Suprema Corte de Justicia de la Nación

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2022-0-03100-20-0380-2023

Modalidad: Presencial

Núm. de Auditoría: 380

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 2022 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	290,783.5
Muestra Auditada	65,329.8
Representatividad de la Muestra	22.5%

El universo seleccionado por 290,783.5 miles de pesos corresponde al monto de los gastos realizados por la Suprema Corte de Justicia de la Nación (SCJN), en materia de contratación de Tecnologías de Información y Comunicaciones (TIC); la muestra auditada se integra por tres contratos relacionados con los servicios administrados de operaciones de ciberseguridad y de infraestructura de procesamiento y almacenamiento de datos, así como servicios de estudio e investigación de información y tendencias digitales, con pagos ejercidos por 65,329.8 miles de pesos, que representan el 22.5% del universo seleccionado.

Adicionalmente, la auditoría comprende el análisis presupuestal de la Cuenta Pública de 2022 de la SCJN en relación con los gastos en materia de Tecnologías de Información y Comunicaciones, la revisión de las actividades y del cumplimiento de las responsabilidades en materia de ciberseguridad, continuidad de las operaciones y centro de datos. Los recursos objeto de revisión en esta auditoría se encuentran reportados en la Cuenta de la

Hacienda Pública Federal del ejercicio de 2022, Tomo V, apartado Información Presupuestaria en el "Estado Analítico del Ejercicio del Presupuesto de Egresos en Clasificación Económica y por Objeto del Gasto", correspondiente al programa presupuestario R001 "Otras actividades".

Antecedentes

Los artículos 49 y 50 de la Constitución Política de los Estados Unidos Mexicanos establecen que, en nuestro país, el Supremo Poder de la Federación se divide, para su ejercicio, en Legislativo, Ejecutivo y Judicial. Asimismo, el artículo 94 de nuestra Carta Magna, establece que el ejercicio del Poder Judicial de la Federación se deposita en una Suprema Corte de Justicia, en un Tribunal Electoral, en Plenos Regionales, en Tribunales Colegiados de Circuito, en Tribunales Colegiados de Apelación y en Juzgados de Distrito.

La Suprema Corte de Justicia de la Nación se integra por once ministras y ministros que tienen como propósito fundamental vigilar que las leyes y actos de autoridad se apeguen a la Constitución y no vulneren los derechos humanos de las personas, garantizando la separación de poderes, el principio democrático y los derechos fundamentales para beneficio de todas las personas que habitan el territorio nacional.

La Oficialía Mayor de la Suprema Corte de Justicia de la Nación, tiene entre sus atribuciones, administrar los recursos humanos, materiales, tecnológicos, financieros y presupuestarios de la Suprema Corte, de conformidad con las disposiciones jurídicas aplicables; para ello, la Dirección General Tecnologías de la Información, adscrita a dicha Oficialía Mayor, es la responsable de administrar los recursos en materia de tecnologías de la información y comunicación, así como proveer los servicios que se requieran en la materia y cuenta con las atribuciones necesarias para suscribir, en el ámbito de su competencia, los contratos y convenios relacionados con la adquisición de bienes y servicios informáticos, de conformidad con las disposiciones jurídicas aplicables.

Durante la fiscalización superior de la Cuenta Pública de 2015, se realizó en la SCJN, la auditoría número 4-GB con título "Auditoría de TIC", en la que se determinaron diez Recomendaciones.

Entre 2018 y 2022, la SCJN invirtió 1,245,646.4 miles de pesos de su presupuesto en partidas relacionadas con Tecnologías de Información y Comunicaciones, integrados de la manera siguiente:

RECURSOS INVERTIDOS EN MATERIA DE TIC POR LA SCJN

(Miles de pesos)

Periodo de inversión	2018	2019	2020	2021	2022	Total
Monto por año	196,641.4	210,842.2	265,579.4	281,799.9	290,783.5	**1,245,646.4**

FUENTE: Elaborado por la ASF con base en la información proporcionada por la Suprema Corte de Justicia de la Nación.

NOTA: Estos importes se integran de las partidas del capítulo 2000, 3000 y 5000.

Evaluación del control interno

Con base en el análisis efectuado mediante procedimientos de auditoría, se evaluaron los mecanismos de control implementados con el fin de establecer si son suficientes para el cumplimiento de los objetivos de las contrataciones de TIC, así como determinar el alcance, naturaleza y muestra de la revisión, y 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 2022, publicado en el Diario Oficial de la Federación (DOF) el 29 de noviembre de 2021, a la SCJN se le aprobó un presupuesto de 5,284,902.8 miles de pesos.

En el análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio de 2022, se identificó que la SCJN tuvo un presupuesto ejercido de 923,096.6 miles de pesos en los capítulos 2000, 3000 y 5000 con partidas vinculadas con las TIC, de los que 290,783.5 miles de pesos corresponden a recursos relacionados con las contrataciones en materia de TIC, que representaron el 31.5% del presupuesto ejercido, como se muestra a continuación:

RECURSOS EJERCIDOS POR LA SCJN EN LOS CAPÍTULOS VINCULADOS A LAS TIC DURANTE 2022

(Miles de pesos)

Capítulo	Descripción	Ejercido	Ejercido en contratos TIC	% Ejercido en contratos TIC
2000	Materiales y Suministros	65,143.8	737.2	0.1%
3000	Servicios Generales	841,477.9	284,257.8	30.8%
5000	Bienes Muebles, Inmuebles e Intangibles	16,474.9	5,788.5	0.6%
	Total:	**923,096.6**	**290,783.5**	**31.5%**

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

Los recursos ejercidos en materia de TIC por 290,783.5 miles de pesos se integran de la manera siguiente:

RECURSOS EJERCIDOS POR LA SCJN EN LOS CAPÍTULOS VINCULADOS A CONTRATACIONES EN MATERIA DE TIC

(Miles de pesos)

Capítulo / P. Presupuestaria	Subpartida	Descripción	Presupuesto ejercido
2000		**Materiales y suministros**	
2900	29301	Refacciones y accesorios menores de mobiliario y equipo de administración, educacional y recreativo.	10.5
2900	29401	Refacciones y accesorios para equipo de cómputo y telecomunicaciones	726.7
3000		**Servicios generales**	
3100	31401	Servicio telefónico	1,164.3
3100	31501	Servicio de telefonía celular	1,239.5
3100	31601	Servicio de radiolocalización	2,238.6
3100	31603	Servicio de internet	1,191.7
3100	31701	Servicio de conducción de señales analógicas y digitales	73,659.4
3100	31904	Servicios integrales de infraestructura de cómputo	4,315.6
3200	32301	Arrendamiento de equipo y bienes informáticos	73,351.1
3200	32303	Arrendamiento de equipo de telecomunicaciones	121.2
3200	32701	Patentes, derechos de autor, regalías y otros	57,861.9
3300	33301	Servicios de desarrollo de aplicaciones informáticas	46,384.0
3300	33304	Servicios de mantenimiento de aplicaciones informáticas	9.9
3300	33501	Estudios e investigaciones	5,870.2
3300	33606	Servicios de digitalización	7,568.6
3500	35301	Mantenimiento y conservación de bienes informáticos	9,281.9
5000		**Bienes muebles, inmuebles e intangibles**	
5100	51501	Bienes informáticos	586.9
5200	52101	Equipos y aparatos audiovisuales	534.4
5200	,52301	Cámaras fotográficas y video	68.6
5600	56501	Equipos y aparatos de comunicaciones y telecomunicaciones	4,598.6
		Total:	**290,783.5**

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

NOTA: Diferencias por redondeo.

Del universo seleccionado en 2022 por 290,783.5 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 65,329.8 miles de pesos en tres contratos que representan el 22.5% del universo seleccionado, los cuales se integran de la manera siguiente:

MUESTRA DE CONTRATOS CON PAGOS EJERCIDOS DURANTE 2022

(Miles de pesos)

Contrato	Proveedor	Objeto del contrato	Vigencia		Monto mínimo total	Monto máximo total	Ejercido 2022
			De	Al			
SCJN/DGRM/DSG-009/05/2019	METRICS TO INDEX GROUP, S.A.P.I. DE C.V.	Servicio integral para el estudio e investigación de información y tendencias en medios digitales a través de un visor de datos.	01/06/2019	15/12/2022	-	46,936.6	10,010.9
SCJN/DGRM/DPC-038/12/2019	FOCUS ON SERVICES, S.A DE C.V.	Servicio integrado de infraestructura de procesamiento y almacenamiento, en consumo bajo demanda.	01/01/2020	31/12/2023	89,928.2	128,858.7	16,324.6
SCJN/DGRM/DCP-026/10/2021	TOTALSEC, S.A DE C.V.	Servicio administrado para un centro de operaciones de ciberseguridad.	06/10/2021	31/12/2023	73,394.8	80,761.6	38,994.3
				Total:	**163,323.0**	**256,556.9**	**65,329.8**

FUENTE: Elaborado con base en la información proporcionada por la SCJN.

Se verificó y se confirmó que los pagos fueron reconocidos en las partidas presupuestarias correspondientes.

El análisis de los contratos de la muestra se presenta en los resultados subsecuentes.

2. Contrato número SCJN/DGRM/DSG-009/05/2019 “Servicio integral para el estudio e investigación de información y tendencias en medios digitales a través de un visor de datos”

Se revisó el contrato número SCJN/DGRM/DSG-009/05/2019, suscrito con Metrics to Index Group, S.A.P.I. de C.V., adjudicado directamente con fundamento en los artículos 41, fracción I y 91, del Acuerdo General de Administración VI/2008, del 25 de septiembre de 2008, del Comité de Gobierno y Administración de la SCJN. La vigencia del contrato fue del 1 de junio del 2019 al 15 de diciembre de 2022, por un monto total de 46,936.6 miles de pesos, para la prestación del “Servicio integral para el estudio e investigación de información y tendencias en medios digitales a través de un visor de datos”. Durante el ejercicio de 2022, se realizaron pagos por 10,010.9 miles de pesos. En el análisis de esta contratación se determinó lo siguiente:

Alcance del servicio

El contrato tuvo como objeto proporcionar un servicio integral, oportuno y permanente de investigación, análisis y estudio de tendencias en medios digitales por medio de un visor de datos con el uso de una licencia de representación de medios digitales en tiempo real, así como investigaciones y estudios mensuales para todo el Poder Judicial de la Federación, integrado por la la Suprema Corte de Justicia de la Nación, el Consejo de la Judicatura

Federal, el Tribunal Electoral del Poder Judicial de la Federación y los Tribunales de Circuito (colegiados y unitarios), con finalidad de guiar la comunicación y la toma de decisiones. El servició consideró las características siguientes:

- Servicio disponible las 24 horas los 365 días del año por medio de un visor de datos.

- Licencia de representación de datos de medios digitales en tiempo real, multiusuarios y sin límite de consultas, permitiendo extraer y representar en tableros la información de medios públicos, sociales y de grupos de información que el Poder Judicial de la Federación requiera para la toma de decisiones en tiempo real. Este visor se destinó para el uso del personal de la Dirección General de Comunicación Social para poder consultar a detalle información específica que requiriera.

- Aprovisionamiento de equipamiento técnico para el visualizador el cual incluyó:

    - Tres pantallas (monitores) mayores a 32 pulgadas.

    - Un servidor con capacidad mínima de 10 TB de almacenamiento.

    - Un equipo de alimentación ininterrumpida (UPS).

    - Tres minicomputadoras o en su defecto una tarjeta divisoria que permita transmitir los reportes a los tres monitores.

    - Una computadora de transmisión.

    - Un firewall.

    - Soportes de pared y cable necesarios para la instalación de los equipos, así como su conexión en red.

    - Dos servidores de internet.

- Generación de estudios e investigaciones mensuales de medios digitales que incluyeran menciones al Poder Judicial de la Federación, a los 11 Ministros, a los Magistrados y a los Jueces que lo componen. Entre otros aspectos, los reportes generados incluyeron un balance informativo de la actitud hacia el Poder Judicial de la Federación (PJF), al Ministro Presidente y los demás ministros de la corte, así como un resumen de las principales tendencias en medio digitales con alusiones al PJF.

La responsabilidad de la administración del servicio, así como de la infraestructura proporcionada, recayó en la Dirección General de Comunicación Social de la SCJN.

Pagos

En la revisión de los pagos realizados al proveedor Metrics to Index Group, S.A.P.I. de C.V., por los servicios proporcionados, se observó que los procesos de recepción de facturas, de aceptación de los servicios y de solicitud de pago cumplieron con los requerimientos y objetivos establecidos en la normativa aplicable.

Cumplimiento técnico y funcional de los servicios y entregables establecidos

- El documento identificado como "Acuses recepción de carpetas con entregables 2022", presenta un error en la fecha, toda vez que indica que es del “8 de agosto de abril 2021”.

- Los entregables denominados “Análisis - Coyunturales” de enero a abril de 2022; no fueron reportados en las actas de entrega-recepción por lo que no existe una formalización de su entrega y tampoco es posible determinar la fecha en que fueron recibidos por la SCJN. Adicionalmente, la totalidad de entregables proporcionados por el proveedor no cuentan con nombre y firma del personal responsable ni fecha de elaboración; tampoco permiten acreditar la fuente de información utilizada para su elaboración.

- El contrato y su anexo único no incluyeron la definición de niveles de servicio; tampoco establecieron fechas o una periodicidad para la entrega de los servicios y reportes y no se especificó el contenido mínimo que debían contener los entregables.

Por lo anterior, se concluye que existieron deficiencias en la administración y supervisión del contrato, toda vez que existen errores en la calidad de los entregables y en las actas de entrega-recepción que no fueron identificados por el personal a cargo de su validación; adicionalmente, se identificaron áreas de oportunidad en el proceso de definición del anexo técnico, debido a que en éste no se especificaron los niveles de servicio ni las fechas para la entrega de los servicios y reportes, así como el contenido mínimo que debían incluir dichos reportes.

2022-0-03100-20-0380-01-001 **Recomendación**

Para que la Suprema Corte de Justicia de la Nación realice las acciones que le permitan robustecer sus mecanismos de control interno a fin de que, para futuras contrataciones en materia de Tecnologías de Información y Comunicaciones, los instrumentos contractuales y sus anexos técnicos incluyan el detalle de los entregables requeridos, así como la definición de niveles de servicio; asimismo, fortalezca sus controles de supervisión y validación que le permitan verificar el cumplimiento de las obligaciones derivadas de los contratos, para que los entregables y servicios se proporcionen en los términos, y con la calidad y veracidad requeridos y, en caso de incumplimiento, se apliquen las penalizaciones o deductivas correspondientes, con la finalidad de asegurar las mejores condiciones para la Suprema

Corte de Justicia de la Nación y que los servicios contratados cumplen con los objetivos para los cuales fueron requeridos.

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

3. Contrato número SCJN/DGRM/DPC-038/12/2019 "Prestación de servicios integrados de infraestructura de procesamiento y almacenamiento, en consumo bajo demanda"

Se revisó el contrato abierto número SCJN/DGRM/DPC-038/12/2019, suscrito con Focus On Services, S.A. de C.V., adjudicado por medio de la Licitación Pública Nacional No. CFJ/SEA/DGRM/LPN/029/2019, con fundamento en los artículos 327, fracción II y 358, primer párrafo, del Acuerdo General del Pleno del Consejo de la Judicatura Federal, que establece las disposiciones en materia de actividad administrativa del propio Consejo, en adelante "Acuerdo Administrativo". La vigencia del contrato fue del 1 de enero de 2020 al 31 de diciembre de 2023, por un monto mínimo total de 89,928.2 miles de pesos y un máximo total de 128,858.7 miles de pesos, para la "Prestación de servicios integrados de infraestructura de procesamiento y almacenamiento, en consumo bajo demanda". Durante el ejercicio de 2022, se pagaron 16,324.6 miles de pesos. A partir del análisis de esta contratación se determinó lo siguiente:

Alcance del servicio

La SCJN requirió la implementación de un modelo de aprovisionamiento bajo demanda de servicios de infraestructura central de procesamiento y almacenamiento en sus instalaciones, además, se consideró los servicios siguientes:

- **Servicio de instalación y configuración de infraestructura:** migración, instalación y puesta en operación de toda la solución solicitada por la SCJN.

- **Servicio de soporte reactivo:** atención, apoyo y reacción ante cualquier eventualidad presentada en la infraestructura de procesamiento y almacenamiento.

- **Servicio de monitoreo:** detección de anomalías dentro de las plataformas de hardware y software de los servicios de aprovisionamiento de la infraestructura de procesamiento y almacenamiento.

- **Servicio de medición y facturación del consumo:** seguimiento y medición del consumo de los recursos de procesamiento y almacenamiento para realizar la facturación correspondiente y el pronóstico de capacidad para la determinación de crecimientos.

- **Servicio de administración de cambios:** evaluación de impactos y autorización a los cambios de manera ordenada evitando afectaciones en el modelo de consumo bajo demanda.

- **Servicio de hiperconvergencia:** implementación de una arquitectura hiperconvergente de procesamiento y almacenamiento para sus centros de datos.

- **Servicio de infraestructura de Firma Electrónica Certificada del Poder Judicial de la Federación (FIREL):** renovación de la infraestructura de cómputo y almacenamiento de la Firma Electrónica del Poder Judicial de la Federación.

- **Infraestructura de respaldo/restauración y archivado de copias de seguridad:** implementación y gestión de una solución integral para el respaldo, la restauración y el archivado de copias de seguridad de datos.

Adicionalmente, se incluyeron actividades de migración de servidores físicos y virtuales hacia los nuevos equipos de procesamiento y almacenamiento proporcionados como parte del servicio.

Pagos

En la revisión de los pagos realizados al proveedor Focus On Services, S.A. de C.V., por los servicios proporcionados, se observó que los procesos de recepción de facturas, de aceptación de los servicios y de solicitud de pago cumplieron con los requerimientos y objetivos establecidos en la normativa aplicable.

Cumplimiento técnico y funcional de los servicios y entregables establecidos

Se realizó la revisión técnica, funcional y de entregables del resto de los servicios proporcionados del periodo del 1 de enero al 31 de diciembre de 2022 con base en lo establecido en el Anexo Técnico, y se observó que los servicios y entregables fueron proporcionados en tiempo y forma y que la dependencia realizó las validaciones correspondientes, por lo que el servicio cumplió con los requerimientos y objetivos establecidos; sin embargo, existen áreas de oportunidad en las actividades de validación al cumplimiento de las especificaciones técnicas establecidas en el contrato, toda vez que no se realizaron pruebas de verificación al mecanismo de réplica de información automatizado que existe entre los servidores que soportan los sistemas de información de la aplicación FIREL y no se proporcionó evidencia que acredite que la herramienta utilizada valide la integridad de la información replicada.

La(s) acción(es) vinculada(s) a este resultado se presenta(n) en el(los) resultado(s) con su(s) respectiva(s) acción(es) que se enlista(n) a continuación:

Resultado 6 - Acción 2022-0-03100-20-0380-01-003

4. Contrato número SCJN/DGRM/DPC-026/10/2021 "Prestación del servicio Administrado para un Centro de Operaciones de Ciberseguridad"

Se revisó el contrato abierto número SCJN/DGRM/DPC-026/10/2021, suscrito con Totalsec, S.A. de C.V., adjudicado por medio del concurso por invitación restringida número CIR/SCJN/DGRM/001/2021, con fundamento en los artículos 21, fracción XXIII, 77, fracción II, 82 y 85, fracción VI, del "*Acuerdo General de Administración XIV/2019, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, del siete de noviembre de dos mil diecinueve, por el que se regulan las procedimientos para la adquisición, arrendamiento, administración y desincorporación de bienes y la contratación de obras y prestación de servicios requeridos para la Suprema Corte de Justicia de la Nación*". La vigencia del contrato fue del 6 de octubre de 2021 al 31 de diciembre de 2023, por un monto mínimo total de 73,394.84 miles de pesos y un máximo total de 80,761.58 miles de pesos, cuyo objeto fue la "Prestación del servicio Administrado para un Centro de Operaciones de Ciberseguridad". Durante el ejercicio de 2022, se pagaron 38,994.3 miles de pesos. En el análisis de esta contratación se determinó lo siguiente:

Alcance del servicio

La SCJN requirió un servicio administrado que incluyera un Centro de Operaciones Especializado y Certificado en Procesos de Ciberseguridad (COC) con el objeto de monitorear, detectar, mitigar y gestionar los incidentes de seguridad informática que se presentaran en la red LAN de la SCJN y en el ciberespacio, fortaleciendo la protección y continuidad de la operación de los sistemas informáticos jurídicos y administrativos. El contrato integró los servicios siguientes:

- **Servicio de Centro de Operaciones en Ciberseguridad (COC):** monitoreo, identificación, análisis, registro y apoyo en la resolución de cualquier incidente en materia de ciberseguridad.

- **Servicio de modelado de tráfico:** administración y gestión del ancho de banda del servicio de internet.

- **Servicio de detección y protección de amenazas avanzados con base en comportamiento:** monitoreo integral de la seguridad informática de la red LAN de la SCJN (tráfico interno) y de los puntos finales (equipos de cómputo de usuarios y equipos servidores).

- **Servicio de protección para puntos finales (EDR):** protección de los equipos de cómputo de la SCJN contra cualquier amenaza o malware.

- **Modelo Institucional de Gobierno de Seguridad:** aplicado a los activos informáticos de la Dirección General de Tecnologías de la Información (DGTI) bajo el marco del estándar ISO27001.

Adicionalmente, el servicio incluyó la administración, mantenimiento, soporte técnico, actualizaciones de versión y parches de las herramientas y soluciones de seguridad informática de la SCJN, además de las configuraciones requeridas para su operación durante la vigencia del contrato.

El servicio se prestó en seis edificios de la SCJN ubicados en la Ciudad de México, así como en 40 casas de la cultura jurídica distribuidas en todo el territorio nacional.

Pagos

En la revisión de los pagos realizados al proveedor Totalsec, S.A. de C.V., por los servicios proporcionados, se observó que los procesos de recepción de facturas, de aceptación de los servicios y de solicitud de pago cumplieron con los requerimientos y objetivos establecidos en la normativa aplicable.

Cumplimiento técnico y funcional de los servicios y entregables establecidos

Servicio de Centro de Operaciones de Ciberseguridad (COC)

Los reportes integrales mensuales del "Servicio de Centro de Operaciones de Ciberseguridad (COC)" no contaron con el apartado correspondiente al reporte de detección de amenazas requerido en el anexo técnico del contrato; adicionalmente, los reportes de enero a agosto y de octubre a diciembre de 2022, no se encontraban estandarizados toda vez que las tablas de los registros de cambios y de incidentes presentaron campos y columnas diferentes por mes, es decir, no reportaron la misma información; asimismo, el formato de la hora en el campo de tiempo de atención no se encontraba homologado y no se incluyó el campo de fecha de cierre de los registros de cambios y de incidentes; no obstante, la SCJN homologó los formatos para el ejercicio de 2023.

Servicio de protección para puntos finales (EDR)

Los documentos correspondientes al “Reporte Mensual Servicio de protección para puntos finales (EDR)” del periodo de enero a diciembre de 2022, no cuentan con un apartado donde se especifiquen las altas, bajas y modificaciones realizadas como se requirió en el anexo técnico del contrato.

Herramientas y soluciones de seguridad informática

El “Plan de trabajo general” de fecha 15 de octubre de 2021, proporcionado por el proveedor, estableció como fecha de inicio el 26 de julio y de término el 28 de julio del 2021 para las tareas de ejecución e implementación de las soluciones tecnológicas como son los certificados SSL, la herramienta de protección de sitios web en la nube, el correlacionador de eventos, las herramientas de análisis forense y recuperación de información, la solución antispam y el analizador de vulnerabilidades; sin embargo, el contrato inició su vigencia el 6 de octubre de 2021.

Por lo anterior se concluye que existen áreas de oportunidad en la administración y supervisión al cumplimiento técnico del contrato, toda vez que los entregables proporcionados no cumplieron con algunas de las características establecidas en el anexo técnico y presentaron errores en su elaboración.

La(s) acción(es) vinculada(s) a este resultado se presenta(n) en el(los) resultado(s) con su(s) respectiva(s) acción(es) que se enlista(n) a continuación:

Resultado 2 - Acción 2022-0-03100-20-0380-01-001

5. Ciberseguridad

Para evaluar la ciberseguridad de la SCJN, el grupo auditor realizó pruebas al 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), con los resultados siguientes:

Evaluación de Ciberseguridad basada en el CIS

El alcance de la auditoría consideró 18 controles de seguridad críticos (CSC) que incluyen 158 actividades de control individuales para evaluar el diseño y la efectividad operativa con sus respectivos objetivos de cumplimiento.

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 33.0% del cumplimiento de los requerimientos por control.
- **Requiere fortalecer el control - Amarillo:** entre el 33.0 y el 67.0% del cumplimiento de requerimientos por control.
- **Aceptable - Verde:** más del 67.0% del cumplimiento a los requerimientos por control.

SEMÁFORO DE CUMPLIMIENTO DE LOS CONTROLES DE CIBERSEGURIDAD EN LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

Control	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2022	79%	56%	58%	63%	36%	80%	93%	83%	86%	100%	71%	100%	100%	63%	10%	55%	75%	0%

Aceptable

Requiere fortalecer el control

Carencia de control

FUENTE: Elaborado con base en la información proporcionada por la SCJN.

Como resultado de la revisión, se identificó que, de los 18 controles evaluados, 10 (55.6%) obtuvieron un nivel aceptable, 6 (33.3%) obtuvieron un nivel que se requiere fortalecer y 2 (11.1%) se determinaron con una carencia de control.

El detalle de las observaciones y hallazgos de cada uno de los controles de seguridad críticos es el siguiente:

CSC 1: Inventario y control de los activos empresariales

- La SCJN no utiliza el módulo para la administración de dispositivos móviles con el que cuenta la herramienta utilizada para el control de sus activos; adicionalmente, no se tienen políticas ni lineamientos formalizados para que los equipos personales accedan a los recursos de la SCJN.

- Se careció de un procedimiento formalizado para la gestión de activos no autorizados.

CSC 2: Inventario y control de activos de software

- Se identificaron licencias vencidas en uso y registradas en el inventario de activos de software; asimismo, existe software utilizado por la SCJN que no se encuentra registrado en dicho inventario.

- Existen áreas de mejora en los mecanismos para detectar software no autorizado en la infraestructura de cómputo, así como para identificar si el software instalado cuenta con soporte por parte del fabricante.

- Se careció de controles y listas de aplicaciones permitidas, así como de la utilización de bibliotecas de software autorizadas.

CSC 3: Protección de datos

- Existen oportunidades de mejora en los controles implementados para el acceso a los sistemas locales y remotos.

- No se contó con una herramienta automatizada para la prevención de pérdida de datos.

- Se observaron carencias en los mecanismos de cifrado en la infraestructura de la SCJN.

- Se identificaron áreas de mejora en las normativas, políticas y procedimientos en materia de gestión, retención, flujo, clasificación, confidencialidad y borrado seguro de los datos.

CSC 4: Configuración segura de activos y software empresarial

- Existen deficiencias en los mecanismos implementados en la SCJN para la configuración segura de los activos de la entidad.

- No se contó con mecanismos para el borrado remoto de los datos de los dispositivos portátiles cuando se considere apropiado.

CSC 5: Administración de cuentas

- Existen deficiencias en la gestión de cuentas de usuario en las bases de datos, sistemas y aplicaciones de la SCJN.

CSC 6: Gestión de control de accesos

- Existen oportunidades de mejora en los mecanismos implementados para la autenticación de accesos remotos.

- No se contó con un inventario de sistemas de autenticación y autorización en la SCJN.

CSC 7: Gestión continua de vulnerabilidades

- Durante el ejercicio de 2022 no se realizó la revisión y actualización del procedimiento para el análisis de vulnerabilidades de la infraestructura tecnológica de aplicaciones de la SCJN; adicionalmente, no existen normativas o lineamientos formalizados que garanticen la revisión y actualización periódica de dicho procedimiento.

CSC 8: Gestión de registros de auditoría

- Se careció de políticas y procedimientos para la gestión de registros (logs) de auditoría, que consideren la recopilación y retención centralizada de los registros.

CSC 9: Protecciones del correo electrónico y navegador web

- Existen áreas de mejora en los mecanismos implementados para la protección de correo electrónico y navegadores web.

CSC 11: Recuperación de datos

- Durante el ejercicio de 2022 no se realizó la revisión y actualización del procedimiento para la administración de respaldos y restauración de información; adicionalmente, no existen normativas o lineamientos formalizados que garanticen la revisión y actualización periódica de dicho procedimiento.

- La SCJN no contó con una instancia aislada para la recuperación de datos.

CSC 14: Concientización en seguridad y formación de habilidades

- No se proporcionó evidencia que acredite la realización de capacitaciones al personal de nuevo ingreso en materia de seguridad informática, ni se tiene definida la frecuencia de capacitación al personal en aspectos relacionados con la seguridad de la información.

- La capacitación impartida en materia de seguridad de la información no consideró las habilidades específicas requeridas para cada función o rol.

CSC 15: Gestión de proveedores de servicios

- Se careció de una política definida y formalizada para la gestión de proveedores de servicios de TIC, que considere la generación y actualización de un inventario de proveedores.

- No se contó con un lineamiento formalizado que garantizara que los contratos celebrados con proveedores de servicios de TIC incluyeran requisitos en materia de seguridad de la información.

CSC 16: Seguridad en el software de aplicación

- No se capacitó al personal en temas de seguridad de aplicaciones y codificación segura, pruebas de penetración ni en modelos de amenazas.

- Existen deficiencias en la gestión de seguridad en el *software* de aplicación de la SCJN.

CSC 17: Gestión de respuesta a incidentes

- Durante el ejercicio de 2022 no se realizó la revisión y actualización del procedimiento de respuesta a incidentes de seguridad Informática; adicionalmente, no existen normativas o lineamientos formalizados que garanticen la revisión y actualización periódica de dicho procedimiento.

- El proceso de respuesta a incidentes de seguridad de la SCJN presentó deficiencias.

CSC 18: Pruebas de penetración

- Se identificaron deficiencias en los mecanismos implementados para la realización de pruebas de penetración a la infraestructura y aplicaciones de la SCJN.

Por lo anterior, se concluye que existen áreas de oportunidad en los controles de ciberdefensa, relacionadas con las directrices, infraestructura y herramientas informáticas de la Suprema Corte de Justicia de la Nación.

2022-0-03100-20-0380-01-002 **Recomendación**

Para que la Suprema Corte de Justicia de la Nación fortalezca sus mecanismos de control en materia de seguridad de la información, con procedimientos y controles para inventario y control de activos de software, protección de datos, configuración segura de activos y software empresarial, administración de cuentas, gestión de control de accesos, gestión continua de vulnerabilidades, gestión de registros de auditoría, protecciones del correo electrónico y navegador web, así como establecer y mantener programas de capacitación y concientización en materia de seguridad, gestión de proveedores de servicios, mantener un proceso de desarrollo seguro de aplicaciones, respuesta y manejo de incidentes de ciberseguridad, así como pruebas de penetración.

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. Continuidad de las operaciones

Como parte de los trabajos de auditoría se verificaron las condiciones que la SCJN presenta en los procesos de continuidad de las operaciones de TIC y de recuperación contra desastres para garantizar la disponibilidad de la información y continuidad de los servicios, tomando como marco de referencia los requerimientos del estándar ISO 22301:2019, norma internacional para sistemas de gestión de la continuidad de negocio (SGCN). En el análisis realizado se identificó lo siguiente:

Sistema de gestión de la continuidad de negocio

- La SCJN no formalizó ni implementó un Sistema de Gestión de Continuidad del Negocio. A la fecha de la auditoría (diciembre de 2023), la implementación de este mecanismo se encontraba en proceso de definición por parte del Comité de Control Interno Institucional de la SCJN.

- Se careció de un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) y de un Plan de Recuperación contra Desastres (DRP, por sus siglas en inglés) definido, formalizado e implementado a nivel institucional.

Recuperación contra Desastres

- Los tres centros de datos que soportan las operaciones de la SCJN se encuentran ubicados en un mismo punto de la república mexicana, por lo que, ante desastres naturales, conflictos sociales o cualquier otra situación que se presente en la ciudad, éstos podrían verse afectados de manera simultánea y las operaciones interrumpidas.

- La SCJN no realizó actividades de revisión, evaluación y auditorías para verificar el correcto funcionamiento de los mecanismos implementados para asegurar la

continuidad de las operaciones y que consideraran la ejecución de pruebas integrales para la verificación del funcionamiento de réplica de información entre los centros de datos de la SCJN.

- Se careció de procedimientos formalizados en materia recuperación de desastres que consideren actividades para invocar los mecanismos de recuperación, así como de comunicación para la gestión de dichos mecanismos.

- No existen políticas y procedimientos formalizados para el control de accesos físicos a los centros de datos, así como para la para la gestión del control ambiental (temperatura, ventilación, humedad, vibración y ruido) y suministro de energía eléctrica dentro de éstos.

- Se identificaron áreas de oportunidad en el reforzamiento de las puertas y ventanas del centro de datos ubicado en el edifico alterno de la SCJN.

- No se contó con un sistema de gestión de la configuración para mantener las versiones actuales de los documentos relacionados con la gestión de los centros de datos, así como de los inventarios de *software* y activos.

- Se careció de una política formalizada para la retención de respaldos de información dentro de los centros de datos, que establezca los tiempos de retención de éstos.

- La SCJN no proporcionó el "Procedimiento de detección de errores" complementario al protocolo de activación de contingencia de la Plataforma FIREL.

- No se impartió capacitación al personal de la SCJN respecto a los procedimientos, actividades y mecanismos para la recuperación de desastres.

- La SCNJ no acreditó contar con seguros contra la pérdida o daño de equipos y medios de almacenamiento relacionados con los centros de datos.

Por lo anterior, se concluye que existen áreas de oportunidad en los controles y actividades implementados por la SCJN para la gestión de la continuidad del negocio y la recuperación en caso de desastres y que las deficiencias identificadas podrían afectar la integridad y disponibilidad de la información.

2022-0-03100-20-0380-01-003 **Recomendación**

Para que la Suprema Corte de Justicia de la Nación fortalezca sus mecanismos de control interno, en materia de continuidad de las operaciones, que le permitan definir, formalizar e implementar un Sistema de Gestión de Continuidad del Negocio para poder identificar y establecer mecanismos de atención ante interrupción de las operaciones y que considere medidas de mitigación, roles y responsabilidades, áreas involucradas, mecanismos de comunicación y evaluación así como las políticas y procedimientos que permitan gestionar cada uno de los elementos que conformaran el sistema; definir y formalizar en conjunto con

las áreas usuarias, un Plan de Continuidad del Negocio (BCP) basado en un Análisis de Impacto al Negocio (BIA), y un Plan de Recuperación en caso de Desastres (DRP), que incluya procedimientos y políticas formalizadas para la gestión de acceso físico, controles ambientales y gestión eléctrica en los centros de datos; adicionalmente, determinar procedimientos de pruebas periódicas que permitan evaluar el funcionamiento del Plan de Continuidad de Negocio ante una contingencia, así como de los mecanismos de réplica de información de respaldos y entre los centros de datos, con la finalidad de garantizar la continuidad de las operaciones y que se cuenta con la capacidad suficiente de recuperación.

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.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: 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:

3 Recomendaciones.

Consideraciones para el seguimiento

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

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

Dictamen

El presente se emite el 6 de febrero de 2024, 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, la Suprema Corte de Justicia de la Nación cumplió con las disposiciones legales y normativas aplicables en la materia, excepto por los aspectos observados siguientes:

- De la muestra seleccionada de tres contratos, se evaluó el cumplimiento técnico y funcional de los servicios y entregables establecidos y se identificaron deficiencias en relación con la calidad de los entregables proporcionados.

- 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 18 controles, 10 cuentan con un nivel aceptable, se requiere fortalecer 6 controles y 2 carecen de control, por lo que existen áreas de oportunidad en su administración y operación.

- La SCJN no cuenta con un Sistema de Gestión de Continuidad del Negocio; tampoco ha definido, formalizado e implementado un Plan de Continuidad del Negocio ni un Plan de Recuperación contra Desastres; adicionalmente, existen oportunidades de mejora en los controles y actividades implementados por la SCJN para la gestión de la continuidad del negocio y la recuperación en caso de desastres, las cuales podrían afectar la continuidad de las operaciones.

Servidores públicos que intervinieron en la auditoría:

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

Comentarios de la Entidad Fiscalizada

Es importante señalar que la documentación proporcionada por la entidad fiscalizada para aclarar o justificar los resultados y las observaciones presentadas en las reuniones fue analizada con el fin de determinar la procedencia de eliminar, rectificar o ratificar los resultados y las observaciones preliminares determinados por la Auditoría Superior de la

Federación y que se presentó a este órgano técnico de fiscalización para efectos de la elaboración definitiva del Informe General Ejecutivo del Resultado de la Fiscalización Superior de la Cuenta Pública.

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública se corresponden con las registradas en el estado del ejercicio del presupuesto y que cumplen con las disposiciones y normativas aplicables y 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 procedimiento de contratación, el cumplimiento de las especificaciones técnicas y la distribución del bien o servicio de acuerdo con las necesidades requeridas por las áreas solicitantes; revisar que los bienes adquiridos se contemplaron en el Programa Anual de Adquisiciones, Arrendamientos y Servicios; verificar la situación fiscal de los proveedores para conocer el cumplimiento de sus obligaciones fiscales, aumento o disminución de obligaciones, entre otros.

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

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, el 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, los entregables (términos, vigencia, entrega, resguardo, garantías, pruebas de cumplimiento y sustantivas); la implementación y el soporte de los servicios; verificar que el plan de mitigación de riesgos fue atendido, 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), y las políticas de respaldos, replicación de datos, planeación de la capacidad y disponibilidad de la infraestructura tecnológica, entre otros. Verificar la seguridad física y lógica del centro de datos en sus componentes como el control de acceso físico; el sistema de videovigilancia; la prevención y extinción de incendios; el sistema de detección de líquidos; el control de medio ambiente y el sistema eléctrico, entre otros.

Áreas Revisadas

La Oficialía Mayor, la Dirección General de Presupuesto y Contabilidad, la Dirección General de Recursos Materiales, la Dirección de Servicios Generales, la Dirección General de Tecnologías de Información, la Dirección de Seguridad Informática, la Dirección General de Comunicación Social, la Dirección de Continuidad de Operaciones y la Subdirección de Infraestructura de Servicios de Centros de Datos, todas ellas de la SCJN.

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: Acuerdo General de Administración VI/2008, del veinticinco de septiembre de dos mil ocho, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, Art. 142, Frac. II y IX, Art.154, Frac. VI, Par. Tercero, Art. 167 y 172; Acuerdo General de Administración número VIII/2022, del Comité de Gobierno y Administración de la Suprema Corte de Justicia de la Nación, de siete de noviembre de dos mil veintidós, Art. 151, 155 y 162, Frac. I y IV; contrato número SCJN/DGRM/DSG-009/05/2019, cláusulas Décima sexta y Vigésima quinta; anexo único del contrato número SCJN/DGRM/DSG-009/05/2019, anexo 2a, sección A, numerales 3 y 3.1; anexo técnico del contrato número SCJN/DGRN/DPC-038/12/2019, apartado F, subpartida 2, apéndice 4, sección 6.1, punto 10; anexo técnico del contrato número SCJN/DGRM/DPC-026/10/2021, numeral 5.3; Manual de Organización Específico de la Dirección General de Tecnologías de la Información, numeral 1.2.1.5, función 3, numeral 1.2.2, función 3, numeral 1.2.3,

función 2, numeral 1.3, funciones 4 y 6, numeral 1.3.1.2.1, objetivo, numeral 1.3.2, objetivo y función 3, numeral 1.3.2.2.1, función 7, numeral 1.3.2.3, función 1, numeral 1.3.3, función 3, numeral 1.3.3.1, función 3, numeral 1.4.2, función 5, numeral 1.5, función 8

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.