Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2021-0-44100-20-0176-2022

Modalidad: Presencial

Núm. de Auditoría: 176

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 2021 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.

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	64,956.2
Muestra Auditada	13,672.1
Representatividad de la Muestra	21.0%

El universo seleccionado por 64,956.2 miles de pesos corresponde al total de pagos ejercidos en los contratos relacionados con las Tecnologías de Información y Comunicaciones (TIC) en el ejercicio fiscal de 2021. La muestra auditada está integrada por dos contratos que corresponden al Servicio de Terciarización de Servicios de Soporte a Infraestructura, Desarrollo, Seguridad, Mantenimiento y Soporte a Aplicativos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y a los Servicios de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia, con pagos ejercidos por 13,672.1 miles de pesos, que representan el 21.0% del universo seleccionado, registrados en el Tomo VI “Órganos Autónomos” de la Cuenta Pública de 2021.

Adicionalmente, la auditoría comprende la revisión de Ciberseguridad, Continuidad de las Operaciones y el Ciberataque a la Plataforma Nacional de Transparencia (PNT).

Antecedentes

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo público autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales; para el primero, garantiza que cualquier autoridad en el ámbito federal, órganos autónomos, partidos políticos, fideicomisos, fondos públicos y sindicato; o cualquier persona física, moral que reciba y ejerza recursos públicos o realice actos de autoridad entregue la información pública que la ciudadanía solicite; para el segundo, garantiza el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información.

La misión del INAI es garantizar los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa en el estado mexicano.

El INAI administra la Plataforma Nacional de Transparencia (PNT), que es una plataforma electrónica que permite cumplir con los procedimientos, obligaciones y disposiciones establecidas en las leyes en materia de transparencia, y atiende a las necesidades de accesibilidad de los usuarios.

Los lineamientos de la funcionalidad, operación y mejoras de la PNT establecen, entre otros, que:

- Artículo 12. En el caso de que la Plataforma Nacional presente una falla técnica, el Instituto, como administrador de ésta, deberá hacer del conocimiento de los Organismos Garantes y Sujetos Obligados la magnitud de la falla y el tiempo de recuperación, para que se encuentren en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas responsabilidades.

- Artículo 21. El administrador general deberá contar con la infraestructura necesaria para el mantenimiento y correcta funcionalidad de la PNT.

- Artículo 71. El administrador general, por mutuo propio o a petición de la Comisión de Tecnologías o de los Organismos Garantes, podrá desarrollar e implementar proyectos tecnológicos que aprovechen la información contenida en los sistemas que conforman la PNT, sin poner en riesgo su funcionalidad, seguridad y protección de los datos personales que ésta contiene.

La PNT está integrada por cuatro sistemas, de conformidad con lo previsto en el artículo 50 de la Ley General de Transparencia y Acceso a la Información Pública y son los siguientes:

- Sistema de portales de obligaciones de transparencia (SIPOT).
- Sistema de solicitudes de acceso a la información (SISAI).
- Sistema de gestión de medios de impugnación (SIGEMI).
- Sistema de comunicación entre Organismos Garantes y Sujetos Obligados (SICOM).

Durante la fiscalización superior de la Cuenta Pública 2016 se llevó a cabo en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, la auditoría número 129-GB con título "Plataforma Nacional de Transparencia", en donde se validaron dos contratos relacionados con el desarrollo de dicha plataforma.

Entre los años de 2017 y 2021, en el INAI se han invertido 349,386.9 miles de pesos en materia de Tecnologías de la Información, como se detalla a continuación:

RECURSOS EROGADOS EN MATERIA DE TIC EN EL INAI

(Miles de pesos)

Periodo de Erogación	2017	2018	2019	2020	2021	Total
Monto por Año	61,845.2	82,460.6	68,279.6	71,845.3	64,956.2	349,386.9

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

NOTA: Diferencias por redondeo

En el análisis de la gestión de las tecnologías de información y comunicaciones, efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados, con el fin de verificar si son suficientes para el cumplimiento de los objetivos de las contrataciones y funciones de las TIC sujetas a 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 2021, publicado en el Diario Oficial de la Federación (DOF) el día 30 de noviembre de 2020, al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se le aprobó un presupuesto de 905,335.6 miles de pesos.

En el análisis de la información presentada en la Cuenta de la Hacienda Pública Federal en el ejercicio de 2021, se identificó un presupuesto ejercido en el capítulo 3000 "Servicios

Generales" de 166,633.6 miles de pesos, del cual se erogaron 64,956.2 miles de pesos correspondientes a recursos relacionados con las Tecnologías de Información y Comunicaciones (TIC), lo que representa el 21.0% del presupuesto ejercido, como se muestra a continuación:

RECURSOS EJERCIDOS EN CONTRATACIONES RELATIVAS A LAS TIC EN EL INAI DURANTE 2021

(Miles de pesos)

Presupuesto aprobado	Capítulo	Descripción	Presupuesto Ejercido	Recursos ejercidos en materia de TIC
905,335.6	3000	Servicios Generales	166,633.6	64,956.2
		TOTAL	**166,633.6**	**64,956.2**

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

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

Los recursos ejercidos en materia de TIC por 64,956.2 miles de pesos se integran de la manera siguiente:

GASTOS EN MATERIA DE TIC EN EL INAI DURANTE 2021

(Miles de pesos)

Capítulo Partida		Descripción	Presupuesto pagado
3000		**SERVICIOS GENERALES**	
	31603	Servicios de internet	0.6
	31904	Servicios integrales de infraestructura de cómputo	4,548.3
	32301	Arrendamiento de equipo y bienes informáticos	10,432.7
	32303	Arrendamiento de equipo de telecomunicaciones	14,685.1
	32701	Patentes, derechos de autor, regalías y otros	23,236.2
	33301	Servicios de desarrollo de aplicaciones informáticas	4,717.3
	33304	Servicios de mantenimiento de aplicaciones informáticas	6,821.5
	34601	Almacenaje, embalaje y envase	37.1
	35301	Mantenimiento y conservación de bienes informáticos	477.4
		TOTAL	**64,956.2**

FUENTE: Elaborado con información proporcionada por el INAI.

NOTA: Diferencias por redondeo.

Del universo seleccionado en 2021 por 64,956.2 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 13,672.1 miles de pesos en dos contratos que representan el 21.0% del universo seleccionado, los cuales se integran de la siguiente forma:

MUESTRA DE LOS PAGOS EJERCIDOS EN LOS CONTRATOS RELACIONADOS CON LAS TIC DURANTE 2021
(Miles de pesos)

Proceso de Contratación	Contrato	Proveedor	Objeto del Contrato	Vigencia		Monto		Pagos en 2021
				De	Al	Mínimo	Máximo	Total
Licitación pública de carácter nacional con número de clave interna LPN-04421099-022-2020 y clave electrónica LA-04421099-E40-2020 conforme a lo dispuesto en los artículos 26, fracción I, y 47 del Reglamento de adquisiciones, arrendamientos y servicios del INAI.	OA/C005/ 2021	Negocios Digitales, S.A. de C.V. en participación conjunta con Endeavor Technologies Systems, S.A. de C.V.	Servicio de Terciarización de Servicios de Soporte a Infraestructura, Desarrollo, Seguridad, Mantenimiento y Soporte a Aplicativos del INAI	01/01/2021	31/12/2021	4,142.4	10,356.0	12,426.8
	CM del Contrato OA/C005/ 2021		Ampliación de monto del contrato OA/C005/2021	01/01/2021	31/12/2021	N/A	2,071.2	
					Subtotal	4,142.4	12,427.2	12,426.8
Licitación Pública de carácter nacional con número de identificación electrónica LA-006HHE001-E65-2017 y número interno LPN-006HHE001-013-17, conforme a lo dispuesto en los artículos 3, fracción VIII, 23, fracción I, 24, fracción II, 25, tercer párrafo, 26, fracción I, 27, 29, primer párrafo y 47, del Reglamento de Adquisiciones, Arrendamientos y Servicios del INAI.	OA/C036/17	Raxo Telecomunicaciones, S.A. de C.V.	Servicios de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia	07/11/2017	06/11/2020	5,976.0	14,940.0	N/A
	Primer CM del Contrato OA/C036/17		Ampliación de vigencia y monto del contrato OA/C036/17	07/11/2020	31/01/2021	N/A	1,171.6	414.3
	Segundo CM del Contrato OA/C036/17		Ampliación de vigencia y monto del contrato OA/C036/17	01/02/2021	31/03/2021	N/A	830.0	831.0
					Subtotal	**5,976.0**	**16,941.6**	**1,245.3**
					Total	**10,118.4**	**29,368.8**	**13,672.1**

FUENTE: Contratos y facturas proporcionadas por el INAI.

NOTA: Diferencias por redondeo

Se verificó que los pagos provenientes de recursos presupuestales se reconocieron en las partidas presupuestarias correspondientes. El análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

2. Contrato número OA/C005/2021, Servicio de Tercerización de Servicios de Soporte a Infraestructura, Desarrollo, Seguridad, Mantenimiento y Soporte a Aplicativos del INAI

Se revisó el contrato número OA/C005/2021 suscrito con ND Negocios Digitales, S.A. de C.V., en participación conjunta con Endeavor Technologies Systems, S.A. de C.V., mediante un procedimiento de contratación por Licitación Pública Nacional, con fundamento en los artículos 26, fracción I, y 47, del Acuerdo mediante el cual se aprueba el Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (RAAS).

La vigencia del contrato fue del 1 de enero al 31 de diciembre de 2021, por un monto mínimo de 4,142.4 miles de pesos y un máximo de 10,356.1 miles de pesos, con el Impuesto al Valor Agregado (IVA) incluido, con el objeto de prestar el Servicio de Tercerización de Servicios de Soporte a Infraestructura, Desarrollo, Seguridad, Mantenimiento y Soporte a Aplicativos del INAI. El 6 de agosto 2021 se llevó a cabo el primer y único convenio modificatorio del contrato número OA/C005/2021 con el fin de ampliar el monto del contrato por 2,071.2 miles de pesos. Durante el ejercicio de 2021, se pagaron 12,426.8 miles de pesos. En el análisis de esta contratación se determinó lo siguiente:

Objetivo

Permitir al INAI la tercerización de servicios profesionales de informática en un concepto de servicios bajo demanda, para operar alineado a marcos de referencia, metodologías, mejores prácticas y estándares internacionales en materia de servicios de información y gobernabilidad.

Alcance de los servicios

Permitir a la Dirección General de Tecnologías de la Información (DGTI) del INAI fortalecer el cumplimiento de sus funciones establecidas en el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, donde destacan las siguientes:

- Coadyuvar en el desarrollo, administración, implementación, funcionamiento, estabilidad y seguridad de la Plataforma Nacional de Transparencia (PNT), de conformidad con la normativa que establezca el Sistema Nacional.

- Apoyar a las diferentes unidades administrativas del instituto, en la automatización de los procesos sustantivos, mediante el desarrollo o implementación de sistemas de información y comunicaciones.

Descripción del Servicio

- Servicio de Dirección del Proyecto.

- Servicios de Soporte, Mantenimiento y Desarrollo de Aplicativos.
- Servicios de Soporte de Infraestructura.
- Servicios de Monitoreo de Niveles de Seguridad.
- Servicios de Administración de Bases de Datos (BD).
- Servicios de Administración Mesa de Ayuda y Procedimientos.
- Servicios de Transferencia Tecnológica.

Investigación de Mercado

La investigación de mercado no cuenta con fecha de elaboración, ni con el nombre y la firma del personal con las facultades para su realización.

Pagos

- No se cuenta con los oficios de provisión de pago de enero a noviembre de 2021.

Revisión técnica y funcional de los servicios

Servicio de dirección del proyecto

- El anexo técnico no estableció entregables o reportes detallados que permitieran identificar que se ejecutaron la totalidad de las actividades solicitadas para este servicio.

Servicios de soporte, mantenimiento y desarrollo de aplicativos

Este rubro contempló dos tipos de elementos: “Servicio de continuidad operativa” (diagnósticos, correcciones o mejoras menores en los elementos de aplicaciones productivas del INAI) y “Servicio de desarrollo y mantenimiento de aplicaciones de software” (gestión de proyectos de desarrollo de nuevas aplicaciones o mantenimientos), respecto de los cuales se observó lo siguiente:

Servicio de continuidad operativa

- A la fecha de la revisión (agosto de 2022), la DGTI no contó con la base de datos de las solicitudes generadas que debieron ser almacenadas en la herramienta de gestión de tickets, aun cuando era una obligación del proveedor exportarla, con base en lo especificado en el anexo técnico del contrato.
- Se identificaron diferencias en las horas reportadas en los informes ejecutivos mensuales para dos perfiles.

Servicio de desarrollo y mantenimiento de aplicaciones de software

- No se solicitó al proveedor realizar pruebas integrales y de seguridad al desarrollo, acorde con lo especificado en el anexo técnico del contrato.

- El INAI avaló el cumplimiento de los desarrollos conforme a los puntos específicos de codificación segura sin que contara con evidencia.

- El INAI no cuenta con una metodología de desarrollo donde se especifique, de acuerdo con la complejidad y al nivel de riesgo de los aplicativos, la ejecución de un análisis de seguridad de aplicaciones que incluya pruebas de penetración, análisis de vulnerabilidades y de codificación segura. El INAI formalizó el documento "Proceso de atención de requerimientos de desarrollo y mantenimiento de aplicaciones" en diciembre de 2021, por lo que su cumplimiento durante el ejercicio de 2021 no fue verificado.

Servicios de transferencia tecnológica

- El anexo técnico estableció que el proveedor debió entregar la documentación soporte de la transferencia tecnológica y llevar a cabo sesiones teórico-prácticas con personal de la DGTI; no obstante, no documentó los servicios, por lo que no se tiene evidencia de su prestación al instituto.

Servicios de soporte de infraestructura

- La DGTI no presentó evidencia de la definición conjunta de los entregables del servicio con el proveedor mediante mesas de trabajo, tal como se estableció en el anexo técnico.

- Al término del contrato, el proveedor debía depositar la información generada en el repositorio del INAI; no obstante, no fue realizado.

Servicio de monitoreo de niveles de seguridad

- La DGTI no demostró que el proveedor haya utilizado herramientas de análisis de vulnerabilidades y pruebas de intrusión para la prestación del servicio.

- Los nueve reportes realizados en septiembre, octubre y diciembre de 2021 para la verificación y análisis de vulnerabilidades a los sitios web del instituto carecen de elementos que indiquen que se generaron por alguna herramienta para estos fines, sin que se cuente con elementos para acreditar la prestación del servicio.

- La DGTI no documentó la atención de las vulnerabilidades presentadas en los reportes entregados por el proveedor ni ejecutó nuevamente un análisis para asegurar su remediación.

- La DGTI presentó los reportes de los análisis de vulnerabilidades a los aplicativos; sin embargo, se realizaron en los últimos cuatro meses del contrato, por lo que de enero a agosto de 2021 no se cuenta con evidencia de su prestación.

- Los reportes mensuales del monitoreo y el análisis de vulnerabilidades no contaron con el soporte documental de las actividades de supervisión conforme a lo solicitado en el anexo técnico.

- El anexo técnico estableció el concepto “apoyo” por parte del proveedor para la generación del marco normativo de seguridad del instituto; sin embargo, no definió el alcance del mismo.

Servicio de administración de bases de datos

- La herramienta de inteligencia de negocio no se utilizó durante 2021, por lo que este servicio no se aprovechó aun cuando fue requerido contractualmente.

- El control de cambios de las bases de datos fue establecido como responsabilidad del proveedor; sin embargo, la DGTI carece de evidencia de dicho control.

Servicios de administración mesa de ayuda y procedimientos

- No se cuenta con evidencia de la utilización de la herramienta Altiris y su integración con la mesa de ayuda.

- El proveedor no exportó la base de datos de la mesa de servicios a una base de datos compatible con Microsoft SQL, por lo cual se carece de evidencia de los tickets generados durante el servicio.

- Se carece del soporte de la administración de la consola de antivirus.

- El anexo técnico estableció que la administración de la consola antivirus se realizaría sobre un total de 1,068 equipos tipo escritorio o laptop; sin embargo, en los reportes proporcionados de febrero a diciembre de 2021, se contabilizaron 592 equipos encendidos mientras que 344 se encontraron inactivos, los 132 restantes no reportaron ningún estatus debido a un largo periodo de inactividad; en consecuencia, sólo se utilizó el 55.4% de la capacidad que fue requerida por la DGTI. Asimismo, el administrador del contrato no elaboró un plan de acción para reactivarlos a fin de contar con las actualizaciones que los proteja contra software malicioso.

- El documento "Reporte de inventario de equipos del INAI" contempló un listado de equipos tecnológicos (pc, laptops, tabletas), se identificó que los campos del inventario no cuentan con nombre, contienen registros vacíos y tienen información incompleta.

- El proveedor Endeavor Technologies Systems, S.A. de C.V., no presentó documentación del cumplimiento de la metodología ITIL (*Information Technology Infrastructure Library*,

por sus siglas en inglés) para la mesa de servicio, requerido por el INAI en el anexo técnico.

Adicionalmente, se identificó lo siguiente:

- La DGTI carece de la evidencia de la evaluación de las capacidades de los recursos humanos del proveedor para cada uno de los perfiles solicitados.

- La actualización de las líneas base de las aplicaciones institucionales no cuentan con mecanismos de verificación que permitan identificar su versión, su fecha de elaboración y a los responsables, además de no estar estandarizadas.

- La política de respaldos utilizada por el proveedor no cuenta con la revisión y aprobación por parte del personal autorizado del INAI.

- La cláusula Décima Quinta "Penas convencionales" del contrato número OA/C005/2021, no contempla la aplicación de penalizaciones en caso de que el proveedor no entregue los servicios con la calidad requerida.

Por lo anterior, se concluye que:

Se identificaron áreas de oportunidad en la supervisión de la DGTI del INAI en la ejecución y entrega de los servicios brindados por los proveedores. ya que en sólo dos servicios se establecieron mejores prácticas y para los cinco servicios restantes el proveedor no demostró haber utilizado algún marco de referencia conforme a lo requerido en el contrato.

El director del proyecto firmó los entregables de los servicios de "Monitoreo de niveles de seguridad" y "administración mesa de ayuda y procedimientos" sin que éstos cumplieran con la calidad y las especificaciones solicitadas en el anexo técnico.

Se observaron pagos injustificados por 3,416.9 miles de pesos al proveedor Endeavor Technologies Systems, S.A. de C.V., debido a la falta de evidencia que justifique que se realizaron las actividades siguientes: análisis de vulnerabilidades, pruebas de intrusión, borrado seguro y el monitoreo de equipos de seguridad relacionadas con el servicio de "Monitoreo de Niveles de Seguridad" y las actividades relacionadas con la "Administración Mesa de Ayuda y Procedimientos" las cuales son: la atención a llamadas, el registro de solicitudes de atención y solución de incidentes y requerimientos mediante el uso de la herramienta de registro y administración (Altiris) y la atención y solución vía telefónica a solicitudes de incidentes y requerimientos que no requieran de asistencia en sitio y cuando si se requiera, mismas que no fueron proporcionadas de acuerdo a lo solicitado por el instituto mediante el contrato número OA/C005/2021 y su anexo técnico. Lo anterior incumplió el artículo 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria publicado en el Diario Oficial de la Federación el 28 de junio de 2006 y su última reforma publicada en el mismo medio el 13 de noviembre de 2020; el artículo 48, fracciones VII, X, XIII y XIX, del Acuerdo mediante el cual se aprueba el Estatuto

Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el Diario Oficial de la Federación el 17 de enero de 2017, y sus reformas publicadas en el mismo medio de difusión oficial al 23 de septiembre de 2020; la declaración I.4, cláusulas primera, segunda, séptima y octava, del contrato número OA/C005/2021; los numerales 3 Objetivo, 4 Beneficios esperados, 5 Alcance, 5.4 Servicio de monitoreo de niveles de seguridad, 5.6 Servicio de Administración mesa de ayuda y procedimientos, 8.4 Servicio de administración de mesa de ayuda y 12 'Entregables del proyecto', del anexo técnico del contrato número OA/C005/2021, y funciones 4, 7, 9, 11 y 14, de la Dirección General de Tecnologías de la Información, del Manual de Organización del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el 16 de febrero de 2021.

2021-0-44100-20-0176-01-001 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en futuras contrataciones de tecnologías de información y comunicaciones, analice la viabilidad de incluir en la documentación de notificación de fallo la relación de licitantes cuyas proposiciones se desecharon, y se expresen todas las razones legales, técnicas o económicas que sustentaron tal determinación; asimismo, se indiquen los puntos específicos de la convocatoria incumplidos con el fin de identificar al proveedor que resulte viable técnica y económicamente para la prestación de los servicios.

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.

2021-0-44100-20-0176-01-002 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en futuras contrataciones en materia de tecnologías de información y comunicaciones relacionadas con el desarrollo o mantenimiento de aplicativos, implemente procedimientos que garanticen el cumplimiento de las mejores prácticas del ciclo de vida de desarrollo de software, y se documenten cada una de las etapas de las metodologías utilizadas; que se definan contractualmente los entregables para todos los servicios requeridos; que se implementen los mecanismos de control que le permitan asegurar que, a pesar de que exista un cambio de proveedores, se resguarde la información de las actividades ejecutadas en sus sistemas y herramientas empleadas; que se utilicen las encuestas de satisfacción como parámetro de referencia para evaluar la calidad del servicio brindado por el proveedor, que se validen y documenten las capacidades de los recursos asignados por el proveedor para la entrega del servicio y que se genere y documente la evidencia de las actividades consideradas en el pago de los servicios proporcionados.

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.

2021-0-44100-20-0176-01-003 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en futuras contrataciones de tecnologías de información y comunicaciones, defina criterios para evaluar la calidad de los entregables y establezca penas convencionales en caso de su incumplimiento.

2021-0-44100-20-0176-06-001 **Pliego de Observaciones**

Se presume un probable daño o perjuicio, o ambos, a la Hacienda Pública Federal por el pago que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos realizó al amparo del contrato número OA/C005/2021 en beneficio del proveedor Endeavor Technologies Systems, S.A. de C.V., por un monto de 3,416,947.20 pesos (tres millones cuatrocientos dieciséis mil novecientos cuarenta y siete pesos 20/100 M.N.), por los servicios de `Monitoreo de Niveles de Seguridad' y `Administración Mesa de Ayuda y Procedimientos', más los rendimientos financieros que se generen desde la fecha de su pago y hasta su recuperación o reintegro, ya que las actividades indicadas en los reportes mensuales de dichos servicios carecen de la evidencia que acredite que se ejecutaron las actividades de: análisis de vulnerabilidades, pruebas de intrusión, borrado seguro y monitoreo de equipos de seguridad realizados diariamente, la atención y solución vía telefónica a solicitudes de incidentes y requerimientos que no requieran de asistencia en sitio y cuando si se requiera, la atención a llamadas, el registro de solicitudes de atención y solución de incidentes y requerimientos mediante el uso de la herramienta de registro y administración (Altiris), de acuerdo con lo solicitado por el instituto mediante el contrato número OA/C005/2021 y su anexo técnico; en incumplimiento del artículo 66, fracciones I y III, del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria publicado en el Diario Oficial de la Federación el 28 de junio de 2006 y su última reforma publicada en el mismo medio el 13 de noviembre de 2020; el artículo 48, fracciones VII, X, XIII y XIX, del Acuerdo mediante el cual se aprueba el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el Diario Oficial de la Federación el 17 de enero de 2017, y sus reformas publicadas en el mismo medio de difusión oficial el 23 de septiembre de 2020; la declaración I.4, cláusulas primera objeto, segunda relación de anexos, séptima supervisión y octava responsabilidades del proveedor, del contrato número OA/C005/2021; los numerales 3 Objetivo, 4 Beneficios esperados, 5 Alcance, 5.4 Servicio de monitoreo de niveles de seguridad, 5.6 Servicio de Administración mesa de ayuda y procedimientos, 8.4 Servicio de administración de mesa de ayuda y 12 'Entregables del proyecto', del anexo técnico del contrato número OA/C005/2021, y del Numeral 23000000 funciones 4, 7, 9, 11 y 14, de la Dirección General de Tecnologías de la Información, del Manual de Organización del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el 16 de febrero de 2021.

Causa Raíz Probable de la Irregularidad

Falta de documentación, supervisión y control de las actividades realizadas por el proveedor.

3. Contrato número OA/C036/17 "Servicio de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia"

Se revisó el contrato número OA/C036/17, celebrado con el proveedor Raxo Telecomunicaciones, S.A. de C.V., mediante el procedimiento de Licitación Pública Nacional con número de identificación electrónica LA-006HHE001-E65-2017 y número interno LPN-006HHE001-013-17, suscrito con fundamento en los artículos 3, fracción VIII, 23, fracción I, 24, fracción II, 25, tercer párrafo, 26, fracción I, y 47 del Acuerdo mediante el cual se aprueba el Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (RAAS).

La vigencia del contrato fue del 7 de noviembre de 2017 al 6 de noviembre de 2020, por un monto mínimo de 5,976.0 miles de pesos y un máximo de 14,940.0 miles de pesos con el Impuesto al Valor Agregado (IVA) incluido, que tiene el objeto de prestar el Servicio de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia; asimismo, el 6 de noviembre de 2020 se realizó el primer convenio modificatorio con el objeto de ampliar la vigencia al 31 de enero de 2021, incrementando el monto del contrato por 1,171.6 miles de pesos; el 28 de enero de 2021 se llevó a cabo el segundo convenio modificatorio que amplió la vigencia del 1 de febrero al 31 de marzo de 2021 e incrementó el monto del contrato por 830.0 miles de pesos. Durante el ejercicio de 2021, se realizaron pagos por 1,245.3 miles de pesos por los servicios prestados y se determinó lo siguiente:

Objetivo

Proveer la infraestructura necesaria para la replicación del sistema Plataforma Nacional de Transparencia, el cual sería publicado en internet en caso de una contingencia en el centro de procesamiento de datos del INAI. El servicio solicitado debió ofrecer disponibilidad de la operación las 24 horas del día todos los días del año.

Alcance

Recuperar la funcionalidad de la Plataforma Nacional de Transparencia mediante los servidores que lo componen. Esto debió permitir que en un lapso no mayor de 36 horas la PNT haya restablecido su operación en el lugar alterno sin ninguna dependencia técnica del sitio original mediante la replicación de la información con una sincronización mínima de 24 horas.

Investigación de Mercado

- El documento no cuenta con la fecha de elaboración, con el nombre, ni con la firma del personal que lo elaboró; tampoco incluye un cuadro comparativo de las propuestas económicas de los solicitantes que respondieron a las solicitudes de contratación.

Revisión técnica y funcional de los servicios

De acuerdo con el anexo técnico del contrato número OA/C036/2017 las características de los Servicios de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia requeridos por el instituto fueron las siguientes: infraestructura de procesamiento virtual, servicio de centro de datos, servicio de telecomunicaciones, servicio de seguridad perimetral, servicio de monitoreo y servicio de centro de contacto; los cuales debían trabajar de forma conjunta en caso de que algún incidente afectara la operación de la PNT por más de 72 horas en el centro de procesamiento de datos del INAI, por lo que los ambientes del proveedor se volverían productivos sin alguna dependencia del sitio original mediante la replicación de la información de las máquinas virtuales del INAI hacia el sitio alterno del proveedor.

Infraestructura de procesamiento virtual

- Mediante el protocolo de pruebas se identificó la verificación de la instalación e integración de la infraestructura por parte del proveedor, que comprobó la funcionalidad de los servicios; sin embargo, sólo se realizaron pruebas de conectividad.

- No se establecieron pruebas de verificación en las cuales se hayan comprobado las características de replicación necesarias en caso de una contingencia.

Servicios del centro de datos

El proveedor debió revisar las condiciones operativas, la configuración de red de equipos de procesamiento de los ambientes, incluidos, software, administración de respaldos, administración de plataforma; en la revisión se observó lo siguiente:

- Plataforma de virtualización: el servicio estableció que la DGTI entregaría al proveedor el software (sistema operativo, bases de datos, servidores de aplicaciones, etc.) para el funcionamiento de la PNT; no obstante, la DGTI no comprobó que la infraestructura provista por medio del contrato haya tenido la capacidad de replicar los sistemas productivos de la PNT con el software del INAI.

- Administración de respaldos: los respaldos se realizarían en el centro de datos del proveedor sólo en caso de contingencias; durante la vigencia del contrato, el servicio no fue requerido.

Servicio de telecomunicaciones

Este incluyó los servicios LAN mediante la asignación de un segmento privado, servicio de acceso y publicación a internet, servicio de balanceo de carga de servidores y gestión de certificados digitales; de la revisión se identificó lo siguiente:

- En las pruebas realizadas al balanceador se mostraron los servicios apagados, por lo que no se ejecutaron las pruebas que demostraran la funcionalidad de la replicación en caso de contingencia.

Servicio de acceso y publicación de Internet

- No se generaron reportes de verificación de este servicio. La DGTI no comprobó que las aplicaciones que conforman la PNT fueran publicadas.

Servicio de seguridad perimetral

Este servicio incluyó la instalación, configuración y puesta en operación del servicio de firewall e IPS virtual para soportar la capacidad de salida a internet, configuración de VPN, y servicio antidenegación de servicios distribuidos; de la revisión se identificó que la DGTI carece de documentación que demuestre haber probado los servicios de seguridad y antidenegación de servicios distribuidos.

Pruebas y entrega

La DGTI, no solicitó una prueba integral que replicara los ambientes de producción con los que la PNT operaba a fin de asegurar y comprobar que la infraestructura, los servicios de acceso, los servicios de publicación a internet y los servicios de seguridad solicitados en el contrato operarían conjuntamente y con ello tener tiempos de recuperación razonables para el instituto en caso de alguna contingencia.

Por lo anterior, se concluye:

La DGTI no comprobó que la infraestructura del proveedor Raxo Telecomunicaciones, S.A. de C.V., replicara los servicios de la PNT a fin de restablecer y probar su funcionamiento; los servicios de este contrato no demostraron que brindaran las capacidades de recuperación ante contingencias de la PNT.

La DGTI, en su Plan de Recuperación de Desastres (DRP) del INAI, no estableció los escenarios en los que los servicios del contrato número OA/C036/17 entraran en operación.

2021-9-44100-20-0176-08-001 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que, en su gestión, no realizaron las acciones para asegurar que la Plataforma Nacional de Transparencia contara con un esquema de continuidad operativa, objeto del contrato número OA/C036/17, ya que no se establecieron pruebas integrales para comprobar las capacidades de replicación y continuidad de la Plataforma Nacional de Transparencia (PNT) ante contingencias, por lo que los servicios otorgados por el proveedor Raxo Telecomunicaciones, S.A. de C.V., al amparo del contrato número OA/C036/17 no demostraron brindar capacidades de recuperación de la PNT; en incumplimiento del artículo 48, fracciones II, IV, X, y XIII, del Acuerdo mediante el cual se aprueba el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el día 17 de enero de 2017 y modificación del 23 de septiembre de 2020; del numeral 23000000, Dirección General de Tecnologías de la Información, funciones 1, 13, y 14, del Manual de Organización del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el Diario Oficial de la Federación el 16 de febrero de 2021; de la cláusula séptima supervisión del contrato número OA/C036/17 'Servicio de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia', y del numeral 8, del anexo técnico del contrato número OA/C036/17.

4. Ciberseguridad

Para evaluar la ciberseguridad del INAI, la Auditoría Superior de la Federación utilizó el marco CIS (Controles Críticos de Seguridad del Centro de Seguridad de Internet, por sus siglas en inglés) para la infraestructura crítica de las TIC (Centro de Datos, Telecomunicaciones, Seguridad Perimetral, Ambientes de Desarrollo y Controles de Acceso).

Evaluación de Ciberseguridad basada en el CIS

El alcance de la auditoría consideró 20 controles de seguridad críticos (CSC), que incluyen 171 actividades de control individuales para evaluar el diseño y la efectividad operativa con sus respectivos objetivos de cumplimiento.

Medición

Para determinar el nivel de cumplimiento de cada control, se evaluó cada subcategoría que lo compone; el criterio utilizado fue el siguiente:

- **Carencia de Control - Rojo:** menos del 30.0% del cumplimiento a los requerimientos por control.

- **Requiere fortalecer el control - Amarillo:** entre el 31.0 -79.0% del cumplimiento de requerimientos por control.

- **Aceptable - Verde:** más del 80.0% del cumplimiento a los requerimientos por control.

SEMÁFORO DE MADUREZ DE LOS CONTROLES DE CIBERSEGURIDAD EN EL INAI DURANTE 2021

Control	Indicador
CSC Control 1: Inventario y control de activos de hardware	🔴
CSC Control 2: Inventario y control de activos de software	🔴
CSC Control 3: Gestión continua de vulnerabilidad	🔴
CSC Control 4: Uso controlado de privilegios administrativos	🟡
CSC Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	🔴
CSC Control 6: Mantenimiento, supervisión y análisis de registros de auditoría	🔴
CSC Control 7: Protección de correo electrónico y navegador web	🔴
CSC Control 8: Defensa contra malware (software malicioso)	🟡
CSC Control 9: Restricción y control de puertos, protocolos y servicios	🟡
CSC Control 10: Capacidad de recuperación de datos	🔴
CSC Control 11: Configuración segura para dispositivos de red, tales como cortafuegos, enrutadores y conmutadores	🟡
CSC Control 12: Seguridad perimetral	🟡
CSC Control 13: Protección de datos	🟡
CSC Control 14: Control de acceso basado en necesidad de saber	🟡
CSC Control 15: Control de acceso inalámbrico	🟡
CSC Control 16: Monitoreo y control de cuentas	🟡
CSC Control 17: Implementar un programa de capacitación y concientización de seguridad	🔴
CSC Control 18: Seguridad del software de aplicación	🟡
CSC Control 19: Respuesta y gestión incidentes	🔴
CSC Control 20: Pruebas de penetración y ejercicios de equipo rojo	🔴

FUENTE: Elaborado con información proporcionada por el INAI.

Indicador: 🟢 Cumplimiento aceptable 🟡 Requiere fortalecer el control 🔴 Carencia de control

Los hallazgos más relevantes de cada uno de los controles de seguridad son los siguientes:

CSC 1: Inventario y control de activos de *hardware*

- Se mantiene un inventario de activos de *hardware*; sin embargo, no se identifica el área a la cual pertenecen los activos.

- Sus inventarios (institucional y de TIC) no son conciliados.

- No se detectan activos no autorizados conectados a la red; en consecuencia, no tiene la capacidad para eliminarlos de la red, ponerlos en cuarentena y realizar su actualización.

- No se utiliza el control de acceso a nivel de puerto y certificados de cliente para autenticar los activos de *hardware* que se conectan a la red del instituto.

CSC 2: Inventario y control de activos de software

- Se carece de una lista actualizada que contenga la totalidad del *software* autorizado.

- Se carece de política y procedimientos institucionales para recibir y actualizar la totalidad de las aplicaciones de *software.*

- La herramienta para la gestión del inventario de *software* no se encuentra en operación.

- No se cuenta con un procedimiento para detectar *software* no autorizado.

- No se cuenta con evidencia de que se hayan gestionado las listas blancas de aplicaciones.

- El inventario de activos de *hardware* y *software* no se encuentra vinculado.

- No se identificó la separación física y lógica de las aplicaciones de alto riesgo.

CSC 3: Gestión continua de vulnerabilidades

- El 90.9% de los sistemas del INAI no fue escaneado mediante el sistema de gestión de las vulnerabilidades.

- La DGTI no documentó el procedimiento de atención de las vulnerabilidades identificadas hasta su mitigación, ni cuenta con un procedimiento para su gestión.

- No se realizaron análisis de vulnerabilidades con agentes que se ejecuten de forma local.

- Las bitácoras de los análisis de vulnerabilidades no mostraron la utilización de una cuenta vinculada específicamente para tal propósito.

- No se utilizan herramientas para garantizar que el *software* de terceros cuente con las actualizaciones de seguridad más recientes.

- No se compararon de forma regular los resultados de los escaneos de vulnerabilidades consecutivos, a fin de verificar que las vulnerabilidades se hayan remediado.

- No se cuenta con un proceso documentado de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.

- No se verificó ni se documentó que las actualizaciones de las herramientas tipo *OpenSource* utilizadas fueran configuradas de forma segura y no comprometieran la integridad de los datos o procesos de los aplicativos en los que se utilizaron.

CSC 4: Uso controlado de privilegios administrativos

- Se carece de una herramienta centralizada que identifiqué y monitoreé las actividades de todas las cuentas administrativas y con privilegios para todos sus sistemas operativos y aplicativos críticos.

- La Política de Seguridad de la Información del instituto no incluye las características mínimas o recomendables para la generación de contraseñas seguras, incluidas las cuentas de usuarios con nivel administrador.

- Existen herramientas que utilizan usuarios predeterminados en sus módulos de usuarios y éstas no han sido modificadas.

- El monitoreo de sus sistemas no emite alertas sobre cambios en registros e intentos fallidos de acceso a las cuentas administrativas.

- No se cuenta con herramientas o aplicaciones que permitan identificar los intentos de acceso a equipos con contraseñas no autorizadas.

- No se utilizan máquinas dedicadas para las tareas que requieran niveles de acceso elevados.

- No se cuenta con un inventario de roles para la totalidad de sus sistemas por lo que no se identifica a la totalidad de sus cuentas privilegiadas y no realiza su gestión.

CIS Control 5: Configuración segura para *hardware* y *software* en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

- Carece de estándares de configuración de seguridad documentados y formalizados para todos los sistemas operativos y *software* autorizados.

- No se cuenta con imágenes seguras o plantillas para la totalidad de los sistemas operativos y soluciones tecnológicas con los que cuenta el instituto; las existentes no se resguardan en servidores seguros y no se verifica su integridad.

- No se cuenta con herramientas para la gestión y cumplimiento de la configuración de los sistemas a fin de verificar los elementos, excepciones y alertas de cambios no autorizados.

- No se tienen implementadas herramientas de gestión de configuración que validen automáticamente los ajustes de configuración autorizados.

- No se cuenta con un proceso documentado para la totalidad de las actualizaciones de sus sistemas, herramientas y aplicativos.

CSC 6: Mantenimiento, supervisión y análisis de registros de auditoría

- No se utilizan al menos tres fuentes de tiempo para asegurar la consistencia de las marcas de tiempo de los registros.

- El registro local de eventos mediante logs no se encuentra habilitado en la totalidad de sus sistemas, aplicativos y dispositivos de red.

- Los registros generados por los sistemas y aplicativos del instituto no son revisados por la DGTI de forma periódica.

- No se utilizan herramientas de correlación de eventos, los registros no son analizados por un sistema central en tiempo real.

CSC 7: Protección de correo electrónico y navegador web

- No se identificó el uso de técnicas para analizar y bloquear archivos adjuntos de correo electrónico de comportamiento malicioso.

- No se restringe la ejecución de lenguajes de secuencias de comandos en los navegadores web y clientes de correo electrónico.

- No se bloquean o restringen navegadores web y clientes de correo electrónico no institucionales.

- No se cuenta con sitios web bloqueados, ya que no se establecen en las políticas.

- No se cuenta con un procedimiento formal sobre la generación de bitácoras de los archivos adjuntos de correo electrónico que se analizaron y bloquearon.

- No se documentó la totalidad de las bitácoras de 2021 de la herramienta para protección de correo electrónico, sólo se resguarda un historial de 3 meses.

CSC 8: Defensa contra *malware (software malicioso)*

- No se contó con evidencia de los eventos generados en 2021; ni se identificó la utilización del *software antimalware* centralizado.

- No existen elementos para asegurar que las firmas del *software antimalware* se hayan actualizado.

- Durante el 2021 no se configuró el análisis *antimalware* en los dispositivos extraíbles.

- No se contó con evidencia de la utilización de herramientas antiexplotación durante 2021.

CSC 9: Restricción y control de puertos, protocolos y servicios

- No se incluyó en su inventario la asociación de puertos, servicios y protocolos a los activos de *hardware*.

- No se documentó la ejecución de escaneos de puertos automatizados de manera regular.

- No se documentaron los esquemas y diagramas de la estructura de la red del instituto a fin de identificar la ubicación de sus elementos críticos.

CSC 10: Capacidad de Recuperación de Datos

- La política de respaldos del INAI de 2014 carece de alcances, responsables y procedimientos.

- Durante 2021 sólo se respaldó de manera completa el 38.0% de los sistemas críticos.

- Se identificaron respaldos que no se encuentran cifrados.

- Los respaldos no son probados periódicamente, a fin de verificar la integridad de los datos mediante su restauración.

- La DGTI no cuenta con políticas formalizadas y procedimientos de administración de capacidad.

- Los ejercicios de volumetría no tienen definida una periodicidad para verificar la capacidad y rendimiento de la infraestructura de TIC y no se documenta el incremento en los volúmenes de datos.

CSC 11: Configuración segura para dispositivos de red, tales como cortafuegos, enrutadores y conmutadores

- No se mantienen estándares de configuración de seguridad documentados para todos los dispositivos de red.

- Los dispositivos de red no cuentan con mecanismos de autenticación multifactor y sesiones cifradas.

- No se cuenta con configuraciones de seguridad aprobadas y documentadas para los dispositivos de red.

- No se utiliza una máquina dedicada para las tareas administrativas y tareas que requieran de acceso elevado.

- El INAI depende de sus proveedores para implementar y administrar activamente (rastrear, informar y corregir) la configuración de seguridad de los dispositivos de infraestructura de red, por lo que existe el riesgo de falta de experiencia del personal del instituto.

CSC 12: Defensa de fronteras/límites de red

- Se detectaron deficiencias en la seguridad perimetral.

CSC 13: Protección de datos

- No se cuenta con un inventario de la información confidencial almacenada, procesada o transmitida por los sistemas tecnológicos del instituto, incluidos aquellos ubicados con proveedores de servicios.

- No se eliminan los datos confidenciales de los sistemas a los que el instituto no accede regularmente.

- No se cuenta con una herramienta automatizada que monitoreé la transferencia no autorizada de información confidencial.

- No se utilizan procedimientos y herramientas para el cifrado de datos; en consecuencia, no se supervisa el uso no autorizado de mecanismo de cifrado del tráfico del instituto.

- No se delimita el uso de dispositivos de almacenamiento USB (*Universal Serial Bus*, por sus siglas en inglés) en la red institucional, salvo en el centro de datos, por lo que, no se tienen configurados los sistemas a fin de permitir el uso de dispositivos de almacenamiento sólo en casos específicos.

- Los medios de almacenamiento USB utilizados en la red institucional no son cifrados.

CSC 14: Control de acceso basado en la necesidad de saber

- No se tienen implementadas tecnologías con capacidad de cifrar la información confidencial en tránsito.

- No se utiliza una herramienta de descubrimiento activo para identificar toda la información confidencial almacenada, procesada o transmitida por los sistemas tecnológicos del instituto, incluidos aquellos ubicados con los proveedores de servicios remoto.

- No se utilizan aplicaciones de *software* para la prevención de pérdida de datos basada en *host*.

- No se configuran registros de auditoría detallados para monitorear el acceso a datos confidenciales y los cambios que se ejecuten en ellos.

- No se utilizan herramientas de monitoreo de integridad de archivos o herramientas de monitoreo de eventos de seguridad.

CSC 15: Control de acceso inalámbrico

- No se utilizan protocolos de autenticación para acceso en redes inalámbricas.

- El acceso periférico inalámbrico de dispositivos *Bluetooth* y NFC *(Near Field Communication,* por sus siglas en inglés) no se encuentra documentado, no se identificaron restricciones ni configuraciones específicas para su uso.

CSC 16: Monitoreo y control de cuentas

- No se cuenta con autenticación multifactor en ninguna de sus cuentas de usuario.

- No se cuenta con procedimientos para la protección de las credenciales de autenticación en tránsito.

- No se desactivan de forma automática las cuentas inactivas después de un período determinado.

- No se establecen procesos automatizados para revocar el acceso a los sistemas del instituto mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado.

- No son deshabilitados los usuarios por defecto de la totalidad de sus herramientas.

- No se cuenta con herramientas para monitorear los intentos de acceso a cuentas desactivadas.

- Se carece de las bitácoras de monitoreo de herramientas que alerten a la DGTI cuando los usuarios se desvían del comportamiento normal de inicio de sesión.

CSC 17: Implementar un programa de capacitación y concientización de seguridad

- No se realizan análisis de brechas de habilidades para conocer la capacidad de su fuerza laboral.

- No se generó un programa de concientización sobre la autenticación segura.

- Los miembros de la DGTI relacionados con roles de seguridad no se encuentran capacitados a fin de identificar indicadores comunes de incidentes y cómo reportarlos.

CSC 18: Seguridad del software de aplicación

- Se establecieron prácticas de codificación seguras a sus proveedores; no obstante, no se solicitaron entregables para cada una de las etapas de desarrollo de *software.*

- No se establecen estándares de codificación segura por lenguaje de programación y entorno de desarrollo.

- Para el *software* desarrollado internamente, no se documentó la verificación de errores explícito para todas las entradas.

- No se documentaron los procedimientos, herramientas y responsables de verificar que las versiones del *software* de terceros fueron compatibles con la infraestructura del INAI.

- Utiliza sistemas operativos sin soporte del proveedor.

- No se usan algoritmos de cifrado durante el ciclo de vida de desarrollo de *software*.

- El personal del instituto no recibe capacitación en la escritura de código seguro conforme a sus responsabilidades y atribuciones.

- Se identificaron deficiencias en la seguridad del *software* de aplicación.

- No se estableció la segregación de funciones de cada uno de los ambientes de desarrollo.

- Para las aplicaciones que dependen de una base de datos, el instituto no documentó la utilización de plantillas de configuración de protección estándar.

CSC 19: Respuesta y gestión de incidentes

- No se define a los responsables, sus roles y funciones acorde al entorno y la estructura organizacional de la DGTI y las tareas que realizarán durante las fases del manejo/gestión de incidentes; los roles relacionados con el Centro de Operaciones de Seguridad (*Security Operation Center* (SOC), por sus siglas en inglés) no se encuentran formalizados.

- No se estableció un equipo de manejo a incidentes.

- No se cuenta con estándares aplicables a todo el instituto respecto a cuándo y cómo informar eventos anómalos al equipo de manejo de incidentes.

- No se reúne información de contacto de terceros para informar los incidentes de seguridad.

- No se cuenta con un esquema de priorización y puntuación de incidentes basado en el impacto potencial.

- No se concientiza a su personal respecto a la notificación de incidentes y anomalías informáticas.

- No se planifican ni llevan a cabo pruebas de incidentes de rutina, ejercicios de respuesta y escenarios; no se prueban los canales de comunicación, la toma de decisiones y las capacidades técnicas de los roles que atienden los incidentes.

CISC 20: Pruebas de penetración y ejercicios del equipo rojo

- Se identificaron deficiencias en las pruebas de penetración y ejercicios del equipo rojo.

- El instituto no documentó el control y monitoreo de la cuenta utilizada para realizar pruebas de intrusión a fin de asegurarse de que sólo se use para fines legítimos.

En la evaluación de 20 controles por el CIS se identificó que en 10 (50.0%) se carece de control y en los 10 (50.0%) restantes se requiere fortalecer el control.

Durante el 2021, el INAI no contó con una Estrategia de Seguridad Institucional; a la fecha de la revisión (agosto de 2022), el instituto aún se encuentra en proceso de desarrollo e implementación de su Sistema de Gestión de Seguridad de la Información (SGSI).

2021-0-44100-20-0176-01-004 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Dirección General de Tecnologías de la Información, defina y aplique los mecanismos de control, incluyendo las actividades que considere pertinentes, a fin de atender y mitigar las observaciones de los controles que en la evaluación se identificaron como 'Carencia de control' y 'Requiere fortalecer el control', para garantizar la disponibilidad, integridad y confidencialidad de la información que resguarda el instituto, y que las acciones coadyuven al desarrollo, administración, implementación, funcionamiento, estabilidad y seguridad de la Plataforma Nacional de Transparencia, y que en su conjunto fortalezcan las labores de la Dirección General de Tecnologías de la Información para alcanzar las metas y objetivos del instituto.

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.

2021-0-44100-20-0176-01-005 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Dirección General de Tecnologías de la Información, analice la viabilidad de desarrollar, implementar y difundir una Estrategia de Seguridad Institucional que le permita conocer su estado actual y definir los planes y tácticas para alcanzar un estado de seguridad de la información y ciberseguridad que involucre la coordinación de las áreas responsables de los diferentes aspectos de la seguridad de la información del instituto, a nivel técnico, físico, personal y cibernético.

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.

5. Continuidad de las operaciones

Plan de Continuidad del Negocio (BCP)

El INAI cuenta con el "Plan de Recuperación de Desastres de los servicios tecnológicos del INAI" de febrero de 2021 que contiene los elementos de su Gestión de Continuidad de Negocio (BCM, por sus siglas en inglés), en la revisión se identificó lo siguiente:

- Los elementos descritos en el BCM no se encuentran desarrollados respecto de la operación crítica del INAI, no cuenta con un análisis de riesgos, carece de una estrategia que establezca prioridades para su recuperación y no tiene definidos los procedimientos y escenarios ante eventos adversos.

- El INAI no tiene documentadas las estrategias mediante las cuales daría continuidad a sus servicios esenciales.

- A la fecha de la revisión (agosto de 2022), no ha probado su BCM.

Análisis de Impacto al Negocio (BIA)

- El INAI no ha realizado un análisis de impacto a su operación crítica.

Plan de Recuperación de Desastres (DRP)

- Los elementos enunciados en el DRP no se encuentran orientados a su operación crítica.

- La DGTI no definió métricas para la efectividad de los esfuerzos de restablecimiento de sus operaciones mediante el Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés) y Punto Objetivo de Recuperación (RPO, por sus siglas en inglés), de acuerdo con su presupuesto, recursos y prioridades para cumplir con sus objetivos.

- El INAI no cuenta con una estrategia de recuperación en caso de desastres que incluya los escenarios ante eventos adversos y su impacto en los tiempos de normalización de los servicios críticos, por lo cual la recuperación y el restablecimiento de operación podría ser mayor a lo deseado.

Protocolo de Recuperación

- No cuenta con un plan de comunicaciones ante una crisis que considere un procedimiento de evaluación del evento, notificaciones, el nivel de comunicación requerido, mensajes y audiencia.

- Carece de responsables y alcances.

- El personal de la mesa de servicios desconoce las actividades que deberían realizar en caso de desastres, a pesar de ser el punto central de interacción con los usuarios del instituto.

Plan de Pruebas y capacitación para equipos de trabajo que participan en el DRP

- La DGTI no tiene desarrollados, desplegados e implantados los elementos de su DRP; no ha realizado ejercicios de prueba y no se han establecido los actores involucrados.

- El personal de la DGTI no cuenta con capacitación sobre los roles en la ejecución del Plan de Recuperación de Desastres de los servicios tecnológicos y quién los debe ejecutar.

Directriz rectora de respuesta a incidentes de Seguridad

- La DGTI no ha desarrollado ni establecido las acciones de cada uno de los recursos humanos definidos en la directriz, incluidos los procedimientos para la atención de los incidentes.

- Los roles involucrados con la aplicación y cumplimiento de la directriz Coordinador del centro de operaciones de seguridad (SOC), Especialista del SOC, Ingeniero en operación y Representante de la Dirección no se encuentran designados.

- La directriz no cumplió con su objetivo de establecer los mecanismos de respuesta a incidentes y detección de riesgos que permitiera proteger los activos críticos y recursos del instituto, a fin de garantizar la integridad, confidencialidad y disponibilidad de los datos almacenados en el instituto y terceros.

Centro de Datos

- La matriz de riesgos del centro de datos no considera riesgos lógicos, físicos y ambientales.

- No cuenta con políticas y procedimientos sobre la atención de incidentes de ambiente físico.

- Los sistemas de prevención de incendios no son probados.

- Las paredes no cuentan con retardante en caso de incendio.

- Se identificaron materiales flamables al interior del centro de datos.

- Las unidades UPS (*Uninterruptible Power Supply,* por sus siglas en inglés) se encontraron rodeadas de ventiladores, denotando un sobrecalentamiento.

Por lo anterior, se concluye que:

La estrategia de recuperación del instituto tiene áreas de oportunidad para mitigar los impactos ocasionados en los servicios en caso de una falla o interrupción de su operación, ya que no cuenta con procesos documentados acordes a su operación que desarrollen y profundicen en cada uno de los elementos que lo componen y doten al instituto de capacidades de gestión para sus programas de continuidad.

2021-0-44100-20-0176-01-006 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Dirección General de Tecnologías de la Información, defina, desarrolle e implemente estrategias de continuidad que le permitan identificar sus funciones críticas y los requerimientos asociados con sus contingencias; cuente con objetivos de recuperación, prioridades de restauración y métricas como el Punto Objetivo de Recuperación y el Tiempo Objetivo de Recuperación; establezca roles de contingencia, responsabilidades y personal asignado considerando la restauración de los sistemas sin deteriorar las medidas de seguridad planeadas e implementadas originalmente mediante estrategias revisadas y aprobadas por el personal capacitado; asimismo, difunda el plan de contingencia al personal clave del instituto; coordine las actividades del plan de contingencia con las actividades de manejo de incidentes para asegurar el cumplimiento de los objetivos de recuperación y prioridades de restauración, mediante una estrategia de continuidad viable y efectiva en costos, y finalmente que brinde capacidades de continuidad de las operaciones al instituto frente a eventos adversos.

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.

6. Ciberataque a la Plataforma Nacional de Transparencia (PNT)

Antecedentes

El Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en su Tercera Sesión Extraordinaria de 2021, celebrada el 26 de agosto de 2021 de manera virtual, aprobó las actividades y compromisos de los organismos garantes para la puesta en operación del SISAI 2.0., instrumento normativo que entró en vigor al momento de su aprobación y que se publicó en el Diario Oficial de la Federación el 8 de septiembre de 2021, cuyo proyecto fue realizado por la DGTI del INAI.

El 13 de septiembre de 2021 entró en operación el SISAI 2.0 que formó parte del proceso de reingeniería de la Plataforma Nacional de Transparencia, y se advirtió una alta demanda de usuarios y falta de transferencia de la totalidad de los datos e información de las solicitudes que originalmente ingresaron por la PNT.

A las 16:47 horas del lunes 20 de septiembre de 2021, el INAI, mediante un comunicado oficial en su cuenta oficial en Twitter (@INAImexico), informó *"…la Plataforma Nacional de Transparencia ha tenido un comportamiento intermitente, debido a un ataque o hackeo de tipo explotación de criptomonedas…" (sic)*, e indica que su área de tecnologías llevaba a cabo las acciones necesarias para detener el hackeo y estabilizar la operación de la PNT.

El INAI llevó a cabo acciones por medio de contrataciones con terceros, de los cuales la ASF identificó lo siguiente:

- Los intentos de múltiples conexiones se detectaron por las herramientas que forman parte del contrato número OA/C043/19 "Arrendamiento sin opción a compra de una solución de seguridad perimetral" cuyo proveedor es Grupo de Tecnología Cibernética, S.A. de C.V. (Grupo Tecno), con vigencia del 1 de enero de 2020 al 31 de diciembre de 2022, con pagos durante 2021 por 10,432.65 miles de pesos, quien aplicó mecanismos de mitigación el mismo día.

- La Dirección General de Administración del INAI realizó una compra directa conforme al artículo 42 del RAAS del INAI, (pago sin formalización de contrato o pedido), con el proveedor Borealix, S.C., por el servicio "Aplicación de filtros personalizados para seguridad de red" por un monto con IVA de 46.7 miles de pesos.

- El personal de la Dirección de Soluciones Tecnológicas de la DGTI implementó mecanismos de seguridad adicionales en la PNT con el apoyo de la empresa Borealix, S.C.

- El 21 de septiembre de 2021 persistieron los múltiples intentos de conexión a la PNT proveniente de un bloque de direcciones IP diferentes.

- La DGTI adjudicó el contrato número OA/053/2021 con el proveedor CIIME Consultoría Integral en Informática de México S.A. de C.V., con vigencia del 8 de diciembre al 31 de diciembre de 2021, por concepto de "*Licencias de análisis de vulnerabilidades, Pruebas de Intrusión y de Seguridad en la Nube WAF para la Detección de intrusos, Protección de aplicaciones Web, Prevención de ataques, Denegación de Servicio Distribuido DDoS para los Sistemas del INAI*", que contemplaba dos partidas, de lo cual se observó:

    - El anexo técnico del contrato número OA/053/2021 no fue actualizado, ya que en la partida 1, no está considerado el importe de la contratación erogado bajo el contrato número OA/C052/2021 con el proveedor SafeLink S. de R.L. Se identificó un anexo técnico para las dos partidas, no obstante, cada una fue contratada con proveedores diferentes.

En el análisis de los eventos indicados, la ASF observó:

- Las actividades que se ejecutaron para mitigar y remediar el ciberataque no se encuentran documentadas por la DGTI conforme a sus procedimientos formalizados de respuesta a incidentes.

- La DGTI recurrió a esquemas de seguridad adicionales para mitigar las amenazas, lo cual generó erogaciones adicionales al instituto.

- Posteriormente al comunicado oficial, el INAI identificó que por las características del ataque correspondió a una denegación de servicios.

- El INAI no resguardó una cadena de custodia del ciberataque que le permitiera tener la capacidad de reconocer, recopilar y salvaguardar los indicios probatorios digitales.

- La DGTI no realizó un análisis forense del ciberataque del 20 de septiembre de 2021.

- Las acciones legales que el instituto ha emprendido para deslindar responsabilidades ante las instancias pertinentes incluyen la revisión del caso por parte de un perito; sin embargo, utilizó como evidencia la proporcionada por el INAI dos meses después de suscitado el ataque sin una adecuada cadena de custodia.

- El Órgano Interno de Control (OIC) del INAI no programó auditorías durante 2020 y 2021 a los activos de la PNT y tampoco realizó investigaciones para deslindar responsabilidades del incidente.

- De la revisión de los tickets generados durante el evento, se concluye que antes del ataque informático las herramientas de seguridad del instituto no habían sido configuradas de acuerdo a las necesidades del INAI y no operaban de forma conjunta con su seguridad perimetral.

- El personal del INAI no verificó que las herramientas y sistemas operativos del instituto estuvieran actualizados, no se presentó evidencia de que las configuraciones realizadas se adaptaron al entorno y que funcionaran correctamente, y que aún mostraran alertas activas.

- Del reporte de vulnerabilidades del SISAI (de fecha 25 de junio sin especificar el año) se observaron vulnerabilidades “altas” y “medias”, el instituto no presentó evidencia de la mitigación de las vulnerabilidades identificadas, por lo que existe el riesgo que no hayan sido resueltas. El personal auditor de la ASF no pudo verificar el alcance y configuración de las herramientas utilizadas en 2021 para la atención de vulnerabilidades, ya que de acuerdo con la DGTI éstas se instalaron en los equipos del proveedor, quien a la fecha de la revisión (agosto de 2022) ya había retirado sus equipos; no se presentó evidencia de los certificados de borrado seguro, a fin verificar que la información del instituto haya sido resguardada.

- El instituto se encuentra en proceso de desarrollo de su SGSI, por lo que aún no se encuentran implementados controles de seguridad aplicados bajo esas directrices, incluida la PNT.

- El Subdirector de Seguridad de la Información durante el 2021 no supervisó ni revisó la seguridad del *software,* las bases de datos, los archivos y demás componentes relacionados con la PNT; no cumplió con su función de guiar al cuerpo directivo y a la institución ante incidentes de seguridad conforme el Plan de Respuesta a Incidentes.

Por lo que se concluye que el INAI presentó deficiencias en las políticas, los procedimientos y el personal capacitado para detectar, contener y responder ante el incidente de seguridad ocurrido el 20 de septiembre de 2021.

2021-0-44100-20-0176-01-007 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Dirección General de Tecnologías de la Información, desarrolle, documente y establezca una arquitectura de seguridad efectiva basada en un Sistema de Gestión de Sistemas de Información que le permita contar con controles de seguridad basados en las mejores prácticas y marcos de referencia en materia de ciberseguridad, y así cumplir con su mandato constitucional, con el apoyo de soluciones robustas de tecnologías de información y comunicaciones, que sean verificados mediante un ciclo de mejora continua y que protejan los activos del instituto de ataques o eventos informáticos fortuitos; asimismo, para que verifique y documente las actividades reactivas de los ataques provenientes del interior o del exterior, a fin de establecer la cadena de custodia y se resguarde la información involucrada, con el propósito de que exista trazabilidad.

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.

2021-0-44100-20-0176-01-008 **Recomendación**

Para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante la Dirección General de Tecnologías de la Información, defina y establezca procesos documentados acordes a su operación que permitan al instituto formalizar la ejecución de análisis de riesgos y gestión de incidentes de seguridad; definir e implementar procedimientos de monitoreo, supervisión y control para el cumplimiento de las actividades relacionados con la seguridad de la información y ciberseguridad, a fin de que, en futuros incidentes, cuente con elementos para comprobar que sus activos no se encuentren comprometidos, y de procurar los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por el instituto en sus activos.

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.

2021-9-44100-20-0176-08-002 **Promoción de Responsabilidad Administrativa Sancionatoria**

La Auditoría Superior de la Federación emite la Promoción de Responsabilidad Administrativa Sancionatoria para que el Órgano Interno de Control en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o su equivalente realice las investigaciones pertinentes y, en su caso, inicie el procedimiento administrativo correspondiente por las irregularidades de los servidores públicos que, en su gestión, emitieron el comunicado oficial a nombre del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales bajo el término `ataque de tipo criptomonedas', sin contar con los elementos probatorios que acreditaran el tipo de ataque, la magnitud y afectación a la Plataforma Nacional de Transparencia; por no haber coordinado el desarrollo y administración de soluciones tecnológicas que mitigaran de forma proactiva los ataques informáticos hacia la Plataforma Nacional de Transparencia; no haber definido, establecido, implementado y evaluado el Sistema de Gestión de Seguridad de la Información a fin de preservar la confidencialidad, integridad y disponibilidad de sus activos; por no haber determinado los requerimientos tecnológicos para satisfacer las necesidades de seguridad de la información del instituto a fin de garantizar el desempeño de los servicios de la Plataforma Nacional de Transparencia; por no haber supervisado y revisado la seguridad informática del software, bases de datos, archivos y demás información para el aseguramiento de la Plataforma Nacional de Transparencia, por no haber propuesto y coordinado análisis de riesgos en seguridad de la información a fin de conocer el nivel de riesgo aceptable dentro del instituto, por no haber detectado y mitigado las vulnerabilidades de la Plataforma Nacional de Transparencia, lo cual impidió el acceso a

la plataforma, afectando la disponibilidad de la misma, por no haber guiado al cuerpo directivo del instituto ante el ciberataque debido a las deficiencias del Plan de Recuperación de Desastres, y por no haber resguardado la cadena de custodia que permitiera llevar a cabo los análisis forenses necesarios para verificar la confiabilidad e integridad de los activos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a fin de comprobar que la Plataforma Nacional de Transparencia no se encuentre comprometida; en incumplimiento del artículo 48, del Acuerdo mediante el cual se aprueba el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el día 17 de enero de 2017 y su modificación del 23 de septiembre de 2020; de los numerales 23000000, Director General de Tecnologías de la Información, objetivo, funciones 1, 2, 4, 7 y 13, 23020000 Director de Soluciones Tecnológicas, objetivo, funciones 1, 2, 5 y 7, 23021000 Subdirector de Operaciones, objetivo, funciones 1, 4, 5 y 8 y, 23023000 Subdirección de Seguridad de la Información, funciones 2, 3, 4, 5, 6, 7, 8 y 9, del Manual de Organización del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el 16 de febrero de 2021.

Montos por Aclarar

Se determinaron 3,416,947.20 pesos pendientes por aclarar.

Buen Gobierno

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

Resumen de Resultados, Observaciones y Acciones

Se determinaron 6 resultados, de los cuales, en uno no se detectó irregularidad y los 5 restantes generaron:

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

Consideraciones para el seguimiento

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

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

Dictamen

El presente dictamen se emite el 31 de enero de 2023, 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, 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 Transparencia, Acceso a la Información y Protección de Datos Personales cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- Del contrato número OA/C005/2021 celebrado con ND Negocios Digitales, S.A. de C.V., en participación conjunta con Endeavor Technologies Systems, S.A. de C.V., se carece de soporte documental de los entregables que den certeza que los servicios de Monitoreo de Niveles de Seguridad y Administración de la Mesa de Ayuda y Procedimientos se hayan prestado por los que se realizaron pagos por 3,416.9 miles de pesos.

- Para el contrato número OA/C036/17 celebrado con Raxo Telecomunicaciones, S.A. de C.V., no se demostró que los servicios brindaron las capacidades de recuperación ante contingencias para la Plataforma Nacional de Transparencia, por lo que se presumen omisiones por parte del administrador del contrato, debido a que no realizó pruebas para verificar que el INAI contara con un esquema de recuperación en un sitio alterno.

- En la revisión de los Controles Críticos de Seguridad del Centro de Seguridad de Internet, con los que se evaluó la infraestructura tecnológica crítica de la entidad, se observó que, de los 20 controles del CIS, en 10 (50.0%) se carece de control y en los 10 restantes se requiere fortalecer el control.

- Respecto de la Continuidad de las Operaciones, se observó que el "Plan de Recuperación de Desastres de los servicios tecnológicos del INAI" de febrero de 2021, no se encuentra acorde a su operación, no define roles y responsabilidades, no precisa los mecanismos de replicación que aseguren la continuidad operativa de la PNT en caso de desastres, ni tiene establecidos escenarios y procedimientos para recuperar sus operaciones críticas dentro de los tiempos de recuperación aceptables, ya que no se han establecido métricas para su recuperación.

- En el análisis del Ciberataque a la PNT se identificó que el INAI no guardó una cadena de custodia que le permitiera tener la capacidad de reconocer, recopilar y salvaguardar los indicios probatorios digitales y garantizar su integridad. Tuvo deficiencias en las políticas, los procedimientos y personal capacitado para gestionar y contener el incidente.

Servidores públicos que intervinieron en la auditoría:

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

Comentarios de la Entidad Fiscalizada

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública se corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen 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, y 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 se incluyeron 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 la pertinencia de su penalización o 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 de información, telecomunicaciones y demás relacionados con las TIC para verificar antecedentes, investigación de mercado, adjudicación, beneficios esperados, entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento y sustantivas), implementación y soporte de los servicios; verificar que el plan de mitigación de riesgos se atendió, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, con un enfoque en las acciones fundamentales que cada entidad debe implementar para mejorar la protección de sus activos de información,

como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; pruebas de penetración a las redes y sistemas, entre otros.

7. Evaluar la gestión de los programas de continuidad de las operaciones en sus elementos como el análisis de impacto al negocio (BIA); el plan de continuidad del negocio (BCP); el plan de recuperación ante desastres (DRP); las políticas de respaldos; la replicación de datos; la planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros.

Áreas Revisadas

La Dirección General de Tecnologías de la Información; la Dirección de Sistemas; la Dirección de Soluciones Tecnológicas; la Subdirección de Seguridad de la Información; la Subdirección de Operaciones y la Subdirección de Calidad e Implementación, adscritas a la Secretaría Ejecutiva y la Dirección de Recursos Financieros; la Dirección de Recursos Materiales y la Subdirección de Adquisiciones y Control Patrimonial, adscritas a la Dirección General de Administración, todas del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

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: El artículo 66, fracciones I y III del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria publicado en el Diario Oficial de la Federación el 28 de junio de 2006 y su última reforma publicada en el mismo medio el 13 de noviembre de 2020; el artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, publicado en el Diario Oficial de la Federación el 28 de julio de 2010; el artículo 48, numerales I, II, IV, VII, VIII, X, XI y XIII del Acuerdo mediante el cual se aprueba el Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el día 17 de enero de 2017 y su modificación del 23 de septiembre de 2020; los artículos 38, 45, fracción XXII y 52, del Acuerdo mediante el cual se aprueba el Reglamento de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el 29 de noviembre de 2017; la declaración I.4, cláusulas primera objeto, segunda relación de anexos, séptima supervisión y octava responsabilidades del proveedor, del contrato OA/C005/2021; los numerales 3 Objetivo, 4 Beneficios esperados, 5 Alcance, 5.4 Servicio de monitoreo de niveles de seguridad, 5.6 Servicio de

Administración mesa de ayuda y procedimientos, 8.4 Servicio de administración de mesa de ayuda y 12 'Entregables del proyecto', del anexo técnico del contrato número OA/C005/2021; la cláusula séptima supervisión, del contrato número OA/C036/17 'Servicio de Centro de Datos para Hospedaje de la Plataforma Nacional de Transparencia' y el numeral 8 del anexo técnico del contrato número OA/C036/17; de los numerales 23000000 Dirección General de Tecnologías de la Información, funciones 1, 2, 4, 5, 7, 8, 9, 10, 11, 13 y 14, 23020000 Director de Soluciones Tecnológicas, objetivo, funciones 1, 2, 4, 5, 6 y 7, 23021000 Subdirector de Operaciones, objetivo, funciones 1, 2, 4 y 8, y 23023000 Subdirección de Seguridad de la Información, funciones 2, 3, 4, 5, 6, 7, 8 y 9, del Manual de Organización del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales publicado en el Diario Oficial de la Federación el 16 de febrero de 2021.

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.