generales Relativas a las Tecnologías de Información y Comunicaciones de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias y Filiales formalizado el 10 de diciembre de 2015 Cuyo objeto es normar la implementación, actualización, supervisión, seguimiento, control y vigilancia del Gobierno y Gestión en materia de Tecnologías de la Información y Comunicaciones en la Comisión Federal de Electricidad, sus empresas subsidiarias y en su caso, sus empresas filiales, a fin de contribuir a la consecución de la misión, visión, objetivos, metas, productividad y rentabilidad. Así mismo tienen el propósito de establecer las directrices, principios, normas, procesos, procedimientos y mecanismos de verificación y evaluación en materia de tecnologías de la información y comunicaciones, de la Comisión Federal de Electricidad y sus empresas productivas subsidiarias y su administración de riesgos.	**Lineamientos en Materia de Seguridad de la Información de la CFE y sus Empresas Productivas Subsidiarias, Filiales y Terceros formalizado el 11 de noviembre de 2016** Tienen como objetivo establecer los criterios en materia de seguridad de la información que observarán los usuarios para la protección de la información y uso racional de los recursos y sistemas informáticos de la CFE y sus Empresas, reduciendo el impacto de ataques informáticos dirigidos contra la información, equipos e infraestructura informática, sistemas sustantivos, críticos y administrativos y de la operación de la red eléctrica nacional de la CFE, a través de un esquema integral de seguridad de la información y mecanismos de supervisión y control para la implementación de estos lineamientos.

FUENTE: Elaborado por la ASF.

Evaluación de ciberseguridad en la EPS CFE Transmisión

La Auditoría Superior de la Federación desarrolló un modelo para evaluar la ciberseguridad en la EPS CFE Transmisión, específicamente del Sistema EMS/SCADA, basado en el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología - 1800 (NIST por sus siglas en inglés y compuesto de 108 subcategorías), NIST 1800-7 “Conciencia situacional para las empresas eléctricas”, conformado por 16 subcategorías, los estándares NERC CIP (Protección de Infraestructura Crítica, por sus siglas en inglés) y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano (Acuerdo por el que se emite el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista publicado en el Diario Oficial de la Federación el 04 de diciembre de 2017, Código de Red con acuerdos publicados en el Diario Oficial de la Federación el 08 de abril de 2016 y el Manual de programación de Salidas publicado en el Diario Oficial de la Federación el 13 de noviembre de 2017).

Agrupación de subcategorías de ciberseguridad del Marco de Referencia de Ciberseguridad

El modelo desarrollado por la ASF analizó las 108 subcategorías contenidas en el Marco de Referencia de Ciberseguridad NIST, las 16 subcategorías del NIST 1800-7 “Conciencia situacional para las empresas eléctricas”, los estándares NERC CIP del 002 al 014, y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano; como resultado, se obtuvieron 67 subcategorías las cuales integran las

subcategorías anteriormente mencionadas y que se agrupan en las 5 funciones y 18 categorías siguientes:.

Funciones

1.- Identificar

Se refiere a la comprensión del contexto de la organización, los activos que soportan los procesos críticos de las operaciones y los riesgos asociados. Esta comprensión permite definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos. Las categorías dentro de esta función son:

Tabla 7. Categorías de la función identificar

ID.AM - Gestión de Activos
ID.BE - Entorno Empresarial
ID. GV - Gobernanza
ID.RA - Evaluación de Riesgos

FUENTE: Marco de Referencia de Ciberseguridad NIST.

2.- Proteger

Es una función vinculada a la aplicación de medidas para garantizar la entrega de los servicios críticos. Las categorías dentro de esta función son:

Tabla 8. Categorías de la función proteger

PR.AC - Gestión de Identidad y Control de Acceso
PR.AT - Concienciación y Capacitación
PR.DS - Seguridad de Datos
PR. IP - Procesos y Procedimientos de Protección de la Información
PR.MA - Mantenimiento
PR.PT - Tecnología de Protección

FUENTE: Marco de Referencia de Ciberseguridad NIST.

3.- Detectar

Es la definición y ejecución de actividades apropiadas para la identificación de los incidentes de ciberseguridad. Las categorías que la componen son:

Tabla 9. Categorías de la función detectar

DE.AE - Anomalías y Eventos
DE.CM - Monitoreo continuo de la seguridad
DE. DP - Procesos de Detección

FUENTE: Marco de Referencia de Ciberseguridad NIST.

4.- Responder

Se refiere a la definición y ejecución de actividades apropiadas para tomar medidas en caso de detección de un evento de ciberseguridad. El objetivo es reducir el impacto de un potencial incidente de ciberseguridad. Las categorías dentro de esta función son:

Tabla 10. Categorías de la función responder

RS.CO - Comunicaciones
RS.AN - Análisis
RS.MI - Mitigación
RS.IM - Mejoras

FUENTE: Marco de Referencia de Ciberseguridad NIST.

5.- Recuperar

Está vinculada a la definición y ejecución de las actividades dirigidas a la gestión de los planes de resiliencia para restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética. El objetivo es asegurar la resiliencia de los sistemas e instalaciones y, en caso de incidentes, apoyar la recuperación oportuna de las operaciones. Las categorías dentro de esta función son:

Tabla 11. Categorías de la función recuperar

RC.RP - Planificación de recuperación
RC.CO - Comunicaciones

FUENTE: Marco de Referencia de Ciberseguridad NIST.

Resultado de la evaluación de la EPS CFE Transmisión

El resultado de la evaluación para cada subcategoría del NIST que conforma el marco, se realizó en función de la información proporcionada a este ente fiscalizador como parte de las

solicitudes de información realizadas a la EPS CFE Transmisión y de la atención a las Actas Administrativas Circunstanciadas aplicadas a la Gerencia de Control y Comunicaciones y de la información.

Para medir el nivel de cumplimiento el criterio utilizado fue el siguiente:

- **Bajo:** 0-30% del cumplimiento de los requerimientos por subcategoría.
- **Medio:** 40-70% del cumplimiento de requerimientos por subcategoría.
- **Establecido:** 80-90 % del cumplimiento a los requerimientos por subcategoría.

Del análisis del Marco de Ciberseguridad (NIST - NERC – Código de Red –Manual de TIC para la operación del SEN y MEM), conformado por 5 funciones, 18 categorías y 67 subcategorías de control, se concluye que la EPS CFE Transmisión obtuvo la siguiente evaluación:

Identificar

La función Identificar presentó un promedio de 65.7 % de cumplimiento, es la función que obtuvo un mayor nivel; sin embargo, se tienen que reforzar e incrementar las medidas para definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos.

Proteger

La función Proteger presentó un promedio de 58.1% de cumplimiento, lo que indica que se debe continuar con la implementación de medidas para proteger los procesos y los activos de la organización.

Detectar

La función Detectar presentó un promedio de 47.3 % de cumplimiento, es la función que obtuvo el promedio más bajo, por lo que se tienen que incrementar acciones para tener una adecuada definición y ejecución de actividades dirigidas a la identificación temprana de los incidentes de seguridad.

Responder

La función Responder presentó un promedio de 52.8% de cumplimiento, por lo que se tiene que continuar con la definición y ejecución de actividades apropiadas para tomar medidas en caso de detección de un evento de seguridad con el objetivo de reducir el impacto de un potencial incidente de ciberseguridad.

Recuperar

La función Recuperar presentó un promedio de 50.0% de cumplimiento, lo que indica que se deben incrementar las acciones para probar y actualizar los planes de resiliencia, que les

permitan restablecer cualquier capacidad o servicio que se haya visto afectado, debido a un incidente de ciberseguridad, así como gestionar ante los medios una respuesta inmediata en caso de contingencias.

Por subcategoría

- 9 subcategorías del marco (13.4%) obtuvieron una calificación de establecido.
- 45 subcategorías (67.2%) obtuvieron una calificación de medio.
- 13 subcategorías (19.4%) obtuvieron una calificación de bajo.

Por lo anterior, se observa que la EPS CFE Transmisión debe incrementar las acciones para gestionar los riesgos de ciberseguridad, proteger los activos de información, fortalecer las políticas y procedimientos relacionados con el desarrollo de software relacionados con la infraestructura que soporta a los sistemas SCADA; debe de actualizar y validar los planes de respuesta y recuperación, con el objeto de restablecer cualquier servicio que se vea afectado ante un incidente de ciberseguridad, los cuales de verse materializados podrían afectar los servicios provistos por esta EPS, así como al SEN .

Normativa interna CFE

Dentro las funciones de la Coordinación de Servicios Tecnológicos se señalan las siguientes:

- Definir y coordinar los estándares, arquitectura y requerimientos tecnológicos, normatividad y lineamientos corporativos en materia de gobierno de datos, comunicaciones, portales y TIC, entre otros, para contar con una infraestructura homologada e interoperable en la CFE y EPS.

- Ejercer la gobernanza corporativa de las TIC en la CFE y sus EPS, a través de las políticas en la materia, sus lineamientos y normatividad específica aplicable, para garantizar el adecuado uso y aprovechamiento de las TIC.

Del análisis de la información, se observó que, a la fecha de la auditoría (julio de 2021), las políticas establecidas por la Coordinación de Servicios Tecnológicos (CST), en materia de Tecnologías de información, no incluyen el concepto de Tecnologías de Operación (TO) ni se tiene definida la responsabilidad de la supervisión y monitoreo de los equipos que pertenecen a las TO; asimismo, en la EPS CFE Transmisión se carece de lineamientos y políticas en materia de ciberseguridad específica e interna que se alinee con lo solicitado en el Código de Red y en el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional.

La EPS CFE Transmisión desarrolló la estrategia “Soluciones de Ciberseguridad para la protección de activos e infraestructura de la Red Eléctrica Inteligente”; sin embargo, no considera toda la infraestructura de las TO con las que opera esta subsidiaria.

Asimismo, se observa que la EPS CFE Transmisión no ha considerado, en la alineación de sus procesos, mejores prácticas o un marco de referencia del Sector Energético como lo es el NIST y los CIP NERC, que den certidumbre que las actividades realizadas permitan una continuidad a las operaciones y en caso de contingencias e incidentes de seguridad, la EPS CFE Transmisión pueda recuperarse en el tiempo requerido para evitar que la trasmisión de la energía se vea interrumpida y afecte a la población en general. .

2020-6-90UIW-20-0466-01-005 **Recomendación**

Para que la CFE Transmisión robustezca su estrategia de Seguridad de la información y Ciberseguridad conforme a las mejores prácticas y marcos de referencia como el NIST 1800-7 'Conciencia situacional para las empresas eléctricas' (Instituto Nacional de Estándares y Tecnología), NERC CIP (Conjunto de estándares de la Corporación Norteamericana de Confiabilidad Eléctrica NERC para la Protección de las Infraestructuras Críticas) e ISO 27001 (Sistemas de Gestión de Seguridad de la Información), en el que desarrolle procedimientos y políticas específicas e implante un sistema de gestión para gobernar la seguridad de la información en la infraestructura de las Tecnologías de Operación, incluidas las que no están en el alcance de los sistemas EMS/SCADA.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-6-90UIW-20-0466-01-006 **Recomendación**

Para que la CFE Transmisión implemente en las Gerencias Regionales de Transmisión los mecanismos de control y actividades para elevar los niveles de ciberseguridad que evaluó la ASF con base en las mejores prácticas, como el North American Electric Reliability Corporation (NERC) y National Institute of Standards and Technology (NIST), con el fin de atender y mitigar las observaciones detectadas en las funciones identificar, proteger, detectar, responder y recuperar, defina y supervise la ejecución un plan de trabajo de implementación de controles apegados a las mejores prácticas de la industria o estándares de ciberseguridad el cual priorice los de mayor riesgo, facilidad de adopción y fortalezca los mecanismos de gestión de incidentes y pruebas para evaluar la capacidad de la organización ante ataques cibernéticos.

Los términos de esta recomendación y los mecanismos para su atención, por parte de la entidad fiscalizada, quedan asentados en el Acta de la Reunión de Presentación de Resultados Finales y Observaciones Preliminares en los términos del artículo 42 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

Montos por Aclarar

Se determinaron 5,410,133.01 pesos pendientes por aclarar.

Buen Gobierno

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

Resumen de Resultados, Observaciones y Acciones

Se determinaron 6 resultados, de los cuales, 6 generaron:

13 Recomendaciones, 2 Promociones de Responsabilidad Administrativa Sancionatoria y 1 Pliego de Observaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 15 de octubre de 2021, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar los controles de ciberseguridad de los sistemas relacionados con la distribución de energía eléctrica, así como 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, específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance; se concluye que, en términos generales, la Comisión Federal de Electricidad cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

Se acreditaron incumplimientos de los términos y condiciones en los contratos de adquisición de bienes y servicios revisados:

- En el contrato número 800938585, celebrado con Tecniman, S.A. de C.V., la Gerencia de Abastecimiento y la Coordinación de Servicios Tecnológicos no optaron por las mejores condiciones para el estado ya que no se justificó el beneficio económico que obtuvo el proveedor, por 5,410.1 miles de pesos, puesto que subcontrató el 100.0% de los servicios y que la ASF identificó que este proveedor solo actuó como intermediario, ya que no acreditó con información justificativa y comprobatoria su participación en los servicios proporcionados a la CFE, ya que no contaba con la capacidad técnica y humana para realizarlos, la única actividad identificada por este ente fiscalizador fue haber participado en el proceso de licitación.

- La herramienta Tenable, adquirida por medio del contrato número 800938585, se encuentra instalada y es funcional en la CFE; sin embargo, del total de las 10,000 licencias que se suministraron no han sido utilizadas el 45.8%; asimismo, no se utilizan la mayoría de las características ofrecidas por la herramienta.

- En el contrato número 700511947, celebrado con Siemens, S.A. de C.V., se identificaron deficiencias en la planeación, administración y supervisión en la infraestructura adquirida ya que a la fecha de la auditoría (julio de 2021) ésta se encontraba alojada en un almacén durante 7 meses, el programa para la puesta de servicio no contiene el avance real de las actividades por lo que no se tiene una fecha compromiso para la puesta en servicio de la totalidad de los elementos adquiridos y se corre el riesgo que la garantía de los equipos expire.

- Respecto de la gestión y gobierno de las TIC, la CFE no cuenta con indicadores que le permitan medir el éxito y los beneficios esperados de los proyectos; se celebran contrataciones de TIC en las EPS, sin que se les brinde asesoría por parte de las áreas de tecnologías correspondientes, no se han incluido en la definición de riesgos de TIC los de las EPS y empresas filiales con el fin de garantizar la confiabilidad y correcta operación de los servicios de TI.

- La CFE no gestiona actividades de evaluación a la capacidad de los centros de datos, lo que repercute en los servicios proporcionados a otras áreas; a la fecha de la auditoría, (julio de 2021), no ha mitigado los problemas de obsolescencia tecnológica en la infraestructura de cómputo, la cual ha dejado de tener soporte del fabricante, y pudiera ser más vulnerable a ataques externos.

- Como resultado de los atrasos en la implementación del proyecto de la Red Eléctrica Inteligente (REI) se tiene el riesgo de que éste no sea implementado en la fecha establecida en el Manual de Requerimientos de TIC para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista (noviembre de 2022).

- La CFE no cuenta con una definición formalizada y establecida en sus políticas de las Tecnologías de Operación (la cual es la que soporta la infraestructura critica de la Trasmisión Eléctrica del país) y Tecnologías de Información, tampoco se cuenta con el

monitoreo de dicha infraestructura ni se verifica que sea evaluada tomando como referencia las mejores prácticas de ciberseguridad de la industria.

- La EPS CFE Transmisión no tiene contemplada la implementación de los controles NERC CIP (Protección de Infraestructura Crítica, por sus siglas en inglés) o de algún otro estándar de ciberseguridad en sus procesos operativos, con la finalidad de homologar la confiabilidad del Sistema Eléctrico y estandarizarlo.

- En la revisión de la evaluación de ciberseguridad, de acuerdo al modelo desarrollado por la ASF, basado en el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología - 1800 (NIST por sus siglas en inglés), NIST 1800-7 "Conciencia situacional para las empresas eléctricas", los estándares NERC CIP (Protección de Infraestructura Crítica, por sus siglas en inglés) y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano, de un total de 5 funciones, 18 categorías y 67 subcategorías evaluadas se detectó que la CFE obtuvo una calificación alta en 9 (13.4%) subcategorías del marco, una calificación media en 45 (67.2%) subcategorías del marco y una calificación baja en 13 (19.4%) subcategorías del marco, estas últimas relacionadas con la de definición de roles y responsabilidades de seguridad cibernética, planes de respuesta y recuperación, procesos para la gestión de respaldos, procesos de desarrollo y control de cambios, análisis de impacto de posibles incidentes de seguridad. La CFE debe incrementar acciones que le permitan la identificación temprana de incidentes de ciberseguridad, así como, la actualización y validación de los planes de resiliencia con objeto de restablecer cualquier servicio que se vea afectado ante un incidente de ciberseguridad.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Ing. Nohema Lara Blanco	Mtro. Roberto Hernández Rojas Valderrama

Comentarios de la Entidad Fiscalizada

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que, para los capítulos del gasto relacionados con las TIC, las cifras reportadas en la Cuenta Pública se corresponden con las registradas en el estado del ejercicio del presupuesto, de conformidad con las disposiciones y normativas aplicables; analizar la integración del gasto ejercido en materia de TIC en los capítulos asignados de la Cuenta Pública fiscalizada.

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

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones; 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 las penalizaciones y 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 sustantivos, telecomunicaciones y demás relacionados con las TIC para verificar antecedentes; beneficios esperados; entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento/sustantivas); implementación y soporte de los servicios; verificar la gestión de riesgos, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, como el inventario y autorización de dispositivos y software; configuración del

hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de vulnerabilidades, entre otros.

7. Evaluar que el gobierno de las tecnologías de información y comunicaciones considera las necesidades, condiciones y opciones de las partes interesadas para determinar objetivos organizacionales equilibrados y acordados; valorar el nivel de alineación de la estrategia de TIC con los objetivos de la organización, así como de los mecanismos de medición, seguimiento y cumplimiento de sus metas.

Áreas Revisadas

La Dirección Corporativa de Administración, la Dirección Corporativa de Finanzas, la Dirección Corporativa de Negocios Comerciales, la Gerencia de Tecnologías de Información, la Gerencia de Control y Evaluación Financiera, la Gerencia de Abastecimiento, la Gerencia de Presupuestos, la Coordinación de Servicios Tecnológicos, el Laboratorio de Pruebas de Equipos y Materiales, de la Comisión Federal de Electricidad; así como la Gerencia de Comunicaciones y Control, y la Unidad de Finanzas de la EPS CFE Transmisión.

Disposiciones Jurídicas y Normativas Incumplidas

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

1. Otras disposiciones de carácter general, específico, estatal o municipal: Lo establecido en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, párrafo tercero; en el Apartado 7. Funciones, numeral 1.3.0.1.2.0.0.0.0.0.2, Oficina de Coordinación Administrativa, octavo párrafo y el Numeral 6. Organigrama, numeral 1.3.0. 1.2 Gerencia de Tecnologías de la Información, del Manual de Organización de la Gerencia de Tecnologías de la Información de fecha 27 de noviembre de 2012; Capítulo V.- Procedimientos de Contratación de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de la CFE y sus EPS y su última reforma en el Diario Oficial de la Federación el 29 de noviembre de 2017; del Objetivo, los Numerales 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11 y 5.12 y el Numeral 5.9.4, 5.10.3, de los Lineamientos en Materia de Seguridad de la Información de la CFE y sus Empresas Productivas Subsidiarias, Filiales y Terceros, de fecha 11 de noviembre de 2016 y Artículo 20, fracción III de las Políticas Generales Relativas a las Tecnologías de Información y Comunicaciones de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias y Filiales, de fecha 10 de diciembre de 2015; de los artículos 93 fracción I y 102, párrafo II de la Ley de la Comisión Federal de Electricidad publicada en el Diario Oficial el 11 de agosto de 2014; las Disposiciones 3, 5, fracciones I, X y XII, 25, fracción III y 45 de las Disposiciones Generales en Materia de Adquisiciones, Arrendamientos, Contratación de Servicios y Ejecución de Obras de

la CFE y sus EPS publicadas en el Diario Oficial de la Federación el 23 de junio de 2015 y su última reforma publicada en el mismo medio el 29 de noviembre de 2019; en los artículos 7 fracciones I y VI, 69 y 70 de la Ley General de Responsabilidades Administrativas de los Servidores Públicos publicada en el Diario Oficial de la Federación el 18 de julio de 2016; el artículo 47, fracción III del Estatuto Orgánico de la Comisión Federal de Electricidad publicado en el Diario Oficial de la Federación el 12 de abril de 2017; el numeral 5, Estructura Orgánica, en el Objetivo y funciones 1, 3, 4, 6 y 13 del inciso 1.4.0.3, Coordinación de Servicios Tecnológicos, del Manual de Organización General de la Comisión Federal de Electricidad publicado en la normateca interna de la CFE el 25 de abril de 2018 y numeral 1.3.0.1.2.3.0.0.3., Unidad de Proyectos, funciones, párrafos cuarto y quinto del Manual de Organización de la Gerencia de Tecnologías de Información, publicado en la normateca interna de CFE el 27 de agosto de 2012, de la Cláusula Tercera. -Términos y condiciones en que se realizará el pago y moneda del Contrato Número 700511947 Adquisición de SCADA SAS IEC61850 para la Comisión Federal de Electricidad Transmisión; de los Capítulos 2, 3 y 4 del Acuerdo por el cual se emite el Manual de Programación de salidas, publicado en el Diario Oficial de la Federación 13 de noviembre de 2017, y Numeral 5.7 de los Lineamientos en Materia de Seguridad de la Información de la CFE y sus Empresas Productivas Subsidiarias, Filiales y Terceros, de fecha 11 de noviembre de 2016; de los Capítulos III y IV, y en los artículos 3, 24 y 27 de las Políticas Generales Relativas a las Tecnologías de Información y Comunicaciones de la Comisión Federal de Electricidad y sus Empresas Productivas Subsidiarias y Filiales, de fecha 10 de diciembre de 2015; fracciones XVIII y XXII del Artículo 5, inciso g, fracción IX, artículo 26 del Estatuto Orgánico de CFE Transmisión publicado en el Diario de Oficial de la Federación el 7 de diciembre de2017;

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.