Fiscalía General de la República

Auditoría de TIC

Auditoría De Cumplimiento a Tecnologías de Información y Comunicaciones: 2019-0-17100-20-0097-2020

97-GB

Criterios de Selección

Esta auditoría se seleccionó con base en los criterios establecidos por la Auditoría Superior de la Federación para la integración del Programa Anual de Auditorías para la Fiscalización Superior de la Cuenta Pública 2019 considerando lo dispuesto en el Plan Estratégico de la ASF.

Objetivo

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

Consideraciones para el seguimiento

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

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

Alcance

	EGRESOS
	Miles de Pesos
Universo Seleccionado	1,058,168.4
Muestra Auditada	431,559.8
Representatividad de la Muestra	40.8%

El universo seleccionado por 1,058,168.4 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 2019; la muestra auditada está integrada por seis contratos para prestar servicios informáticos de infraestructura de TIC, servicios integrales de impresión, digitalización y fotocopiado de documentos, así como con los servicios de licenciamiento, soporte premier y cómputo en la nube, con pagos ejercidos por 431,559.8 miles de pesos, que representan el 40.8% del universo seleccionado.

Adicionalmente, la auditoría comprendió la revisión de la función de TIC en la Fiscalía General de la República (FGR) en 2019, relacionada con el Gobierno de las TIC, Seguridad de la Información, Continuidad de las Operaciones y Centro de Datos.

Antecedentes

La Fiscalía General de la República (FGR) tiene como fin la investigación de los delitos y el esclarecimiento de los hechos, otorgar una procuración de justicia eficaz, efectiva, ajustada a derecho, que contribuya a combatir la inseguridad y disminuirla, la prevención del delito, fortalecer el Estado de derecho en México, procurar que el culpable no quede impune, así como promover, proteger, respetar y garantizar los derechos de verdad, reparación integral y de no repetición de las víctimas, ofendidos en particular y de la sociedad en general.

La Unidad de Gobierno Digital de la Secretaría de la Función Pública autorizó a la FGR la cartera ejecutiva de proyectos de Tecnologías de Información y Comunicaciones (TIC) consistentes en los servicios de mantenimiento y soporte de licencias de software, soporte premier, cómputo en la nube y soporte proactivo; servicios informáticos integrales de impresión, digitalización y fotocopiado de documentos; servicios de informática que incluyen la actualización, soporte de uso de licencia para herramientas de seguridad informática Symantec (antivirus, antispam, protección avanzada contra amenazas) y programas para la administración automatizada de los equipos de cómputo, así como servicios de mantenimiento y soporte especializado al sistema informático Justici@net, entre otros.

Entre 2015 y 2019, se han invertido 5,099,704.2 miles de pesos en sistemas de información e infraestructuras tecnológicas, integrados de la manera siguiente:

Recursos invertidos en materia de TIC
(Miles de pesos)

PERIODO DE INVERSIÓN	2015	2016	2017	2018	2019	TOTALES
MONTO POR AÑO	970,987.2	1,189,258.3	854,479.9	952,324.3	1,132,654.5	**5,099,704.2**

Fuente: Elaborada con información proporcionada por la Fiscalía General de la República.

Resultados

1. Análisis Presupuestal

En relación con el Decreto de Presupuesto de Egresos de la Federación para el Ejercicio Fiscal 2019 publicado en el Diario Oficial de la Federación el 28 de diciembre de 2018, se autorizó a la entonces Procuraduría General de la República (PGR), ahora Fiscalía General de la República (FGR), en el Ramo 17 un presupuesto de 15,351,082.7 miles de pesos, del cual se asignó al Sector Central un presupuesto de 14,730,422.0 miles de pesos.

Del análisis de la información presentada en la Cuenta de la Hacienda Pública Federal del ejercicio 2019, se concluyó que la Fiscalía General de la República (Sector Central) tuvo un presupuesto ejercido de 14,525,847.0 miles de pesos, de los cuales 1,132,654.4 miles de pesos corresponden a recursos relacionados con las TIC, lo que representa el 7.8% del presupuesto, como se muestra a continuación:

RECURSOS EJERCIDOS EN LA FISCALÍA GENERAL DE LA REPÚBLICA DURANTE 2019
(Miles de pesos)

Capítulo	Descripción	Presupuesto Ejercido	Recursos relativos a las TIC
1000	Servicios personales	10,271,348.6	74,396.3
2000	Materiales y suministros	341,043.9	12.1
3000	Servicios generales	3,875,860.1	1,058,246.0
4000	Transferencias, asignaciones, subsidios y otras ayudas	36,887.0	0.0
8000	Participaciones y Aportaciones	707.4	0.0
	TOTAL	**14,525,847.0**	**1,132,654.4**

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

Los recursos ejercidos en materia de TIC por 1,132,654.4 miles de pesos, se integran de la manera siguiente:

GASTOS TIC 2019 EN LA FISCALÍA GENERAL DE LA REPÚBLICA (SECTOR CENTRAL)
(Miles de pesos)

Capítulo	Partida	Descripción	Presupuesto Ejercido
1000		**SERVICIOS PERSONALES**	**74,396.3**
2000		**MATERIALES Y SUMINISTROS**	**12.1**
3000		**SERVICIOS GENERALES**	**1,058,246.0**
	31401	Servicio Telefónico Convencional	21,875.0
	31501	Servicio de telefonía celular	5,202.6
	31601	Servicio de radiolocalización	1,934.6
	31602	Servicio de Telecomunicaciones	482,928.3
	31701	Servicios de Conducción de Señales Analógicas y Digitales	44,834.6
	31904	Servicios Integrales de Infraestructura de Cómputo	1,417.4
	32301	Arrendamiento de Equipo y Bienes Informáticos	112,042.8
	32701	Patentes, derechos de autor, regalías y otros	169,734.2
	33301	Servicios de Desarrollo de Aplicaciones Informáticas	2,915.4
	33602	Otros servicios comerciales	198,933.0
	33903	Servicios integrales	12,158.9
	35301	Mantenimiento y conservación de bienes informáticos	4,191.6
	37201	Pasajes terrestres nacionales para labores en campo y de supervisión	19.2
	37504	Viáticos nacionales para servidores públicos en el desempeño de sus funciones	51.6
	39202	Otros impuestos y derechos	6.8
		TOTAL	**1,132,654.4**

Fuente: Elaborado con información proporcionada por FGR.

Las partidas específicas relacionadas con servicios personales (capítulo 1000) corresponden a los costos asociados de la plantilla del personal de las áreas de TIC con una percepción anual de 74,396.3 miles de pesos durante el ejercicio fiscal 2019; considerando 224 plazas, el promedio anual percibido por persona fue de 332.1 miles de pesos.

Del universo seleccionado en 2019 por 1,058,168.4 miles de pesos que corresponden al total de pagos ejercidos en contratos relacionados con las TIC, se erogaron 431,559.8 miles de pesos en seis contratos que representan el 40.8% del universo seleccionado, el cual se integra de la manera siguiente:

MUESTRA DE CONTRATOS DE PRESTACIÓN DE SERVICIOS EJERCIDOS DURANTE 2019
(Miles de Pesos)

Procedimiento de Contratación	Contrato/Convenio	Proveedor	Objeto del Contrato	Vigencia		Monto		Ejercido 2019		
				Del	Al	Mínimo	Máximo	Proveedor	TESOFE[1]	TOTAL
Adjudicación directa	PGR/AD/CN/SERV/013-9/2017	Hewlett-Packard México, S. DE R.L DE C.V.	Servicios informáticos de infraestructura TIC	15/09/2017	31/12/2018	54,400.0	136,000.0	55,841.4	620.7	56,462.1
	CM 1		Ampliar la vigencia e incrementar el presupuesto 20.0%	31/12/2018	31/03/2019	10,880.0	27,200.0			
	CM 2		Ampliar la vigencia del contrato	29/03/2019	30/04/2019	0.00	0.00			
						65,280.0	163,200.0	55,841.4	620.7	56,462.1
Adjudicación directa	FGR/AD/CN/SERV/009-05/2019	Hewlett-Packard México, S. DE R.L DE C.V.	Servicios informáticos de infraestructura TIC	15/05/2019	31/12/2019	29,037.7	72,594.1	55,106.6	474.1	55,580.7
	CM 1		Ampliar la vigencia del contrato	31/12/2019	29/02/2020	0.00	0.00			
						29,037.7	72,594.1	55,106.6	474.1	55,580.7
Adjudicación directa	PRG/AD/CN/SERV/005-7/2017	Organización Mitamex, S.A. de C.V.	Servicios Informáticos Integrales de Impresión, Digitalización y Fotocopiado de documentos	04/08/2017	31/12/2018	124,000.0	310,000.0	100,662.8	854.4	101,517.3
	CM 1		Ampliar la vigencia e incrementar el presupuesto 20.0%	31/12/2018	31/03/2019	24,800.0	62,000.0			
	CM 2		Ampliar la vigencia del contrato	29/03/2019	30/04/2019	0.00	0.00			
						148,800.0	372,000.0	100,662.8	854.4	101,517.3
Adjudicación directa	FGR/AD/CN/SERV/006-5/2019	Organización Mitamex, S.A. de C.V.	Servicios Informáticos Integrales de Impresión, Digitalización y Fotocopiado de documentos	15/05/2019	31/12/2019	61,200.0	153,000.0	97,024.2	391.5	97,415.7
	CM 1		Ampliar la vigencia del contrato	31/12/2019	31/03/2020	0.00	0.00			
						61,200.0	153,000.0	97,024.2	391.5	97,415.7
Adjudicación directa	PGR/AD/CN/SERV/004-3/2018	Microsoft Corporation	Servicios de licenciamiento, soporte premier y cómputo en la nube	05/04/2018	20/11/2018	0.00	96,485.4[2]	18,164.7	0.00	18,164.7
	CM 1		Ampliar la vigencia e incrementar el presupuesto 20.0%	20/11/2018	31/01/2019	0.00	18,164.7			
						0.00	114,650.1	18,164.7	0.00	18,164.7
Adjudicación directa	FGR/AD/CN/SERV/006-3/2019	Microsoft Corporation	Servicios de licenciamiento, soporte premier y cómputo en la nube	01/03/2019	31/12/2019	0.00	102,419.4	99,717.0	2,702.4	102,419.4
			TOTALES			**304,317.7**	**977,863.6**	**426,516.7**	**5,043.1**	**431,559.8**

Fuente: Elaborado con información proporcionada por la FGR.
Nota [1]: Recursos transferidos a la TESOFE por concepto de diferencias cambiarias y deductivas aplicadas a los proveedores.
Nota[2]: Conversión al tipo de cambio 20.2217 pesos por dólar publicado en el Diario Oficial de la Federación el 30 de noviembre de 2018.

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

2. Contratos números PGR/AD/CN/SERV/013-9/2017 y FGR/AD/CN/SERV/009-5/2019 "Prestación de servicios informáticos de infraestructura TIC"

Se analizó la información de los contratos números PGR/AD/CN/SERV/013-9/2017 y FGR/AD/CN/SERV/009-5/2019, así como sus convenios modificatorios, celebrados con Hewlett-Packard México, S. de R.L. de C.V., mediante el procedimiento de adjudicación directa de conformidad con los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 2, fracción III, 22, fracción II, 26, fracción III, 40, 41, fracciones I y IV y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 71, 72 fracciones I y IV y 85 de su Reglamento; 50 de la Ley de Presupuesto y Responsabilidad Hacendaria, y 147 de su Reglamento, vigentes del 15 de septiembre de 2017 al 29 de febrero de 2020, por un monto mínimo de 54,400.0 miles de pesos y máximo de 235,794.1 miles de pesos, con el objeto de prestar los "Servicios informáticos de infraestructura TIC", de los cuales se pagaron al proveedor 110,948.0 miles de pesos durante el ejercicio 2019, y se determinó lo siguiente:

Alcance del servicio

Dar continuidad a los servicios de tecnologías de información y comunicaciones (TIC), a través del suministro, instalación, configuración, soporte técnico y mantenimiento de los equipos de cómputo y periféricos siguientes:

Integración de los equipos del contrato número FGR/AD/CN/SERV/009-5/2019
(Unidades)

Descripción	Cantidad mínima
Computadora de escritorio	21,682
Computadora portátil	3,182
Cámara de video portátil	91
Cámara digital fotográfica	356
Computadora portátil MacBook Air de 11.6	25
Digitalizador de alta velocidad	339
Equipo de escritorio iMac	97
Equipo portátil MacBook Pro	70
Impresora portátil a color de inyección de tinta	474
iPad con pantalla retina (WiFi + celular)	262
iPad Mini (WiFi + celular)	63
UPS 6 KVA	5
UPS 10 KVA	8
UPS 3 KVA	77
Video proyector de tecnología DLP de 3000 lúmenes	371
Webcam	101

Fuente: Elaborado con información proporcionada por FGR mediante el oficio FGR/CPA/SAMC/007/2020 de fecha 14 de enero de 2020.

Proceso de contratación

La Dirección General de Tecnologías de Información y Comunicaciones (DGTIC) señaló que, como resultado del estudio de mercado, se confirmó la existencia de un solo proveedor en todo el país; sin embargo, en el mercado, se encuentran otras empresas con servicios y productos similares tales como LENOVO, DELL, entre otras.

Gestión de inventarios

En la revisión de los entregables, se identificó lo siguiente:

- La Fiscalía no reporta los números de serie de los equipos de cómputo para realizar el pago de los servicios, en contravención a lo establecido en el apartado "Reportes" del anexo técnico de los contratos; tampoco se tiene evidencia de los controles de cambio y revisiones físicas de los equipos como parte de la gestión del control de inventarios, con la finalidad de verificar que los equipos pagados mensualmente corresponden a servicios efectivamente devengados.

- No se identificaron acciones de mejora continua del servicio de conformidad con los resultados de las encuestas de satisfacción de los usuarios, en incumplimiento del apartado "Reportes" del anexo técnico del contrato.

- De conformidad con el anexo técnico del contrato, la infraestructura de TIC que suministre el proveedor debe ser con equipos de cómputo o periféricos que aún se encuentren en el catálogo vigente publicado en la página de internet del fabricante, sin incidentes que impidan contar en tiempo con la disponibilidad de partes, refacciones y componentes, asimismo, deben tener una antigüedad menor a cuatro años contados a partir del inicio de la prestación del servicio; sin embargo, se identificaron 18,620 equipos de cómputo que, de acuerdo con lo antes señalado, la Fiscalía debió solicitar su reemplazo al proveedor durante el periodo de marzo 2018 a mayo 2019, lo cual no llevó a cabo, los equipos son los siguientes:

Equipos descontinuados que no fueron reemplazados en la gestión del contrato número PGR/AD/CN/SERV/013-9/2017
(Unidades)

Cantidad de equipos	Fecha de reemplazo
3	Marzo 2018
944	Abril 2018
2743	Julio 2018
7084	Agosto 2018
1656	Septiembre 2018
3084	Noviembre 2018
133	Marzo 2019
2973	Mayo 2019

Fuente: Elaborado con documentación proporcionada por la FGR.

Pruebas del Inventario de Equipos

Se realizó una prueba de recorrido con el propósito de verificar los requisitos técnicos de los equipos. De un universo de 27,203 equipos, se revisó una muestra de 379 (95% nivel de confianza y 5% error); de 250 computadoras de escritorio, 18 (7.2%) no tenían cargada la imagen de software y 11 (4.4%) no contaban con una unidad óptica.

Cumplimiento técnico del proveedor

- No se cuenta con el certificado del administrador del contrato.

- Se carece de la documentación de siete especialistas para brindar el servicio de acuerdo con los requisitos del apartado "Constancias, diplomas o documentos análogos que acrediten el grado de conocimiento técnico sobre los equipos materia del contrato".

- El responsable del servicio presentó una constancia de estudios con la cual no acredita el grado de conocimiento técnico sobre los equipos materia del contrato.

Se concluye que existen algunas deficiencias en el proceso de investigación de mercado que sólo encontró un proveedor en todo el país, siendo que existen otros; se carece de los números de serie de los equipos de cómputo para acreditar el pago de los servicios; no se tiene evidencia del control de cambios ni revisiones físicas de los equipos como parte de la gestión de inventarios; asimismo, los equipos descontinuados no fueron reemplazados durante la gestión del contrato.

2019-0-49100-20-0097-01-001 **Recomendación**

Para que la Fiscalía General de la República fortalezca los mecanismos de control, supervisión, validación y evaluación de la gestión de servicios administrados de equipos de cómputo, así como verifique que se cuente con los números de serie de los equipos, el soporte documental de las revisiones y los controles de cambios a los inventarios para verificar el detalle de los equipos pagados, con la finalidad de asegurar el adecuado ejercicio del presupuesto de la Fiscalía en esta materia.

3. Contratos números PRG/AD/CN/SERV/005-7/2017 y FGR/AD/CN/SERV/006-5/2019 "Servicios Informáticos Integrales de Impresión, Digitalización y Fotocopiado de documentos"

Se analizó la información de los contratos números PGR/AD/CN/SERV/005-7/2017 y FGR/AD/CN/SERV/006-05/2019, así como sus convenios modificatorios, celebrados con Organización Mitamex, S.A. de C.V., mediante el procedimiento de adjudicación directa de conformidad con los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 2, fracción III, 22, fracción II, 26, fracción III, 40, 41, fracciones I y IV y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 71, 72 fracciones I y IV y 85,

de su Reglamento; 50 de la Ley de Presupuesto y Responsabilidad Hacendaria, y 147 de su Reglamento; vigentes del 4 de agosto de 2017 al 31 de marzo de 2020, por un monto mínimo de 124,000.0 miles de pesos y monto máximo por 525,000.0 miles de pesos, con el objeto de prestar los "Servicios Informáticos Integrales de Impresión, Digitalización y Fotocopiado", de los cuales se pagaron al proveedor 197,687.1 miles de pesos durante el ejercicio 2019, y se determinó lo siguiente:

Alcance de los servicios

Dotar nacionalmente, bajo un esquema de demanda, de las herramientas para realizar en formato monocromático o a color el fotocopiado, impresión, impresión de gran formato (plotter) y digitalización de documentos para un aproximado de 59 inmuebles en la Ciudad de México y 183 inmuebles distribuidos en el resto de los Estados de la República.

Investigación de mercado

- No se identificó la participación de la Dirección General de Tecnologías de Información y Comunicaciones (DGTIC) en la elaboración de la investigación de mercado.

- Se carece del resultado de la investigación de mercado que incluya las condiciones y lugares de entrega de los bienes o servicios; la forma, cantidad o volumen requerido y términos de pago; las características técnicas de los bienes o servicios y demás circunstancias que permitan la comparación objetiva entre bienes o servicios iguales o de la misma naturaleza.

- La DGTIC señaló la existencia de un solo proveedor en todo el país para la prestación de los servicios; no obstante, en el mercado, se encuentran disponibles productos alternativos de las empresas SHARP, XEROX, entre otras.

Entregables del servicio

- El reporte "Incidentes y requerimientos de servicio" no indica el número de ticket asignado por la mesa de servicios ni la descripción de la solución.

- El reporte "Altas, bajas, reemplazos y reubicaciones de infraestructura" no incluye los datos mínimos establecidos en el Anexo Técnico, tales como el número de ticket asociado a la solicitud, fecha y hora del levantamiento del ticket, fecha y hora de terminación del ticket, así como el nombre del usuario.

Gestión del inventario de equipos

- El grupo auditor solicitó comprobar que los equipos no estuvieran descontinuados, para tal efecto, el proveedor remitió una carta donde manifestó que los equipos se

encontraban dentro del catálogo vigente; no obstante, dicha carta no consideró 12 modelos incluidos en la propuesta técnica de los servicios.

- Se identificaron nueve modelos con características técnicas menores a las requeridas tales como la pantalla, velocidad de impresión, tiempo de salida de la primera página, memoria, procesador, disco duro, ciclo de trabajo mensual máximo, administración y tipo de papel soportado, no obstante, la Fiscalía no estableció deductivas por estos incumplimientos.

- De las 68 personas encargadas del soporte en sitio, se presentó documentación de 22 (32.4%) para acreditar la capacitación obtenida para la operación y servicio técnico de los equipos; del resto del personal, el formato de curriculum vitae que presentó el proveedor no permite verificar que cumplen con el perfil solicitado, lo cual no fue previsto por la Fiscalía como un incumplimiento en el contrato.

Gestión del monitoreo de los servicios

- En relación con la función de "Enviar alertas a través de correo electrónico tanto el centro de monitorio del proveedor, así como el administrador del contrato y a las personas que este designe", no se tienen correos electrónicos que muestren las alertas detectadas.

- Se carece de evidencias del monitoreo de los equipos de impresión que se conectan por medio del puerto USB, en consecuencia, no se visualiza a través de la consola si dichos equipos reportan fallas ni los niveles de consumo de tinta para su reabastecimiento.

- No se tienen evidencias de la capacitación por parte del prestador de servicios para la operación de las herramientas de monitoreo.

Se concluye que existen deficiencias en la investigación de mercado para conocer las condiciones y características técnicas de los bienes o servicios; asimismo en la búsqueda de la oferta en el mercado debido a que se señaló la existencia de un solo proveedor en todo el país, siendo que existen otros; los reportes de gestión de la infraestructura no incluyen los datos mínimos establecidos en el Anexo Técnico; se identificaron modelos con características técnicas menores a las requeridas en el contrato; sólo se comprobó que el 32.4% de los técnicos de soporte en sitio estaban capacitados para la operación y servicio de los equipos; por último, no se tienen evidencias del monitoreo de la totalidad de los equipos de impresión para conocer sus fallas y niveles de consumo.

2019-0-49100-20-0097-01-002 **Recomendación**

Para que la Fiscalía General de la República fortalezca los procedimientos para realizar investigaciones de mercado donde se revise con amplitud la existencia de proveedores con la posibilidad de cumplir con las necesidades de la contratación, el análisis de las características

técnicas de los bienes o servicios, así como la participación del área técnica; con la finalidad de contar con una comparación objetiva entre bienes y servicios iguales o de la misma naturaleza y asegurar las mejores condiciones disponibles en cuanto a precio, calidad y financiamiento en beneficio de la Fiscalía.

2019-0-49100-20-0097-01-003 **Recomendación**

Para que la Fiscalía General de la República fortalezca los mecanismos de control, verificación y supervisión de los entregables en los contratos de Tecnologías de Información y Comunicaciones, que cumplan con los criterios de aceptación señalados en los Anexos Técnicos; asimismo, que los perfiles del personal que participa en las prestación de los servicios cumplan con las competencias técnicas requeridas, con la finalidad de mejorar la calidad y el servicio del portafolio de contrataciones de Tecnologías de Información y Comunicaciones.

4. Contratos números PGR/AD/CN/SERV-004-3/2018 y FGR/AD/CN/SERV/006-3/2019 "Servicios de licenciamiento, soporte premier y cómputo en la nube"

Se analizó la información de los contratos números PGR/AD/CN/SERV-004-3/2018 y FGR/AD/CN/SERV/006-3/2019, así como sus convenios modificatorios, celebrados con Microsoft Corporation, mediante el procedimiento de adjudicación directa de conformidad con los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 2, fracción III, 22, fracción II, 26, fracción III, 40, 41, fracciones I y XX y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 71 y 72 de su Reglamento, vigentes del 5 de abril de 2018 al 31 de diciembre de 2019, por un monto máximo de 217,069.5 miles de pesos, con el objeto de prestar los "Servicios de licenciamiento, soporte premier y cómputo en la nube", de los cuales se pagaron al proveedor 117,881.7 miles de pesos durante el ejercicio 2019, y se determinó lo siguiente:

Alcance de los servicios

Asegurar la continuidad operativa de los servicios que existen en el centro de cómputo, las computadoras personales y laptops, los servicios de infraestructura y la plataforma bajo demanda de la nube de Microsoft (denominada Microsoft Azure); para tal efecto, se cuenta con servicios de licenciamiento para 20,000 equipos, actualización de versiones, administración de infraestructura, aplicaciones administrativas, servicios de cómputo en la nube (almacenamiento, directorio activo, servicio de base de datos, mensajería, colaboración, streaming de video), servicio de soporte premier (administrador del servicio, asistencia, soporte dedicado, resolución de problemas, base de conocimientos, talleres y eventos), entre otros.

Proceso de contratación

No se identificaron en el Contrato ni en su Anexo Técnico, las características técnicas (máquinas virtuales, procesamiento, almacenamiento, entre otras) de los servicios de cómputo en la nube que fueron requeridos por la Fiscalía.

Entregables del servicio

- En las pantallas que corresponden al acceso del entregable, no se observa la cantidad de licencias a las que se tiene derecho.

- No se identificaron en el Contrato ni en su Anexo Técnico, los documentos para acreditar la entrega del servicio de soporte premier (programa de análisis a plataformas, salud de la plataforma Microsoft, ingeniero de soporte dedicado, reportes mensuales de resolución de problemas, implementación de metodologías de procesos de operación y capacitación de entrega avanzada de las tecnologías Microsoft, entre otros); esta situación no permite la trazabilidad de las actividades ni el seguimiento y evaluación del desempeño del proveedor.

Servicio de Asignación de Licenciamiento de Cuentas de Correo Electrónico

De un total de 218 solicitudes del servicio ABC de correo electrónico del contrato número PGR/AD/CN/SERV-004-3/2018, se analizaron 68 (con un nivel de confianza 95.0% y error del 10.0%) y se obtuvo lo siguiente:

- El 29.4% (20 solicitudes) presenta inconsistencias en el llenado del formato como la falta del puesto del solicitante y del personal que autoriza la solicitud; asimismo, las fechas del formato no concuerdan con la fecha del registro en la mesa de servicio.

- El 11.7% (8 solicitudes) no cumple con lo establecido en el manual de procedimientos debido a que el tipo de solicitud no concuerda con lo registrado en la mesa de servicio o se carece del registro en la mesa.

En relación con las 400 solicitudes del servicio ABC de correo electrónico del contrato número FGR/AD/CN/SERV/006-3/2019, se revisaron 105 (con un nivel de confianza 95.0% y error del 8.3%) y se identificó lo siguiente:

- El 27.6% (29 solicitudes) presentan inconsistencias en el llenado del formato, como la falta de los datos del titular de la cuenta de correo, puesto del solicitante y personal que autoriza la solicitud; asimismo, las fechas del formato no concuerdan con el registro en la mesa de servicio.

- El 20.0% (21 solicitudes) no cumple debido a que el tipo de solicitud establecido en el formato no concuerda con lo asentado en la mesa de servicio o se carece del registro.

- Se identificó que los registros en la mesa de servicio no muestran el estado de las solicitudes (en atención, resuelto, pendiente, cerrado, entre otros) ni la fecha en que se da atención a la solicitud.

Servicio de Soporte Premier

- De la revisión de las horas del servicio “Account Management” (administrador de cuenta) y “Support Assistance” (asistente de soporte), se utilizaron la totalidad de las horas contratadas; sin embargo, no fue proporcionado el soporte documental para conocer las actividades efectuadas por el proveedor.

- Con relación al consumo de las horas de “Soporte Extendido” y DSE “Ingeniería de Soporte Dedicado”, no se cuenta con el desglose de las horas utilizadas en cada componente, situación que no permite el seguimiento de los servicios contratados.

- Respecto del “Soporte de Resolución de Problemas de los Servicios de Soporte Premier”, el ente público no proporcionó la justificación de la contratación de 200 horas adicionales del segundo nivel de soporte premier; misma situación en el servicio “Software Assurance” (aseguramiento de programas) en el cual no se justificó el incremento de 400 horas en el periodo de agosto a diciembre de 2019.

- Sobre los cursos de capacitación y entrenamiento técnico incluidos en el "Segundo Nivel de Soporte Premier", éstos no se llevaron a cabo debido a que la FGR indicó que fueron entregados a cambio los servicios “Custom Proactive Onsite” (servicios personalizados en sitio); no obstante, no se proporcionó evidencia para conocer el desarrollo de los cursos.

Gestión de los Servicios de Cómputo en la Nube

- La Fiscalía no realizó un análisis para evaluar los riesgos inherentes a las modalidades de cómputo en la nube y con ello establecer mecanismos de control apropiados para su administración, tampoco se proporcionó evidencia de la alineación de los servicios de cómputo en la nube con el marco de gestión del riesgo organizacional.

- No se cuenta con el histórico de los incidentes del servicio, lo que deriva en la falta de trazabilidad y análisis de las causas de los incidentes recurrentes, antes de que se conviertan en problemas que afecten la operación de los servicios.

- En la revisión de la operación de los servicios de cómputo en la nube, de conformidad con las mejores prácticas y el modelo de responsabilidad compartida con el proveedor, se identificó que se carece de políticas y procedimientos para: la autenticación de los dispositivos móviles con los sistemas para controlar su ingreso y seguimiento; el control de identidades de los usuarios y acceso a los sistemas; la privacidad y encriptación de los datos sensibles para asegurar la confidencialidad, disponibilidad e integridad de los activos de información; así como el monitoreo de

las cuentas de acceso, las pistas de auditoría y el análisis de las transacciones para detectar ingresos o cambios no autorizados a los datos.

En conclusión, se carece de detalle para conocer las actividades del servicio de soporte premier, así como para verificar la trazabilidad de las actividades y la evaluación del desempeño del proveedor; no se cuenta con control de acceso a los sistemas y encriptación de los datos sensibles para asegurar la confidencialidad, disponibilidad e integridad de la información; no se realiza la protección de los datos, se delega toda la responsabilidad al prestador de servicios, lo que podría contribuir en la vulnerabilidad de los activos de información ante un incidente cibernético.

2019-0-49100-20-0097-01-004 **Recomendación**

Para que la Fiscalía General de la República implemente procedimientos y mecanismos de control para verificar que, en las propuestas técnicas, económicas, contratos y anexos técnicos, se incluya la descripción pormenorizada de los bienes, arrendamientos o servicios objeto del contrato adjudicado; asimismo, se verifique el detalle de las actividades realizadas por los proveedores para dar cumplimiento a los criterios de aceptación de los entregables pactados en las contrataciones, con la finalidad de permitir la trazabilidad de las actividades realizadas, así como el adecuado seguimiento y evaluación de los proveedores de Tecnologías de Información y Comunicaciones.

2019-0-49100-20-0097-01-005 **Recomendación**

Para que la Fiscalía General de la República implemente políticas, procedimientos y controles para: la autenticación de los dispositivos móviles con los sistemas en la nube; el control de acceso e identidades, privacidad y encriptación de los datos sensibles de los sistemas; así como el monitoreo de las cuentas de acceso, las pistas de auditoría y el análisis de las transacciones de las bases de datos; con la finalidad de fortalecer la seguridad de la información en los aplicativos y sistemas para mitigar las vulnerabilidades que puedan comprometer la integridad, confidencialidad y disponibilidad de los activos de información.

5. Gobierno de las TIC

El 20 de diciembre de 2018, entró en vigor el Decreto que establece la autonomía de la Fiscalía General de la República, a partir de esa fecha no se encontraba obligada a dar cumplimiento a los procesos del Manual Administrativo de Aplicación General en las materias de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI); no obstante, la Fiscalía entró en una etapa de transición y siguió operado bajo los procesos definidos en el MAAGTICSI, sus apéndices y mejores prácticas relacionadas.

En el análisis al Gobierno de las TIC, respecto a las soluciones e infraestructura tecnológica del ente público, de conformidad con los procesos de Planificación Estratégica, Administración del Servicio y Administración de la Seguridad de la Información de los marcos

rectores antes mencionados, así como con las políticas y lineamientos proporcionados por la Fiscalía en esta materia, se observó lo siguiente:

Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

- No se cuenta con el análisis de la situación actual y futura para el diseño del gobierno de las TIC.

- Se carece de modelos documentados y formalizados para la toma de decisiones, así como para los niveles de autoridad en materia de Seguridad de la Información.

- No se tiene evidencia de la supervisión para la ejecución y efectividad del gobierno de TIC de la Fiscalía.

- El Grupo Estratégico de Seguridad de la Información (GESI) no se encuentra activo.

- Se carece de mecanismos de control para verificar el cumplimiento de los servicios proporcionados por los proveedores externos.

Asegurar la entrega de beneficios

- Se carece de evidencia de la evaluación continua de las inversiones, servicios y activos del portafolio de TIC.

- No se cuenta con indicadores clave y métricas para determinar el grado en que las TIC generan valor, así como los beneficios de los servicios e inversiones en la materia.

Asegurar la optimización del riesgo

- No se realizan actividades para analizar y evaluar el efecto del riesgo sobre el uso actual y futuro de las TIC en la Fiscalía.

- Se carece de evidencia del análisis de riesgos en materia de TIC y Seguridad de la Información, por lo anterior, no se tienen mecanismos para identificar y gestionar los riesgos en los servicios.

Asegurar la optimización de recursos

- No se tiene evidencia del análisis y evaluación de las necesidades para los recursos actuales y futuros de las TIC.

- No se cuenta con métricas asociadas a la gestión de recursos de TIC ni procedimientos para la detección y seguimiento de problemas que se presenten en su administración.

Asegurar la transparencia hacia las partes interesadas

- Se carece de la designación de responsabilidades de los miembros del Comité de Gobierno y dueños de los procesos con excepción del encargado de Seguridad de la Información.

- No se tiene un plan operativo de las TIC con el detalle de las actividades, tareas, cronogramas, presupuesto y personal asignado con la finalidad de cumplir con los objetivos estratégicos del ente público.

En la revisión del proceso de Gobierno de las TIC, los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para la Fiscalía son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIA DE LOS CONTROLES PARA EL GOBIERNO DE LAS TIC

Factor crítico	Riesgo
Establecimiento y mantenimiento del marco de referencia de gobierno	La carencia de un marco de gobierno podría poner en riesgo el cumplimiento de los objetivos definidos por el ente público e impactar en el desempeño y eficiencia de los servicios que son proporcionados por la Fiscalía.
Asegurar la entrega de beneficios	La falta de evaluación en la entrega de beneficios podría poner en riesgo la eficiencia y eficacia de las TIC para alcanzar los objetivos a un costo razonable.
Asegurar la optimización del riesgo	La falta de procedimientos para la gestión de riesgos en cada una de las iniciativas de las TIC, podría afectar la planificación de las acciones para su manejo en los procesos, servicios financieros, transparencia de la información, seguridad de la información, trámites regulatorios, entre otros.
Asegurar la optimización de recursos	La carencia de indicadores para el control de los recursos no permite una evaluación oportuna y precisa de los resultados para alcanzar el máximo beneficio en su administración.

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

2019-0-49100-20-0097-01-006 **Recomendación**

Para que la Fiscalía General de la República implemente políticas, procedimientos y lineamientos en materia de Gobierno de las TIC para el establecimiento y mantenimiento del marco de referencia de gobierno, asegurar la entrega de beneficios, gestionar la optimización del riesgo y maximizar el manejo de los recursos con la finalidad de alcanzar una mayor eficiencia en los procesos institucionales y asegurar el cumplimiento de los objetivos estratégicos de la Fiscalía.

6. Seguridad de la Información

Se revisó la información relacionada con la administración y operación de los controles de seguridad de la Información vinculados con las soluciones e infraestructura tecnológica, de conformidad con los procesos de Administración de la Seguridad de la Información y Operación de los Controles de Seguridad de la Información y del ERISC del MAAGTICSI, sus

apéndices y mejores prácticas, así como con las políticas y lineamientos proporcionados por la Fiscalía en la materia y se observó lo siguiente:

Contexto de la organización

- No se cuenta con la designación del Grupo Estratégico de Seguridad de la Información ni de los roles y responsabilidades asociadas a su atención.

- En relación con la Estrategia de Seguridad de la Información se carece de evidencia de su difusión, así como de los planes y cronogramas para su operación.

- No se tiene evidencia de la implementación ni mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), tampoco de su aprobación por parte de la Alta Dirección de la Fiscalía.

- Se carece de evidencia de la difusión de las políticas de seguridad de la información al interior del ente público.

Planeación

No fueron definidos los riesgos de la información ni los controles de seguridad que son relevantes y aplicables a la FGR, tampoco se cuenta con evaluaciones periódicas del riesgo.

Soporte

La FGR no proporcionó evidencia de que el personal de TIC cuenta con las competencias requeridas en materia de seguridad de la información.

Evaluación del desempeño

- No fueron realizadas auditorías internas en materia de Seguridad de la Información.

- Se carece de la aplicación de metodologías para evaluar el rendimiento del SGSI.
- No se tienen acciones correctivas para evitar la recurrencia de incidentes informáticos.

Políticas de seguridad de la información

Se carece de la política de Intercambio de Información descrita en la política general de seguridad de la información.

Seguridad de la información en la organización

- La Fiscalía no tiene contacto con grupos de interés en materia de seguridad de la información.

- No se cuenta con una metodología formalizada e implementada para la gestión de proyectos en materia de seguridad de la información.

- Se carece de políticas para la conexión remota de equipos como apoyo a las medidas de seguridad de la FGR.

Seguridad en recursos humanos

- No se cuenta con evidencia de programas de concientización en materia de seguridad de la información para el personal de la FGR.

- Se carece de un procedimiento formalizado e implementado para la baja o salida de personal en materia de seguridad de la información.

Gestión de activos

La Fiscalía no demostró una adecuada gestión de sus activos debido a las deficiencias en el manejo de los inventarios, sin controles de cambios ni revisiones periódicas para asegurar el cumplimiento de las políticas de seguridad de la información.

Control de acceso

- No se cuenta con procedimientos para la asignación de usuarios temporales ni permisos de acceso.

- Se carece de políticas para la gestión de contraseñas que se pueden utilizar en la FGR.

- No se cuenta con políticas para el monitoreo de bitácoras de transacciones ni pistas de auditoría.

Criptografía

Se carece de procedimientos de cifrado para la información que se transmite y resguarda en los servidores de la plataforma Linux con sistemas de misión crítica.

Seguridad física y del entorno

- Se carece de políticas de seguridad en las áreas de carga y descarga de equipos de cómputo.

- No se tienen procedimientos para la protección del equipo de cómputo en las instalaciones, con el objeto de reducir las oportunidades de acceso no autorizado.

- No se cuenta con evidencia de programas de mantenimiento a la infraestructura tecnológica.

- No se realizan los lineamientos de borrado seguro en los equipos de cómputo antes de su retiro o reutilización en otras áreas.

Seguridad de las operaciones

- Se carece de procedimientos definidos e implementados para la operación de la seguridad de la información.

- El 74.4% de los equipos de cómputo tienen una protección antivirus, por lo que el resto pone en riesgo los activos de información de la Fiscalía.

- En relación con los procedimientos de respaldo y restauración, no se cuenta con evidencia de su implementación.

- Se carece de evidencia de la remediación de las vulnerabilidades identificadas en las pruebas de penetración a las soluciones e infraestructura tecnológica.

Seguridad de las comunicaciones

No se tienen políticas para la protección de la información que se transmite en las redes institucionales ni lineamientos para el uso del correo electrónico.

Adquisición, desarrollo y mantenimiento de los sistemas de información

- Se carece de evidencia del uso de herramientas para la revisión de la seguridad y calidad del código fuente de los aplicativos.

- No se cuenta con evidencia del control de cambios en el desarrollo de software, ni de controles para prevenir cambios no autorizados a los sistemas.

- No se tiene evidencia de los resultados de seguridad en las pruebas realizadas a los sistemas después de cambios menores, mayores o urgentes.

- Se carece de mecanismos para la protección de los datos en la fase de pruebas.

- No se cuenta con evidencia de la supervisión y monitoreo de las actividades de desarrollo de sistemas realizadas por los prestadores de servicios.

- No se realizan análisis de vulnerabilidades a los aplicativos de manera previa a su puesta en marcha en el ambiente productivo.

Relación con proveedores

No se tiene evidencia de la alineación de los proveedores a las políticas de seguridad de la información de la Fiscalía.

Gestión de incidentes de seguridad de la información

No se cuenta con un plan de gestión de incidentes de seguridad de la información ni en materia de ciberseguridad.

Aspectos de seguridad de la información para la gestión de la continuidad de negocio

- No se cuenta con la definición, implementación, revisión y evaluación del plan de continuidad del negocio.

- Se carece de procedimientos y pruebas para la validación del proceso de respaldo y recuperación de la información.

Cumplimiento

Se carece de la revisión de la Seguridad de la Información de conformidad con los acuerdos técnicos, estándares y políticas de seguridad del Ente Público.

Como resultado de la revisión de los objetivos de control para la Seguridad de la Información, los principales riesgos para las operaciones y activos de la Fiscalía son los siguientes

Principales riesgos por la carencia o inconsistencia de los objetivos de control para la seguridad de la información

Objetivo de Control	Riesgo
Sistema de Gestión de Seguridad de la Información (SGSI)	La falta del SGSI puede ocasionar la pérdida de la confidencialidad de la información que podría ser conocida y utilizada por personas que no tienen autorización; carencia de integridad ya que los datos podrían ser alterados, provocando posibles pérdidas económicas; falta de disponibilidad para permitir que los usuarios accedan a las aplicaciones cuando lo requieran; así como la falta de reconocimiento de las transacciones en caso de deslindar responsabilidades.
Organización de la seguridad de la información	Debido a la falta de controles se podrían efectuar modificaciones no autorizadas en los datos sin que se cuente con la información necesaria para deslindar responsabilidades.
Seguridad física y del entorno	Posible pérdida o robo de información que podría afectar a los activos de información y a la continuidad de las operaciones.
Seguridad de las operaciones	La omisión de la gestión y análisis de registros de auditoría en las transacciones puede provocar la falta de identificación y detección oportuna de posibles intromisiones que afecten la integridad de la información.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Se carece de procedimientos que permitan prevenir, detectar y corregir las debilidades de seguridad en los desarrollos de sistemas de información.
Relación con proveedores	La falta de alineación a las políticas de seguridad por parte de los proveedores podría causar un impacto en los productos o servicios que ofrecen para las operaciones del ente público.
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	La carencia de los planes para la continuidad de las operaciones podría ocasionar que la recuperación de los sistemas tarde más tiempo de lo esperado o no se lleve a cabo, y que se afecten los procesos sustantivos de la Fiscalía.
Cumplimiento	La falta de revisión del cumplimiento de las políticas y lineamientos puede producir brechas en la seguridad de la información que podrían poner en riesgo a los activos de información y operaciones de la Fiscalía.

Fuente: Elaborado con la información proporcionada por la FGR.

2019-0-49100-20-0097-01-007 **Recomendación**

Para que la Fiscalía General de la República fortalezca las políticas, procedimientos y controles para la implementación del Sistema de Gestión de Seguridad de la Información, así como de los objetivos relacionados con la Organización de la seguridad de la información; Seguridad de las operaciones; Adquisición, desarrollo y mantenimiento de los sistemas de información; Relación con proveedores; así como los Aspectos de seguridad de la información para la gestión de la continuidad de negocio y su cumplimiento; con la finalidad de mitigar las vulnerabilidades de las soluciones e infraestructura tecnológica ante un incidente cibernético, que podría afectar a los activos de información y operación de los procesos sustantivos de la Fiscalía.

7. Continuidad de las Operaciones y Centro de Datos

En el análisis a la información relacionada con la continuidad de los servicios de Tecnologías de Información y Comunicaciones, así como con la seguridad física y lógica del centro de datos secundario, de conformidad con los procesos de Administración de Servicios y Administración de la Operación del MAAGTICSI, sus apéndices y mejores prácticas, así como con las políticas y lineamientos proporcionados por la Fiscalía en la materia, se observó lo siguiente:

Programa de continuidad de las operaciones

- El programa de continuidad no se encuentra actualizado, tampoco considera un plan de recuperación de desastres (DRP) ni un plan de gestión de respuesta a incidentes de seguridad y ciberseguridad.
- Se carece de elementos para corroborar que las prioridades de recuperación y los activos críticos de información se encuentran actualizados; asimismo, no fue posible verificar que el programa se encuentra alineado a los sistemas, aplicativos, infraestructura tecnológica y necesidades actuales de operación de la FGR.

- No se establece la totalidad de las acciones requeridas para la recuperación de los servicios de TIC, tampoco se define el costo de los servicios ni el detalle de los procedimientos para conocer el desarrollo, implementación y revisión de cada elemento contenido en el programa.

- Se carece de evidencia de la configuración de los escenarios de pruebas en caso de ciberataque, inundación, sismo, entre otros, que pueden activar el programa de continuidad.

Análisis de impacto al negocio (BIA)

- Se carece de la definición de los puntos de recuperación objetivo (RPO) para conocer la antigüedad de los archivos que se deben recuperar de las copias de seguridad para reanudar las operaciones.

- No se establecen los recursos y dependencias (proveedores, sistemas, marcos regulatorios, entre otros) para priorizar las actividades para el restablecimiento de los procesos y servicios

Plan de recuperación de desastres (DRP)

- La Fiscalía cuenta con un software para la replicación de datos hacia un centro de datos alterno; no obstante, es sólo uno de los elementos del plan de recuperación de desastres, el cual debe complementarse con los procedimientos para la notificación de incidentes, identificación de los sistemas y aplicativos que podrían ser afectados ante una contingencia, recuperación de los servicios, reactivación del sitio primario, políticas de protección de los activos de información contra desastres naturales, responsabilidades del equipo de respuesta a incidentes, plan de capacitación a las áreas involucradas sobre la ejecución del DRP, entre otros; tampoco se cuenta con los resultados de un plan de pruebas para corroborar su efectividad.

- Se carece de políticas y procedimientos para la clasificación y resguardo de la información.

Programa de capacidad

- Se carece de evidencia para corroborar que el Programa de Capacidad se actualiza conforme a los resultados del consumo y disponibilidad de los recursos de cómputo.

- No se tiene evidencia de la evaluación de los elementos del programa de capacidad tales como el monitoreo de los niveles de servicio, análisis de los incidentes, verificación de tendencias de cargas de trabajo de los componentes de la infraestructura, acciones a realizar cuando la capacidad y rendimiento no estén en el nivel requerido, actualización de activos de TIC, entre otros.

Procedimientos de respaldo de información

- Se carece de políticas y procedimientos para el respaldo y recuperación de la información que se procesa, almacena y transmite desde los centros de datos.

- No se tiene evidencia del procedimiento para el resguardo de los respaldos de información críticos.

Seguridad física y lógica del centro de datos secundario

- Se identificó que fue migrada parte de la operación de los aplicativos críticos al centro de datos secundario sin un análisis de viabilidad ni criterios para distribuir los aplicativos críticos entre los centros de datos.

- Cabe señalar que el centro de datos principal cuenta con una certificación de ICREA de alto nivel de disponibilidad (99.999%), mientras que el centro de datos secundario

no cuenta con certificaciones para acreditar el nivel de disponibilidad necesario para la operación de aplicaciones y sistemas de misión crítica.

- La distancia entre el centro de datos principal y secundario representa un riesgo moderado ya que se encuentran en el mismo corredor industrial, lo cual no evita los puntos de falla ante un desastre natural o incidentes en la prestación de servicios de la región. Cabe señalar que no se tiene un análisis de los riesgos de la ubicación de los centros de cómputo, ni los criterios para su diseño, dimensionamiento y distribución de los equipos.

- El centro de datos secundario se encuentran en operación; no obstante, no cuenta con un contrato de soporte y mantenimiento preventivo vigente, lo que ocasiona la falta de sostenimiento de los sistemas de acceso, videovigilancia, sistema contra incendios, controles ambientales, sistema eléctrico, energía de respaldo y plantas de emergencia, situación que pone en riesgo de falla a los equipos con los que operan dichos sistemas, lo que puede propiciar la interrupción de los procesos sustantivos del ente público.

Se detectó que los principales riesgos por la carencia o inconsistencia de los controles y sus consecuencias potenciales para las operaciones y activos de la Fiscalía son los siguientes:

PRINCIPALES RIESGOS POR LA CARENCIA O INCONSISTENCIA DE LOS CONTROLES EN LA CONTINUIDAD DE LAS OPERACIONES Y CENTRO DE DATOS SECUNDARIO

Factor Crítico	Riesgos
Plan de Recuperación de Desastres	La carencia de un plan de recuperación de desastres impide el restablecimiento satisfactorio de los sistemas, aplicativos e infraestructura tecnológica que soporta los procesos sustantivos del ente público, además del incumplimiento de los tiempos y objetivos de la alta dirección para la continuidad de los servicios que ofrece la Fiscalía.
Políticas de Respaldo	La falta de políticas y procedimientos para el respaldo y recuperación de datos, puede implicar el riesgo de que los respaldos no sean funcionales en el momento de su restauración o que la información respaldada no sea la requerida por la Fiscalía para la continuidad de sus operaciones.
Mantenimiento preventivo a los equipos y sistemas de soporte del centro de datos	La falta de mantenimiento preventivo a los sistemas de detección y extinción de incendios, ventilación, aire acondicionado y climatización, puertas y alarmas sonoras, circuito cerrado de televisión, así como a los equipos de energía eléctrica, plantas de emergencia y sistemas de respaldo, puede propiciar el riesgo de que se presenten fallas o incidentes en los sistemas que puedan interrumpir la operación de los procesos de la Fiscalía.

Fuente: Elaborado con información proporcionada por la FGR mediante los oficios FGR/CPA/SAMC/0169/2019 y FGR/CPA/SAMC/0108/2020 de fechas 30 de octubre de 2019 y 31 de agosto de 2020, respectivamente.

2019-0-49100-20-0097-01-008 **Recomendación**

Para que la Fiscalía General de la República fortalezca el diseño, componentes, pruebas y difusión del Programa de Continuidad, Plan de Gestión de Incidentes de Seguridad de la Información y Plan de Recuperación de Desastres, así como la generación de métricas de seguimiento al Programa de Capacidad; adicionalmente, implemente las políticas y procedimientos para el respaldo y recuperación de los activos de información críticos, con la

finalidad de asegurar la continuidad operativa de los procesos sustantivos, soluciones e infraestructura tecnológica en caso de una contingencia.

2019-0-49100-20-0097-01-009 **Recomendación**

Para que la Fiscalía General de la República evalúe las capacidades de funcionamiento y resiliencia de los centros de datos para determinar el sitio con las mejores condiciones para la operación de los sistemas, aplicativos, bases de datos e infraestructura tecnológica que soportan los procesos sustantivos de la Fiscalía; asimismo, implemente un programa de mantenimiento preventivo en los centros de datos para asegurar que todos los equipos y sistemas se encuentren en óptimas condiciones de operación.

Buen Gobierno

Impacto de lo observado por la ASF para buen gobierno: Liderazgo y dirección, Planificación estratégica y operativa, Controles internos, Aseguramiento de calidad y Vigilancia y rendición de cuentas.

Resumen de Resultados, Observaciones y Acciones

Se determinaron 7 resultados, de los cuales, en uno no se detectó irregularidad y los 6 restantes generaron:

9 Recomendaciones.

Dictamen

El presente se emite el día 20 de enero de 2021, fecha de conclusión de los trabajos de auditoría, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable. Con base en los resultados obtenidos en la auditoría practicada, cuyo objetivo fue fiscalizar 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 Fiscalía General de la República cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- En relación con el Contrato para la “Prestación de servicios informáticos de infraestructura TIC”, se carece de los números de serie, el control de cambios y las revisiones físicas de las computadoras para verificar los equipos pagados.

- Sobre el Contrato para los “Servicios Informáticos Integrales de Impresión, Digitalización y Fotocopiado de documentos”, se determinan deficiencias en la investigación de mercado debido a que se señaló la existencia de un solo proveedor en todo el país, siendo que existen otros; asimismo, se comprobó que sólo el 32.4% de los técnicos de soporte en sitio estaban capacitados para la operación y servicio de los equipos.

- Respecto al Contrato para los “Servicios de licenciamiento, soporte premier y cómputo en la nube”, no se tiene el detalle para verificar la entrega del servicio de soporte premier, así como para conocer la trazabilidad de las actividades y evaluación del desempeño del proveedor; se carece del control de acceso e identidades, privacidad y encriptación de los datos sensibles de los sistemas; así como del monitoreo de las cuentas de acceso, las pistas de auditoría y el análisis de las transacciones de las bases de datos, lo que pone en riesgo la confidencialidad, disponibilidad e integridad de los activos de información ante un incidente informático.

- En relación con el Gobierno de las TIC, se carece de indicadores y métricas para determinar los beneficios de los servicios e inversiones de TIC; no se gestionan los riesgos de los servicios e iniciativas de las soluciones e infraestructura tecnológica; no se tiene un plan operativo de las TIC para cumplir con los objetivos estratégicos de la Fiscalía.

- En materia de Seguridad de la Información se tienen deficiencias en la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información; no se cuenta con programas de concientización al personal en materia de seguridad de la información; se carece de políticas para la gestión de contraseñas; no se realiza el borrado seguro de los equipos de cómputo; no se ejecuta el análisis de vulnerabilidades a los aplicativos de manera previa a su puesta en marcha en el ambiente productivo; asimismo, se carece del plan de gestión de incidentes de ciberseguridad para responder ante ataques cibernéticos.

- Respecto a la Continuidad de las Operaciones, el Plan de Recuperación de Desastres carece de procedimientos para la notificación de incidentes, la identificación de los sistemas que podrían ser afectados ante una contingencia, la capacitación a las áreas involucradas sobre la ejecución del plan, entre otros; el Programa de Capacidad no evalúa aspectos como el monitoreo de los niveles de servicio, las tendencias de cargas de trabajo de los componentes de la infraestructura, entre otros; el Programa de Respaldo y Recuperación de la información carece de políticas y procedimientos para asegurar que la información se encuentre disponible y actualizada cuando sea requerida; el Programa de Mantenimiento Preventivo al Centro de Datos Secundario no se encuentra en operación, lo que puede contribuir a fallas en los equipos y sistemas de misión crítica, así como en la interrupción de los procesos sustantivos de la Fiscalía.

Los procedimientos de auditoría aplicados, la evidencia objetiva analizada, así como los resultados obtenidos fundamentan las conclusiones anteriores.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Genaro Héctor Serrano Martínez	Mtro. Roberto Hernández Rojas Valderrama Firma en suplencia por ausencia del Director General de Auditoría de Tecnologías de Información y Comunicaciones con fundamento en lo dispuesto por el artículo 65 del Reglamento Interior de la Auditoría Superior de la Federación.

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 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, los costos de mantenimiento, soporte y operación que

impliquen la contratación, vinculados con el factor de temporalidad para determinar la conveniencia de adquirir, arrendar o contratar servicios, así como la investigación de mercado.

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

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permiten su fiscalización, corresponden a trabajos efectivamente devengados que justifiquen las facturas pagadas y la autenticidad de los comprobantes fiscales; verificar la entrega en tiempo y forma de los servicios, así como 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 fue atendido, así como el manejo del riesgo residual y la justificación de los riesgos aceptados por la entidad.

6. Evaluar el nivel de gestión de los procesos relacionados con la dirección, el control y la administración de riesgos en materia de Tecnologías de la Información y Comunicaciones; analizar la planeación estratégica, así como las funciones sustantivas y administrativas de las TIC que lleva a cabo la entidad fiscalizada; evaluar el nivel de alineación de la estrategia de TIC con los objetivos de la Organización, así como los mecanismos de medición, seguimiento y cumplimiento de las contrataciones de TIC.

7. Evaluar el nivel de implementación del Sistema de Gestión de Seguridad de la Información para la protección de los activos de información críticos de la entidad, así como los procedimientos para disminuir el impacto de eventos adversos, que podrían afectar los objetivos de la institución; revisar el control de accesos y privilegios, segregación de funciones, controles de las cuentas funcionales y privilegiadas en los aplicativos y bases de datos sustantivas; verificar los mecanismos implementados para la transferencia de datos sobre canales seguros, así como los estándares aplicados para el cifrado de datos.

8. Verificar la gestión del programa de continuidad de las operaciones; evaluar la seguridad física y lógica del centro de datos (control de accesos, incendio, inundación, monitoreo, enfriamiento, respaldos, replicación de datos, entre otros).

Áreas Revisadas

Las direcciones generales de Tecnologías de Información y Comunicaciones, Recursos Materiales y Servicios Generales, así como la Unidad de Tesorería adscritas a la Coordinación de Planeación y Administración de la Fiscalía General de la República.

Disposiciones Jurídicas y Normativas Incumplidas

Durante el desarrollo de la auditoría practicada, se determinaron incumplimientos de las leyes, reglamentos y disposiciones normativas que a continuación se mencionan:

1. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Artículos 26, primer párrafo; 45, numeral V; 48, fracción II; y 84;

2. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público: Artículos 29, fracción II, 30, 66, fracción III y 103;

3. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria: artículo 66, fracciones I y III;

4. Otras disposiciones de carácter general, específico, estatal o municipal: Anexo técnico del contrato número PGR/AD/CN/SERV/013-9/2017, numeral 1.2, apartado "Reportes"; Anexo técnico del contrato número FGR/AD/CN/SERV/009-5/2019, numeral 2.2, apartado "Reportes"; Contrato número PRG/AD/CN/SERV/005-7/2017, cláusula décima cuarta; Contrato número FGR/AD/CN/SERV/006-05/2019, cláusula décima quinta; Anexo Técnico del Contrato número PRG/AD/CN/SERV/005-7/2017, numerales 4.8 "Mesa de Ayuda", 5 "Soporte en Sitio a Nivel Nacional", 9, 11; Anexo Técnico del Contrato número FGR/AD/CN/SERV/006-05/2019, numerales 3.8 "Mesa de Ayuda", 4 "Soporte en Sitio a Nivel Nacional", 8, 10; Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de la Fiscalía General de la República, numeral "5.22 Garantías"; Marco de referencia COBIT 2019, Objetivos de gestión APO09, APO010, APO13, MEA02, MEA03 y DSS02, Objetivos de gobierno EDM01, EDM02, EDM03, EDM04 y EDM05, Proceso de Gestión "BAI04 Gestionar la disponibilidad y la capacidad", "DSS04 Gestionar la continuidad", Práctica de gestión "DSS04.02 Mantener una estrategia de continuidad", "DSS04.07 Gestionar acuerdos de respaldo"; Norma ISO 24762/2008 "Técnicas de seguridad-Directrices para los Servicios de Recuperación de Desastres de Tecnología de la Información y Comunicaciones", Apartados 5.3, 5.7.5.1, 7.9.2, 7.15.4 y 7.16.4; Norma ISO/IEC 27001 "Sistemas de Gestión de Seguridad de la Información", A.11, "Tecnología de la información-Técnicas de seguridad-Administración de los sistemas de seguridad de la información"; Norma ISO/IEC 27017, Objetivos de Control A.6, A.11, A.12, A.14, A.15, A.17, A.18; NIST 800-53v4;

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.