Instituto Nacional de Estadística y Geografía

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2019-0-40100-20-0094-2020

94-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 2019 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

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

Consideraciones para el seguimiento

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

En tal virtud, las recomendaciones y acciones que se presentan en este informe individual de auditoría se encuentran sujetas al proceso de seguimiento, por lo que en razón de la información y consideraciones que en su caso proporcione la entidad fiscalizada, podrán confirmarse, solventarse, aclararse o modificarse.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	1,099,220.8
Muestra Auditada	489,423.5
Representatividad de la Muestra	44.5%

El universo seleccionado por 1,099,220.8 miles de pesos corresponde al total ejercido en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2019; la muestra auditada está integrada por dos contratos relacionados con la compra de 185,824 Dispositivos de Cómputo Móvil para el Censo de Población y Vivienda 2020, así como con la compra de 11,023 computadoras laptop con cámara frontal y 2,802 computadoras laptop sin cámara frontal, con pagos ejercidos por 489,423.5 miles de pesos, que representan el 44.5% del universo seleccionado.

Adicionalmente, la auditoría comprende la revisión de las acciones realizadas en materia de TIC por la Coordinación General de Informática (CGI) del INEGI en 2019, relacionadas con Ciberseguridad, Continuidad de las Operaciones y Centros de Datos.

Antecedentes

El 25 de enero de 1983 se creó, por decreto presidencial, el Instituto Nacional de Estadística, Geografía e Informática (INEGI) como un organismo público autónomo responsable de normar y coordinar el Sistema Nacional de Información Estadística y Geográfica, así como de captar y difundir información de México en cuanto al territorio, los recursos, la población y economía, que permita dar a conocer las características de nuestro país y ayudar a la toma de decisiones. Con la promulgación de la Ley del Sistema Nacional de Información Estadística y Geográfica (LSNIEG) el 16 de abril de 2008, el INEGI cambió su denominación a Instituto Nacional de Estadística y Geografía, así como su personalidad jurídica, adquiriendo autonomía técnica y de gestión rigiéndose por una Junta de Gobierno, que es su órgano superior de dirección.

Con su creación, el INEGI modernizó la valiosa tradición que tenía nuestro país en materia de captación, procesamiento y difusión de información acerca del territorio, la población y la economía, por lo que conjuntó en una sola institución la responsabilidad de generar la información estadística y geográfica.

En la fiscalización de la Cuenta Pública 2016, se llevó a cabo la auditoría número 119-GB con título “Auditoría de TIC”, en donde se validaron dos contratos (el primero, para contar con el Derecho de uso de programas de software, y el segundo para la Adquisición de 11,330 dispositivos de cómputo móvil); adicionalmente, se revisaron los procesos de Gobierno y Administración de las Tecnologías de la Información y Comunicaciones, así como la Gestión de la Seguridad de la Información y Continuidad de las Operaciones. De la revisión realizada se determinaron 10 Recomendaciones y una Promoción de Responsabilidad Administrativa Sancionatoria.

Entre 2015 y 2019, el INEGI invirtió 3,646,108.0 miles de pesos en Tecnologías de Información y Comunicaciones (TIC), como se muestra a continuación:

Recursos Invertidos en Materia de TIC
(Miles de Pesos)

Periodo de inversión	2015	2016	2017	2018	2019	Total
Monto por año	755,122.5	612,806.4	504,839.3	674,119.0	1,099,220.8	**3,646,108.0**

Fuente: Elaborado con base en la información proporcionada por el INEGI.

Resultados

1. Análisis Presupuestal

En el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019, publicado en el Diario Oficial de la Federación el día 28 de diciembre de 2018, se estableció que el presupuesto aprobado para el INEGI sería de 12,129,702.8 miles de pesos.

Durante el ejercicio 2019, el INEGI ejerció 10,479,065.4 miles de pesos como se muestra a continuación:

ESTADO ANALÍTICO DEL EJERCICIO DEL PRESUPUESTO DE EGRESOS
(Miles de Pesos)

Capítulo	Descripción	Presupuesto Autorizado	Presupuesto Devengado	Presupuesto Ejercido
1000	Servicios Personales	7,988,501.3	7,988,501.3	7,984,887.4
2000	Materiales y Suministros	266,856.8	266,856.8	208,848.4
3000	Servicios Generales	2,028,877.4	2,028,877.4	1,808,758.3
4000	Transferencias, Asignaciones, Subsidios y Otras Ayudas	37,542.6	37,542.6	37,542.6
5000	Bienes muebles, inmuebles e intangibles	888,850.1	888,850.1	426,508.2
6000	Inversión pública	12,715.3	12,715.3	12,520.5
	TOTAL	**11,223,343.5**	**11,223,343.5**	**10,479,065.4**

Fuente: Elaborado con base en la información proporcionada por el INEGI.

Se observó que en el Estado Analítico del Ejercicio del Presupuesto de Egreso no se reconoce el efecto de los compromisos devengados no pagados al cierre del ejercicio, por lo que el presupuesto devengado y ejercido no son consistentes.

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC), por 1,099,220.8 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2019
(Miles de Pesos)

Capítulo	Partida Presupuestaria	Descripción	Presupuesto Ejercido
1000		**Servicios Personales**	**288,113.3**
2000		**Materiales y Suministros**	**19,930.5**
	21401	Materiales y útiles consumibles para el procesamiento en equipos y bienes informáticos	5,683.2
	21501	Material de apoyo informativo	856.4
	29401	Refacciones y accesorios para equipo de cómputo y telecomunicaciones	13,390.9
3000		**Servicios Generales**	**224,088.5**
	31401	Servicio telefónico convencional	1,651.1
	31501	Servicio de telefonía celular	942.0
	31601	Servicio de radiolocalización	95.9
	31603	Servicios de internet	17,258.5
	31701	Servicios de conducción de señales analógicas y digitales	7,300.0
	31901	Servicios integrales de telecomunicación	3,361.6
	31904	Servicios integrales de infraestructura de cómputo	17,996.8
	32701	Patentes, derechos de autor, regalías y otros	128,281.3
	33301	Servicios de desarrollo de aplicaciones informáticas	1,949.2
	33304	Servicios de mantenimiento de aplicaciones informáticas	14,068.5
	33501	Estudios e investigaciones	2,132.1
	33606	Servicios de digitalización	551.4
	35301	Mantenimiento y conservación de bienes informáticos	28,500.1
5000		**Bienes muebles, inmuebles e intangibles**	**567,088.5**
	51501	Bienes informáticos	529,149.6
	56501	Equipos y aparatos de comunicaciones y telecomunicaciones	37,938.9
	TOTAL		**1,099,220.8**

Fuente: Elaborado con base en la información proporcionada por el INEGI.

Las partidas específicas relacionadas con los servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC, con un gasto anual de 288,113.3 miles de pesos durante el ejercicio fiscal 2019, que considera 369 plazas (358 de confianza y 11 por tiempo fijo); el promedio anual percibido por persona fue de 780.8 miles de pesos. No obstante, en la plantilla de personal proporcionada se incluyeron diversas áreas (Presidencia, Dirección General de Estadísticas Sociodemográficas, Dirección General de Estadísticas Económicas, Dirección General de Geografía y Medio Ambiente, Dirección General de Vinculación y Servicio Público de Información, entre otras) de las que no fue posible identificar su relación con labores de TIC, y que difieren de las señaladas por el INEGI como las áreas temáticas de TIC.

Del total ejercido en 2019 por 1,099,220.8 miles de pesos, que corresponden al total de recursos asignados en materia de TIC, se seleccionó una muestra de dos contratos por 489,423.5 miles de pesos, que representan el 44.5% del universo y se integran de la manera siguiente:

Muestra de Contratos de Prestación de Servicios ejercidos en 2019
(Miles de Pesos)

Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto	Pagos		
			De	Al [1]		2019[2]	2020[3]	Total
CA/09/CGI/2019	Comercializadora Milenio, S.A. de C.V.	Venta de 185,824 Dispositivos de Cómputo Móvil para el Censo de Población y Vivienda 2020.	16/07/2019	06/02/2020	322,687.1	80,671.8	242,015.3	322,687.1
CA/10/CGI/2019	Innovation, Business and Infraestructures in Technology, S.A. de C.V. Mainbit Servicios, S.A. de C.V. Mainbit, S.A. de C.V.	Venta de los bienes consistentes en: Partida 1: 11,023 computadoras laptop con cámara frontal y Partida 2: 2,802 computadoras laptop sin cámara frontal.	25/09/2019	27/02/2020	166,736.7	-	166,736.4	166,736.4
				Total	**489,423.8**	**80,671.8**	**408,751.7**	**489,423.5**

Fuente: Elaborado con base en la información proporcionada por el INEGI.
Nota [1]: Información obtenida del portal CompraNet.
Nota [2]: Único importe reconocido en la Cuenta Pública 2019 como Presupuesto Pagado.
Nota [3]: Pagos reconocidos en el presupuesto comprometido al cierre del ejercicio 2019.

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

2019-0-40100-20-0094-01-001 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía verifique que el Estado Analítico del Ejercicio del Presupuesto de Egresos revele los momentos contables de los egresos conforme a lo establecido en el Acuerdo por el que se emiten las normas y metodología para la determinación de los momentos contables de los egresos, publicado por el Consejo Nacional de Armonización Contable (CONAC), y el artículo 4, fracciones XVI y XVII, de la Ley General de Contabilidad Gubernamental (LGCG), con la finalidad de que los Estados Presupuestales presenten la situación que guardan las cuentas de forma pertinente, clara, confiable y oportuna de acuerdo con los diferentes grados de desagregación que se requiera.

2. Contrato CA/09/CGI/2019 para la adquisición de "185,824 Dispositivos de cómputo móvil para el Censo de Población y Vivienda 2020"

Con la revisión del contrato número CA/09/CGI/2019 con la empresa Comercializadora Milenio, S.A. de C.V., mediante el procedimiento de Licitación Pública Internacional Mixta Abierta a la Participación de cualquier interesado, celebrada bajo la cobertura de los Tratados Internacionales, número LA-040100992-E11-2019, con fundamento en el artículo 21, fracción I, de las Normas en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Estadística y Geografía, con objeto de que el "proveedor venda al Instituto los bienes consistentes en 185,824 dispositivos de cómputo móvil para el censo de

población y vivienda 2020", con una vigencia que se inició a partir de la fecha de su formalización (16 de julio de 2019) y concluiría hasta el cumplimiento total de las recíprocas obligaciones, por un monto total 322,687.1 miles de pesos, que fueron pagados en su totalidad durante el ejercicio 2019, se determinó lo siguiente:

El alcance de los trabajos consistió en la adquisición de 185,824 Dispositivos de Cómputo Móvil (DCM) para realizar el Censo de Población y Vivienda 2020; dichos equipos serían nuevos y debían cumplir con las características y especificaciones técnicas solicitadas; incluirían accesorios como audífonos, carcasa y tarjeta de memoria USB de mínimo 4 Gb de capacidad. El proveedor proporcionaría los dispositivos con Sistema Operativo y utilerías originales del fabricante, los cuales deberían estar liberados para ser conectados a una red de telecomunicaciones e incluir las aplicaciones entregadas por el Instituto; éstos contarían con un año de garantía en sitio, sin costo adicional para el Instituto y el prestador de servicios realizaría la reparación o reemplazo del equipo en caso de una falla; asimismo, se tendría disponibilidad de partes y refacciones que fueran necesarias para mantener los DCM en condiciones adecuadas de funcionamiento durante tres años a partir de la fecha de la aceptación total de los dispositivos por parte del Instituto.

Proceso de contratación

En el análisis realizado a las actividades llevadas a cabo por el INEGI para el proceso de contratación, se observó que éste cumplió con lo establecido en las normativas aplicables, por lo que no se identificaron observaciones.

Contrato

En la cláusula tercera del instrumento jurídico, no se estableció una vigencia específica para el contrato.

Cumplimiento Técnico y Funcional de los Servicios y Entregables Establecidos

De un total de 185,824 Dispositivos de Cómputo Móvil (DCM) adquiridos por el INEGI, considerando un nivel de confianza del 95.0%, se seleccionó una muestra aleatoria de 2,000 dispositivos, de los cuales se realizó la validación de características físicas y la comprobación de la actualización de éstos dentro del inventario de equipos. En la revisión realizada no fue posible identificar la localización y estatus de 24 DCM registrados en el inventario del Instituto, por lo que el INEGI emprendió las acciones necesarias para que el personal asignado para su guarda y custodia brinde la información necesaria que permita identificar los dispositivos antes señalados o, en su caso, justifique su ausencia. Para 4 dispositivos se proporcionaron los reportes de daño del equipo, sin incluir las constancias de hechos que acrediten la falla o daño de éstos, tampoco se especificó en sus resguardos que se les hayan entregado la carcasa y audífonos; no se tiene certeza de si 3 equipos fueron reparados o reemplazados a causa del daño que presentaron en la pantalla, únicamente se proporcionó la constancia de hechos en donde se señala la falla, pero no indican su estado actual. Por

último, para un DCM entregaron correos electrónicos en donde se señala que el equipo se encuentra en reparación; sin embargo, no se proporcionó la documentación que lo acredite.

Con el análisis del contrato, anexos, entregables y pagos, así como de la ejecución de pruebas, se comprobó que no existen desviaciones importantes respecto a su cumplimiento, ya que no se tuvieron observaciones relevantes.

3. Contrato CA/10/CGI/2019 para la "Adquisición de 13,825 Computadoras Laptop para el Censo de Población y Vivienda 2020"

Se revisó el contrato número CA/10/CGI/2019 celebrado de forma conjunta por las empresas Innovation, Business and Infraestructures in Techology, S.A. de C.V.; Mainbit Servicios, S.A. de C.V., y Mainbit, S.A. de C.V., mediante el procedimiento de Licitación Pública Internacional Mixta número LA-040100992-E19-2019, con fundamento en el artículo 21, fracción I, de las Normas en Materia de Adquisiciones, Arrendamientos, y Servicios del Instituto Nacional de Estadística y Geografía, con objeto de la "Adquisición de 13,825 Computadoras Laptop para el Censo de Población y Vivienda 2020", con una vigencia que se inició a partir de la fecha de su formalización (25 de septiembre de 2019) y concluiría hasta el cumplimiento total de las recíprocas obligaciones, por un monto total de 166,736.7 miles de pesos, los cuales fueron pagados en su totalidad.

El alcance del contrato contempló la adquisición de 13,825 computadoras portátiles divididas en dos partidas:

EQUIPOS REQUERIDOS CONTRATO CA/10/CGI/2019

Partida	Descripción	Cantidad
1	Computadora laptop Modelo ThinkPad E595, Marca Lenovo con cámara frontal.	11,023
2	Computadora laptop Modelo ThinkPad E595, Marca Lenovo sin cámara frontal.	2,802
	Total	**13,825**

Los equipos deberían ser nuevos y cumplir con las características y especificaciones técnicas solicitadas en el contrato, el proveedor otorgaría una garantía de tres años al equipo de cómputo y de un año a las baterías de éstos, debiendo cubrir cualquier defecto de fabricación sin costo adicional para el INEGI, por lo que repararía o reemplazaría los equipos o componentes correspondientes; asimismo, garantizarían la disponibilidad de partes y refacciones necesarias para mantener los equipos de cómputo en condiciones adecuadas durante 5 años a partir de la fecha de aceptación total de las laptop por parte del Instituto.

Proceso de contratación

En el análisis realizado a las actividades llevadas a cabo por el INEGI para el proceso de contratación, se observó que éste cumplió con lo establecido en las normativas aplicables, por lo que no se identificaron observaciones

Cumplimiento Técnico y Funcional de los Servicios y Entregables Establecidos

De un universo de 13,825 computadoras portátiles, considerando un nivel de confianza del 95.0%, se seleccionó una muestra aleatoria de 1,000 equipos (7.2%), para los cuales se realizó la validación de sus características físicas y la comprobación de la actualización de éstos dentro del inventario del Instituto; se identificó que éstos cumplen con lo establecido en el contrato.

Por lo anterior, de la revisión de los servicios, pagos y entregables establecidos en el contrato y su anexo técnico, se concluye que no existieron observaciones relevantes.

4. Ciberseguridad

Con la revisión de la información proporcionada por el INEGI, relacionada con la administración y operación de los controles de ciberseguridad para la infraestructura de hardware y software del Instituto, se analizaron las directrices, infraestructura y herramientas informáticas en esta materia, para llevar a cabo la evaluación e identificación de las estrategias, políticas, procedimientos y controles de ciberdefensa implementados en el Instituto. En el análisis realizado se identificó lo siguiente:

- No se cuenta con evidencia que acredite que el Instituto utiliza una herramienta para identificar equipos conectados a la red de la organización y a la vez ésta pueda actualizar el inventario de activos hardware de forma automática.

- No se tienen controlados los accesos de los activos que se conectan a la red ni existe evidencia que garantice que los activos no autorizados se eliminen de la red del Instituto.

- Se carece de la documentación que acredite que el INEGI cuenta con listas de aplicaciones confiables (listas blancas) en todos sus activos, con la finalidad de garantizar que solo el software autorizado pueda ser utilizado. Asimismo, no se tiene un proceso para la remoción de software no autorizado.

- No fue posible identificar si los escaneos para la detección de vulnerabilidades son realizados por una cuenta única y administrada por la institución, o si en su caso se cuenta con el listado de las personas que tienen acceso a estas herramientas, en el que se contemplen los privilegios, estaciones de trabajo y dirección IP del personal interno y externo que lleva a cabo dichas actividades.

- Se carece de un lineamiento o procedimiento en el cual se describan los pasos a seguir para integrar nuevos activos en la infraestructura tecnológica del INEGI.

- El Instituto no cuenta con políticas o lineamientos en donde se considere que en los equipos de cómputo se encuentre restringido el acceso a herramientas de scripting, considerando aquellas excepciones o usuarios que por sus funciones requieran del acceso.

- No se identificó si las imágenes y plantillas de configuración para los servidores del Instituto se encuentran almacenadas de forma segura y si éstas son monitoreadas, a fin de garantizar que los cambios realizados en las mismas sean únicamente los autorizados por el personal correspondiente.

- No se cuenta con una herramienta de gestión de las configuraciones de sistema, en la que sean administradas y monitoreadas de manera centralizada las configuraciones de la infraestructura tecnológica; a fin de generar alertas cuando sufran algún cambio no autorizado.

- No se identificó el lugar en donde son almacenadas las bitácoras de los activos de la infraestructura tecnológica ni el espacio que fue asignado para dicho resguardo; tampoco cuenta con una herramienta para el registro, análisis y manejo de incidentes y errores relacionados con la seguridad de la información.

- No se efectúan actividades donde se garantice que sólo los navegadores web y los clientes de correo electrónico autorizados que cuentan con soporte completo puedan ejecutarse en el Instituto. Asimismo, no se monitorea, desinstala o deshabilita cualquier plugin o aplicación add-on para garantizar que se utilicen solo los autorizados.

- Si bien el INEGI realiza el filtrado de contenido a través de herramientas, no fue posible validar que éstas contemplen la última actualización de la base de datos en donde se definen las categorías de sitios web más recientes, con la finalidad de que los sitios no categorizados sean bloqueados de manera predeterminada.

- El Instituto se encuentra en proceso de implementación del servicio de protección de amenazas y filtrado del Sistema de Nombres de Dominio (DNS), el cual cuenta con la capacidad de identificar y bloquear dominios, URLs y direcciones IPs; se tiene contemplada finalizar en octubre de 2020; sin embargo, no proporcionó el plan de trabajo correspondiente.

- Si bien, el Instituto cuenta con un software antimalware para monitorear y proteger sus equipos, no proporcionó evidencia del alcance que tiene dicha herramienta.

- El INEGI cuenta con herramientas para visualizar los puertos y protocolos de los activos de TIC; sin embargo, al no tener un inventario de activos, éstos no pueden ser asociados y validados.

- Como parte de los análisis de vulnerabilidades, el Instituto realiza el escaneo de puertos; sin embargo, esta actividad se ejecuta ante la solicitud de evaluación de un equipo en específico y no mediante escaneos automáticos de forma regular contra todos los sistemas, tampoco se advierte si se detectan puertos no autorizados en algún sistema.

- Si bien, los respaldos de información son responsabilidad de cada Unidad Administrativa del Instituto, no se proporcionó evidencia del seguimiento o verificación por parte de los enlaces informáticos respecto a que éstos se realicen bajo las condiciones establecidas por el área de Seguridad Informática. Asimismo, no se proporcionó evidencia de lo establecido por cada Unidad Administrativa en materia de respaldos para las aplicaciones críticas, por lo que los respaldos se realizan por evento y no periódicamente.

- No se realizan pruebas a la integridad de los datos en los medios de copia de respaldo de forma periódica mediante la realización de un proceso de restauración de datos para garantizar que la copia de respaldo funcione correctamente.

- El Instituto no tiene documentada ni formalizada la configuración de seguridad para todos los equipos de red autorizados, para que con base en ella se configuren nuevos equipos. Por lo anterior, no es posible realizar ejercicios de comparación de la configuración de los equipos de red contra las configuraciones de seguridad aprobadas.

- No se tiene establecido un procedimiento o alguna actividad relacionada con la instalación de las últimas versiones estables de cualquier actualización de seguridad.

- No se identificó que en la infraestructura tecnológica del Instituto se tenga implementada la autenticación multifactor, con la finalidad de garantizar que los usuarios validen su identidad utilizando dos o más métodos de verificación antes de autenticarse.

- No se presentó evidencia que acredite que el Instituto se asegura de que los administradores de la red utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren un acceso elevado, misma que se debe segmentar de la red principal y no tener acceso a Internet.

- Si bien se cuenta con un inventario actualizado de todos los bordes de red del INEGI, este no se encuentra formalizado.

- El Instituto señaló que se encuentra en proceso de elaboración y formalización del proceso para realizar escaneos desde el exterior del perímetro de cada red de confianza para detectar cualquier conexión no autorizada accesible a través del borde; sin embargo, no se proporcionó evidencia que lo acredite.

- El Instituto no ha implementado mecanismos de monitoreo y seguridad suficientes que garanticen que el tráfico de y hacia Internet provenga solo de sitios seguros.

- No se proporcionó el avance, acciones y plan a seguir para la salida a producción de la herramienta que garantizará que cada una de las políticas de seguridad del Instituto se apliquen de manera homogénea a todos los dispositivos de red.

- Se cuenta con lineamientos para la clasificación de activos de información, los cuales no están actualizados, debido a que su fecha de elaboración es del año 2016. Asimismo, el listado de activos de información crítica presentado no cuenta con firmas o documentos aprobatorios por parte del presidente del Comité del Sistema de Seguridad de la Información.

- Se mantiene en línea información y sistemas que ya no son utilizados, por lo que cualquier persona con acceso a la red del instituto podría consultarla.

- El INEGI no proporcionó evidencia que demuestre que, con base en su inventario de activos de información crítica, los elementos cuyo nivel de confidencialidad, integridad y disponibilidad sea alto, son incluidos en la herramienta de prevención de pérdida o fuga de información (DLP).

- Se carece de un inventario de dispositivos USB autorizados, así como con una herramienta que permita configurar el uso de dispositivos específicos y realizar el cifrado de la información contenida en éstos.

- El Instituto manifestó que se encuentran en proceso de llevar a cabo una clasificación de datos, a fin de que con las herramientas que se tienen actualmente se pueda identificar toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología del Instituto, incluidos los ubicados en el sitio o en un proveedor de servicios remoto.

- El Instituto indicó que cuenta con documentación sobre el cifrado de información sensible; sin embargo, no proporcionó evidencia que acredite la aplicación de dichos cifrados sobre toda la información sensible en reposo.

- Se mencionó por el INEGI que se encuentran realizando la evaluación para implementar la funcionalidad que permita mantener referencias de registros de auditoria sobre los datos protegidos, con lo que se podrá identificar cuando se

accedan o realicen cambios en los datos sensibles; sin embargo, no se proporcionó evidencia que lo acredite.

- No se tiene una plataforma o consola centralizada donde se gestionen y concentren todas las notificaciones de los eventos (accesos inalámbricos no autorizados) relativos a dispositivos y estos notifiquen este tipo de alertas al personal responsable. Derivado de los trabajos de auditoría y con la finalidad de fortalecer y subsanar las áreas de oportunidad en esta materia, el INEGI está llevando a cabo un proceso de adquisición de un Sistema de Gestión en el que se contemplarán estas situaciones.

- No se cuenta con mecanismos para deshabilitar las cuentas que no se encuentran asociadas a algún proceso de negocio o un propietario de la organización. Derivado de los trabajos de auditoría, el INEGI se encuentra ejecutando un análisis para identificar las cuentas que se encuentran en esta situación y señaló que a más tardar el 30 de octubre de 2020 presentará a los administradores de los aplicativos una propuesta para llevar a cabo una depuración de usuarios.

- Se proporcionó el "Proceso de Depuración y Mantenimiento de Cuentas de Usuario y Grupos de Directorio Activo" de fecha 16 de febrero de 2017, el cual no se encuentra formalizado; también se observó que no se ha llevado a cabo actividades de revisión con la finalidad de actualizarlo.

- Se cuenta con una bitácora de autenticación de su infraestructura tecnológica en la que se observan los intentos de acceso a sus cuentas; pero no se puede diferenciar entre las cuentas activas y no activas, a fin de observar los intentos de inicio de sesión con cuentas desactivadas a través de registros de auditoría, tampoco se observó que consideren a los usuarios que presentan un comportamiento anormal en los inicios de sesión.

- No se realizan actividades para verificar errores de entrada incluidos el tamaño, el tipo de datos y los rangos o formatos aceptables para los desarrollos de sistemas informáticos; no se proporcionó evidencia que acredite como se documentan las fases de iniciación, elaboración, modelo de datos, fase de construcción y de transición descritas en el Manual de estándares para el desarrollo de sistemas informáticos en el Instituto Nacional de Estadística y Geografía para los aplicativos o bases de datos desarrollados internamente.

- El personal del área de desarrollo de software carece de capacitación que permita que éstos escriban código seguro para su entorno de desarrollo y responsabilidades específicas; no obstante, derivado de los trabajos de auditoría, el Instituto señaló realizarían un ejercicio para la detección de necesidades de capacitación.

- No se proporcionó documentación formalizada que permita identificar las actividades realizadas por el Instituto para el escaneo de vulnerabilidades al código fuente de sus aplicativos, bases de datos o cualquier desarrollo. Asimismo, no se cuenta con un procedimiento que permita identificar el seguimiento realizado a las vulnerabilidades identificadas en los aplicativos liberados en el ambiente productivo, con la finalidad de mitigar los riesgos que estas brechas de seguridad pudieran provocar en la operación del Instituto.

- Se carece de la documentación que acredite las actividades realizadas por el Instituto para verificar la herramienta para el monitoreo de tráfico y protección para aplicaciones Web, previo a su implementación en el ambiente productivo, con la finalidad de identificar y configurar aquellos huecos de seguridad al ser una herramienta de software libre.

- No se cuenta con un plan formalizado para llevar a cabo la evaluación de seguridad de los componentes de TIC (hardening), que permita garantizar la reducción de vulnerabilidades en la infraestructura del INEGI; asimismo, no se documentan las líneas bases de configuración de seguridad.

- El seguimiento y documentación de los incidentes de seguridad identificados, no se realizan de manera homogénea, debido a que los reportes presentados no son documentados conforme lo establecido en una plantilla o estructura; asimismo, éstos no se encontraban formalizados y no se identificó al personal que participó en el seguimiento y remediación correspondiente.

- El Instituto lleva a cabo pruebas de penetración sobre aplicaciones mediante el uso de herramientas que permiten evaluar contra las mejores prácticas en materia de seguridad; sin embargo, no se cuenta con un calendario de ejecución de pruebas, que permita identificar si éstas fueron realizadas en tiempo y forma, así como su alcance.

- Se carece de la documentación que acredite que las cuentas de los usuarios que ejecutan las pruebas de penetración son temporales y su vigencia corresponde exclusivamente a la fase destinada para el análisis de vulnerabilidades, con la finalidad de garantizar que solo se utilicen para este fin y no se haga mal uso de éstas; tampoco se cuenta con un procedimiento en donde se describa el proceso realizado.

Por lo anterior, se concluye que existen deficiencias en los controles de ciberdefensa implementados en el INEGI, en incumplimiento de lo señalado en el Reglamento Interior del Instituto Nacional de Estadística y Geografía, artículo 46 Bis; Políticas para la seguridad informática. Dirección General de Administración, Dirección General Adjunta de Informática, Apartado V. Políticas Generales, Inciso A. Organización de la Seguridad Informática, numeral 5, inciso f, 6 incisos b, f, h, i, m, n, o, p y t, numeral 10, incisos g, i y k,

numeral 13, incisos c, f y l, inciso B. Administrador de los Activos Informáticos; Lineamientos en materia de tecnologías de la información y comunicaciones del Instituto Nacional de Estadística y Geografía, Coordinación General de Informática, Capítulo VI. Sistema Integral de Seguridad Informática y de Comunicaciones, numeral 90, acciones I, III, IV y V; así como del Manual de Organización Específico de la Coordinación General de Informática, sección V. Atribuciones.

2019-0-40100-20-0094-01-002 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía evalué la viabilidad de implementar herramientas para identificar automáticamente los equipos que se conectan a la red, enlistar y controlar el software que se ejecuta en la infraestructura tecnológica, con la finalidad de contar con un inventario de equipos preciso, que asegure la integridad de los archivos y el control de cambios al software, disminuya los riesgos que pudieran impactar en la óptima operación y manejo de la información en el INEGI; así como para la definición, clasificación, seguimiento y atención de los incidentes de seguridad. Adicionalmente, ejecute análisis de riesgos, de vulnerabilidades y pruebas de penetración periódicamente, a fin de identificar posibles amenazas que pudieran ocasionar una afectación a la confidencialidad, la disponibilidad e integridad de la información del Instituto; implemente mecanismos para remediar las incidencias detectadas en dichos ejercicios para el sistema; establezca una política en donde se definan los puertos y protocolos seguros que deben ser ejecutados en la infraestructura del INEGI, así como la línea base de configuración de seguridad para los equipos de comunicaciones como son Firewalls, Routers y Switches, con la finalidad de prevenir vulnerabilidades asociadas a los puertos y fortalecer las configuraciones de la infraestructura tecnológica para mitigar los impactos de las posibles amenazas.

2019-0-40100-20-0094-01-003 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía implemente los controles y acciones necesarias en relación con los servicios de Internet y correo electrónico, para asegurar que únicamente los navegadores y clientes de correo electrónico autorizados se ejecuten en el Instituto y que cualquier plugin o aplicación add-on sea desinstalado o deshabilitado; lleve a cabo la implementación del servicio de filtrado del Sistema de Nombres de Dominio (DNS) para ayudar a bloquear el acceso a dominios maliciosos conocidos; instrumente las acciones en materia de seguridad y protección contra ataques, que permitan realizar regularmente escaneos automatizados de puertos, para garantizar que sólo los puertos y protocolos aprobados sean ejecutados, con la finalidad de prevenir las vulnerabilidades asociadas a los puertos y los diferentes ataques que puede sufrir el Instituto en caso de contar con alguno de éstos abierto; defina, documente y formalice la configuración segura para todos los equipos de red, con la cual se puedan descubrir y alertar las desviaciones identificadas en los equipos del Instituto; lleve a cabo regularmente escaneos desde el exterior del borde de cada red de confianza para detectar cualquier conexión no autorizada accesible a través del borde; finalmente, continúe con los esfuerzos

para la implementación de herramientas de monitoreo de Integridad de Archivos o de administración de eventos y seguridad de la información (SIEM).

2019-0-40100-20-0094-01-004 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía revise y en su caso actualice los criterios para la clasificación de activos de información, así como el listado de activos de información crítica por lo menos una vez al año; configure la herramienta para la prevención de pérdida de datos (DLP) con base en el listado de activos de información crítica establecido; y considere segmentar la red según el nivel de clasificación de la información almacenada en los servidores y cifrar la información sensible tanto en tránsito, como en reposo; asimismo, establezca una periodicidad para la ejecución de respaldos e implemente mecanismos para la verificación de las copias de seguridad, para que en caso de que se presenten errores, se definan las acciones necesarias a fin de corregirlos y garantizar que la información se encuentre íntegra y disponible en caso de requerirla.

5. Continuidad de TIC y Centro de Datos

Antecedentes

En la fiscalización de la Cuenta Pública 2016, en la auditoría número 119-GB se emitieron dos recomendaciones (16-0-40100-02-0119-01-009 y 16-0-40100-02-0119-01-010) al Instituto Nacional de Estadística y Geografía, relacionadas con el proceso de Continuidad de las TIC, en las cuales se sugirió al Instituto implementar mecanismos de control y las acciones necesarias para la instrumentación del Análisis de Impacto al Negocio (BIA), Plan de Continuidad de Negocio (BCP) y Plan de Recuperación en caso de Desastres (DRP), con la finalidad de garantizar una óptima continuidad operativa de los procesos, aplicativos sustantivos e infraestructura tecnológica del Instituto; así como documentar un plan de capacidad de la infraestructura tecnológica, que garantice que todos los servicios de TI cuenten con un correcto dimensionamiento de procesamiento y almacenamiento con la finalidad de que los recursos sean aprovechados adecuadamente y que éstos aseguren los niveles de servicio requeridos para una óptima operación del Instituto.

Por lo anterior, en la Cuenta Pública 2019, durante la revisión de las actividades mencionadas se verificaron las condiciones, esfuerzos y avances que el Instituto ha llevado a cabo con relación a la continuidad de las operaciones de TIC para garantizar la disponibilidad de la información y sus servicios. En el análisis realizado se observó lo siguiente:

Continuidad de la Operación

- El INEGI se encuentra trabajando en el desarrollo del Sistema de Gestión de Continuidad Institucional (SGCI), por lo que cuenta con un cronograma de las actividades para la implementación de éste; en dicho cronograma se observó a la fecha de la auditoría (agosto de 2020) un avance del 65.0% y la fecha de conclusión

se estableció hasta el primer trimestre del 2022. Por lo anterior, el Instituto se encuentra en proceso de determinar los criterios que le permitirán definir los productos y activos esenciales, y por lo tanto, carece de un catálogo de servicios de TIC actualizado; asimismo, se encuentra trabajando en el "Manual de Administración de las Tecnologías de Información y Comunicaciones en el INEGI", en el cual se contemplará la administración de los servicios; sin embargo, en éste no se establece la frecuencia en la que se revisará y actualizará dicho catálogo.

- Como acción derivada de los trabajos de auditoría (agosto 2020), la Coordinación General de Informática (CGI) actualizó el listado de los responsables de servicios informáticos. Dicho listado no había sido actualizado desde su emisión en 2011.

- Durante 2019 no se realizaron pruebas para la estrategia de "sede alterna", a fin de identificar áreas de oportunidad a sus controles compensatorios.

- No se identificó documentación que permita verificar la gestión de los activos críticos del Instituto, así como los controles implementados para su protección con la finalidad de mitigar riesgos y amenazas para asegurar su correcto funcionamiento.

- Debido a que se carece de la identificación de los productos y servicios esenciales, no se cuenta con las bases para la determinación del análisis de impacto al negocio (BIA) definido en conjunto con las áreas de negocio del Instituto, en el que se identifiquen todas las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona el INEGI que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC. El Instituto señaló que se encuentra en el proceso de ejecución de una prueba piloto para cuatro productos esenciales, la cual inició en el segundo semestre de 2019, con sus resultados (esperados para el segundo semestre del 2020) les permitirá elaborar un análisis de impacto al negocio (BIA) para estos cuatro productos; sin embargo, no se proporcionó documentación en la que se muestren los avances.

- Se proporcionaron las estrategias implementadas con relación a la continuidad operativa del Instituto; sin embargo, datan del año 2016 y 2018, por lo que no se tiene certeza de si éstas contemplan los procesos e infraestructura de hardware y software con la que cuenta actualmente el INEGI. Adicionalmente, no se tiene implementado un Plan de Continuidad de Negocio (BCP), que permita identificar y proteger sus procesos críticos en caso de presentarse alguna contingencia.

- Se identificó que, si bien el INEGI cuenta con algunos controles compensatorios implementados para la continuidad operativa, en donde se tiene contemplado una estrategia de traslado a sede alterna, así como esquemas de redundancia para los centros de datos; carece de la definición e implementación de un Plan de Recuperación de Desastres (DRP), el cual, en caso de presentarse alguna

contingencia (siniestro, desastre) que imposibilite el funcionamiento de los recursos informáticos en forma parcial o total, reduzca al máximo sus efectos y establezca las actividades, tiempos, personal y activos que permitan reanudar rápidamente los servicios críticos del Instituto.

- No se cuenta con mecanismos para identificar los impactos cuantitativos de las contingencias operativas en el SGCI, el INEGI indica que se integrará en la metodología para el BIA; sin embargo, ésta aún no ha sido desarrollada.

De la revisión de los controles de los planes de Continuidad de las Operaciones de TIC, se concluye que los principales riesgos por la carencia o inconsistencia de éstos y sus consecuencias potenciales para las operaciones y activos del INEGI son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA DE CONTROLES DE CONTINUIDAD DE LAS OPERACIONES

Factor crítico	Riesgo
Definición del Análisis de Impacto al Negocio (BIA), Plan de Continuidad de Negocio (BCP) y Plan de Recuperación de Desastres (DRP)	Al carecer de la implementación de un Análisis de Impacto al Negocio y los planes de continuidad y recuperación de desastres, no es posible estimar la afectación que podría padecer el Instituto como resultado de la ocurrencia de algún incidente o un desastre, debido a que no se tendrían identificados los posibles impactos que pudiera sufrir, lo que no permite establecer acciones preventivas ni planes para la recuperación de sus operaciones críticas, en caso de que se presente la interrupción de uno o más servicios de TIC.
Activos críticos, productos y servicios esenciales	La falta de la identificación de los procesos críticos y activos de información representa un riesgo de que el Instituto no implante de manera adecuada los controles que aseguren la disponibilidad, confidencialidad e integridad de los activos de información crítica.

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

Centro de Datos

En la revisión a la documentación proporcionada por el INEGI relacionada con sus Centros de Datos se identificó lo siguiente:

- Se carece de una matriz de riesgos del Centro de Datos formalizada, en la que se definan los riesgos lógicos, físicos y ambientales, así como su impacto en la operación del Instituto.

- No se identificó que los lineamientos para la atención de incidentes de ambiente físico del Centro de Datos se encuentren formalizados, y en éstos no se observó la descripción de las actividades por realizar, el personal responsable de su aplicación y tampoco se cuenta con evidencia de su difusión.

- El INEGI indicó que el Centro de Datos cuenta con mecanismos de protección contra incendios; sin embargo, no se tienen paneles y ductos resistentes al fuego.

- Durante 2019 los detectores de humo no se encontraban operando; sin embargo, a raíz de los trabajos de auditoría se activó el sistema de detección de incendios, del cual no se cuenta con documentación que acredite si se le ha dado mantenimiento; adicionalmente, se entregó evidencia de la solicitud de investigación de mercado para iniciar el proceso de adquisición de un sistema inalámbrico de detección y alertamiento de incendios.

- No se cuenta con los Manuales de Operación de dispositivos para evitar, detectar o corregir los riesgos físicos del centro de cómputo.

- No se proporcionó el procedimiento para ingresar, instalar y configurar un dispositivo en el Centro de Datos; tampoco se acreditó que se realizó el borrado seguro en los equipos retirados del centro de cómputo.

Por lo tanto se concluye que existen deficiencias en el Centro de Datos relacionadas con la implementación de mecanismos de detección y control de incendios; se carece de políticas o lineamientos relacionados con la atención de incidentes de ambiente físico, para el ingreso, instalación, configuración y retiro de dispositivos del Centro de Datos, así como de Manuales de Operación de dispositivos, en incumplimiento de lo establecido en el Reglamento Interior del Instituto Nacional de Estadística y Geografía, artículo 46 Bis, apartados III y IX; el Manual de Organización Especifico de la Coordinación General de Informática, Sección V. Atribuciones, fracciones V y VII, función número 3 de la Subdirección de Administración de la Infraestructura de Cómputo; funciones números 4 y 9 del Departamento de Operación y Monitoreo de Servidores; los Lineamientos en Materia de Tecnologías de la Información y Comunicaciones del Instituto Nacional de Estadística y Geografía de la Coordinación General de Informática, artículos 28, fracción XV; 88, fracciones I, II, IV y V; 90, fracción IV; así como de las Políticas en materia de Tecnologías de la Información y Comunicaciones del Instituto Nacional de Estadística y Geografía de la Coordinación General de Informática, Apartado IV. Políticas Generales Cuadragésima Primera, Cuadragésima Segunda y Cuadragésima Tercera; las Políticas para la Seguridad Informática, Dirección General de Administración, Dirección General Adjunta de Informática, Apartado V. Políticas Generales, inciso A. Organización de la Seguridad Informática, numeral 10, inciso b, el numeral 13, incisos i, m, n, o, el numeral 14, inciso d; y el inciso E. Seguridad de los Servicios Informáticos del INEGI, numeral 6, inciso f.

2019-0-40100-20-0094-01-005 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía continúe con los esfuerzos para concluir con las acciones necesarias para desarrollar un Análisis de Impacto al Negocio (BIA) que considere la totalidad de las actividades que permita identificar los tipos de impacto, así como las afectaciones y consecuencias sobre los procesos críticos, a partir del cual se defina un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación en caso de Desastres (DRP), así como realizar las pruebas a los mismos, que aseguren que se cuenta con la capacidad suficiente de recuperación en caso de presentarse un desastre que ocasione la interrupción de las operaciones.

2019-0-40100-20-0094-01-006 **Recomendación**

Para que el Instituto Nacional de Estadística y Geografía le dé mantenimientos a los mecanismos de control de incendios del Centro de Datos; defina, actualice e implemente políticas o lineamientos de seguridad física y lógica para los Centros de Datos, en los que se considere la atención de incidentes del ambiente físico, el ingreso, instalación, configuración y retiro del equipamiento tecnológico.

Buen Gobierno

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

Resumen de Resultados, Observaciones y Acciones

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

6 Recomendaciones.

Dictamen

El presente se emite el 12 de octubre de 2020**,** fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar la gestión financiera de las contrataciones relacionadas con las TIC, su adecuada gobernanza, administración de riesgos, seguridad de la información, continuidad de las operaciones, calidad de datos, desarrollo de aplicaciones y aprovechamiento de los recursos asignados en procesos y funciones, así como comprobar que se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada que se establece en el apartado relativo al alcance, se concluye que, en términos generales, el Instituto Nacional de Estadística y Geografía (INEGI) cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- El presupuesto ejercido del Estado Analítico del Ejercicio del Presupuesto de Egreso no reconoce los compromisos devengados no pagados al cierre del ejercicio, por lo que el presupuesto devengado y ejercido no son consistentes. Asimismo, existen áreas de las que no fue posible identificar su relación con las labores de TIC; sin embargo, se encuentran registradas en la plantilla de personal de TIC del Instituto.

- Se identificaron deficiencias en la administración y operación de los controles de Ciberseguridad para la infraestructura de hardware y software del Instituto, relacionadas con las directrices, infraestructura y herramientas informáticas en esta materia.

- El INEGI se encuentra trabajando en el desarrollo del Sistema de Gestión de Continuidad Institucional (SGCI), por lo que cuenta con un cronograma de las actividades para la implementación de éste; en dicho cronograma se observó a la fecha de la auditoría (agosto de 2020) un avance del 65.0% y la fecha de conclusión se estableció hasta el primer trimestre del 2022; por lo que no se cuenta con un Análisis de Impacto al Negocio (BIA) que considere la totalidad de las actividades que permita identificar los tipos de impacto, así como las afectaciones y consecuencias sobre los procesos críticos, a partir del cual se defina un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación en caso de Desastres (DRP), así como realizar las pruebas a los mismos, que aseguren que se cuenta con la capacidad suficiente de recuperación en caso de presentarse un desastre que ocasione la interrupción de las operaciones.

- Se carece de políticas o lineamientos relacionados con la atención de incidentes de ambiente físico, para el ingreso, instalación, configuración y retiro de dispositivos del Centro de Datos, así como de Manuales de Operación de dispositivos.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
C. Jazmín Gabriela Pantoja Soto	Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que para los Capítulos del gasto relacionados con las TIC, las cifras reportadas en la Cuenta Pública correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; Analizar 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 comprenda el análisis de las contrataciones vigentes; la determinación de la procedencia de su renovación; la pertinencia de realizar contrataciones consolidadas; los costos de mantenimiento, soporte y operación que impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

3. Verificar el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio de acuerdo a 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 estén debidamente soportados, cuenten con controles que permitan su fiscalización, correspondan a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como 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.

7. Verificar la gestión de los programas de continuidad de las operaciones; Evaluación de la seguridad física y lógica del Centro de Datos principal (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, DRP, estándares).

Áreas Revisadas

Las direcciones generales de Administración, de Geografía y Medio Ambiente; de Estadísticas Sociodemográficas; y de Vinculación, Servicio Público de Información y Relaciones Institucionales; las direcciones generales adjuntas de Administración de Riesgos y Transparencia; de Recursos Materiales y Servicios Generales; de Programación, Organización y Presupuesto; de Integración de Información Geoespacial, Difusión y Servicio Público de Información; y del Censo de Población y Vivienda; la Coordinación General de Informática; así como las direcciones de Planeación y Normatividad Informática, Cómputo y Comunicaciones; de Seguridad Informática; y de Provisión de Bienes y Servicios Informáticos del Instituto Nacional de Estadística y Geografía.

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. Ley General de Contabilidad Gubernamental: Art. 4 Frac. XVI y XVII.

2. Otras disposiciones de carácter general, específico, estatal o municipal: Acuerdo por el que se emiten las normas y metodología para la determinación de los momentos contables de los egresos publicado por el Consejo Nacional de Armonización Contable (CONAC); Contrato CA/09/CGI/2019, cláusula Quinta; Manual de Organización Específico de la Coordinación General de Informática, apartado V. Atribuciones de la Coordinación General de Informática, Frac. XIV, V y VII; y funciones 1 y 2 asignadas al Departamento de Distribución de Activos Informáticos, función número 3 de la Subdirección de Administración de la Infraestructura de Cómputo; funciones números 4 y 9 del Departamento de Operación y Monitoreo de Servidores; Reglamento Interior del Instituto Nacional de Estadística y Geografía, Art. 46 Bis; Políticas para la seguridad informática, Dirección General de Administración, Dirección General Adjunta de Informática, Apartado V. Políticas Generales, Inciso A. Organización de la Seguridad Informática, Numeral 5 inciso f, numeral 6 incisos b ,f , h, i, k, m, n, o, p y t, numeral 10 incisos b, g, i y k, numeral 13 incisos c, f, i, l, m, n, o, numeral 14, inciso d; Inciso B. Administrador de los Activos Informáticos; inciso E.- Seguridad de los Servicios

Informáticos del INEGI, numeral 6 inciso f; Lineamientos en materia de tecnologías de la información y comunicaciones del Instituto Nacional de Estadística y Geografía, Coordinación General de Informática, Art. 28 Frac. XV; Art. 88 Frac. I, II, IV y V; Art. 90 Frac. IV; Capítulo VI. Sistema Integral de Seguridad Informática y de Comunicaciones, Numeral 90, acciones I, III, IV y V; Políticas en materia de Tecnologías de la Información y Comunicaciones del Instituto Nacional de Estadística y Geografía de la Coordinación General de Informática, Apartado IV. Políticas Generales, Cuadragésima primera, Cuadragésima Segunda y Cuadragésima Tercera.

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.