Comisión Reguladora de Energía

Auditoría de Ciberseguridad del Sector Energía

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-0-45100-20-0112-2021

112-GB

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	83,315.8
Muestra Auditada	34,203.9
Representatividad de la Muestra	41.1%

El universo seleccionado por 83,315.8 miles de pesos que corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal 2020; la muestra auditada está integrada por dos contratos que corresponden al Servicio de desarrollo y mantenimiento a los sistemas de información en la modalidad de fábrica de software y el Servicio de seguridad integral de la Comisión Reguladora de Energía, con pagos ejercidos por 34,203.9 miles de pesos, que representan el 41.1% del universo seleccionado.

Antecedentes

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).

Se realizó esta auditoría a la Comisión Reguladora de Energía (CRE) en la cual se revisaron aspectos relacionados con la cuenta pública, su normativa, y contrataciones de TIC, así como las atribuciones ejercidas respecto a la supervisión de la Ciberseguridad en el Sector Energía.

En esta misma auditoría se incluyó a la Secretaria de Energía (SENER) en la que se revisó el seguimiento realizado a los proyectos estratégicos relacionados con TIC y ciberseguridad en dicho sector y el estado que guarda la Ciberseguridad en el Sector Energía.

[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.

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, 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.
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. [6]
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. [7] 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. 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.

FUENTE: Elaborado por la ASF.

Sistema Eléctrico Nacional

El Sistema Eléctrico Nacional (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 Centro Nacional de Control de Energía (CENACE), utilizados para llevar a cabo el control operativo del SEN.

[6] Definición de acuerdo con el NIST Special Publication 800-53.
[7] Definición de acuerdo con la publicación Estado de preparación en ciberseguridad del sector eléctrico en América Latina.

- Los demás elementos que determine la SENER.

La infraestructura de transmisión y distribución del SEN hacen 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.

Comisión Reguladora de Energía (CRE)

La Comisión Reguladora de Energía (CRE) es una dependencia de la Administración Pública Federal centralizada, con carácter de Órgano Regulador Coordinado en Materia Energética, como se establece en el párrafo octavo, del artículo 28 de la Constitución Política de los Estados Unidos Mexicanos. La CRE está dotada de autonomía técnica, operativa y de gestión, y cuenta con personalidad jurídica propia y capacidad para disponer de los ingresos que deriven de las contribuciones y contraprestaciones establecidas por los servicios que preste conforme a sus atribuciones y facultades.

Tiene a su cargo el ejercicio de las atribuciones y el despacho de los asuntos que le encomiendan la Ley de los Órganos Reguladores Coordinados en Materia Energética (LORCME), la Ley de Hidrocarburos, la Ley de la Industria Eléctrica, la Ley de Transición Energética, la Ley General de Cambio Climático y las demás disposiciones jurídicas aplicables, a fin de fomentar el desarrollo eficiente de la industria, promover la competencia en el sector, proteger los intereses de los usuarios, propiciar una adecuada cobertura nacional y atender a la confiabilidad, estabilidad y seguridad en el suministro y la prestación de los servicios.

Dirección General de Tecnologías de la Información (DGTI)

La Dirección General de Tecnologías de la Información (DGTI) de acuerdo al Manual de Organización General (MOG) de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación (DOF) el 24 de noviembre de 2017, tiene como objetivo fortalecer el desarrollo y uso de sistemas computarizados, que contribuyan al desempeño eficiente de las funciones de la Comisión a través de la automatización de los procesos sustantivos y administrativos, así como asegurar la continuidad de los servicios informáticos y de telecomunicaciones a través del soporte oportuno y eficiente, y dirigir la modernización y construcción de la infraestructura tecnológica que dé soporte a los servicios de comunicación de voz, datos e imagen de la Comisión.

Secretaría de Energía

A la Secretaría de Energía (SENER) le corresponde, entre otras atribuciones, “Regular y, en su caso, expedir normas oficiales mexicanas sobre producción, comercialización, compraventa, condiciones de calidad, suministro de energía y demás aspectos que promuevan la modernización, eficiencia y desarrollo del sector, así como controlar y vigilar su debido cumplimiento” (artículo 33 de la Ley Orgánica de la Administración Pública

Federal publicada en el Diario Oficial de la Federación el 29 de diciembre de 1976 y su reforma publicada en el mismo medio el 9 de agosto de 2019).

Entre los años 2016 y 2020, en la CRE se han invertido 448,363.9 miles de pesos en materia de Tecnologías de la Información, entre otros, integrados de la manera siguiente:

Recursos erogados en materia de TIC en la CRE

(Miles de pesos)

PERIODO DE EROGACIÓN	2016	2017	2018	2019	2020	Total
MONTO POR AÑO	54,528.6	85,895.3	117,656.1	106,968.1	83,315.8	448,363.9

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

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 funciones de las TIC sujetas de revisión, así como, determinar el alcance, naturaleza y muestra de la revisión; se obtuvieron los resultados que se presentan en este informe.

Resultados

1. Análisis Presupuestal

De acuerdo con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2020, publicado en el Diario Oficial de la Federación el 11 de diciembre de 2019, a la CRE se le aprobó un presupuesto de 252,881.4 miles de pesos.

Respecto del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2020 se identificó un presupuesto ejercido para el Capítulo 3000 de 69,975.6 miles de pesos; no obstante, en la documentación proporcionada por la Comisión Reguladora de Energía se identificó un presupuesto ejercido de 83,315.8 miles de pesos correspondientes a recursos relacionados con las TIC, lo que representa el 32.9% del presupuesto aprobado, como se muestra a continuación:

Recursos ejercidos en contrataciones relativas al TIC en la CRE durante 2020

(Miles de Pesos)

Presupuesto aprobado	Capítulo	Descripción	Presupuesto Ejercido	Recursos ejercidos en TIC
252,881.4	3000	Servicios Generales	69,975.6	83,315.8
		TOTAL	**69,975.60**	**83,315.8**

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

Nota: Sólo se incluyen los capítulos con partidas relacionadas a los gastos de contrataciones de TIC, no incluye el capítulo 1000 de servicios personales.

Se identificó una diferencia de 13,340.2 miles de pesos entre el presupuesto ejercido reportado en la Cuenta Pública 2020 y los recursos ejercidos en Gastos de TIC respecto al capítulo 3000.

Los recursos ejercidos en materia de TIC por 83,315.8 miles de pesos se integran de la manera siguiente:

Integración del gasto de las contrataciones relacionadas con las TIC 2020 en la CRE

(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
3000		**SERVICIOS GENERALES**	**83,315.8**
	31401	Servicio telefónico convencional	10.3
	31603	Servicios de Internet	1,374.4
	31904	Servicios integrales de infraestructura de cómputo	31,050.3
	32301	Arrendamiento de equipo y bienes informáticos	16,912.0
	32701	Patentes, derechos de autor, regalías y otros	26,022.1
	33301	Servicios de desarrollo de aplicaciones informáticas	7,946.7
		TOTAL	**83,315.8**

FUENTE: Elaborado con información proporcionada por la CRE.

Del universo seleccionado en 2020 por 83,315.8 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 34,203.9 miles de pesos en cuatro contratos que representan el 41.1% del universo seleccionado, el cual se integra de la manera siguiente:

Muestra de los pagos ejercidos en los contratos relacionados con las TIC durante 2020

(Miles de pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Ejercido con recursos de Cuenta Pública 2020	Ejercido con recursos de Fideicomiso
				De	Al	Mínimo	Máximo		
Adjudicación Directa (Artículo 1 de la LAASSP)	CRE/21/2019	Instituto Potosino de Investigación Científica y Tecnológica, C.A.	Servicio de desarrollo y mantenimiento a los sistemas de información en la modalidad de fábrica de software	01/06/2019	31/12/2019	10,631.0	26,557.6	1,312.4	6,634.3
	CM/01/2019		Ampliación de Vigencia del Convenio CRE/21/2019	01/01/2020	31/03/2020	N/A	N/A	N/A	
					Subtotal	**10,631.0**	**26,557.6**	**1,312.4**	**6,634.3**
							Total	**7,946.7**	

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Ejercido con recursos de Cuenta Pública 2020	Ejercido con recursos de Fideicomiso
				De	Al	Mínimo	Máximo		
Licitación Pública Nacional Electrónica con número de procedimiento LA-045000001-E108-2018	CRE/55/2018		Servicio de seguridad integral de la Comisión Reguladora de Energía				76,584.0	6,564.3	19,692.9
	CM/01/2018	Retro Industrial, S.A. de C.V.	Modificar la Cláusula Quinta. - Lugar y Forma de pago donde se especifica que los pagos se realizaran a nombre de la empresa Clear Leasing, S.A. de C.V.	01/09/2018	31/07/2021		N/A	N/A	N/A
	CM/02/2021		Modificar Cláusula Segunda Vigencia y Cláusula Cuarta del Monto del contrato.	01//08/2021	31/12/2021		10,940.6	N/A	N/A
					Subtotal		**87,524.6**	**6,564.3**	**19,692.9**
							Total	**26,257.2**	
					Total		**114,082.2**	**34,203.9**	

Fuente**:** Contratos y facturas proporcionadas por la CRE

Nota 1: En la suma total de los montos de los contratos se tomó como referencia el monto máximo del Convenio CRE/21/2019

Los pagos de las partidas “33301 Servicios de Desarrollo de Aplicaciones Informáticas” y “31904 Servicios Integrales de Infraestructura de Cómputo” para el Convenio número CRE/21/2018 “Servicio de desarrollo y mantenimiento a los sistemas de información en la modalidad de fábrica de software” se realizaron con recursos de la Cuenta Pública 2020 que ascienden a 1,312.4 miles de pesos; respecto al Contrato número CRE/55/2018 “Servicio de seguridad integral de la Comisión Reguladora de Energía”, se realizaron pagos con recursos del ejercicio 2020 por un monto de 6,564.3 miles de pesos lo que da un total de 7,876.7 miles de pesos. Con recursos provenientes del Fideicomiso de la CRE número 20164531401590, se realizaron pagos para ambas contrataciones por un monto total de 26,327.3 miles de pesos.

Normativa

El 24 de noviembre del 2017, se publicó en el Diario Oficial de la Federación el Manual de Organización General de la Comisión Reguladora de Energía que tiene como objetivo describir la estructura organizacional y las funciones de la Comisión, con el propósito de ser

un instrumento de consulta, apoyo administrativo y orientación, para los servidores públicos de la misma y de otras Instituciones Públicas; así como el hacer transparente ante la ciudadanía las actividades operativas y administrativas de las unidades administrativas de la Comisión.

La Dirección General de Tecnologías de la Información (DGTI) tiene como objetivo fortalecer el desarrollo y uso de sistemas computarizados, que contribuyan al desempeño eficiente de las funciones de la Comisión a través de la automatización de los procesos sustantivos y administrativos, así como asegurar la continuidad de los servicios informáticos y de telecomunicaciones a través del soporte oportuno y eficiente y dirigir la modernización y construcción de la infraestructura tecnológica que dé soporte a los servicios de comunicación de voz, datos e imagen de la Comisión.

El Manual de Organización General de la CRE no contiene la estructura y las funciones de las diferentes áreas que conforman a la DGTI que, a su vez, no cuenta con un manual específico ni con políticas establecidas que normen sus funciones.

Se revisó el Manual de Organización General de la Secretaría de Energía publicado en el Diario Oficial de la Federación el 6 de mayo de 2016, donde se establecen las funciones de la Unidad del Sistema Eléctrico Nacional y Política Nuclear, así como el Manual de Organización Específico de la Unidad del Sistema Eléctrico Nacional y Política Nuclear del 4 de julio de 2016.

Los resultados subsecuentes relacionados con las contrataciones de la CRE son los números 2 y 3. El resultado asociado a la Supervisión de la Ciberseguridad en el Sistema Eléctrico Nacional por parte de la CRE es el resultado número 4 y por parte de la SENER es el resultado número 5.

2020-0-45100-20-0112-01-001 **Recomendación**

Para que la Comisión Reguladora de Energía, en colaboración con la Unidad de Administración y la Unidad de Asuntos Jurídicos, realice el Manual especifico de Organización que describa la estructura orgánica y las funciones de la DGTI y que éstas sean acordes al Reglamento Interno, con el fin de que la DGTI tenga claridad en sus alcances y funciones.

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. Convenio Número CRE/21/2019, Celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C.

Se revisó el Convenio número CRE/21/2019, celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C. (IPICYT), mediante un proceso de contratación por adjudicación directa con fundamento en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; el artículo 1° de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y el artículo 4 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP); con vigencia del 1° de junio de 2019 al 31 de diciembre de 2019, con plazo de vigencia ampliado al 31 de marzo de 2020, por medio de la celebración de su primer convenio modificatorio el 18 de diciembre de 2019, por un monto mínimo de 10,631.0 miles de pesos y un monto máximo de 26,577.6 miles de pesos IVA incluido, que tiene por objeto ~~el~~ prestar el Servicio de desarrollo y mantenimiento a los sistemas de información en la modalidad de fábrica de software. Durante el ejercicio 2020, se realizaron pagos por 7,946.7 miles de pesos, tras el análisis de esta contratación se determinó lo siguiente:

Objetivo

Fortalecer la capacidad de atención de la DGTI mediante un servicio que apoyará en la definición de nuevos proyectos de tecnologías de la información y mantenimiento a las soluciones tecnológicas ya existentes en la CRE, que permitieran a las Unidades Administrativas de la CRE automatizar procedimientos administrativos para garantizar el cumplimiento de sus funciones de manera eficiente, proporcionando información confiable y oportuna para la toma de decisiones, así como empoderar al consumidor y proteger sus intereses fomentando mayor acceso a la información.

Descripción del servicio

- El Servicio se realizó bajo el esquema de “Tiempos y Materiales” lo que permitió a la Dirección General de Tecnologías de la Información (DGTI) solicitar al IPICYT, elementos técnicos y administrativos, quienes prestaron sus servicios en la gestión y ejecución de proyectos de desarrollo (persona con conocimiento técnico o administrativo para la ejecución de proyectos de desarrollo, mantenimiento y operación de software asignado a la oficina de proyectos), mantenimiento y operación de software, así como en la validación de los productos existentes o nuevos y de los procesos que los rigen. Los elementos fueron asignados por un periodo de tiempo con base en los perfiles y cantidades definidos en el “Apéndice A” de los términos de Referencia.

- El IPICYT prestó sus servicios por medio de elementos conforme a su perfil y fueron asignados por líderes de la CRE, pudiendo participar en el desarrollo de nuevos sistemas, mantenimiento a sistemas existentes, operación de sistemas que se encuentren en producción, en el análisis de la validación de productos de software, así como en la definición y mejora continua de los procesos de la DGTI.

- Los sistemas a los que se les dio mantenimiento se listaron en el “Apéndice B”, siendo un listado enunciativo mas no limitativo y que evolucionó conforme a las necesidades de la CRE.

Investigación de Mercado

- En el apartado 2 de búsqueda de contrataciones similares, no se indicaron los parámetros utilizados en la consulta de proveedores relacionados con los servicios solicitados que demuestren que no había proveedores de desarrollo de software que se apegaran a las necesidades de la Comisión.

- El formato FO-CON 04 para la elaboración de la solicitud de cotizaciones enviado a los proveedores carece del “inciso d” relacionado con la capacidad de cumplimiento de los requisitos de participación de acuerdo con lo establecido en el punto 4.2 Contratación, 4.2.1.1.10 Realizar Investigación de Mercado del Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público (MAAGMAASSP).

Justificación de la Excepción a la Licitación Pública

El documento presentado como justificación carece del lugar de emisión. En el análisis realizado a la justificación se identificó que la fundamentación bajo la cual se realizó la contratación carece de documentación que soporte los elementos para identificar que eran sistemas especializados y las circunstancias que podrían provocar pérdidas o costos adicionales importantes, cuantificados y justificados, en caso de no contar con este servicio en la CRE.

Penalizaciones y Deductivas

- Se identificó una falta de control en el área administrativa que aplicó un cobro en exceso al proveedor por 19.7 miles de pesos por una penalización derivada de la desincorporación de elementos del equipo de transición y atención de incidentes.

- No se consideraron posibles penalizaciones o deductivas al proveedor ante la ocurrencia de fallas durante los procesos de desarrollo y pruebas.

Entregables

En el convenio número CRE/21/2019 no se especificaron los entregables que debían proporcionarse para demostrar la ejecución de los servicios para cada una de las etapas del ciclo desarrollo de software, ya sea por metodología ágil o tradicional.

- Se identificaron 10 proyectos y 2 requerimientos en los que no se generaron documentos de especificación de requerimientos o de diseño.

- 12 proyectos y 5 requerimientos relacionados con servicios de desarrollo no contaron con un documento de especificación de pruebas.

- No se consideraron pruebas de seguridad o pruebas de estrés para verificar el rendimiento de los desarrollos y pruebas para validar su integración en caso de contar con dependencia o interconexión a bases de datos u otros aplicativos.

- Se identificó que 4 proyectos y un requerimiento fueron entregados en el ambiente de calidad en marzo 2020, no obstante, tienen 21 meses sin ser utilizados.

- 4 proyectos y un requerimiento pagados en 2020 no completaron su fase de pruebas, uno de los cuales no es compatible con la infraestructura; la CRE y el IPICYT no detectaron dicha incompatibilidad.

- La DGTI aceptó los desarrollos de software entregados por el IPICYT, aun cuando tenía identificadas actividades pendientes para su implementación y puesta en marcha en el ambiente de producción.

- La DGTI no aplicó deductivas y penalizaciones por la falta de calidad en los desarrollos proporcionados, dado que el convenio no los estipuló.

Ciclo de vida de desarrollo de Sistemas en la CRE

A la fecha de la auditoría (noviembre de 2021):

- La CRE no cuenta con lineamientos y metodología formalizada y difundida para la administración de proyectos de desarrollo de software.

- La CRE carece de mecanismos institucionales para la estimación de horas/hombre para servicios de desarrollo de software.

- El proceso de ciclo de vida para desarrollo de sistemas que utiliza se basa en una metodología tradicional; sin embargo, la documentación y las actividades generadas por cada etapa no están especificadas ni formalizadas en un procedimiento interno o política.

- El proceso control de cambios no se encuentra formalizado y no existe un comité de cambios para infraestructura de TIC, quien lleva este proceso es el área de desarrollo, y no se evalúan los impactos de las implementaciones.

- No elabora cartas de liberación de aplicaciones y sistemas, por lo que no se cuenta con un mecanismo de verificación respecto a los componentes que son integrados a la infraestructura ni con registros de las fechas en que fueron aplicados dichos cambios.

- No se cuenta con herramientas o algún otro mecanismo para el registro de los cambios en infraestructura de TI y de liberación de software.

Por lo anterior se observa que la contratación no cumplió con la fundamentación por la cual se otorgó la excepción a la licitación pública, dado que los servicios de desarrollo y mantenimiento a los sistemas de información que se solicitaron no requerían de alguna especialización técnica, ni se especificaron si existían circunstancias que pudieran provocar pérdidas o costos adicionales importantes, cuantificados y justificados por el hecho de que no se realizaran; además, se comprobó que 5 servicios de desarrollo de software tienen más de 21 meses sin ser utilizados por la CRE y en caso de liberarse a producción, requieren modificaciones adicionales; dichos desarrollos fueron pagados sin que hayan tenido utilidad y beneficio para la CRE. Durante 2020, se generaron pagos por 298.2 miles de pesos relacionados a estos proyectos como se muestra en la tabla siguiente:

Costo de los proyectos y requerimientos liberados en ambiente de calidad pagados en 2020, por proyecto
(Miles de Pesos)

Número de Proyecto	Nombre del proyecto	Horas/hombre	Monto Hora/ Hombre	Monto determinado	IVA	Monto total
CRE-IPICYT-PRY-002-2019	Formulario para Carga de Precios GLP	22	0.4	8.0	1.3	9.2
CRE-IPICYT-PRY-015-2019	Migración de Aplicación Móvil de AmiGas LP	420	0.4	152.1	24.3	176.4
CRE-IPICYT-PRY-005-2020	Liberación a Producción los Formularios Electrónicos de Electricidad	26	0.4	9.4	1.5	10.9
CRE-IPICYT-PRY-010-2020	Formulario Unidades de Inspección – Terceros Expertos	98	0.4	35.5	5.7	41.2
CRE-IPICYT-REQ-006-2020	Pantalla de Seguimiento de Acta de Verificación	144	0.4	52.1	8.3	60.5
		710	0.4	**257.1**	**41.1**	**298.2**

FUENTE: Elaborado por la ASF con información proporcionada por la CRE

Se observó que se realizaron pagos con recursos de la Cuenta Pública 2019 a las actividades de desarrollo de software que entregó el proveedor en ambiente de calidad por un monto de 2,034.6 miles de pesos, sin que el ente fiscalizado demostrara que fueran de utilidad y beneficio para la CRE.

Al respecto se procederá en términos del artículo 22 de la Ley de Fiscalización y Rendición de Cuentas de la Federación.

2020-0-45100-20-0112-01-002 **Recomendación**

Para que la Comisión Reguladora de Energía establezca dentro de los procesos de contratación, integrar un documento que acredite que los servicios solicitados cuentan con la característica de ser un servicio especializado e incluir los análisis técnicos que respalden dicha justificación.

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.

2020-0-45100-20-0112-01-003 **Recomendación**

Para que la Comisión Reguladora de Energía formalice una política institucional de desarrollo de software que incluya las actividades de supervisión a los prestadores de servicios de fábrica de software, incluya una metodología de estimación horas/hombre y desarrolle mecanismos e indicadores para su revisión; formalice un procedimiento para la gestión de cambios en la infraestructura de TIC y de liberación de aplicativos y sistemas el cual solicite la ejecución de pruebas de vulnerabilidades y/o penetración a los aplicativos críticos antes de la salida a producción o, en su defecto, defina una fecha compromiso para la ejecución de dichas actividades y se elaboren cartas de liberación de los desarrollos de software especificando los componentes proporcionados, fecha de liberación, versión y ambiente; establezca un comité de cambios que evalúe los impactos y dé su visto bueno a la actualización, alta y baja de servicios y de desarrollos de software en la infraestructura 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.

2020-0-45100-20-0112-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 298,200.85 pesos (doscientos noventa y ocho mil doscientos pesos 85/100 M.N.), por los pagos realizados por concepto de los servicios de desarrollo de software de 4 proyectos con números CRE-IPICYT-PRY-002-2019, CRE-IPICYT-PRY-015-2019, CRE-IPICYT-PRY-005-2020, CRE-IPICYT-PRY-010-2020, así como del requerimiento con número CRE-IPICYT-REQ_006-2020, realizados bajo el amparo del convenio número CRE/21/2019, los cuales no fueron liberados en el ambiente de producción durante la vigencia del convenio. El Director General de Tecnologías de Información en su figura de Administrador del

Contrato no supervisó el desarrollo de estos servicios; no dio cumplimiento al numeral 2.3.1, inciso c), subinciso (iii), del Manual de Vigilancia del Mercado, dado que el aplicativo desarrollado en el proyecto número CRE-IPICYT-PRY-010-2020, tenía como finalidad apoyar las actividades de supervisión del SEN, por lo que al no liberarse en ambiente de producción, no cumplió con el propósito por el cual fue requerido; no validó que el desarrollo del proyecto con número CRE-IPICYT-PRY-015-2019 fuera diseñado y desarrollado por el proveedor conforme a los requisitos solicitados y fuera compatible con la infraestructura de la Comisión Reguladora de Energía, asimismo, no dio seguimiento con la Unidad de Electricidad, la Dirección General de Mercados de Hidrocarburos, la Dirección General de Gas Natural y Petróleo, y la Dirección General de Normalización y Verificación de Petrolíferos para que autorizaran la liberación de los proyectos con números CRE_IPICYT_PRY_002-2019, CRE_IPICYT_PRY_005-2020 y CRE_IPICYT_PRY_010-2020, y del requerimiento con número CRE_IPICYT_REQ_006-2020. Estas consideraciones han provocado que estos desarrollos se encuentren almacenados en un repositorio desde la conclusión del convenio, sin dar continuidad para la utilización y funcionalidades por las cuales fueron desarrollados, en virtud de que no han estado disponibles para las áreas usuarias que las solicitaron, aunado a que 1 de estos desarrollos requiere de modificaciones adicionales para el adecuado funcionamiento con la infraestructura con la que opera actualmente la Comisión Reguladora de Energía; más los intereses generados desde la fecha de pago hasta la de su recuperación, en incumplimiento de lo establecido en el artículo 1, 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 Diario Oficial de la Federación el 19 de noviembre de 2019, en el Proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factor crítico 3, del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014, con última reforma publicada en el mismo medio el 23 de julio de 2018; en las Cláusulas Tercera (Lugar de prestación del servicio), Décima Séptima (Representantes responsables de administrar y vigilar el cumplimiento del convenio) y Décima Octava (Supervisión y aceptación de los servicios) del convenio número CRE/21/2019 celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C.; en los numerales 4 - objetivo y 5 - beneficios del anexo técnico del convenio número CRE/21/2019 celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C.; en los objetivo y funciones 2, 3, 4 y 5 del numeral IV.4, Dirección General de Tecnologías de la Información del Manual de Organización General de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación el 24 de noviembre de 2017; y en el numeral 2.3.1, inciso c), subinciso (iii), del Acuerdo por el que se emite el Manual de Vigilancia del Mercado, publicado en el Diario Oficial de la Federación el 12 de enero de 2018.

Causa Raíz Probable de la Irregularidad

Deficiencias en la supervisión de las actividades del proveedor respecto al desarrollo de los servicios.

3. Contrato CRE/55/2018 Servicio de Seguridad Integral de la Comisión Reguladora de Energía (SSICRE)

Se revisó el contrato número CRE/55/2018, celebrado con el proveedor Reto Industrial S.A. de C.V., mediante el procedimiento de Licitación Pública Nacional Electrónica número LA-045000001-E108-2018, bajo el fundamento de los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 26, fracción I, 26 Bis, fracción II y 28, fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y el artículo 39 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP), con vigencia del 1° de septiembre de 2018 al 31 de diciembre de 2021 por un monto total de 87,524.6 miles de pesos con IVA incluido, que tiene el objeto de prestar el Servicio de Seguridad Integral de la Comisión Reguladora de Energía (SSICRE). Durante el ejercicio 2020, se realizaron pagos por 26,257.2 miles de pesos y se determinó lo siguiente:

Objetivo

Proteger todos los elementos susceptibles a ser atacados, preservar los servicios, información y bienes informáticos en la Institución procurando la integridad, confidencialidad, disponibilidad de la información mediante herramientas que apoyen a minimizar los riesgos a la infraestructura tecnológica.

Características del servicio

El servicio integró:

- Una solución de sistema de infraestructura de equipo activo de telecomunicaciones que permitió la correcta conectividad para usuarios y elementos informáticos de la Comisión mediante la implementación de enlaces de alta velocidad y esquemas de redundancia.

- Una solución de infraestructura pasiva de telecomunicaciones que permitió la instalación, montaje, correcta operación, monitoreo e interconexión de todo el equipo activo necesario para brindar los servicios solicitados por la Comisión mediante el Anexo Técnico del contrato número CRE/55/2018.

- Un servicio administrado de la seguridad interna que permitió administrar el acceso a los recursos de red, de datos y aplicativos de la Comisión únicamente al autorizado para ello, llevando además un registro detallado para conocer cuales usuarios han accedido a los recursos y facilitar las auditorias ante posibles brechas de seguridad.

- Una solución de seguridad perimetral multicapa que aseguró la disponibilidad de los servicios con conexión a la red pública de internet, mediante esquemas de alta redundancia y simultáneamente proteja a la Comisión contra amenazas externas mediante tecnologías de cifrado de datos, filtrado de comunicaciones, registro de eventos y detección temprana de amenazas de ciberseguridad.

En el Anexo Técnico del contrato número CRE/55/2018, se indicó que los servicios requeridos eran compatibles con la infraestructura de telecomunicaciones que operaba en la CRE al inicio de la vigencia del contrato.

Pagos

- Las facturas de marzo a diciembre de 2020 no cuentan con el sello o firma de validación de los requisitos fiscales y de recepción en ventanilla. La factura de fecha 1° de abril de 2020 no cuenta con el sello o firma de la validación por parte de la Dirección de Tecnologías de la Información.

- Se carece del desglose de los costos unitarios de los servicios proporcionados en el contrato para verificar que los pagos por los servicios devengados sean efectuados correctamente.

Deductivas

Se identificó que en el contrato se especificaron deducciones por la calidad de los servicios respecto al tiempo de solución máximo de los eventos correspondientes a la Mesa de Ayuda, pero no por deficiencias en ellos.

Soluciones tecnológicas

Se identificaron características de las soluciones tecnológicas ofertadas que no están siendo aprovechadas por la CRE correspondientes al concentrador VPN SSL, filtrado web, DNS público y firewall de base de datos, que coadyuvarían a robustecer la seguridad mediante la explotación de reportes, habilitación de funcionalidades, actividades de análisis proactivas y configuraciones de seguridad.

En el anexo técnico del contrato número CRE/55/2018 se solicitaron especificaciones técnicas de las soluciones de seguridad para una herramienta SIEM (Security Information and Event Management, por sus siglas en inglés), que no fueron utilizadas toda vez que la CRE no cuenta con dicha herramienta; no obstante, fueron solicitadas desde la convocatoria.

Entregables del servicio

La CRE no tuvo un control centralizado de los tickets, ya que se identificaron discrepancias en la información que proporcionó respecto al servicio de mesa de ayuda. En el reporte general se observaron 148 requerimientos, mientras que en el conteo realizado de cada reporte mensual se identificaron 329 requerimientos.

Respecto al contenido de los reportes se observó lo siguiente:

- Se identificó un error en el apartado de estadísticas de tráfico para 4 interfaces del CORE, reportada en todos los meses del 2020; estos hallazgos no fueron atendidos.

- En los entregables mensuales, no se especificó el cumplimiento de los niveles de servicio, ni los tiempos de solución de las solicitudes realizadas a la mesa de ayuda, por lo que la CRE no contó con información para medir su cumplimiento.

- De las gestiones realizadas por el proveedor para tramitar la solución de caídas en los enlaces de internet de la CRE, se identificó que solo el 64.3% de éstas fueron efectuadas por dicho proveedor; no obstante, era su responsabilidad atender la totalidad de estos eventos.

Reportes de Mantenimiento

No se cuenta con la evidencia de la ejecución de los planes de mantenimiento lógico presentados para las soluciones tecnológicas. Asimismo, no se proporcionó evidencia de los mantenimientos físicos del equipo de infraestructura de seguridad, ni fue posible validar si se llevaron a cabo de forma calendarizada y si fueron exitosos o no durante el periodo de 2020.

Reportes de Pruebas de Seguridad

En 2020, no se realizaron pruebas de seguridad para detectar el nivel de vulnerabilidad de los sistemas institucionales, aplicativos e infraestructura frente a ataques externos, sin embargo, se observó que en 2021 se realizaron 4 pruebas continuas, por lo que se considera que no existió una planeación previa y una calendarización adecuada para realizarlas. El administrador y el supervisor del contrato no coordinaron ni dieron seguimiento a la ejecución de dichas pruebas de seguridad, atribuciones conferidas en el MOG.

No se identificaron acciones por parte de la CRE para eliminar, mitigar o reducir los riesgos detectados por medio de este servicio o un plan de trabajo para ejecutar actividades con este fin. Durante el 2020, no se ejecutaron las segundas pruebas de seguridad (especificadas en el contrato) que confirman que las correcciones realizadas para las vulnerabilidades se aplicaron de manera correcta, por lo que dicho servicio no representó un beneficio para la CRE. No obstante, se realizaron pagos por la ejecución de dichas pruebas por 1,750.5 miles de pesos, como se señala a continuación:

Erogaciones del servicio de pruebas de seguridad de 2020.

(Miles de pesos)

Servicio	Sin IVA		Con IVA
Pruebas de seguridad	Pago de Servicio por mes	Pago total durante el 2020	Pago erogado en 2020
	125.7	1,509.0	1,750.5

Fuente: Elaborado por la ASF.

Nota: Diferencias por redondeo.

Políticas y Procedimientos de Seguridad

Se solicitó al proveedor desarrollar y documentar políticas y procedimientos que permitieran administrar y preservar la seguridad de la infraestructura tecnológica, así como la seguridad e integridad de la información conforme al Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI). En 2020, el proveedor presentó un documento llamado políticas y procedimientos de seguridad de TIC; no obstante, este documento no está definido como política de cumplimiento institucional y no fue formalizado ni difundido; en caso de cambios de administración, podrá ser reemplazado al no ser oficial, por lo que el costo erogado por esta actividad no ha tenido utilidad ni representó un beneficio para la CRE.

Por lo anterior, se concluye:

- La CRE requirió funcionalidades y características del servicio indicadas en la convocatoria, sin que a la fecha de la ejecución del contrato las aproveche o las utilice como el caso de la herramienta SIEM, lo que encarece el monto del servicio y acotó la participación de proveedores en la licitación por requerimientos que no fueron necesarios.

- Las herramientas que conforman la Solución Integral de Seguridad de la CRE no fueron aprovechadas en su totalidad, dado que la CRE no utilizó todas las características brindadas o no contó con el equipamiento adicional que complementara su integración con los equipos de seguridad.

- La CRE no contó con una estrategia de ejecución de pruebas de seguridad en razón de que los análisis no fueron calendarizados o planeados con antelación.

- La CRE no ha tenido una adecuada administración del contrato lo que ha originado que falte seguimiento a las actividades del proveedor.

2020-0-45100-20-0112-01-004 **Recomendación**

Para que la Comisión Reguladora de Energía especifique, en los contratos en materia de TIC, mecanismos de penalización respecto a la calidad de los servicios proporcionados, con el fin de garantizar que la prestación de los servicios no se realice de forma deficiente y sea conforme a las necesidades y beneficios esperados por la CRE.

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.

2020-0-45100-20-0112-01-005 **Recomendación**

Para que la Comisión Reguladora de Energía establezca, en las contrataciones en materia de TIC y las relacionadas a servicios integrales en dicha materia, el desglose unitario de los costos por cada uno de los servicios que lo conforman, con el fin de verificar que las actas de entrega-recepción contengan los servicios recibidos a entera satisfacción de la Comisión y así verificar en las respectivas facturas que éstos sean congruentes con las especificaciones de precios y montos establecidos en las contrataciones.

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

2020-0-45100-20-0112-01-006 **Recomendación**

Para que la Comisión Reguladora de Energía ejecute la estrategia de mitigación de las vulnerabilidades generadas por las plataformas tecnológicas utilizadas por los aplicativos legados con el objetivo de incluirlos en el alcance de protección del Firewall y documente dichas acciones.

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.

2020-0-45100-20-0112-01-007 **Recomendación**

Para que la Comisión Reguladora de Energía implemente mecanismos de control en la elaboración de los anexos técnicos en materia de TIC para que sean acorde a sus necesidades, en las que se contemplen las características técnicas que sean compatibles con las soluciones que estén en operación a fin de que los servicios sean de utilidad en función del precio y calidad solicitados y en su caso, considerar realizar convenios modificatorios que ajusten los servicios a su operación e infraestructura.

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.

2020-0-45100-20-0112-01-008 **Recomendación**

Para que la Comisión Reguladora de Energía implemente las acciones necesarias para que los proveedores de servicios cumplan con las especificaciones respecto al monitoreo de enlaces y gestione con el proveedor de internet de la CRE la totalidad de eventos de caída del servicio hasta su restauración.

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.

2020-0-45100-20-0112-06-002 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por un monto de 1,750,491.97 pesos (un millón setecientos cincuenta mil cuatrocientos noventa y un pesos 97/100 M.N.), por concepto de pagos injustificados al contrato CRE/55/2018 ya que el servicio no se entregó conforme a lo solicitado en los numerales SSICRE-714 y SSICRE-715 del anexo técnico del contrato citado, toda vez que no se completó el ciclo de las pruebas de seguridad durante 2020 por lo que no cumplió con el objetivo de detectar el nivel de vulnerabilidad de los sistemas institucionales frente a ataques externos, más los rendimientos financieros que se generen desde la fecha de pago hasta el reintegro o recuperación total; el administrador y el supervisor del contrato no dieron seguimiento a la ejecución del ciclo de pruebas de seguridad que podría impactar en la pérdida de continuidad de los servicios, en incumplimiento de lo establecido en el artículo 1, párrafo segundo, de la Ley Federal de Presupuesto y Responsabilidad Hacendaria publicado en el Diario Oficial de la Federación el 30 de marzo de 2006, con última reforma publicada en el mismo medio el 30 de diciembre de 2015; en el artículo 3 del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, con última reforma publicada en el mismo medio el 23 de julio de 2018; en el Apartado III.B Proceso de administración de proveedores (APRO), Objetivo General, objetivos específicos 1 y 2; en la Actividad del proceso APRO 1 General lista de verificación de obligaciones, factores críticos 1 y 2, la Actividad del proceso APRO 2 Monitorear el avance y desempeño del proveedor, factores críticos 1 y 3; en la Actividad del proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factores críticos 1 y 2, del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la

Federación el 08 de mayo de 2014, con última reforma publicada en el mismo medio el 23 de julio de 2018; en el Numeral IV.4, Función 2, numeral IV.4.3, Funciones 4 y 5, del Manual de Organización General de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación el 24 de noviembre de 2017, y en las cláusulas Primera (Objeto del contrato), Cuarta (Monto del contrato), Sexta (Responsabilidad de El Prestador), Novena (Modificaciones), Décima Cuarta (Pena convencional), Décima Octava (Representantes responsables de administrar y vigilar el cumplimiento del contrato) y Décima Novena (Supervisión y aceptación de los servicios) del contrato número CRE/55/2018, numerales SSICRE-714 y SSICRE-715 del Anexo Técnico.

Causa Raíz Probable de la Irregularidad

Deficiencias en la supervisión de las actividades del proveedor respecto al desarrollo de los servicios.

4. Supervisión a la Ciberseguridad en el Sistema Eléctrico Nacional

La CRE debe dar seguimiento a la normativa establecida para la gestión y supervisión del sector eléctrico en México. Dentro de sus facultades está la regulación y seguimiento de las normas de alcance a la infraestructura de TIC que soporta al Sistema Eléctrico Nacional (SEN) y el Mercado Eléctrico Mayorista (MEM), entre las cuales se encuentran:

- La Ley de la Industria Eléctrica, que tiene por objeto regular la planeación y el control del Sistema Eléctrico Nacional, el Servicio Público de Transmisión y Distribución de Energía Eléctrica y las demás actividades de la industria eléctrica.

- El Código de Red, el cual dicta los criterios de eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad, y especifica 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 Sistema Eléctrico Nacional (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.

- El Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, que establece los principios, reglas, directrices, ejemplos y procedimientos a seguir en el uso de las tecnologías de la información, para el control operativo del Sistema Eléctrico Nacional y con la operación del Mercado Eléctrico Mayorista.

La CRE, mediante la Unidad de Electricidad, debe:

- Determinar el marco regulatorio en materia eléctrica y su actualización, en coordinación con la Unidad de Asuntos Jurídicos, así como las disposiciones en materia de separación

operativa, funcional, contable y códigos de conducta a que deben sujetarse los permisionarios y demás participantes del mercado y vigilar el cumplimiento de la regulación, las normas oficiales mexicanas y las disposiciones administrativas de carácter general aplicables a quienes realicen actividades reguladas.

- Formular el programa anual de visitas de verificación, inspección y supervisión ordinarias y extraordinarias, así como dirigir las acciones para que se lleven a cabo; requerir la presentación de información y documentación, para el cumplimiento de la regulación, autorizaciones y obligaciones de los permisos emitidos.

Reporte de Confiabilidad

El objetivo de la regulación de Confiabilidad expedida por la Comisión es garantizar que el suministro eléctrico sea provisto bajo condiciones de seguridad, calidad y continuidad. Es por ello que la CRE emite el reporte de confiabilidad cuya finalidad es informar sobre el desempeño del Sistema Eléctrico Nacional en materia de confiabilidad. A la fecha de la auditoría (noviembre de 2021), se identificó que en los reportes de confiabilidad de 2016 y 2017, y en el Sistema de Administración de Indicadores, no se consideró la evaluación de efectividad de mecanismos de seguridad de la información y ciberseguridad ni se había emitido el reporte de confiabilidad correspondiente a los años de 2018, 2019 y 2020; después de esta auditoría, la CRE emitió los reportes de 2018 y de 2019 (en diciembre 2021).

Normas, estándares y marcos de referencia relacionados con ciberseguridad en el sector de Energía nivel internacional

Dentro de las principales normas, estándares y marcos de referencia en materia de ciberseguridad a nivel internacional para el sector energía se consideran los siguientes:

- **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 cual define 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. Está conformado por un conjunto de controles, entre los que destacan los relacionados con la seguridad física, la seguridad de la información y la ciberseguridad (CIP-002-5.1a - CIP-013-1).

- **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.

- **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.

Estado Actual de la regulación en materia de Seguridad de la información y Ciberseguridad en México para el Sector de Energía

- La ASF realizó una comparativa con el estándar NERC (CIP-002-5.1a - CIP-013-1) y los requisitos plasmados en el Código de Red y el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, en materia de Seguridad de la información y Ciberseguridad para el Sector de Energía, cuyo análisis se presenta a continuación:

Código de Red

En el Código de Red en su capítulo 5 "Disposiciones Generales de Red Eléctrica Inteligente en materia de Telemetría, Interoperabilidad y Seguridad de la Información (REI) para la operación del SEN" se incluye la especificación de controles de seguridad de la información, los cuales son:

Controles de seguridad de la información establecidas en el Código de Red	
5.5 Implementación y desarrollo de Criterios de Interoperabilidad y Seguridad de la Información	
Criterio REI - 15	Los integrantes de la Industria Eléctrica deben implementar los criterios para asegurar la interoperabilidad y seguridad en el SEN.
Criterio REI - 16	Indica que las acciones en materia de Seguridad de la Información deben estar en armonía con los criterios de interoperabilidad y ambos a su vez, con los criterios de eficiencia, confiabilidad, calidad, continuidad, sustentabilidad y seguridad.
Criterio REI - 17	Establece que los participantes deben considerar los principios generales de confidencialidad, conservación, disponibilidad de datos e información, equilibrio, integridad y bidireccionalidad.
5.6 Interoperabilidad de los elementos y sistemas de medición, monitoreo y operación de las redes eléctricas que cuenten con tecnologías de información y comunicación	
Criterio REI - 18	Indica que los integrantes de la Industria Eléctrica deben utilizar estándares o normas nacionales o internacionales en sistemas de medición, monitoreo y operación con TIC de los cuales son responsables.
Criterio REI - 19	Los integrantes de la Industria Eléctrica que sean dependencias y entidades de la Administración Pública Federal deben observar en lo conducente el "Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital

	Nacional, en materia de tecnologías de la información y comunicaciones, así como establecer el manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información".
Criterio REI-20	Los integrantes de la Industria Eléctrica deben observar, implementar y operar mecanismos de Seguridad de la Información para la Infraestructura de TIC del SEN de la cual sean responsables, conforme a las disposiciones generales que, en su caso, emita la CRE.
Criterio REI - 21	Se establecen mecanismos de Seguridad de la Información para la Infraestructura de TIC, consistentes en mantener un modelo de gestión de Seguridad de la Información, identificación de infraestructuras críticas y activos, establecimiento de mecanismos de respuesta inmediata a incidentes de ataques y administración de riesgos, fomento de cultura de seguridad y mención de mecanismos de recuperación.
5.8 Responsabilidades en materia de Interoperabilidad y Seguridad de la Información	
Criterio REI - 22	Establece que los integrantes de la Industria Eléctrica responsables de los elementos y sistemas del SEN, deben observar y aplicar los documentos técnicos o catálogos de estándares aprobados que en su caso emita la CRE en materia de interoperabilidad; y asegurar que los sistemas a su cargo se mantengan actualizados con respecto a los procesos de administración de Seguridad de la Información
Criterio REI - 23	Establece que la CRE emitirá, en su caso Documentos técnicos o catálogos de estándares aprobados en materia de interoperabilidad para los elementos y sistemas de medición; y Disposiciones generales sobre los procesos de administración de Seguridad de la Información

FUENTE: Elaborado por la ASF.

En el análisis de dichos criterios comparados con los estándares del NERC (CIP-002-5.1a - CIP-013-1), se observó lo siguiente:

El único criterio que menciona controles relacionados con la seguridad de la información es el Criterio REI-21, sin embargo, éste no específica períodos de revisión y actualización de los activos, ni criterios de clasificación y de evidencia mínima de cumplimiento, no menciona la necesidad de planes de capacitación y concientización en materia de ciberseguridad, evaluaciones de confianza y reforzamiento de habilidades técnicas, que incluyan entre otros, el conocimiento del marco regulatorio; respecto al modelo de gestión de la seguridad, no establece los alcances, requerimientos mínimos de cumplimiento, periodos de revisión y métricas de evaluación; no solicita un plan de respuesta y notificación a incidentes, que incluya periodos de actualización, clasificación de incidentes, pruebas para validar su funcionamiento, así como la evidencia mínima de las actividades de contención, erradicación y solución. No establece como requisito contar con un plan de recuperación de operaciones como participante, ni define los mecanismos de coordinación conjunta para contar con un plan de recuperación integral que establezca las actividades de recuperación del SEN. No se solicita cumplir con planes de gestión de riesgos y actividades que demuestren la reducción del nivel de exposición.

Respecto al criterio REI-19, establece que, para la gestión de la seguridad de la información las entidades de la Administración Pública Federal pertenecientes al SEN, deben acatarse las disposiciones del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), la CRE no proporcionó evidencia del cumplimiento de los integrantes del SEN a esta normativa (CENACE, CFE y sus EPS) durante 2020. Asimismo, este manual fue derogado por el Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal; a la fecha de la auditoría (noviembre 2021), la CRE aún no había actualizado dicho criterio conforme a la normativa actual ni había verificado que ésta cumpla con lo mínimo requerido para la protección de los procesos de TIC y de seguridad de la información, y el mecanismo de verificación de cumplimiento para los participantes.

En el caso de los criterios REI-22 y REI-23, se indica que la CRE debe emitir las disposiciones generales complementarias para la gestión de procesos de administración de seguridad de la información, que a la fecha de la auditoría (noviembre 2021), no se habían emitido.

En el Código de Red se especifica el criterio de seguridad, sin embargo, dicho criterio se refiere a la seguridad operativa, es decir, a violaciones de límites de voltaje, sobrecarga en líneas o bancos de transformación y pérdida de sincronismo entre centrales eléctricas, entre otras, y no considera aspectos relacionados con la seguridad de la información o ciberseguridad.

Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista

En el Anexo 4 “Requisitos de Ciberseguridad para la Infraestructura de TIC” de dicho Manual, se especifican 20 requisitos generales y 5 específicos para el Control Operativo del SEN y la Operación del MEM, incluida la medición para liquidaciones, sin embargo, no se contemplan controles específicos para las actividades de gestión de accesos físicos y lógicos; supervisión y vigilancia para la administración de proveedores; mecanismos de priorización de activos; gestión de líneas base de configuración; control de cambios; metodologías de desarrollo de aplicaciones utilizadas por las TO orientadas a mejores prácticas; gestión de vulnerabilidades en la infraestructura y en los desarrollos utilizados para el soporte de la operación; monitoreo y gestión de bitácoras; procesos para el respaldo y borrado seguro de la información; gestión de medios extraíbles, mecanismos para la salvaguarda y cifrado de información interna y con entes externos; mecanismos de configuración segura de los equipos utilizados para la operación; un plan de continuidad individual y entre participantes, así como de la gestión a incidentes, procesos de recuperación y análisis forense; y especificaciones de requerimientos en capacitación en materia de ciberseguridad para el personal operativo y técnico.

En ambas normativas se identificó lo siguiente:

No definen quiénes son los responsables de la supervisión de los controles de seguridad de la información y la ciberseguridad en el SEN, los tipos de reportes que se deben proporcionar por parte de los participantes para validar la efectividad de los mecanismos de seguridad de la información, así como los periodos de revisión y actualización de los controles de ciberseguridad establecidos. El carecer de un responsable de vigilar el cumplimiento de los aspectos relacionados con la ciberseguridad origina que no se mida su efectividad y que los sistemas y la infraestructura que dan soporte al SEN pudieran no estar cumpliendo los controles mínimos de seguridad de la información y ciberseguridad.

Los términos de Tecnología de Operación y Tecnologías de Información no están definidos; estos conceptos son de suma importancia en la administración de los componentes que conforman las soluciones de infraestructura crítica que dan soporte a los sistemas que se utilizan para administrar y controlar los procesos de generación, distribución y transmisión de energía.

Se identificó que, aun cuando en ambas normativas se solicitan requisitos y criterios relacionados con la seguridad de la información y la ciberseguridad, éstos describen un cumplimiento general sin considerar aspectos críticos relacionados con la protección, confidencialidad e integridad de la información, así como de la gestión de riesgos, entre otros, que sí son considerados en los estándares publicados por el NERC, el cual fue utilizado como una referencia de mejor práctica en la industria.

Estado de la ciberseguridad en el Sector Eléctrico Mexicano de la APF

La Auditoría Superior de la Federación desarrolló un modelo para evaluar la ciberseguridad en la Empresa Productiva Subsidiaria (EPS) CFE Transmisión y Centro Nacional de Control de Energía (CENACE), 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), 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; en la fiscalización de la CP 2020 se realizaron las auditorías números 397-DE y 466-DE con título Auditoría de Ciberseguridad del Sector Energía, realizadas al CENACE (resultado número 4) y a la EPS CFE Transmisión (resultado número 6), respectivamente; en ellas se realizó la evaluación cuyo resultado fue el siguiente:

En un total de 5 funciones, 18 categorías y 67 subcategorías evaluadas se detectó lo siguiente:

- La EPS CFE Transmisión 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, éstas 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 implementar 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.

- El CENACE obtuvo una calificación alta en 15 subcategorías del marco (22.0%), una calificación media en 50 subcategorías del marco (75.0%) y una calificación baja en 2 subcategorías del marco (3.0%), éstas últimas relacionadas con que los roles y las responsabilidades de seguridad cibernética estén coordinados y alineados con roles internos y socios externos y que las identidades sean verificadas y vinculadas a credenciales y validadas en las operaciones.

De las evaluaciones realizadas por la ASF se concluyó que los controles de ciberseguridad que actualmente son implementados por el CENACE y la EPS CFE Transmisión cumplen con los requisitos mínimos del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, sin embargo, la CRE no verifica su cumplimiento, no los ha evaluado ni ha realizado visitas de inspección. En la evaluación del marco realizado por la ASF no lograron una calificación alta en todas las categorías; estas deficiencias son importantes para la evaluación de la ciberseguridad, por lo que es necesario fortalecer los criterios y requisitos solicitados en la normativa en la industria eléctrica relacionados con la seguridad de la información y ciberseguridad, para evitar brechas respecto a la adecuada gestión de los sistemas críticos para las operaciones del SEN.

Supervisión de servicios de Tecnologías de Información y Comunicaciones que dan soporte al SEN

- La CRE no ha definido indicadores de confiabilidad relacionados con la seguridad de la información y ciberseguridad con el propósito de medir su cumplimiento y que éstos sean revisados durante las visitas de inspección y sean incluidos como parte de los reportes de confiabilidad.

- No ha emitido opinión ante las deficiencias que presenta la normativa actual que regula al Sector Eléctrico del país, respecto a los temas relacionados con Seguridad de la información y Ciberseguridad, ni ha establecido la regulación aplicable en materia de Seguridad Cibernética para el SEN y MEM.

- Asimismo, se identificó que no realizó una verificación al cumplimiento de protocolos para la conexión de los participantes al SEN; al ser un requisito normativo, se observa en el ámbito de vigilancia y verificación de la CRE.

- No ha establecido mecanismos de notificación inmediata de incidentes de seguridad de la información, y de un plan de contingencia y respuesta a estos eventos; no

proporcionó información en la cual los participantes le hubieran notificado de alguno.

- En la normativa no se contempla la revisión de los desarrollos de software que soportan al MEM, los cuales son desarrollados por el CENACE, relacionados con el cumplimiento de desarrollo seguro y evaluación de vulnerabilidades.

Visitas de Supervisión

La finalidad de llevar a cabo visitas de inspección y/o verificación es corroborar el cumplimiento de las obligaciones por parte de los permisionarios y, darles un seguimiento de supervisión regulatoria adecuado. En el análisis de la información de las actividades realizadas duranta las visitas de verificación por parte de la CRE se identificó lo siguiente:

- No ha realizado revisiones en materia de cumplimiento de TIC (controles de TI y TO), de seguridad de la información y ciberseguridad (cumplimiento del anexo 4 del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista y de los criterios REI-15 al 21 establecidos en el Código de Red), ni se han emitido sanciones por su incumplimiento.

- No tiene una definición de las áreas encargadas de la supervisión de aspectos relacionados con la ciberseguridad y seguridad de la información.

- El concepto de “seguridad” sólo hace referencia a la salvaguarda de personal, condiciones de sitios operativos y de alojamiento de equipamiento eléctrico, ante incidencias de tipo físico, incendios, desastres naturales, robo o vandalismo.

- En los programas de verificación, no especifica los sujetos regulados y no regulados, objeto de revisión.

- No realiza una segunda inspección física para validar la atención de las observaciones que derivan de las visitas de verificación e inspección, éstas se atienden solo por la vía documental.

- En la "Guía para la ejecución de los procedimientos de visitas de verificación de la Comisión Reguladora de Energía", no se incluyen formatos y pruebas básicas para la validación de cumplimientos a requisitos de TIC.

Adopción de la normativa NERC CIP en México

El 8 de mayo de 2017, el CENACE, la Comisión Reguladora de Energía y representantes del NERC firmaron el Memorando de Entendimiento (MOU, por sus siglas en inglés), en aras de establecer una relación continua y de cooperación para mejorar la Confiabilidad en los sistemas eléctricos en México y en los Estados Unidos de América.

Se identificó que la CRE en la gestión de este proyecto a la fecha de la auditoría (noviembre 2021):

- De 2017 a la fecha de la auditoría (noviembre 2021) no presentó avances en el análisis de la posible adopción de los estándares publicados por el NERC, no ha dado seguimiento a las actividades realizadas por los integrantes del MOU, no celebró reuniones de verificación con el grupo anual de trabajo, no realizó estudios técnicos y actividades de capacitación y programas de educación continua, no generó reportes técnicos de avances y no ha emitido opinión en su carácter de integrante y miembro del grupo de dirección del MOU ante la falta de continuidad del proyecto.

- No ha verificado con el CENACE que se hayan documentado y justificado las razones para no continuar el proyecto de integración de los controles del NERC al Código de Red.

- Como parte de las actividades realizadas por el MOU, participó como observador en los ejercicios de capacitación y simulación llevados a cabo por GridEx - NERC – CENACE.

Supervisión de proyectos estratégicos del Sector de Energía por parte de la CRE

Proyecto de Red Eléctrica Inteligente (REI)

De conformidad con el artículo 37 de la Ley de Transición Energética (LTE), la implementación de las REI tiene como objetivo apoyar la modernización de la Red Nacional de Transmisión (RNT) y de las Redes Generales de Distribución (RGD), para mantener una infraestructura confiable y segura que satisfaga la demanda eléctrica de manera económicamente eficiente y sustentable, y que facilite la incorporación de nuevas tecnologías que promuevan la reducción de costos del Sector Eléctrico.

La LTE indica además que el Programa de REI deberá identificar, evaluar, diseñar, establecer e instrumentar estrategias, acciones y proyectos en materia de redes eléctricas, entre las cuales se podrán considerar las siguientes:

- El despliegue de tecnologías inteligentes para la medición y comunicación en las REI.

- La integración de equipos y aparatos inteligentes a la Red Nacional de Transmisión y a las Redes Generales de Distribución.

- El desarrollo de estándares de comunicación e interoperabilidad de los aparatos y equipos conectados a la Red Nacional de Transmisión y a las Redes Generales de Distribución, incluyendo la infraestructura que le da servicio a dichas Redes.

- El desarrollo e integración de tecnologías avanzadas para el almacenamiento de electricidad y de tecnologías para satisfacer la demanda en horas pico.

- El proyecto de REI prevé la integración de TIC's en los elementos de medición, monitoreo y operación del SEN, a través de los sistemas y módulos que lo integran.

Se revisaron las actividades de la Dirección General Adjunta de Análisis de Redes Eléctricas de la CRE responsable del seguimiento de este proyecto y se identificó lo siguiente:

- No ha realizado reuniones de seguimiento y no ha dado retroalimentación a los informes de avance proporcionados por la EPS CFE Transmisión.

- No ha emitido directivas o normas para la administración de las Redes Eléctricas Inteligentes considerando aspectos relacionados con la ciberseguridad.

- No especificó de qué manera se lleva a cabo el monitoreo de los indicadores de disponibilidad de servicios de telemetría establecidos en el 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.

- Indicó que el plan de implementación del proyecto de Redes Eléctricas Inteligentes no ha sufrido modificaciones y que la fecha de conclusión factible es a finales de 2023, no obstante, la fecha de término establecida en el Manual de Requerimientos de TIC para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista es noviembre 2022, por lo que se observa que la CRE no ha verificado los plazos de término para este proyecto (resultado 4 de la auditoría 466-DE de título Auditoría de Ciberseguridad del Sector Energía de la CP 2020 realizada a la CFE).

Proyecto estratégico número PE-A-20 denominado "Soluciones de Ciberseguridad para la protección de activos e infraestructura de la Red Eléctrica Inteligente"

La EPS CFE Transmisión realizó la contratación con el Instituto Nacional de Electricidad y Energías Limpias (INEEL) y el Consejo Nacional de Ciencia y Tecnología (CONACYT), para realizar el proyecto de "Soluciones de Ciberseguridad para la protección de activos e infraestructura de la Red Eléctrica Inteligente", cuyo objetivo es 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. En la justificación de dicha contratación se menciona que se derivó de la carencia de actualizaciones en materia de ciberseguridad en el Código de Red por parte de la CRE y de la normativa interna de ciberseguridad en materia de TO; no obstante, la Unidad de Electricidad de la CRE indicó que no tiene conocimiento de dicho proyecto, sin embargo, en el resultado número 4 de la auditoría con número 466-DE y título "Auditoría de Ciberseguridad del Sector Energía" de la fiscalización de la Cuenta Pública 2020, que se llevó a cabo a la CFE, se observó que dicho proyecto no considera toda la infraestructura de las Tecnologías de Operación (TO) con las que opera esta subsidiaria y en plan de trabajo proporcionado se identificó a la CRE como parte del grupo que recibiría capacitación en materia de ciberseguridad. Se observa que la CRE no ha dado seguimiento a este proyecto ni

ha ejercido la facultad para expedir las normas, directivas y demás disposiciones de carácter administrativo en materia de Redes Eléctricas Inteligentes y Generación Distribuidas.

Conclusiones

La CRE a la fecha de la auditoría (noviembre 2021):

- No ha establecido mecanismos de revisión y no ha verificado el cumplimiento de los participantes respecto al Anexo 4 del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, ni de los criterios REI 15 al REI 21 del Código de Red por lo que se corre el riesgo de tener brechas de seguridad que afecten la confiabilidad del SEN.

- No ha emitido documentos técnicos o catálogos de estándares aprobados en materia de interoperabilidad para los elementos y sistemas de medición y de disposiciones generales sobre los procesos de administración de Seguridad de la Información.

- No ha definido los criterios de separación de Tecnología de Operación y Tecnología de Información lo que ha provocado que existan brechas en el alcance de la infraestructura y de los sistemas que soportan al SEN, respecto a su administración, gestión y supervisión.

- No ha dado seguimiento mediante el MOU a la adopción de normas y buenas prácticas establecidas en los NERC-CIP o cualquier otro estándar de ciberseguridad, con la finalidad de homologar la confiabilidad del control operativo del Sistema Eléctrico y estandarizarlo.

- No ha promovido que el CENACE robustezca y actualice los requisitos y criterios relacionados con la Seguridad de la información y la ciberseguridad.

2020-0-45100-20-0112-01-009 **Recomendación**

Para que la Comisión Reguladora de Energía se pronuncie y promueva la evaluación, adopción y priorización de mejores prácticas relacionadas con la seguridad de la información y ciberseguridad en el marco mexicano regulatorio del sector energía (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 y Código de Red), con el fin de que cuente con controles de ciberseguridad especializados para la gestión de sistemas de control industrial y activos críticos que dan soporte a la infraestructura del SEN y el MEM, asimismo, emita catálogos de estándares formalizados en materia de interoperabilidad para los sistemas de control industrial y aquellos relacionados con la administración de seguridad de la información y ciberseguridad.

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.

2020-0-45100-20-0112-01-010 **Recomendación**

Para que la Comisión Reguladora de Energía establezca y formalice los mecanismos de supervisión y vigilancia por parte de los integrantes del SEN respecto al cumplimiento del Anexo 4 en materia de ciberseguridad del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, así como al Capítulo 5. Disposiciones Generales de Red Eléctrica Inteligente en materia de Telemetría, Interoperabilidad y Seguridad de la Información para la operación del SEN y el Código de Red; defina indicadores de cumplimiento a requisitos de Ciberseguridad, Tecnologías de Información y Tecnología de Operación e incluya su evaluación dentro del Plan Anual de visitas y desarrolle guías y procedimientos para la ejecución de actividades de supervisión de la normativa mexicana del sector, a fin de que las revisiones realizadas por la CRE sean integrales y representativas; defina un responsable de supervisar y verificar la implementación de la confiabilidad, calidad, seguridad y disponibilidad en materia de ciberseguridad en el Sistema Eléctrico Nacional; formalice y defina los alcances de los conceptos de Tecnología de Información y Tecnología de Operación en la normativa del sector y asegurar que los participantes del SEN sean evaluados y cumplan con los mecanismos mínimos que garanticen la operación confiable de la infraestructura de Tecnología de Información y Tecnología Operación que dan soporte al SEN.

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.

2020-9-45100-20-0112-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en la Comisión Reguladora de Energía 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, en su figura de supervisores de los criterios de eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad del Sistema Eléctrico Nacional (SEN) y el Mercado Eléctrico Mayorista (MEM), no evaluaron durante las visitas de inspección los criterios REI 15 al REI 21 del Código de Red y los requisitos del anexo 4 del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el SEN y MEM en materia de ciberseguridad y seguridad de la información; no han desarrollado nuevos controles de ciberseguridad ni han fortalecido los existentes ante las constantes amenazas que ha presentado el sector energético a nivel mundial; no han emitido observaciones al Centro Nacional de Control de Energía respecto al incumplimiento

de sus obligaciones establecidas en la Ley de la Industria Eléctrica ante la desactualización de los controles en materia de ciberseguridad y seguridad de la información; no han promovido acciones para definir un proceso de gestión a incidentes de ciberseguridad en el SEN; no han dado seguimiento a las actividades comprometidas con el grupo de trabajo celebrado con el North American Electric Reliability Corporation (NERC) para la adopción de sus controles de ciberseguridad y no han realizado actividades de supervisión a la implementación del proyecto de Red Eléctrica Inteligente desarrollado por la Empresa Productiva Subsidiaria CFE Transmisión así como la adopción de controles de ciberseguridad en dicho proyecto; en incumplimiento de lo establecido en los artículos 1 y 3 del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, así como establecer el Manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014 con última reforma publicada el 23 de julio de 2018; en el artículo 22, fracciones II, X, XI y XIII, de la Ley de los Órganos Reguladores Coordinados en Materia Energética publicado en el Diario Oficial de la Federación el 11 de agosto de 2014; en los artículos 6 y 12, fracciones III, XI, XXXVII, XXXVIII y XLIX, de la Ley de la Industria Eléctrica publicada en el Diario Oficial de la Federación el 11 de agosto de 2014; en los artículos 18, fracción IV, XX y XLIV, y 36, fracciones XII y XIII, del Reglamento Interno de la Comisión Reguladora de Energía (RICRE) publicado en el Diario Oficial de la Federación el 28 de abril de 2017; en los artículos 106, 107, 109, 110 y 118, del Reglamento de la Ley de la Industria Eléctrica publicado en el Diario Oficial de la Federación el 31 de octubre de 2014; en el numerales 4.2.3, Anexo I, y 4 de los Requisitos de Ciberseguridad para la Infraestructura de TIC del 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 14 de diciembre de 2017; en el Inciso b), criterio REI 23, capítulo 5 de la Resolución por la que la CRE expide las Disposiciones Administrativas de carácter general que contienen los criterios de eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad del Sistema Eléctrico Nacional: Código de Red; en el artículo 1° del Acuerdo por el que la Comisión Reguladora de Energía expide los criterios y la metodología para determinar las visitas de verificación o inspección que deberán llevarse a cabo, publicado en el Diario Oficial de la Federación el 11 de noviembre de 2016, y en los Numerales X, objetivo, funciones 1 y 5, X.2, objetivo, funciones 1 y 3, X.2.1, objetivo, funciones 1, X.5, objetivo, funciones 1, 2 y 5, X.5.1, objetivo, funciones 1, 4 y 8, y el numeral X.2.5, objetivo y funciones 1, 2 y 4, del Manual de Organización General de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación el 24 de noviembre de 2017.

5. Supervisión de la Ciberseguridad en el Sistema Eléctrico Nacional por parte de la SENER

A la Secretaría de Energía (SENER) le corresponde, entre otras atribuciones, la de “Regular y, en su caso, expedir normas oficiales mexicanas sobre producción, comercialización, compraventa, condiciones de calidad, suministro de energía y demás aspectos que promuevan la modernización, eficiencia y desarrollo del sector, así como controlar y vigilar su debido cumplimiento” (artículo 33 de la Ley Orgánica de la Administración Pública

Federal publicada en el Diario Oficial de la Federación el 29 de diciembre de 1976 y su reforma publicada en el mismo medio el 9 de agosto de 2019).

En el artículo 6 de la Ley de la Industria Eléctrica, se indica que el Estado establecerá y ejecutará la política, regulación y vigilancia de la industria eléctrica a través de la Secretaría y la CRE, en el ámbito de sus respectivas competencias, teniendo como objetivos, entre otros, los siguientes:

I. Garantizar la eficiencia, calidad, confiabilidad, continuidad y seguridad del Sistema Eléctrico Nacional.

II. Promover que las actividades de la industria eléctrica se realicen bajo criterios de sustentabilidad.

En el artículo 11 de la misma ley, se indica que la Secretaría está facultada, entre otras, para:

I. Establecer, conducir y coordinar la política energética del país en materia de energía eléctrica.

V. Asegurar la coordinación con los órganos reguladores en materia de la industria eléctrica, las demás autoridades relevantes para la industria eléctrica, el CENACE y el Centro Nacional de Control del Gas Natural.

XIII. Preparar y coordinar la ejecución de los proyectos estratégicos de infraestructura necesarios para cumplir con la política energética nacional.

XXXVI. Regular, supervisar y ejecutar el proceso de estandarización y normalización en materia de la seguridad de las instalaciones de los Usuarios Finales.

En el Reglamento Interior de la Secretaria de Energía publicado el 31 de octubre de 2014 en el Diario Oficial de la Federación, y el Manual de Organización Específico de la Unidad del Sistema Eléctrico Nacional y Política Nuclear del 4 de julio de 2016, se establece que las funciones de dicha unidad, entre otras, son las siguientes:

II. Verificar la operación eficiente del Sistema Eléctrico Nacional.

IV. Realizar los actos necesarios para garantizar la eficiencia, calidad, confiabilidad, continuidad y seguridad del Sistema Eléctrico Nacional.

XVII. Dirigir la política, regulación y vigilancia de la industria eléctrica en el ámbito de competencia de la Secretaría.

XXXIV. Coordinar la realización de visitas de verificación, supervisión, inspección o revisión del Sistema Eléctrico Nacional.

XXXVII. Vigilar el cumplimiento de la Ley de la Industria Eléctrica, su Reglamento y demás disposiciones jurídicas aplicables a las atribuciones de la Subsecretaría de Electricidad.

Las funciones para la Dirección General de Seguimiento y Coordinación de la Industria Eléctrica, entre otras, son las siguientes:

VI. Coordinar y dar seguimiento a los actos, estudios e investigaciones sobre la eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad del Sistema Eléctrico Nacional.

VII. Participar en el seguimiento de las Reglas del Mercado Eléctrico y asegurar su congruencia con las políticas y las demás disposiciones que regulan la industria eléctrica.

VIII. Participar en el seguimiento de la operación del Mercado Eléctrico Mayorista y asegurar su congruencia con las políticas y las demás disposiciones que regulan la industria eléctrica.

La normativa mexicana que establece controles de gestión de la seguridad de TIC, para la industria eléctrica mexicana son las siguientes:

- Ley de la Industria Eléctrica Publicada en el Diario Oficial de la Federación el 11 de agosto de 2014.

- Código de Red con acuerdos publicados en el Diario Oficial de la Federación el 08 de abril de 2016.

- 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.

En el análisis de estas normativas se observó lo siguiente:

- La Unidad del Sistema Eléctrico Nacional y Política Nuclear, adscrita a la Subsecretaria de Electricidad, participó en la revisión del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, elaborado por el CENACE con al apoyo de consultores; sin embargo, el Manual no tiene referencias a mejores prácticas en materia de ciberseguridad.

- La SENER no cuenta con evidencia del análisis bajo el cual se determinó que los requisitos plasmados en el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado

Eléctrico Mayorista eran los necesarios y suficientes para mantener un nivel adecuado de seguridad de la información y ciberseguridad del SEN.

- La Ley de la Industria Eléctrica y el Reglamento Interior de la SENER no establecen las áreas responsables para la vigilancia, seguimiento y aplicación de modificaciones a la normativa en materia de TIC y ciberseguridad respecto a la operación del SEN y MEM.

- La SENER no se ha pronunciado respecto a la falta de definición de los conceptos de Tecnología de Información (TI) y Tecnología de Operación (TO).

Supervisión y seguimiento del SEN

Respecto a la vigilancia que ha realizado la Subsecretaria de Electricidad de la SENER en la materia, se identificó lo siguiente:

- Llevó a cabo visitas en 2018 a la Gerencia de Control y al Centro Nacional Alterno del CENACE con el objetivo de conocer los mecanismos que se ejecutan para el control operativo del SEN y de la importancia del sistema SCADA. Sin embargo, sólo fueron visitas de conocimiento no de verificación, por lo que no se generaron recomendaciones u observaciones; además, no demostró haber efectuado una actividad similar en la CFE y sus EPS.

- Realizó el Informe pormenorizado sobre el desempeño y las tendencias de la Industria Eléctrica Nacional, que incluye un apartado sobre el Mercado Eléctrico Mayorista; no obstante, sólo es de carácter operativo, no menciona aspectos relacionados con la Seguridad de la información y la ciberseguridad.

- Ha emitido políticas de confiabilidad, seguridad y sustentabilidad para el SEN, en los años de 2017 y 2020, sin embargo, su alcance es respecto a las operaciones de generación, distribución y transmisión de electricidad y en ellas no se consideran aspectos relacionados con la seguridad de la información y la ciberseguridad.

- El Programa de Desarrollo del Sistema Eléctrico Nacional (PRODESEN) no considera rubros de TIC, seguridad de la información y ciberseguridad.

- No ha realizado actividades de vigilancia de la industria eléctrica sobre temas relacionados con seguridad informática y ciberseguridad.

- La SENER no ha realizado el seguimiento al cumplimiento de las obligaciones de la CRE y el CENACE respecto a la actualización de normativa en materia de seguridad de la información y ciberseguridad.

Por lo anterior, se observó una falta de seguimiento y de verificación de aspectos relacionados con las TIC incluidas la seguridad de la información y ciberseguridad, que podrían derivar en brechas de seguridad en el SEN y MEM.

Supervisión de integrantes del SEN por parte de la SENER

En la supervisión que la SENER ha realizado a la fecha de la auditoría (noviembre 2021) se observó lo siguiente:

- Las últimas visitas a sitios operativos de CENACE fueron en junio y agosto de 2018.

- Las opiniones vertidas por SENER en el Comité de evaluación que revisa el desempeño del Centro Nacional de Control de Energía y del Mercado Eléctrico no incluyeron aspectos relacionados con la infraestructura de TIC y su gestión en materia de ciberseguridad.

- Los reportes de seguimiento para la Infraestructura a largo plazo a cargo de la EPS CFE Transmisión no consideran el seguimiento de proyectos en materia de TIC incluidos los relacionados a infraestructura de TI, TO y ciberseguridad.

Reporte de confiabilidad

La SENER no ha emitido observaciones a la CRE respecto a los atrasos en la emisión del reporte de confiabilidad correspondientes a los años de 2018, 2019 y 2020, ni que en estos reportes a la fecha de la auditoría (noviembre 2021) no se incluyen evaluaciones de la infraestructura de TIC que soporte al SEN.

Supervisión de proyectos estratégicos del Sector Energía

Proyecto de Redes Eléctricas Inteligentes.

En el seguimiento que realizó la Subsecretaría de Electricidad de la SENER a las actividades ejecutadas por la EPS CFE Transmisión y la CFE a este proyecto se identificaron las consideraciones siguientes:

- Sólo en el programa de 2017 incluyó actividades de seguimiento a la seguridad de la información, en los programas subsecuentes no se consideró, incluido el programa de 2021.

- La SENER, por medio de los reportes anuales y el Informe Pormenorizado de Avances en las Obras de Ampliación de la Red Nacional de Transmisión, proporcionados por la EPS CFE Transmisión, da seguimiento a los proyectos efectuados por dicha subsidiaria; sin embargo, se identificó que, para el caso del proyecto REI, sólo existe una mención al plan de trabajo original propuesto, sin detalles específicos de su avance.

- La SENER no ha dado seguimiento y retroalimentación a los informes pormenorizados entregados por la EPS CFE Transmisión en relación con el proyecto REI (Resultado número 4 de la auditoría número 466-DE con título: Auditoría de Ciberseguridad del Sector Energía, de la fiscalización de la CP 2020).

- De 2016 a 2018, por medio del Comité Consultivo de Redes Eléctricas Inteligentes, se ha evaluado el desarrollo del proyecto REI, y en las minutas asociadas a estas reuniones se observa que no se consideraron revisiones en materia de seguridad de la información y de ciberseguridad, y para los años 2019 y 2020 no se ha dado seguimiento.

Modernización de los Sistemas SCADA/EMS del CENACE

Como parte del Resultado número 3 de la Auditoría número 397-DE con título Auditoría de Ciberseguridad del Sector de Energía de la fiscalización de la Cuenta Pública 2020), este ente fiscalizador identificó la contratación para implementar el proyecto Modernización de los Sistemas SCADA/EMS del CENACE (vigencia de 2017- 2022), conviene destacar que este proyecto es relevante para el CENACE dado que con esta contratación se actualizará la infraestructura con la cual se realiza el control supervisor del Sistema Eléctrico Nacional .

Se observó que la implementación de dicho contrato presenta retrasos que podrían incidir en la implementación en tiempo y forma conforme los requerimientos del CENACE.

La SENER no ha dado seguimiento ante posibles desviaciones a los proyectos que está ejecutando el CENACE relacionados a esta infraestructura.

Se identificó que en la SENER no se ha dado seguimiento a la actualización del Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, en función del fortalecimiento de los controles de seguridad de la información y ciberseguridad. Tampoco se ha dado seguimiento a los proyectos asociados al Programa de Redes Eléctricas Inteligentes.

2020-0-18100-20-0112-01-001 **Recomendación**

Para que la Secretaría de Energía realice actividades de seguimiento y retroalimentación al informe pormenorizado enviado por la Empresa Productiva Subsidiaria (EPS) CFE Transmisión, respecto a los avances del proyecto Redes Eléctricas Inteligentes, a fin de identificar retrasos en el proyecto y asegurar el cumplimento con la fecha de término estipulado por la SENER.

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.

2020-0-18100-20-0112-01-002 **Recomendación**

Para que la Secretaría de Energía coordine con la Comisión Reguladora de Energía la verificación del desempeño del Sistema Eléctrico Nacional en materia de seguridad de la información y de ciberseguridad; evalúe el estado de la ciberseguridad del Centro Nacional de Control de Energía (CENACE) con base en el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista y verifique que éste adopte mejores prácticas en materia de ciberseguridad.

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 2,048,692.82 pesos pendientes por aclarar.

Buen Gobierno

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

Resumen de Resultados, Observaciones y Acciones

Se determinaron 5 resultados, de los cuales, 5 generaron:

12 Recomendaciones, 1 Promoción de Responsabilidad Administrativa Sancionatoria y 2 Pliegos de Observaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 31 de enero de 2022, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar 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 Reguladora de Energía cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

El Manual Organizacional General de la CRE no contiene la estructura y las funciones de las diferentes áreas que conforman a la Dirección General de Tecnologías de la Información (DGTI) que a su vez no cuenta con un manual especifico ni políticas establecidas que normen sus funciones.

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

- En el contrato número CRE/21/2019, celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C., no se cumplió con la fundamentación por la cual se otorgó la excepción a la Licitación Pública, dado que los servicios de desarrollo y mantenimiento de los sistemas de información que se solicitaron no requerían de alguna especialización técnica.

- En el proceso de contratación, no se especificó si existían circunstancias que pudieran provocar pérdidas o costos adicionales en el supuesto de no contar con los servicios.

- Se comprobó que 5 servicios de desarrollo de software no fueron utilizados por la CRE, toda vez que fueron entregados por el proveedor en ambiente de calidad (marzo 2020); dichos desarrollos generaron pagos por 298.2 miles de pesos sin que hayan tenido utilidad ni beneficio para la CRE.

- En el contrato número CRE/55/2018, celebrado con Reto Industrial, S.A. de C.V., se identificaron deficiencias en la planeación de las pruebas de seguridad para detectar el nivel de vulnerabilidad de los sistemas institucionales frente a ataques externos; no se realizó la ejecución de un segundo análisis donde se debió validar el éxito o fracaso de las acciones de mitigación. No obstante, se realizaron pagos por la ejecución de dichas pruebas por 1,750.5 miles de pesos.

- Respecto de la gestión del marco regulatorio en materia eléctrica y su actualización, en específico para aspectos relacionados con Seguridad de la Información y Ciberseguridad, la CRE no ha dado seguimiento para que la normativa mexicana que regula la industria eléctrica cuente con criterios y requisitos relacionados con la seguridad de la información y ciberseguridad, y que éstos estén orientados a cumplir con alguna mejor práctica en la industria; en las visitas a los participantes, no mide el cumplimiento en relación con estos temas, ni ha definido indicadores que le permitan evaluar su confiabilidad. Existen proyectos que se encuentran en ejecución por parte del CENACE y la EPS CFE Transmisión a los cuales no les ha dado el seguimiento oportuno por lo que existe el riesgo que no se concluyan en las fechas establecidas por la SENER y con ello provoquen retraso en la implementación del proyecto Red Eléctrica Inteligente, el cual tiene por objetivo desarrollar un mercado eléctrico competitivo en México.

La SENER no ha vigilado ni dado seguimiento a la actualización de los requisitos de seguridad de la información y ciberseguridad contemplados en el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista, ni a las posibles desviaciones al proyecto que está ejecutando el CENACE con la implementación de su nuevo sistema SCADA.

La CRE no ha definido al responsable de supervisar y verificar el cumplimiento de los criterios y requisitos en materia de seguridad de la información y ciberseguridad del Sistema Eléctrico Nacional.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
C. 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 las cifras reportadas en la Cuenta Pública en materia de TIC corresponden con las registradas en el estado del ejercicio del presupuesto; analizar la integración del gasto ejercido en materia de TIC de conformidad con las disposiciones y normativas aplicables.

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, relacionados con la distribución de energía eléctrica, 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.

Áreas Revisadas

La Dirección General de Tecnologías de la Información; la Dirección General Adjunta de Finanzas; la Dirección de Seguridad e Infraestructura; la Dirección de Recursos Material y Bienes Muebles; la Dirección de Adquisiciones; la Coordinación de Finanzas; la Dirección de Fideicomiso e Ingresos por Derechos, Productos y Aprovechamientos; la Unidad de Electricidad y la Unidad de Administración de la Comisión Reguladora de Energía; así como la Unidad del Sistema Eléctrico Nacional y Política Nuclear adscrita a la Subsecretaría de Electricidad de la Secretaría de Energía.

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: Artículo 19 de la Ley Orgánica de la Administración Pública Federal publicada en el Diario Oficial de la Federación el 21 de diciembre de 1976 y sus reformas el 9 de agosto de 2019; artículos 41, fracciones III y XVII, y 45, fracción VI de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público con última reforma publicada en el Diario Oficial de la Federación el 10 de noviembre de 2014; artículo 39, inciso i), punto 4 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público publicado en el Diario Oficial de la Federación el 20 de agosto del 2001 y su última reforma en el mismo medio el 30 de noviembre de 2006; artículo 1 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, publicada en el Diario Oficial de la Federación el 30 de marzo de 2006 y su última reforma publicada en el mismo medio el 19 de noviembre de 2019; artículos 6, 11, fracciones V, VI, XIII, XL, 12, fracciones II, III, XI, XXXVII, XLVII y XLIX, y 157 de la Ley de la Industria Eléctrica publicada en el Diario Oficial de la Federación el 11 de agosto de 2014 con última reforma publicada en el mismo medio el 09 de marzo de 2021; artículos 106, 107, 109, 110 y 118 del Reglamento de la Ley de la Industria Eléctrica publicado en el Diario Oficial de la Federación el 31 de octubre de 2014; artículo 22, fracciones II, X, XI y XIII de la Ley de los Órganos Reguladores Coordinados en Materia Energética publicado en el Diario Oficial de la Federación el 11 de agosto de 2014; artículos 1 y 3 del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, así como establecer el Manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014 con última reforma publicada el 23 de julio de 2018; objetivo específico 2 y 5, apartado III.B Proceso de administración de proveedores (APRO), objetivo general, objetivos específicos 1 y 2, actividad del proceso APRO 1 General lista de verificación de obligaciones, factores críticos 1

y 2, actividad del proceso APRO 2 Monitorear el avance y desempeño del proveedor, factores críticos 1 y 3; actividad del proceso APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos, factores críticos 1, 2 y 3 del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, publicado en el Diario Oficial de la Federación el 08 de mayo de 2014, con última reforma publicada en el mismo medio el 23 de julio de 2018; artículos 10, fracciones II, III, IV, XIV, XVIII y XXXXVII, 18 fracción IV, 20, 36, fracción XII y XIII, y 44 del Reglamento Interior de la Secretaria de Energía publicado en el Diario Oficial de la Federación el 31 de diciembre de 2014; artículo 18, fracciones IV, XX y XLIV, 30, fracción IX, y 34, fracciones XII, del Reglamento Interno de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación el 28 de abril de 2017; anexo 4, Requisitos de Ciberseguridad para la Infraestructura de TIC del 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 14 de diciembre de 2017; criterio REI-21, incisos a, b y c, criterio REI-23 del capítulo 5 de la Resolución por la que la Comisión Reguladora de Energía expide las Disposiciones administrativas de carácter general que contienen los criterios de eficiencia, calidad, confiabilidad, continuidad, seguridad y sustentabilidad del Sistema Eléctrico Nacional: Código de Red; objetivo 2 Expandir y modernizar la Infraestructura de Transmisión e incrementar la Generación Distribuida y Almacenamiento, línea de acción 2.4.1 del Acuerdo por el que la Secretaría de Energía emite el Programa Especial de la Transición Energética, publicado en el Diario Oficial de la Federación el 31 de mayo de 2017; numeral 4.1 del Programa de Redes Eléctricas Inteligentes de fecha 21 de agosto de 2017; numeral 1.2.6 de las Bases del Mercado Eléctrico Mayorista, publicadas en el Diario Oficial de la Federación el 5 de septiembre de 2015; numeral 2.3.1, inciso c, subinciso (iii) del Acuerdo por el que se emite el Manual de Vigilancia del Mercado, publicado en el Diario Oficial de la Federación el 12 de enero de 2018; artículo primero del Acuerdo por el que la Comisión Reguladora de Energía expide los criterios y la metodología para determinar las visitas de verificación o inspección que deberán llevarse a cabo, publicado en el Diario Oficial de la Federación el 11 de noviembre de 2016; numeral X, objetivo, funciones 1 y 5; X.2 objetivo, funciones 1 y 3; X.2.1, objetivo, funciones 1; numeral X.5, objetivo, funciones 1, 2, 5; X.2.5, objetivo y funciones 1, 2 y 4; X.5.1, objetivo, funciones 1, 4 y 8; numeral IV.4 Dirección General de Tecnologías de la Información, objetivo y funciones 2, 3, 4 y 5, Numeral IV.4.3, funciones 1, 3, 4 y 5, Dirección General Adjunta de Infraestructura y Operación de Tecnologías de Información del Manual de Organización General de la Comisión Reguladora de Energía publicado en el Diario Oficial de la Federación el 24 de noviembre de 2017; cláusulas Tercera (Lugar de prestación del servicio), Décima séptima (Representantes responsables de administrar y vigilar el cumplimiento del convenio) y Décima Octava (Supervisión y aceptación de los servicios), numerales 4 y 5 del anexo técnico del convenio número CRE/21/2019 celebrado con el Instituto Potosino de Investigación Científica y Tecnológica, A.C.; y cláusulas Primera (Objeto del contrato), Cuarta (Monto del contrato), Sexta (Responsabilidad de El Prestador), Novena (Modificaciones), Décima Cuarta (Pena convencional), Décima Octava (Representantes responsables de administrar y vigilar el

cumplimiento del contrato) y Décima Novena (Supervisión y aceptación de los servicios) del contrato número CRE/55/2018, numerales SSICRE-714 y SSICRE-715 del Anexo Técnico.

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.