Centro Nacional de Control de Energía

Auditoría de Ciberseguridad del Sector Energía

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2020-1-18TOM-20-0397-2021

397-DE

Criterios de Selección

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

Objetivo

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

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	499,304.7
Muestra Auditada	175,559.4
Representatividad de la Muestra	35.2%

El universo seleccionado por 499,304.7 miles de pesos corresponde al total ejercido en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2020; la muestra auditada está integrada por dos contratos relacionados con la prestación del Servicio Integral Soporte Técnico a la Plataforma de Aplicaciones del Mercado Eléctrico Mayorista y la Modernización de los Sistemas SCADA/EMS del Centro Nacional de Control de Energía (CENACE), con pagos ejercidos por 175,559.4 miles de pesos, que representan el 35.2% del universo seleccionado, contenidos en el Tomo III del RAMO 18-energía.

Antecedentes

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

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

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

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

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

Sistema Eléctrico Nacional

De conformidad con lo que establece la Ley de la Industria Eléctrica (LIE), el Estado ejerce el control operativo del Sistema Eléctrico Nacional (SEN) a través del CENACE. En este sentido, el CENACE tiene la facultad de determinar los actos necesarios para mantener la Seguridad

[1] Gusano informático que provoca una Denegación de servicio.

[2] Gusano informático que afecta a equipos con Windows, permite la ejecución de código malicioso alojado dentro de dispositivos USB sin la necesidad de utilizar un archivo autorun.

[3] Conjunto de dispositivos conectados a Internet (ordenadores personales, servidores, dispositivos móviles, dispositivos IoT, etc.) infectados y controlados por un malware.

[4] Cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario. Es un gusano informático que provoca una Denegación de servicio.

[5] Malware que es capaz de controlar directamente los conmutadores y los interruptores de las subestaciones eléctricas.

[6] Amenaza avanzada persistente (por sus siglas en inglés APT), utiliza técnicas de hackeo continuas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado y potencialmente destructivo.

de Despacho, Confiabilidad, Calidad y Continuidad del SEN que deban realizar los Participantes del Mercado, Transportistas y Distribuidores.

El SEN está integrado por:

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

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

Términos relacionados con la auditoría

Sistemas SCADA

El SCADA (Supervisory Control And Data Acquisition) es un sistema informático 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, ubicadas en diferentes instalaciones, que permite controlar y supervisar el sistema eléctrico, facilitando retroalimentación en tiempo real sobre mediciones y el estado de los equipos en campo, y permitiendo control sobre los mismos. Actualmente los sistemas SCADA son usados en la industria eléctrica en funciones como: Generación, Transmisión y Distribución.

Tecnología de Operación (TO)

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

Tecnología de Información (TI)

Todo equipo o sistema interconectado o subsistema de equipo que se utilice en la adquisición, almacenamiento, manipulación, gestión, movimiento, control, visualización, conmutación,

intercambio, transmisión o recepción automática de datos o información. El término tecnología de la información incluye computadoras, equipos auxiliares, software, firmware y procedimientos, servicios similares (incluidos los servicios de soporte) y recursos relacionados. [7]

Activos de TIC

De acuerdo con el CENACE, son los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.

Sistemas de Control Industrial (SCI)

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

La Tecnología de Operación (TO) incluye todos los dispositivos y Sistemas de Control Industrial (SCI) que permiten la automatización de procesos industriales de producción y de generación de servicios; por ejemplo, dispositivos para el control de válvulas, turbinas, motores para la apertura y cierre de compuertas, entre muchos otros. Los SCI 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 SCI 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 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.

CENACE

El CENACE es un organismo público descentralizado de la Administración Pública Federal, sectorizado a la Secretaría de Energía, con personalidad jurídica y patrimonio propios y tiene por objeto ejercer el Control Operativo del Sistema Eléctrico Nacional (SEN), realizar la operación del Mercado Eléctrico Mayorista (MEM) y garantiza el acceso abierto y no

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

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

indebidamente discriminatorio a la Red Nacional de Transmisión y a las Redes Generales de Distribución.

El CENACE monitorea en tiempo real la generación, la demanda y el consumo de energía eléctrica que se registran en el sistema eléctrico del país.

Desde 2017, el CENACE ha contado con varios proyectos estratégicos en materia de TIC, entre los que destacan: la Licitación "Sistema EMS/SCADA", el Desarrollo de aplicaciones para el MEM y Licitación de Infraestructura para asegurar continuidad del MEM; asimismo, en la Planeación Estratégica 2017-2021 los proyectos de TIC más importantes fueron la Administración del Mercado Eléctrico Mayorista, el Control Operativo del Sistema Eléctrico Nacional, la Planeación de la expansión de la Red Nacional de Transmisión y las Redes Generales de Distribución y Acceso Abierto, así como el Desarrollo de capital humano del CENACE.

Resultados obtenidos en la auditoría 450-DE, con título "Auditoría de TIC"

La Auditoría Superior de la Federación (ASF) en la Cuenta Pública de 2017 efectuó la auditoría número 450-DE, con título "Auditoría de TIC", en la cual se emitieron 13 Recomendaciones, 3 Promociones de Responsabilidad Administrativa Sancionatoria y un Pliego de Observaciones, destacando las recomendaciones siguientes:

- Para que el CENACE desarrolle e implemente políticas y procedimientos donde se establezcan los controles para medir, validar, evaluar y monitorear el cumplimiento de los compromisos contractuales de los prestadores de servicios de tecnologías de información y comunicaciones, para contar con la trazabilidad y el detalle preciso de las actividades efectuadas, soporte realizado, horas devengadas y evidencia de la aceptación del trabajo por parte de las áreas usuarias.

- Para que el CENACE estipule en los contratos o convenios que se celebren en materia de TIC, aun en aquellos realizados entre entidades de la administración pública, los apartados de penalizaciones, deductivas, fianzas y garantías para los casos de incumplimiento de los servicios; asimismo, establezca un mecanismo de control con los proveedores para asegurar el cumplimiento de los niveles de servicio, los compromisos contractuales y el óptimo funcionamiento de las operaciones.

- Para que el CENACE establezca en los Convenios Modificatorios, aun en aquellos celebrados entre entidades de la administración pública, las condiciones siguientes: precisión de precio fijo o la fórmula o condición en aquellos que sean variables; casos para otorgar prórrogas para el cumplimiento de las obligaciones contractuales; supuestos y restricciones de la entidad para contar con la prestación de los servicios; procedimientos para resolución de controversias y las responsabilidades de los proveedores ante defectos, vicios ocultos y calidad de los servicios, con la finalidad de optimizar la gestión de los proveedores y mejorar la calidad de servicio a los usuarios.

A dichas acciones se les dio seguimiento como se muestran en los resultados 2 y 3 del presente informe.

Entre 2016 y 2020, el CENACE erogó 2,411,367.7 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

Tabla 1. Recursos erogados en materia de TIC – CENACE

(Miles de pesos)

PERIODO DE EROGACIÓN	2016	2017	2018	2019	2020	TOTALES
MONTO POR AÑO	7,293.5	475,798.8	618,068.2	787,686.4	522,520.8	2,411,367.7

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

Con base en el análisis de la gestión de las TIC efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados, con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones y función de las TIC sujetas de revisión, 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 de 2020, publicado en el Diario Oficial de la Federación el 11 de diciembre de 2019, al CENACE se le aprobó un presupuesto por 4,318,410.1 miles de pesos. De lo reportado en la Cuenta de la Hacienda Pública Federal en el ejercicio de 2020, el CENACE tuvo un presupuesto pagado por 3,211,721.1 que representó el 88.9% respecto del presupuesto modificado.

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC) por 499,304.7 miles de pesos, se integran de la manera siguiente:

Tabla 2. Gastos de TIC en 2020

(Miles de pesos)

Capítulo /P. Presupuestaria	Descripción	Presupuesto ejercido	%
3000	**SERVICIOS GENERALES**		
31701	Servicios de Conducción de Señales Analógicas y Digitales	59,681.9	12.0
31904	Servicios Integrales de Infraestructura de Cómputo	19,614.2	3.9
32301	Arrendamiento de Equipo y Bienes Informáticos	92,561.4	18.5
33301	Servicios de desarrollo de aplicaciones informáticas	107,734.4	21.6
33303	Servicios relacionados con certificación de procesos	288.8	0.1
33304	Servicios de mantenimiento de aplicaciones informáticas	70,635.2	14.1
35301	Mantenimiento y Conservación de Bienes Informáticos	148,788.8	29.8
	TOTAL	**499,304.7**	**100**

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

Se observó que el presupuesto de TIC se destina principalmente a las partidas 32301 “Arrendamiento de Equipo y Bienes Informáticos” (92,561.4 miles de pesos), 33301 “Servicios de desarrollo de aplicaciones informáticas” (107,734.4 miles de pesos) y 35301 “Mantenimiento y conservación de bienes informáticos” (148,788.8 miles de pesos), ya que en ellas se concentra el 59.3% del presupuesto.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC, con una percepción anual de 32,430.8 miles de pesos durante el ejercicio fiscal 2020; considerando 37 plazas, el promedio anual percibido por persona fue de 876.5 miles de pesos.

Del total ejercido en 2020 en materia de TIC por 499,304.7 miles de pesos, se seleccionó una muestra de dos contratos por los que se realizaron pagos de 175,559.4 miles de pesos que representan el 35.2% del total ejercido, los cuales se integran de la manera siguiente:

Tabla 3. Muestra de Contratos Ejercidos en 2020

(Miles de pesos)

Procedimiento de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Pagado 2020
				Del	Al	Mínimo	Máximo	
Artículo 1 quinto párrafo (LAASSP)	Convenio Específico Número 3 que se desprende del Convenio Principal CENACE/22/I/16	Instituto Nacional de Electricidad y Energías Limpias (INEEL)	Desarrollar el proyecto denominado "Servicio Integral Soporte Técnico a la Plataforma de Aplicaciones del Mercado Eléctrico Mayorista" bajo las especificaciones técnicas y entregables establecidos para tal fin en su respectivo Anexo Técnico y a través de la correspondiente "Orden de Trabajo".	01/12/2017	31/12/2020	176,808.0	347,142.3	63,309.9
Licitación Pública (LAASSP)	CENACE-LP-094-B-017-2017 1er Convenio Modificatorio	Siemens de México, S.A. de C.V.	Servicio Administrado de Ambientes de Prueba y Calidad para Aplicativos Institucionales.	14/12/2017	22/08/2024	33,884.5	1,041,955.7	113,249.5
					Total	**210,692.5**	**1,389,098.0**	**175,559.4**

FUENTE**:** Elaborado por la ASF con base en la información proporcionada por el CENACE.

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

2. Tercer Convenio Específico CENACE/I/SE/18773

Se revisó el Tercer Convenio Específico CENACE/I/SE/18773 celebrado con el Instituto Nacional de Electricidad y Energías Limpias (INEEL), con fundamento en la cláusula primera del contrato marco CENACE/I/SE/18773 y número de referencia CENACE: 22/1/16, con el objeto de prestar el " Servicio integral soporte técnico a la plataforma de aplicaciones del Mercado Eléctrico Mayorista", vigente del 1 de diciembre de 2017 al 31 de diciembre de 2020 por un monto máximo de 347,142.3 miles de pesos y mínimo de 176,808.1 miles de pesos y pagos realizados en 2020 por 62,309.9 miles de pesos, se determinó lo siguiente:

Antecedentes

El 22 de enero de 2016, el ahora INEEL y el Centro Nacional de Control de Energía (CENACE), suscribieron el Contrato Marco de Prestación de Servicios CENACE/I/SE/18773, en términos del artículo 1° de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y del artículo 4° del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP), con objeto de "Establecer los términos y condiciones generales en la prestación de los servicios tecnológicos que el CENACE encomiende al INEEL, sujeto a las condiciones particulares que en cada caso acuerden las partes en las órdenes de trabajo que para tal efecto se requieran, de conformidad con los anexos que en su caso se suscriban, el importe de los servicios estaría pactado en cada caso, en moneda nacional y se acordará en la respectiva Orden de Trabajo", con una vigencia indefinida a partir del 22 de enero de 2016.

El 29 de agosto de 2016, el INEEL y el CENACE formalizaron un convenio modificatorio del contrato principal, que permitió la formalización de convenios específicos.

Primer Convenio Específico

El 2 de septiembre de 2016, el INEEL y el CENACE formalizaron un Primer Convenio Específico derivado del "Contrato Principal" y de su primer convenio modificatorio, que tuvo por objeto el desarrollo del proyecto denominado "Transición de modelos y aplicaciones del Mercado Interno de Energía al Mercado Eléctrico Mayorista planteado por la Reforma Energética".

Segundo Convenio Específico

El 29 de agosto de 2017, el INEEL y el CENACE firmaron un Segundo Convenio Específico para modificar la cláusula primera del contrato marco, en la que ambas partes acordaron la posibilidad de celebrar convenios específicos para llevar a cabo acciones de interés mutuo sobre diversas materias en el marco de sus respectivos objetivos y alcances, entre las cuales destacan, servicios de información tecnológica; servicios de biblioteca; capacitación del personal de ambas instituciones y el establecimiento de alianzas y asociaciones estratégicas para presentar proyectos de forma conjunta; asimismo, que el personal de ambas instituciones participe de manera conjunta en la investigación, metodología y desarrollo, en su caso, de cada uno de los servicios requeridos en los convenios específicos y en las órdenes de trabajo, así como en la colaboración conjunta para obtener un valor agregado en la transmisión de conocimiento y la capacitación de especialistas de ambas instituciones.

Tercer Convenio Modificatorio

Objeto de revisión de esta auditoría, en el que el CENACE especificó que cada vez que requiera el desarrollo de adecuaciones, extensiones o nuevas funciones de las aplicaciones del mercado, el administrador del contrato enviaba un formato firmado donde se detalló el alcance de los servicios requeridos. El INEEL presentó una propuesta de atención que incluía la cotización de la orden de trabajo, el programa de trabajo y sus entregables. La cotización

se realizó con base en las horas hombre y el personal requerido para la ejecución de los servicios con base en su oferta económica propuesta para cada tipo de perfil. La propuesta de cada orden de trabajo debía ser aprobada por el CENACE antes de comenzar con el desarrollo de los trabajos correspondientes y definida de común acuerdo por los servidores públicos designados como encargados de darle cumplimiento.

Asimismo, como parte del convenio se incluyó el concepto de Soporte Técnico y/o Mantenimiento para la atención y monitoreo a las aplicaciones con un costo mensual de 519.2 miles de pesos.

El objeto del Tercer Convenio Modificatorio

Es llevar a cabo el Servicio Integral de Soporte Técnico a las Aplicaciones del Mercado Eléctrico Mayorista que comprende lo siguiente:

1. Servicio de Soporte Técnico 24 x 7, que incluya el mantenimiento preventivo y correctivo de las aplicaciones del Mercado Eléctrico Mayorista.

2. Servicio de desarrollo de adecuaciones, extensiones, nuevas funciones y metodologías para las aplicaciones y procesos del mercado. Comprende el incremento de la funcionalidad y alcance de las aplicaciones actualmente en operación y el desarrollo de otras nuevas, para el cumplimiento de lo establecido en las Bases del Mercado, y de los requerimientos establecidos a partir de la modificación y/o actualización de las Reglas del Mercado según se define en la Ley de la Industria Eléctrica (LIE). La atención del servicio se realizará por medio de órdenes de trabajo/servicio.

Alcance

Este convenio tuvo alcance en el desarrollo y modificaciones a los procesos siguientes:

- Mercado de un día en Adelanto (MDA).
- Mercado de Tiempo Real (MTR).
- Mercado de Mediano Plazo.
- Cálculo de Liquidaciones.
- Sistema de Información de Mercado (SIM).
- Modelos de Planeación de Mediano Plazo.
- Soporte Técnico a las Aplicaciones y Plataforma de Software del Mercado Eléctrico Mayorista (MEM).

Justificación de excepción a la licitación pública

La elección del INEEL se realizó como parte de un proceso de invitación bajo el artículo 1° de la LAASSP y 4° de su reglamento; como resultado del proceso de investigación de mercado,

se observó que este proveedor fue el único que presentó una cotización para la ejecución de los servicios. Sin embargo, en la justificación, el CENACE no mencionó que se hubieran realizado consultas en el sistema COMPRANET o con alguna otra entidad pública o privada, ni demostró que se habían agotado todas las fuentes de consulta disponibles para la búsqueda de información de servicios similares o posibles proveedores que cubrieran los requisitos para los servicios solicitados; tampoco demostró que se compararon servicios similares y que el seleccionar al INEEL se cumplía con las mejores condiciones en cuanto a precio, financiamiento, oportunidad, calidad de servicio, demás circunstancias pertinentes.

Niveles de servicio

El CENACE no contempló en el contrato y sus convenios específicos la definición de niveles de servicios con los cuales pudiera medir el desempeño del proveedor, y ante incumplimientos, contara con un mecanismo de control para resarcir las desviaciones, aplicar sanciones o en su caso establecer tarifas con base en cumplimiento de niveles de servicio. Dado que a la fecha de la auditoría se identificó que, de 12 órdenes de trabajo, en 4 no se cumplió con la fecha estipulada de entrega sin que los retrasos fueran imputables al CENACE; además se observó que no se estableció en qué casos el proveedor podía reprogramar las fechas de entrega pactadas lo cual repercute en los tiempos de entrega.

Análisis de los entregables

Las órdenes de trabajo describen las condiciones particulares y alcances del servicio por realizar y la fecha de entrega, en las cuales se observó lo siguiente:

- El CENACE no cuenta con un criterio o metodología para la estimación de esfuerzo y costo, por lo que no tiene forma de corroborar que la estimación presentada por el proveedor, en las órdenes de trabajo, es acorde con la complejidad del desarrollo solicitado.

- El proveedor utilizó 27 recursos del perfil “Desarrollador 4”, para el servicio de migración de datos de los aplicativos que soportan la operación del Mercado Eléctrico Mayorista; sin embargo, en el convenio está estipulado que solo se podían requerir un máximo de 10 recursos de este tipo; se observó que no realizó un convenio modificatorio/acuerdo formalizado, en el que se establecieran las condiciones en las que era posible incrementar los perfiles establecidos contractualmente.

- En 5 órdenes de trabajo no se realizaron pruebas de vulnerabilidades previo a su salida a producción, por lo que no es posible asegurar la confiabilidad e integridad de los sistemas o aplicativos provistos.

- En los planes de pruebas no se contó con la aceptación y evaluación de las funcionalidades por parte del usuario final (área de negocio).

Soporte técnico y mantenimiento

- No se estipularon las fechas de entrega para los reportes de los servicios de soporte técnico y mantenimiento a los aplicativos del CENACE.

- El CENACE proporcionó el "Lineamiento para el Desarrollo de Software del CENACE", el cual tiene una alineación a la metodología ágil SCRUM; sin embargo, a la fecha de la auditoría (mayo de 2021), el proveedor no aplicó esta metodología; asimismo, se observó que el CENACE solicitó servicios de fábrica de software, soporte a incidencias de aplicativos, migraciones de datos y servicios de consultoría sin que haya plasmado las actividades y los entregables específicos para cada uno de los servicios.

Como resultado de la revisión de los desarrollos y mantenimientos solicitados en las órdenes de trabajo, los principales riesgos observados por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la entidad son los siguientes:

Tabla 4. Principales Riesgos por la Carencia de los Controles para el desarrollo de Soluciones Tecnológicas

Factor crítico	Riesgo
Estimación de esfuerzo	Se carece de documentación que permita validar la metodología o mecanismo que utilizó el proveedor para determinar el número de recursos y horas que se utilizaron para la atención de las solicitudes de trabajo, por lo cual no es posible validar que se están pagando los montos estimados de acuerdo con un cálculo acorde a las necesidades y requerimientos del CENACE. Asimismo, no existe un estándar para la elaboración de planes de trabajo en los que se plasme la asignación específica de actividades y tiempo por cada recurso humano indispensable para el seguimiento de las actividades del personal al proveedor.
Análisis de Vulnerabilidades	El no llevar a cabo un análisis de vulnerabilidades a los aplicativos y sus respectivas modificaciones antes de su salida en producción, representa un riesgo ante la posibilidad de que brechas de seguridad no puedan ser detectadas en tiempo y que se vean materializadas en el ambiente operativo. Asimismo, la ejecución del análisis de vulnerabilidades por el mismo equipo o proveedor de los desarrollos, resta independencia e imparcialidad con respecto a los resultados que se puedan generar.
Seguimiento y supervisión	No realizar revisiones periódicas al avance en la ejecución en las órdenes de trabajo de proyectos de fábrica de software, ocasiona que no se detecten a tiempo desviaciones en la ejecución de servicios y repercute en que los productos finales no estén a tiempo y a disposición para los usuarios finales.
Dependencia al proveedor de servicios	La dependencia de un solo proveedor para la prestación del servicio de fábrica de software para el Mercado Eléctrico Mayorista, como en este convenio, implica que no se aseguren las mejores condiciones en la oferta económica.

FUENTE: Elaborado por la ASF con base en la información proporcionada por el CENACE y los resultados de los recorridos de pruebas.

Subastas de Mediano Plazo

El 10 de octubre de 2019, el CENACE le solicitó a la Secretaría de Energía (SENER) emitir su opinión respecto de la suspensión y, en su caso, posible cancelación de la Subasta de Mediano Plazo; la secretaría remitió su respuesta el 26 de noviembre de 2019, y señaló lo siguiente:

"Que en ejercicio de las facultades conferidas por el artículo 11, fracciones I, XIV, XV, XLII y XLIII de la Ley de la Industria Eléctrica (LIE), esta Dependencia:

- Considera la necesidad de cancelar la Subasta de Mediano Plazo SMP-1/2018 y consecuentemente, cancelar cualquier acto jurídico vinculado con el proceso de subasta antes mencionado y hacerlo del conocimiento de los interesados en términos que se estimen pertinentes.

- Instruye a ese Organismo a no convocar Subastas de Mediano Plazo subsecuentes a la SMP-1/2018, en tanto se definen los instrumentos programáticos complementarios del sector eléctrico."

A la fecha de la auditoría (mayo de 2021), el aplicativo Subastas de Mediano Plazo que desarrolló el INEEL bajo el amparo del Segundo Convenio Específico del contrato CENACE: 22/1/16 entró en estado de suspensión por instrucciones de la Secretaría de Energía, derivado de los cambios en la industria eléctrica del país, cabe mencionar que este aplicativo fue liberado a producción y era utilizado por los participantes, el monto erogado por el CENACE para este aplicativo fue de 7,393.8 miles de pesos. .

Por lo anterior, se concluye que el CENACE carece de una metodología propia que apoye en la estimación de esfuerzo y costo para garantizar que los perfiles y recursos que cotiza el proveedor son acordes con las especificaciones y horas hombre que demanda el CENACE; al no verificar dichas estimaciones, el proveedor determina a discreción la cantidad de recursos y horas hombre por cada orden de trabajo solicitada; al no haber definido niveles de servicio y mecanismo de control se propicia que se reprogramen las órdenes de trabajo, lo que repercute en la puesta en marcha de los servicios solicitados; La subdirección de administración del Mercado Eléctrico Mayorista; tuvo deficiencias en la administración del convenio, dado que no se establecieron procedimientos para resolución de controversias y las responsabilidades de los proveedores ante defectos, vicios ocultos y calidad de los servicios, ni estableció el listado de entregables que debían acompañar las órdenes de trabajo, por lo que se incumple con lo establecido en la fracción III.B Proceso de Administración de Proveedores (APRO), actividad del proceso APRO 2 Monitorear el avance y desempeño del proveedor, factor crítico 1 del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, y sus reformas publicadas el 23 de julio de 2018, y el numeral 5.2 del anexo técnico.

2020-1-18TOM-20-0397-01-001 **Recomendación**

Para que el Centro Nacional de Control de Energía implemente mecanismos internos para la estimación del esfuerzo, recursos y tiempo necesarios para la atención de los servicios de fábrica de software y que puedan conciliarse con el proveedor, con la finalidad de asegurar que los servicios proporcionados se paguen de acuerdo con las necesidades respecto de la gestión de fábrica de software, y cuenten con fundamento en una metodología o mejor práctica en la materia.

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.

2020-1-18TOM-20-0397-01-002 **Recomendación**

Para que el Centro Nacional de Control de Energía implemente mecanismos de validación para los entregables establecidos en los contratos y convenios específicos, y que se definan en dichos documentos todos los requerimientos, sus correspondientes entregables y las fechas límite de entrega.

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

2020-1-18TOM-20-0397-01-003 **Recomendación**

Para que el Centro Nacional de Control de Energía se asegure de que se lleve a cabo la ejecución de pruebas de vulnerabilidades y/o penetración a los aplicativos críticos antes de la salida a producción o, en su defecto, establezca una fecha compromiso para la ejecución de dichas actividades.

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.

2020-1-18TOM-20-0397-01-004 **Recomendación**

Para que el Centro Nacional de Control de Energía estipule en las contrataciones de TIC, incluidas las realizadas al amparo del artículo 1º de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, mecanismos para la definición de entregables específicos por servicios, para que éstos se encuentren soportados y justificados respecto al monto facturado por el proveedor, a efecto de que el Centro Nacional de Control de Energía realice los pagos correspondientes por los servicios efectivamente devengados y sea posible identificar los atrasos o incumplimientos del proveedor con base en los entregables y actas de entrega-recepción; establezca los casos en que podrán otorgarse prórrogas para el cumplimiento de

las obligaciones contractuales, los procedimientos para la resolución de controversias; la responsabilidad de los proveedores ante los defectos y vicios ocultos de los bienes y de la calidad de los servicios, así como de cualquier otra responsabilidad en que hubieren incurrido y, en caso de atraso, el establecimiento de niveles de servicio y mecanismos de control.

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

3. CENACE-LP-094-B-017-2017 "Modernización de los Sistemas SCADA/EMS del CENACE"

Se revisó el contrato número CENACE-LP-094-B-017-2017 celebrado con Siemens, S.A. de C.V., mediante procedimiento de Licitación Pública Electrónica Internacional, bajo la Cobertura de Tratados de Bienes, con fundamento en el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; 25, 26, fracción I, 26 Bis, fracción II, 27 y 28, fracción II, 29, 36 y 36 Bis, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP) y 39 de su reglamento; con el objeto de llevar a cabo la ''Modernización de los Sistemas EMS/SCADA del CENACE", con vigencia del 14 de diciembre de 2017 al 30 de noviembre de 2022, extendida por medio del Primer Convenio Modificatorio, al 22 de agosto de 2024, con un monto mínimo de 1,755.8 miles de dólares y máximo de 52,267.1 miles de dólares, con pagos realizados en 2020 por 5,568.1 miles de dólares que, valuados a los tipos de cambio publicados en el Diario Oficial de la Federación de fecha 30 de septiembre, 24 de diciembre y 30 de diciembre de 2020 ascendieron a 113,249.5 miles de pesos, y se determinó lo siguiente:

Antecedentes

El sistema EMS/SCADA es la herramienta que permite al CENACE ejecutar el control operativo del Sistema Eléctrico Nacional (SEN), además de proporcionar los insumos necesarios para la operación en tiempo real del Mercado Eléctrico Mayorista (MEM), que le permite la ejecución del mismo.

El CENACE cuenta con el sistema EMS/SCADA marca ABB desde 1997, el cual fue sujeto a cuatro contratos de mantenimiento con el proveedor ABB México, S.A. de C.V., el último con una vigencia del 1 de enero de 2017 al 31 de enero de 2019.

Como parte de la modernización del Sistema EMS/SCADA, en 2017 el CENACE formalizó el contrato número CENACE-LP-14-S-14-2017-con Accenture, S.C, con una vigencia del 24 de marzo al 22 de septiembre de 2017, por un monto de 8,715.0 miles de pesos, con el objeto de proveer los servicios de consultoría y colaboración para la modernización de los sistemas SCADA/EMS/MMS/DTS del CENACE. El proveedor concluyó, entre otros, lo siguiente:

- Estipuló que los nuevos sistemas SCADA/EMS del CENACE tuvieran la capacidad de soportar la incorporación gradual de equipos y tecnologías en la red eléctrica, a fin de optimizar los procedimientos operacionales existentes y utilizar las interfaces con las RTUs[9], PMUs[10] y otros dispositivos de campo a través de los equipos de comunicaciones existentes en CENACE.

- Consideró que el nuevo sistema SCADA/EMS comprendiera un entorno informático distribuido con arquitectura de sistema abierto, con el objetivo de permitir la adición de funcionalidad futura, escalabilidad y la sustitución de componentes de hardware sin interrupciones en la operación del sistema, incluyendo una infraestructura importante de almacenamiento de información histórica, debe de estar orientada a servicios (SOA) e incorporar el concepto de bus de servicios (ESB - "Enterprise Service Bus") para el intercambio de información entre aplicaciones propias y de terceros.

El CENACE tiene en operación una infraestructura jerárquica de sistemas de control EMS/ SCADA para gestionar la operación del Sistema Eléctrico Nacional (SEN), la cual consta de dos sitios de control centrales (Primario y Alterno) y nueve centros de control regionales:

- Gerencia del Centro Nacional – (GCN),

- Gerencia del Centro Alterno – (GCA),

- Gerencias de Control Regionales (GCR): Central, Oriental, Occidental, Noroeste, Norte, Noreste, Peninsular, Baja California y Subgerencia de Control La Paz.

Los centros de control GCN y GCA, junto con 8 de los 9 GCR, están equipados con sistemas EMS/SCADA provistos por ABB. El sistema EMS/SCADA existente en el GCR de Baja California Sur fue provisto por el proveedor Siemens, S.A. de C.V.

Alcance del contrato

Las especificaciones técnicas solicitadas en el anexo 1 del contrato son las mismas que definió el proveedor Accenture, como parte de sus entregables.

[9] Unidad Terminal Remota (RTU por sus siglas en inglés), es un dispositivo diseñado para el control y automatización de instalaciones.

[10] Unidad de medida fasorial; Un Sincrofasor (PMU por sus siglas en inglés) es un dispositivo que mide las ondas eléctricas en una Red eléctrica.

Los nuevos sistemas SCADA/EMS Siemens del CENACE tendrán la capacidad de soportar la incorporación gradual de los equipos y tecnologías siguientes en la red eléctrica:

- Recursos Distribuidos de Energía (incluyendo plantas de generación renovables).
- Diseminación de tecnologías de Redes Inteligentes, incluyendo Respuesta de la Demanda.
- Optimización Dinámica de los recursos de la red.
- Tecnologías avanzadas de almacenamiento de energía para asistir en la regulación secundaria de frecuencia, incluyendo las siguientes:
    - Bancos de baterías.
    - Volantes.
- Mayor uso de tecnologías digitales para mejorar la confiabilidad, seguridad y eficiencia de la red.

El CENACE requiere consolidar y simplificar los 11 sistemas EMS/SCADA existentes.

El equipamiento en los GCR tendrá comunicaciones directas con los tipos de RTU siguientes:

- RTU en Plantas de Generación.
- RTU en Subestaciones de Transmisión.

Los nuevos sistemas SCADA/EMS Siemens proveerán, como mínimo, las funcionalidades siguientes:

Tabla 5. Funcionalidades SCADA

Funciones de SCADA.	Monitoreo y Estadísticas de Comunicaciones
Adquisición de Datos.	Modo Escucha
Procesadores Frontales de Comunicaciones Distribuidos.	Definición de Áreas de Responsabilidad, individuales y por grupo
Monitoreo de la Salud del Sistema.	Funciones de Interfaz de Usuarios
Procesamiento de Alarmas y Eventos.	Almacenamiento de Información Histórica y Reportes
Control Supervisorio.	Almacenamiento de Información Histórica y Reportes
Gestión de Etiquetas (Tagging).	Funciones de Generación
Intercambio de Datos vía ICCP	Aplicaciones de Transmisión
Secuencias de Control con lnterlocks	Simulador de Entrenamiento de Despachadores
Gestión Inteligente de Alarmas	Interfaces Externas
Cálculos Avanzados en tiempo real	Gestión de Bases de Datos y Desplegados
Gestión de límites	

FUENTE: elaborada por ASF con información proporcionada por CENACE.

Procedimiento de la contratación

De acuerdo con el Dictamen Técnico y Económico de fecha 12 de diciembre de 2017, elaborado por la Dirección de Tecnologías de la Información y Comunicaciones, se analizaron las proposiciones de los licitantes siguientes:

- ABB MEXICO, S.A. de C.V.
- GE Grid Solutions, S.A. de C.V.
- Open Systems International Inc en participación conjunta con Automatización y Tecnología Mexicana, S.A. de C.V.
- Siemens, S.A de C.V.

El CENACE desechó las propuestas de los licitantes ABB MEXICO, S.A. de C.V., GE Grid Solutions, S.A. de C.V., Open Systems International Inc en participación conjunta con Automatización y Tecnología Mexicana, S.A. de C.V., ya que no cumplían con la razonabilidad

técnica, económica, legal y administrativa. El acta de fallo se generó con fecha 14 de diciembre de 2017, donde se indica que resultó adjudicado el proveedor Siemens, S.A de C.V.

Pagos

Los servicios pagados en 2020 correspondieron a servicios devengados de 2019 y 2020, los cuales ascendieron a 6,327.6 miles de dólares (130,232.1 miles de pesos) y se determinaron penalizaciones por 759.5 miles de dólares que, valuados al tipo de cambio de la fecha de pago ascendieron a 16,982.6 miles de pesos las cuales se aplicaron mediante nota de crédito.

Proceso de conciliación

En marzo de 2020, el proveedor inició un proceso de conciliación respecto a diversas penalizaciones y deducciones por retrasos imputables a él, con el propósito de llegar a un acuerdo conciliatorio, se acordó modificar las fechas de entrega extendiéndose hasta mayo de 2020. Se reconoció la aplicación de la penalidad por un monto de 759.5 miles de dólares que valuados al tipo de cambio de la fecha de pago ascendieron a 16,982.6 miles de pesos, por la entrega con retraso de las pruebas Pre-FAT y las FAT.

Cronograma

Los mecanismos de control y supervisión realizados por el CENACE y el proveedor Siemens, S.A. de C.V., para medir el grado de avance de cada una de las actividades plasmadas en el cronograma no han sido suficientes para garantizar la oportuna corrección de las desviaciones presentadas, debido a que en el Quinto Control de Cambios (cronograma vigente), se identificaron 273 actividades integradas en 43 hitos, las cuales, a la fecha de la auditoría (mayo de 2021), deberían estar terminadas; sin embargo, 65 presentan del 1.0% al 90.0% de cumplimiento, incluyendo entre ellas las pruebas SAT (Pruebas de Aceptación en Sitio, por sus siglas en inglés), y 145 actividades reportaron un avance nulo, por lo que se tenía un 76.9% de retraso respecto al total de actividades; derivado de lo anterior, el proveedor se hizo nuevamente acreedor a la aplicación de penas convencionales por retrasos en la “Integración e Instalación del Sistema”, y por la ejecución de las pruebas SAT por un monto de 129.2 y 242.5 miles de dólares respectivamente, por lo que se solicitó un segundo convenio modificatorio; sin embargo, a la fecha de la auditoría (mayo de 2021) aún no se había formalizado el segundo convenio modificatorio. Lo anterior representa el riesgo de que no se llegue a cumplir en tiempo y forma la liberación del sistema.

Desarrollo de aplicaciones

El CENACE solicitó, como parte integral del proyecto, modificaciones y desarrollo de aplicaciones, entre ellas, el Sistema de Relatorios y Eventos, en cuya revisión se observó lo siguiente:

- Se identificaron deficiencias en la información proporcionada por el proveedor, toda vez que, el control de horas de los servicios carecía de fecha de entrega y firmas de

las horas prestadas y no contó con un control del personal que participó. El CENACE no validó que las horas-hombre relacionadas con el desarrollo del Sistema de Relatorios y Eventos, correspondieran con lo que se devengó.

Plan de mitigación de riesgos

Se observó que:

- En el documento reportes de avances trimestral del programa de trabajo de administración de riesgos, se plasmaron los riesgos estratégicos institucionales; sin embargo, no existe un apartado para los riesgos de proyectos estratégicos y no están definidos los del contrato revisado.

- El CENACE no tiene contemplado el caso de que el proveedor no continúe con el desarrollo y la implementación del sistema SCADA y sus acciones de mitigación correspondientes.

- En la matriz de riesgos para proyectos, los factores de riesgo identificados no fueron clasificados de acuerdo con el grado de impacto y probabilidad de ocurrencia; la matriz no ha tenido actualizaciones desde el 18 de septiembre de 2018; precisando que, se materializó el riesgo "retraso en la Ejecución de las pruebas programadas por causas operativas".

- Cada riesgo contiene el estado, categoría, probabilidad, impacto, exposición, descripción; sin embargo, las acciones de mitigación no estaban incluidas.

Seguridad cibernética

Se identificó lo siguiente:

- Se carece de un marco de seguridad cibernética que especifique los controles que deben aplicarse a los sistemas SCADA.

- No se han corregido todas las fallas de pruebas de seguridad, ni se ha considerado realizar una evaluación independiente de seguridad de todos los aplicativos críticos que soportan la nueva infraestructura SCADA.

- El proveedor mencionó 14 categorías de medidas de seguridad por utilizar, pero a la fecha de la auditoría (mayo de 2021), el CENACE no ha establecido los periodos en los que verificará su cumplimiento.

Código seguro

- El proveedor no proporcionó documentación del uso de prácticas seguras de codificación.

- No se proporcionó evidencia de que todos los programadores que desarrollaron código para el sistema SCADA/EMS y sus componentes, estaban certificados en el programa de capacitación para programadores que imparte el mismo proveedor.

Por lo anterior, se concluye que el contrato presenta retrasos que podrían incidir en la implementación en tiempo y forma conforme lo requiere el CENACE, cabe 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 (SEN); asimismo, existen deficiencias en la administración y mitigación del riesgo, así como, en los mecanismos de supervisión y seguimiento de las actividades plasmadas en el cronograma de trabajo vigente; no se ha verificado el desarrollo seguro de las aplicaciones solicitadas como parte del contrato, ni se ha asegurado que se dé continuidad a las pruebas de análisis de vulnerabilidades, por lo que, no se tiene la certeza de que la plataforma del nuevo sistema SCADA/EMS sea confiable, integra y segura.

2020-1-18TOM-20-0397-01-005 **Recomendación**

Para que el Centro Nacional de Control de Energía actualice la matriz de riesgos de acuerdo con las fases en las que se encuentra el avance de la implementación del contrato número CENACE-LP-094-B-017-2017, incluya las acciones de mitigación y refuerce los mecanismos de supervisión y seguimiento de las actividades establecidas en el cronograma de trabajo vigente para que las desviaciones se detecten de manera oportuna, se corrijan y se cumplan los tiempos especificados para implementar en todo el país el nuevo sistema SCADA/EMS.

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

2020-1-18TOM-20-0397-01-006 **Recomendación**

Para que el Centro Nacional de Control de Energía verifique que el proveedor del contrato número CENACE-LP-094-B-017-2017 implemente prácticas de codificación segura, lleve a cabo pruebas de vulnerabilidades a todas las aplicaciones que conforman la implantación del sistema SCADA/EMS conforme un plan establecido, y se asegure de mitigar los hallazgos detectados; asimismo, que se realicen pruebas de seguridad antes de la implementación del sistema y se solicite la validación de que el nuevo sistema SCADA/EMS cumple con el NERC CIP y las 14 categorías de medidas de seguridad definidas por el proveedor.

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

4. Ciberseguridad en el Sistema EMS/SCADA

Antecedentes

El sistema EMS/SCADA es la herramienta que permite al CENACE ejecutar el control operativo del Sistema Eléctrico Nacional (SEN), además de proporcionar los insumos necesarios para la operación del Mercado Eléctrico Mayorista (MEM) y permitir la ejecución en tiempo real del mismo.

Desde 1997, el CENACE ha contado con el sistema EMS/SCADA marca ABB; como parte de la modernización del sistema SCADA y con el propósito de sustituirlo, a la fecha de la auditoría (mayo de 2021) el CENACE se encontraba en proceso de migrar al sistema Spectrum Power 7 (El contrato se analiza en el Resultado Núm. 3).

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

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

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

Normativa en materia del Sector Energético	
NERC CIP - Conjunto de estándares de la Corporación Norteamericana de Confiabilidad Eléctrica (NERC, por sus siglas en inglés) para la Protección de las Infraestructuras Críticas (CIP, por sus siglas en inglés) El conjunto de estándares del NERC para la Protección de las Infraestructuras Críticas (CIP) definen los requisitos de confiabilidad para planificar y operar el sistema de energía a granel de América del Norte y se desarrollaron utilizando un enfoque basado en resultados que se centra en el desempeño, la gestión de riesgos y las capacidades de la entidad. El modelo de confiabilidad define las funciones que deben realizarse para garantizar que el sistema eléctrico a granel opere de manera confiable y es la base de los estándares de confiabilidad orientados a proteger las redes de distribución de energía eléctrica frente a ciberataques o incidentes de seguridad que comprometan la disponibilidad del servicio energético en los Estados Unidos de América.	**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	**Acuerdo por el que se emite el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista publicado en el Diario Oficial de la Federación el 04 de diciembre de 2017**

Normativa en materia del Sector Energético	
naturales, fallos estructurales, errores humanos y riesgos de privacidad.	Establece los principios, reglas, directrices, ejemplos y procedimientos a seguir en el uso de las Tecnologías de la Información, para que el Centro Nacional de Control de Energía, los Transportistas, los Distribuidores, las Centrales Eléctricas y los Centros de Carga cuenten con los medios de comunicación para transferencia de voz y datos, con calidad de la información, requeridos para cumplir con la Telemetría en Tiempo real en forma directa para el Control Operativo del Sistema Eléctrico Nacional y con la operación del Mercado Eléctrico Mayorista, incluida la medición para liquidaciones
Código de Red con acuerdos publicados en el Diario Oficial de la Federación el 08 de abril de 2016 Dicta los Criterios de eficiencia, Calidad, Confiabilidad, Continuidad, seguridad y sustentabilidad incluidos en este documento, tienen como objetivo permitir e incentivar que el SEN se desarrolle, mantenga, opere, amplíe y modernice de manera coordinada con base en requerimientos técnicos-operativos, y de la manera más eficiente y económica. Lo anterior bajo los principios de acceso abierto y trato no indebidamente discriminatorio. Asimismo, el Código de Red debe ser entendido como el documento que establece los requerimientos técnicos mínimos que los Integrantes de la Industria Eléctrica están obligados a cumplir con relación a las actividades de planeación y operación del SEN, así como establecer las reglas para la medición, el control, el acceso y uso de la infraestructura eléctrica. El Código de Red es de cumplimiento obligatorio para los Integrantes de la Industria Eléctrica y corresponderá a la CRE su interpretación y vigilancia.	

FUENTE: Elaborada por la ASF.

Evaluación de ciberseguridad en el CENACE

La Auditoría Superior de la Federación desarrolló un modelo para evaluar la ciberseguridad en el Centro Nacional de Control de Energía, específicamente del Sistema EMS/SCADA, basado en el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología - 1800 (NIST por sus siglas en inglés y compuesto de 108 subcategorías), NIST 1800-7 “Conciencia situacional para las empresas eléctricas” conformado por 16 subcategorías, los estándares NERC CIP (Protección de Infraestructura Crítica, por sus siglas en inglés) y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano (Acuerdo por el que se emite el Manual de Requerimientos de Tecnologías de la Información y Comunicaciones para el Sistema Eléctrico Nacional y el Mercado Eléctrico Mayorista publicado en el Diario Oficial de la Federación el 4 de diciembre de 2017, el Código

de Red con acuerdos publicados en el Diario Oficial de la Federación el 8 de abril de 2016 y el Manual de programación de Salidas publicado en el Diario Oficial de la Federación el 13 de noviembre de 2017).

Agrupación de subcategorías de ciberseguridad del Marco de Referencia de Ciberseguridad

El modelo desarrollado por la ASF analizó las 108 subcategorías contenidas en el Marco de Referencia de Ciberseguridad NIST, las 16 subcategorías del NIST 1800-7 "Conciencia situacional para las empresas eléctricas", los estándares NERC CIP del 002 al 014, y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano; como resultado, se agruparon 67 subcategorías las cuales integran las subcategorías anteriormente mencionadas y que se agrupan en las 5 funciones y 18 categorías siguientes:.

Funciones

1.- Identificar

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

Tabla 7. Categorías de la función identificar

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

FUENTE: Marco de Referencia de Ciberseguridad NIST.

2.- Proteger

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

Tabla 8. Categorías de la función proteger

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

FUENTE: Marco de Referencia de Ciberseguridad NIST.

3.- Detectar

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

Tabla 9. Categorías de la función detectar

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

FUENTE: Marco de Referencia de Ciberseguridad NIST.

4.- Responder

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

Tabla 10. Categorías de la función responder

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

FUENTE: Marco de Referencia de Ciberseguridad NIST.

5.- Recuperar

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

Tabla 11. Categorías de la función recuperar

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

FUENTE: Marco de Referencia de Ciberseguridad NIST.

Resultado de la evaluación

El resultado de la evaluación para cada subcategoría del NIST que conforma el marco, se realizó en función de la información proporcionada a este ente fiscalizador como parte de las solicitudes de información realizadas al CENACE y de la atención a las Actas Administrativas Circunstanciadas aplicadas a las Gerencias de Control Regional Baja California, Noroeste, Centro Alterno, Centro Nacional, Noreste, Norte, Occidental, Peninsular y Oriental.

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

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

Cabe mencionar que esta evaluación se realizó al sistema EMS/SCADA marca ABB dado que el nuevo sistema SCADA/EMS aún se encuentra en proceso de despliegue e instalación.

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

Identificar

La función Identificar presentó un promedio de 63.3 % de cumplimiento, lo que indica que se debe continuar con la implementación de acciones que permitan definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos.

Proteger

La función Proteger presentó un promedio de 67.7% de cumplimiento, es la función que obtuvo un mayor nivel, sin embargo, se tienen que reforzar e incrementar las medidas para proteger los procesos y los activos de la organización.

Detectar

La función Detectar presentó un promedio de 56.0 % de cumplimiento, es la función que obtuvo el promedio más bajo, por lo que se tienen que incrementar acciones para tener una adecuada definición y ejecución de actividades dirigidas a la identificación temprana de los incidentes de seguridad.

Responder

La función Responder presentó un promedio de 63.3% de cumplimiento, por lo que se tiene que continuar con la definición y ejecución de actividades apropiadas para tomar medidas en caso de detección de un evento de seguridad con el objetivo de reducir el impacto de un potencial incidente de ciberseguridad.

Recuperar

La función Recuperar presentó un promedio de 60.0% de cumplimiento, lo que indica que se debe incrementar las acciones para probar y actualizar los planes de resiliencia, que les permita restablecer cualquier capacidad o servicio que se haya visto afectado debido a un

incidente de ciberseguridad, así como gestionar ante los medios, una respuesta inmediata en caso de contingencias.

Por subcategoría

- 15 subcategorías del marco (22.0%) obtuvieron una calificación de establecido.
- 50 subcategorías del marco (75.0%), obtuvieron una calificación de medio.
- 2 subcategorías del marco (3.0%) obtuvieron una calificación de bajo, relacionadas con los temas siguientes:
    - ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.
    - PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.

El CENACE ha implementado controles alineados al NERC CIP en su Gerencia de Control Regional Baja California; sin embargo, estos aún no están aplicados a nivel nacional, por lo cual existen brechas respecto a la adecuada gestión de los sistemas críticos para las operaciones del CENACE como lo es el EMS/SCADA.

Respecto a la normativa mexicana en el sector, el CENACE cumple con los requisitos básicos 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.

Adopción de la normativa NERC CIP en México

El 8 de mayo de 2017, el CENACE, la Comisión Reguladora de Energía (CRE) y representantes del NERC, firmaron el Memorando de Entendimiento (MOU, por sus siglas en inglés) para colaborar con el NERC en el desarrollo de un proceso de posible adopción de Estándares de Confiabilidad de NERC para incluirlos en el Código de Red emitido por la CRE o en cualquier otro instrumento regulatorio y continuarían explorando oportunidades para una posible participación formal de México en la Organización de Confiabilidad Eléctrica (ERO, por sus siglas en inglés), en dicho documento se establece las actividades siguientes:

- *"La identificación y evaluación de riesgos relacionados con la protección de la infraestructura crítica, la seguridad física y ciberseguridad, incluida la identificación de activos y prácticas esenciales para proteger la información sensible;*
- *La evaluación del desempeño de la confiabilidad y los riesgos, incluyendo, pero no limitado a, la integración de grandes cantidades de generación renovable en el Sistema Eléctrico;*

- *El desarrollo de prácticas, herramientas y técnicas para el análisis de eventos en el Sistema Eléctrico y la gestión de los riesgos de confiabilidad identificados como resultado de dichos eventos;*

- *El desarrollo de capacidades técnicas y regulatorias."*

Asimismo, establece, entre otras, que se podrían realizar reuniones de seguimiento y se crearía un grupo para conducir las actividades de este MOU, que estaría compuesto por un Grupo Directivo, una Secretaria Técnica y los Grupos Técnicos de Trabajo que se requieran para dicho fin. Sin embargo, a la fecha de la auditoría (mayo de 2021), el CENACE no demostró el avance de dicha iniciativa y de la integración del grupo directivo, así como de sus posibles reuniones y acuerdos.

El CENACE no se ha pronunciado respecto a la evaluación y priorización de las normas NERC CIP para su adopción en el marco mexicano regulatorio del sector energía, ya que operativamente, conforme a lo establecido en el Estatuto Orgánico del Centro Nacional de Control de Energía, le corresponde a esta entidad llevar a cabo los procesos de revisión, ajuste, actualización y emisión de procedimientos operativos con sujeción a los mecanismos y lineamientos que establezca la CRE y proponer a ésta las actualizaciones de las reglas generales de interconexión de los diferentes tipos de generación y conexión de los centros de carga.

En el análisis realizado por la ASF, se observó que la Gerencia de Control Regional Baja California, se encuentra en proceso de implementar los controles NERC CIP de los cuales tiene documentados 11, que comprenden el control de accesos, gestión de incidentes, planes de respuesta y capacitación; sin embargo, en el resto de las Gerencias de Control Regional y en el ámbito central, el CENACE no tiene contemplada su implementación o de algún otro estándar de ciberseguridad. A la fecha de la auditoría (mayo de 2021), el CENACE cuenta con controles compensatorios que si bien no se basan en un marco de referencia en la industria eléctrica, le han permitido llevar acabo el control operativo; sin embargo, el CENACE no contaba con acciones a corto, mediano y largo plazo mediante un plan formalizado de actividades para el fortalecimiento de la ciberseguridad en todo el país, es decir en todas las Gerencias de Control Regional, que incluya 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.

2020-1-18TOM-20-0397-01-007 **Recomendación**

Para que el Centro Nacional de Control de Energía implemente en el resto de las Gerencias de Control Regional los mecanismos de control y actividades para elevar los niveles de ciberseguridad que evaluó la ASF con base en las mejores prácticas, como el North American Electric Reliability Corporation (NERC) y National Institute of Standards and Technology (NIST), con el fin de atender y mitigar las observaciones detectadas en las funciones identificar, proteger, detectar, responder y recuperar; defina y supervise la ejecución de un plan de trabajo de implementación de controles apegados a las mejores prácticas de la

industria o estándares de ciberseguridad el cual priorice los de mayor riesgo, facilidad de adopción y fortalezca los mecanismos de gestión de incidentes y pruebas para evaluar la capacidad de la organización ante ataques cibernéticos.

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

2020-1-18TOM-20-0397-01-008 **Recomendación**

Para que el Centro Nacional de Control de Energía se pronuncie respecto de la evaluación, adopción y priorización de las normas NERC en el marco mexicano regulatorio del sector energía.

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

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Liderazgo y dirección.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 4 resultados, de los cuales, en uno no se detectó irregularidad y los 3 restantes generaron:

8 Recomendaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 15 de octubre de 2021, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría

practicada, cuyo objetivo fue fiscalizar los controles de ciberseguridad de los sistemas relacionados con la distribución de energía eléctrica, y la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables, específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, el Centro Nacional de Control de Energía cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

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

- En el convenio específico número 3: CENACE/I/SE/18773 celebrado con el Instituto Nacional de Electricidad y Energías Limpias (INEEL), el CENACE carece de una metodología de estimación de esfuerzo y costo por lo que no tiene forma de verificar que las horas hombre propuestas por el proveedor para realizar los servicios acordados fueran acordes con la complejidad del desarrollo solicitado; el CENACE en contravención a lo establecido en el contrato, permitió que se aumentara el número de recursos humanos para elaborar actividades, aun y cuando había un tope específico para ellos; el CENACE ha extendido en tres ocasiones mediante convenios específicos el Contrato Marco de Prestación de Servicios, el cual no tiene vigencia, celebrado con una institución pública sin buscar mejores alternativas para el estado, dichos convenios no tienen definidos niveles de servicio y mecanismos de control, lo que ha propiciado que se hayan reprogramado órdenes de trabajo, repercutiendo en la puesta en marcha de los servicios solicitados.

- En el contrato CENACE-LP-094-B-017-2017 celebrado con Siemens, S.A. de C.V., se identificaron deficiencias en la administración y supervisión de las actividades del plan de trabajo vigente y en la actualización de los riesgos asociados al proyecto y sus acciones de mitigación, así como un retraso del 76.9% de las actividades establecidas en el cronograma de trabajo, que podría provocar que la implementación del proyecto no se cumpla en tiempo y forma; cabe mencionar que dicho proyecto es relevante, ya que se actualizará la infraestructura con la que el CENACE realizará el control operativo del Sistema Eléctrico Nacional.

En la revisión de la evaluación de ciberseguridad con el modelo desarrollado por la ASF basado en el Marco de Referencia de Ciberseguridad del Instituto Nacional de Estándares y Tecnología - 1800 (NIST por sus siglas en inglés), NIST 1800-7 “Conciencia situacional para las empresas eléctricas”, los estándares NERC CIP (Protección de Infraestructura Crítica, por sus siglas en inglés) y la normativa mexicana que establece controles de gestión de la seguridad en el Sector Eléctrico Mexicano, de un total de 67 subcategorías evaluadas, se detectó que 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 2 subcategorías del marco (3.0%), estas 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.

Servidores públicos que intervinieron en la auditoría:

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

Comentarios de la Entidad Fiscalizada

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

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

Apéndices

Procedimientos de Auditoría Aplicados

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

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

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos fueron contemplados en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; validar la información del registro de accionistas para identificar asociaciones indebidas, subcontrataciones en exceso y transferencia de obligaciones; verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permiten su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como las penalizaciones y deductivas en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, servicios administrados para la operación de infraestructura y sistemas sustantivos, telecomunicaciones y demás relacionados con las TIC para verificar antecedentes; beneficios esperados; entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento/sustantivas); implementación y soporte de los servicios; verificar la gestión de riesgos, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de vulnerabilidades, entre otros.

Áreas Revisadas

La Dirección General de Tecnologías de la Información y Comunicaciones, la Dirección de Administración y Finanzas, la Dirección de Administración del Mercado Eléctrico Mayorista,

la Gerencia del Centro Nacional, la Gerencia del Centro Alterno, la Gerencia de Control Regional Baja California, la Gerencia de Control Regional Central, la Gerencia de Control Regional Noreste, la Gerencia de Control Regional Norte, la Gerencia de Control Regional Noroeste, la Gerencia de Control Regional Occidental, la Gerencia de Control Regional Oriental y la Gerencia de Control Regional Peninsular del CENACE.

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 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; Artículo 7 fracciones I y VI de la Ley General de Responsabilidades Administrativas publicada en el Diario Oficial de la Federación el 18 de julio de 2016; Fracción II del Artículo 8, Artículos 3, 21 y 22 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; Apartado III.B Proceso de administración de proveedores (APRO), Objetivo General, objetivos específicos 1 y 2, Regla del proceso 3 y factor crítico 3, 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, 2, y 3; 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 en el Diario Oficial de la Federación, con última reforma publicada en el mismo medio el 23 de julio de 2018, Objetivo, Función 5; Inciso D, Objetivo, Funciones 1, 2, 4, 7, Jefatura de Unidad de Sistemas de Mercado, Objetivo, Funciones 2 y 3, Inciso B del apartado de la Dirección de Administración y Finanzas, segundo párrafo del artículo 1 y tercer párrafo del artículo 51 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (LFPRH) publicada en el Diario Oficial de la Federación el 30 de marzo del 2006 y su última reforma publicada en el Diario Oficial de la Federación el 06 de noviembre de 2020; fracción I y VI del artículo 7 Ley General de Responsabilidades Administrativas publicada en el Diario Oficial de la Federación el 18 de julio de 2016 y su última reforma publicada el 13 de abril de 2020; fracción IV del artículo 57 y 60 del ESTATUTO Orgánico del CENACE publicado en el Diario Oficial de la Federación el 20 de abril de 2018; Los artículos 16, 19, fracción III, 38 fracción I, y 52 de la Ley General de Contabilidad Gubernamental (LGCG) Publicada en el Diario Oficial de la Federación el 31 de diciembre de 2008 y su última reforma publicada en el mismo medio el 30 de enero de 2018; fracción IV del numeral 5.1.13. de las Políticas, Bases y

Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del CENACE de fecha 25 de septiembre de 2018.

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.