Banco Nacional de Obras y Servicios Públicos, S.N.C.

Auditoría de TIC

Auditoría Cumplimiento Financiero: 2017-2-06G1C-15-0092-2018

92-GB

Criterios de Selección

Durante la primera fase de selección, a fin de establecer un primer universo, se ponderaron los siguientes criterios:

Para el Poder Ejecutivo, Legislativo y Judicial, así como Organismos Autónomos:

Contratos reflejados en CompraNet (Monto)	20%
Gastos de TIC en 2017	20%
Propuestas coincidentes con la Dirección de Programación y Planeación	15%
Proveedores relevantes	15%
Proveedores de riesgo	15%
Notas de prensa	5%
Control Interno	5%
Gasto de TIC en relación con el equipamiento de las entidades	5%

De esta primera evaluación se seleccionaron 38 entidades a las que se les solicitó información relacionada con las TIC.

En el caso de los Estados de la República:

Contratos reflejados en CompraNet (monto)	25%
Gastos de TIC en 2017	25%
Participaciones Federales asignadas	50%

De esta primera evaluación se seleccionaron 5 Estados de la República a los que se les solicitó información relacionada con las TIC.

Objetivo

Fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, 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	403,428.1
Muestra Auditada	87,587.3
Representatividad de la Muestra	21.7%

El universo seleccionado por 403,428.1 miles de pesos corresponde al total de recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC) en el ejercicio fiscal de 2017; la muestra auditada se integra de tres contratos relacionados con servicios para el derecho de uso del sistema base en la modalidad de software como servicio (SaaS) y el soporte al aplicativo para la continuidad operativa del SIBA; de aseguramiento de la calidad para la implementación del Sistema Integral Bancario y Administrativo (SIBA); y de continuidad operativa del sistema integral bancario y administrativo SIBA con pagos ejercidos por 87,587.3 miles de pesos, que representan el 21.7% del universo seleccionado.

Antecedentes

El Banco Nacional de Obras y Servicios Públicos, S.N.C. (BANOBRAS) es una institución de banca de desarrollo con participación estatal mayoritaria, cuenta con personalidad jurídica y patrimonio propios. Tiene como objeto financiar o refinanciar proyectos relacionados directa

o indirectamente con inversión pública o privada en infraestructura y servicios públicos, así como coadyuvar al fortalecimiento institucional de los gobiernos federales, estatales y municipales, con el propósito de contribuir al desarrollo sustentable del país.

Entre el 2013 al 2017, se han invertido 1,423,979.0 miles de pesos en Tecnologías de la Información y Comunicaciones (TIC), relacionados con el capítulo 3000, específicamente a los servicios generales.

Recursos Invertidos en Materia de TIC
(Miles de Pesos)

PERIODO DE INVERSIÓN	2013	2014	2015	2016	2017	TOTALES
MONTO POR AÑO	112,565.7	252,367.7	321,431.7	334,185.8	403,428.1	**1,423,979.0**

Fuente: Elaborado con base en la información definitiva proporcionada por BANOBRAS.

Nota: No incluye el gasto relacionado con servicios personales (capítulo 1000).

Resultados

1. Normativa Interna

Con la revisión, se constató que el Banco Nacional de Obras y Servicios Públicos, S.N.C. (BANOBRAS) cuenta con un Manual General de Organización, actualizado en agosto de 2017, el cual incluye un apartado correspondiente a la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), que tiene como propósito regular y organizar el funcionamiento de la Institución, así como delimitar sus atribuciones y funciones, con el fin de evitar su duplicidad y mejorar el aprovechamiento de los recursos con los que cuenta.

Se observó que la última actualización al Manual de Integración y Funcionamiento del Comité de Adquisiciones, Arrendamientos y Servicios corresponde al 24 de septiembre de 2010.

Análisis Presupuestal

Del análisis de información de la Cuenta de la Hacienda Pública Federal del ejercicio 2017, se identificó que el BANOBRAS tuvo un presupuesto modificado de 6,269,929.0 miles de pesos, de los cuales se ejercieron 5,737,325.0 miles de pesos, que representan el 91.5% respecto del presupuesto modificado, reportando economías por un monto de 532,604.0 miles de pesos.

Se identificó una diferencia de 25,484.8 miles de pesos con respecto a las economías reportadas en la Cuenta Pública y la validación realizada por este ente de fiscalización superior, en donde se observó que el Banco cuenta con economías por un monto de 507,119.2 miles de pesos, esto debido a que los recursos de la institución corresponden a ingresos propios y no contemplan Adeudos de Ejercicios Fiscales Anteriores (ADEFAS), sino que el presupuesto devengado no pagado lo clasifica como economías para ser utilizado en el siguiente ejercicio fiscal, dicho monto se integra como sigue:

CUENTA PÚBLICA 2017

(Miles de pesos)

		A	B	C	D	E	F=B-C
Capítulo	Descripción	Presupuesto Autorizado	Presupuesto Modificado	Presupuesto Devengado	Presupuesto Pagado	Presupuesto Ejercido	Economías
1000	Servicios personales	943,170.8	966,735.4	951,099.7	951,099.7	951,099.7	15,635.7
2000	Materiales y suministros	10,521.8	10,521.8	6,436.8	6,436.8	6,436.8	4,085.0
3000	Servicios generales	1,305,941.5	1,305,296.5	900,328.4	879,690.6	879,690.6	404,968.1
4000	Transferencias, asignaciones, subsidios y otras ayudas	902,290.4	902,332.4	829,944.9	825,097.9	825,097.9	72,387.5
5000	Bienes muebles, inmuebles e intangibles	9,440.0	10,042.9	0.0	0.0	0.0	10,042.9
7000	Otros de inversión	0.0	3,075,000.0	3,075,000.0	3,075,000.0	3,075,000.0	0.0
	TOTAL	**3,171,364.5**	**6,269,929.0**	**5,762,809.8**	**5,737,325.0**	**5,737,325.0**	**507,119.2**

Fuente: Elaborado con base en la información definitiva proporcionada por BANOBRAS.

Los recursos ejercidos en materia de Tecnologías de la Información y Comunicaciones (TIC) por 403,428.1 miles de pesos, se integran de la manera siguiente:

Recursos ejercidos en materia de TIC en 2017
(Miles de pesos)

Capítulo/ P. Presupuestaria		Descripción	Presupuesto Ejercido
3000		**SERVICIOS GENERALES**	**403,428.1**
	33301	Servicios de desarrollo de aplicaciones informáticas	40,101.7
	33304	Servicios de mantenimiento de aplicaciones informáticas	63,430.4
		Partidas no relacionadas con los contratos auditados	299,896.0
		TOTAL	**403,428.1**

Fuente: Elaborado con información definitiva proporcionada por BANOBRAS.

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 27,869.6 miles de pesos durante el ejercicio fiscal 2017, considerando 50 plazas, el promedio anual por plaza fue de 557.4 miles de pesos.

Del total ejercido en 2017 por 403,428.1 miles de pesos de recursos federales asignados en materia de TIC, se erogaron 87,587.3 miles de pesos en tres contratos que representan el 21.7% del total del universo, el cual se integra de la siguiente manera:

Muestra de Contratos Ejercidos en 2017

(Miles de Pesos)

Proceso Contratación	Contrato	Proveedor	Descripción	Vigencia		Monto mínimo		Monto máximo		Pagado 2017
				Del	Al	Dólares	Pesos	Dólares	Pesos	
Adjudicación Directa por Art. 41 fracción V	DAGA/003/2017	ADVANZER DE MÉXICO, S.A. DE C.V.	Prestación de servicios para el derecho de uso del sistema base en la modalidad de software como servicio y el soporte aplicativo para la continuidad operativa del Sistema Integral Bancario Administrativo (SIBA).	13/01/2017	30/06/2017	-	-	-	14,616.0	17,485.2
	Convenio modificatorio al contrato número DAGA/003/2017		Ampliación del costo de los servicios, modificación de la cláusula "forma de pago", ampliación de vigencia, y ampliación del monto de la fianza.	01/07/2017	05/08/2017	-	-	-	2,923.2	
					SUBTOTAL	**-**	**-**	**-**	**17,539.2**	**17,485.2**
Adjudicación Directa por Art. 41 fracción V	DAGA/097/2017	SAP MÉXICO, S.A. DE C.V.	Prestación de servicios de continuidad operativa del Sistema Integral Bancario Administrativo (SIBA).	06/08/2017	31/12/2017	1,290.1	23,058.3	3,225.3	57,646.8	55,673.6
					SUBTOTAL	**1,290.1**	**23,058.3**	**3,225.3**	**57,646.8**	**55,673.6**
Licitación Nacional Pública Mixta número LA-006G1C001-E105-2016	DAGA/084/2016	DELOITTE CONSULTING GROUP, SC. y GALAZ, YAMAZAKI, RUIZ URQUIZA, S.C.	Prestación del servicio de aseguramiento de la calidad para la implementación del Sistema Integral Bancario Administrativo (SIBA).	04/06/2016	31/08/2018	-	-	-	57,611.0	14,428.5
	Convenio modificatorio al contrato número DAGA/084/2016		Adición del servicio "S1. Recepción y elaboración del plan integral del proyecto", ampliación en el costo de los servicios, y ampliación en el monto de la fianza.	04/01/2017	31/08/2018	-	-	-	6,670.0	
					SUBTOTAL	**-**	**-**	**-**	**64,281.0**	**14,428.5**
				TOTAL		**-**	**23,058.3**	**-**	**139,467.0**	**87,587.3**

Fuente: Contratos, facturas y soporte documental proporcionados por BANOBRAS

Nota: Tipo de cambio al 04 de agosto de 2017 (17.8733 pesos por dólar) correspondiente a la fecha de firma del contrato.

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

2017-2-06G1C-15-0092-01-001 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. lleve a cabo la actualización del Manual de Integración y Funcionamiento del Comité de Adquisiciones, Arrendamientos y Servicios, con el objetivo de que éste se encuentre alineado con la forma de operación y situación actual del Banco.

2. Contrato DAGA/003/2017 "Servicios para el Derecho de Uso del Sistema Base en la modalidad de Software como Servicios (SaaS) y el soporte al aplicativo para la continuidad operativa del SIBA"

Con el análisis del contrato número DAGA/003/2017 celebrado con la empresa ADVANZER DE MÉXICO, S.A. DE C.V., mediante el procedimiento de adjudicación directa por excepción a la licitación pública, con fundamento en el artículo 41, fracción V, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); con objeto de recibir los "Servicios para el Derecho de Uso del Sistema Base en la modalidad de Software como Servicio (SaaS) y el Soporte al aplicativo para la continuidad operativa del SIBA", vigente del 13 de enero al 30 de junio de 2017; por un monto de 14,616.0 miles de pesos; con fecha 28 de junio de 2017 se celebró el "Convenio modificatorio al contrato número DAGA/003/2017", con la finalidad de aumentar el monto del contrato a 17,539.2 miles de pesos, modificar la cláusula "forma de pago", ampliar la vigencia al 5 de agosto de 2017, así como el monto de la fianza, se identificó lo siguiente:

Antecedentes

En octubre de 2014, el Banco llevó a cabo la adjudicación del contrato número DAGA/050/2014, con la empresa ADVANZER DE MÉXICO, S.A. DE C.V., con el objeto de prestar los servicios para la implementación del SIBA, con una vigencia del 17 de octubre de 2014 al 30 de junio de 2018.

En marzo de 2015, ante la falta de elementos para proceder con el pago de los servicios del uso del Sistema Base en la modalidad de Software como Servicio (SaaS) el Banco suspendió los pagos. Posteriormente, en octubre de 2015, el proveedor solicitó a la Secretaría de la Función Pública (SFP) realizar un proceso de conciliación a fin de que ésta validará las condiciones para el pago de los servicios, así como la reprogramación del proyecto de automatización de contabilidad; durante este proceso se suspendió la obligación contractual de continuar con los trabajos de la fase de construcción del proyecto y una vez concluida la conciliación los trabajos deberían reanudarse, por lo que se acordó que se reactivaría la ejecución de la automatización de contabilidad hasta que ambas partes encontraran las condiciones que se requerían para concluir con dicha fase.

El 31 de diciembre de 2016 se procedió a realizar la terminación anticipada del contrato DAGA/050/2014, debido a que las condiciones y necesidades que dieron origen a la contratación eran distintas en ese momento y el continuar con los servicios podría ocasionar un daño a BANOBRAS.

Alcance

Por lo anterior, el 13 de enero de 2017 se adjudicó el contrato DAGA/003/2017, objeto de esta revisión, el cual contempló dentro su alcance los siguientes servicios:

1. Derecho de uso del sistema base del SIBA (Sistema Integral Bancario y Administrativo) en la modalidad de software como servicio para los módulos o componentes que se tenían en operación y que soportaban la operación de los procesos de: Automatización de la Administración de Clientes, de la Originación de Crédito del SIBA, así como la infraestructura requerida; utilizando todos los componentes de software que constituyen al SIBA para su correcto y completo funcionamiento, en los ambientes de desarrollo, control de calidad, producción y soporte a contingencias (DRP).
2. Servicios de soporte a los procesos de automatización de la Administración de Clientes y de Originación de Crédito del SIBA implementados en ambiente productivo.

Proceso de Contratación

Se proporcionó el dictamen con la justificación para llevar a cabo la contratación por excepción a la licitación pública, bajo el amparo del artículo 41, fracción V, de la LAASSP, en la cual se justifican los motivos en los que se sustenta el procedimiento de contratación realizado.

Pagos

Se reportaron pagos de enero a agosto de 2017 por un monto de 17,485.2 miles de pesos; sin embargo, se carece de la documentación (fichas de depósito, comprobantes de transferencias, entre otros) que acredite que el pago de las facturas correspondientes a los servicios prestados por el proveedor fue realizado; debido a que únicamente se presentaron las pólizas generales, en donde se observó el apartado del gasto.

Cumplimiento técnico y funcional

- El Banco no verificó que los recursos del proveedor que participaron en la ejecución del servicio contaran con la experiencia, conocimientos y certificaciones en la mejor práctica llamada ITIL, conforme a lo estipulado en el numeral 5.1.1 del anexo técnico del contrato.
- No fue posible obtener información de los incidentes reportados, debido a que el proveedor no contaba con una herramienta propia para su registro y almacenamiento; tampoco se identificaron los parámetros configurados en la herramienta de gestión de incidentes, administrada por un tercero, para establecer los niveles de servicio (tiempos de atención); asimismo, no se cuenta con el detalle de los tickets que fueron atendidos por el proveedor, a fin de validar el cumplimiento de los niveles de servicio.

De lo anterior, BANOBRAS señaló que a partir del 31 de agosto de 2018, firmó un contrato de servicios de Mesa de Ayuda y monitoreo, en donde se contempla una herramienta para la configuración de los niveles de servicio y seguimiento a eventos.

- Se carece de la documentación que acredite que el proveedor instruyó al personal que participó en el proyecto a guardar secrecía y confidencialidad sobre los activos e información requerida para la prestación de los servicios, conforme a lo establecido en el Anexo Técnico en su numeral 12. Confidencialidad; así como de la evidencia que garantice que el Banco haya verificado su cumplimiento.

Se concluye que existieron deficiencias en la gestión de los servicios, en razón de que la entidad no se aseguró de: validar la capacidad técnica de los recursos del proveedor en relación con lo descrito en su Propuesta de Servicios y el entregable S.2 E1 Inicio de operación del servicio; garantizar que al finalizar la relación contractual con el proveedor, la entidad obtuviera toda la base de conocimientos de los tickets atendidos por el prestador de servicios; en incumplimiento de lo establecido en el anexo técnico del contrato DAGA/003/2017, así como a lo establecido en el III.B. Proceso de Administración de Proveedores (APRO), actividad APRO 3 del Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, publicado en el Diario Oficial de la Federación el 8 de mayo de 2014 y sus reformas al 4 de febrero de 2016.

2017-2-06G1C-15-0092-01-002 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. implemente mecanismos para que en futuras contrataciones se valide que los recursos de los proveedores que participarán en la ejecución del servicio cuenten con la experiencia, conocimientos y certificaciones solicitadas; elaborar cartas de confidencialidad de la información, personalizadas para cada uno de los recursos de terceros y que éstas sean firmadas tanto por el recurso del proveedor como por el representante legal del mismo, así como evaluar la implantación de controles que permitan mantener la confidencialidad de la información (controles de acceso, claves criptográficas, etc.) en los aplicativos en los que terceros ejecutan actividades. Asimismo, se recomienda llevar a cabo la gestión de los incidentes, en donde se contemple documentar el inicio de la solicitud hasta su conclusión, a fin de que el Banco verifique el cumplimiento de los niveles de servicio.

3. Contrato DAGA/097/2017 "Servicios de Continuidad Operativa del Sistema Integral Bancario y Administrativo (SIBA)"

Con el análisis del contrato número DAGA/097/2017 celebrado con la empresa SAP MÉXICO, S.A. DE C.V., mediante el procedimiento de adjudicación directa por excepción a la licitación pública, con fundamento en el artículo 41, fracción V, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP); con objeto de recibir los "Servicios de Continuidad Operativa del Sistema Integral Bancario y Administrativo (SIBA)", vigente del

6 de agosto al 31 de diciembre de 2017; por un monto de mínimo de 1,290.1 miles de dólares (23,058.3 miles de pesos, con el tipo de cambio de 17.8733 del 4 de agosto de 2017) y máximo de 3,225.3 miles de dólares (57,646.8 miles de pesos, con el tipo de cambio de 17.8733 del 4 de agosto de 2017), se determinó lo siguiente:

Alcance

El alcance del contrato contempló la habilitación del derecho de uso de productos SAP, el servicio de mantenimiento de software y aplicativos que permitan la continuidad operativa de los procesos de negocio requeridos por el Sistema Integral Bancario y Administrativo (SIBA), así como el servicio de mejora continua bajo demanda para perfeccionar y evolucionar las características del software y aplicativos.

Proceso de Contratación

Se proporcionó el dictamen con la justificación para llevar a cabo la contratación por excepción a la licitación pública, bajo el amparo del artículo 41, fracción V, de la LAASSP, en la cual se justifican los motivos en los que se sustenta el procedimiento de contratación realizado.

Pagos

Se reportaron pagos de agosto a diciembre de 2017 por un monto de 55,673.6 miles de pesos; sin embargo, se carece de la documentación (fichas de depósito, comprobantes de transferencias, entre otros) que acredite que el pago de las facturas correspondientes a los servicios prestados por el proveedor fue realizado; debido a que únicamente se presentaron las pólizas generales, en donde se observó el apartado del gasto.

Cumplimiento técnico y funcional

- No se identificó la fecha de instalación, versiones, así como el historial de actualizaciones de cada elemento de las instancias de SAP.

- No se proporcionó la documentación que permita validar el cumplimiento del nivel de disponibilidad del 99.5% del sistema para los meses de septiembre y octubre de 2017.

- Se carece de la definición y evaluación de los Acuerdos de operación (OLA's) mediante los cuales se realizaría la medición de la disponibilidad del módulo de prevención contra el lavado de dinero y el financiamiento al terrorismo (PLD/FT); en incumplimiento del Apartado 5.2.7 del Anexo Técnico del contrato DAGA/097/2017.

- No se cuenta con la documentación que permita verificar el seguimiento y atención de las vulnerabilidades identificadas en relación con la implementación del módulo PLD/FT.

- No se ejecutó un análisis de vulnerabilidades antes de la liberación del módulo PLD/FT en el ambiente de producción; por lo que existe el riesgo de que no se puedan detectar deficiencias en la seguridad de la información que pudieran ocasionar una afectación a la operación del SIBA.

- El Banco señaló que durante 2017 se llevaron a cabo restauraciones de información; sin embargo, no proporcionó el listado de las restauraciones realizadas, así como su documentación.

- No se proporcionaron las certificaciones que permitan acreditar que el personal del proveedor estuviera capacitado en el uso de la herramienta SAP Solution Manager, utilizada para mantener la trazabilidad completa y detallada de cualquier cambio o ajuste en los procesos, configuración y escenarios de pruebas del SIBA.

- De los trabajos realizados por el personal del proveedor referentes a los servicios bajo demanda de mejora incremental, no fue posible validar la cantidad de horas utilizadas para la ejecución de las actividades, su perfil, así como el costo por hora; a fin de verificar que éstas corresponden a lo estimado en la cotización del prestador de servicios, así como a las tareas efectuadas por el proveedor.

- En relación con la Estrategia de Transferencia de Conocimiento, no se identificó evidencia de la organización de los equipos de trabajo de las partes involucradas para la convocatoria de las sesiones de capacitación, así como al personal convocado. La documentación presentada muestra el estatus de actividades como "no iniciada", por lo que se desconoce si la transferencia de conocimiento fue realizada en su totalidad y a entera satisfacción del Banco.

- No se identificó evidencia del proceso de administración de usuarios externos (altas, bajas y cambios) y que éste haya sido aplicado a los recursos del proveedor que participaron en el proyecto.

- En el listado de usuarios y perfiles autorizado para la liberación del sistema, no se observó si los usuarios corresponden a personal del prestador de servicios o de BANOBRAS; asimismo, para uno de los tres perfiles de SAP utilizados para dicha actividad, no se identificó la definición de sus privilegios y transacciones.

- No se realizó una revisión periódica de las bitácoras de las bases de datos (logs); el Banco señaló que debido a que el módulo PLD/FT no es considerado como aplicativo crítico, no se encuentran obligados a configurar las bitácoras de seguridad conforme a lo establecido en sus Políticas Generales de Seguridad de la Información.

  Sin embargo, dicho módulo comparte recursos con el SIBA, el cual es considerado crítico; por lo que se tiene el riesgo de que en caso de una intrusión, movimientos irregulares o cambios no autorizados, exista oportunidad para que los usuarios

maliciosos puedan ejecutar transacciones no autorizadas que comprometan la integridad de los activos, sin que sean detectados.

- Se carece de la documentación que acredite que el proveedor instruyó al personal que participó en el proyecto a guardar secrecía y confidencialidad sobre los activos e información requerida para la prestación de los servicios, conforme a lo establecido en el Anexo Técnico en su numeral 18. Confidencialidad; así como de la evidencia que garantice que el Banco haya verificado su cumplimiento.

Se concluye que existieron deficiencias en la gestión de los servicios, en razón de que la Institución no se aseguró de validar la capacidad técnica de los recursos del proveedor; no se proporcionó evidencia referente al seguimiento y atención de incidentes, identificación de vulnerabilidades y su remediación; monitoreo de las bitácoras; no se identificó el monitoreo de la disponibilidad del SIBA ni el establecimiento de los OLAS's del proyecto. Asimismo, los administradores del contrato no verificaron el cumplimiento de los entregables proporcionados por el prestador de servicios, ni la cantidad de horas prestadas por el personal asignado al proveedor para ejecutar los servicios bajo demanda de mejora incremental, su perfil, así como el costo por hora; a fin de acreditar que éstas corresponden a lo estimado en la cotización del prestador de servicios y a las actividades ejecutadas por el proveedor relacionadas con este servicio.

2017-2-06G1C-15-0092-01-003 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. realice el monitoreo del nivel de disponibilidad del Sistema Integral Bancario y Administrativo (SIBA) e implemente los Acuerdos de Operación (OLAs), a fin de garantizar el cumplimiento de los niveles de servicio establecidos en el contrato; ejecute un análisis de vulnerabilidades a los proyectos antes de su liberación en el ambiente de producción y lleve a cabo el seguimiento y atención de las vulnerabilidades identificadas en la implementación de los módulos del SIBA, a fin de detectar deficiencias en la seguridad de la información que pudieran ocasionar una afectación a la operación del Sistema.

2017-2-06G1C-15-0092-01-004 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. verifique los perfiles, experiencia y certificaciones de los recursos que el proveedor designe para la prestación del servicio contratado; defina e implemente un proceso de administración de usuarios externos (altas, bajas y cambios); establezca privilegios y transacciones requeridas por los perfiles de SAP utilizados para la liberación del sistema; así como realizar el monitoreo de las bitácoras del aplicativo y bases de datos del Sistema Integral Bancario y Administrativo (SIBA), a fin de detectar oportunamente movimientos irregulares o cambios no autorizados.

2017-2-06G1C-15-0092-01-005 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. defina e implemente mecanismos para el control y supervisión de la cantidad de horas prestadas por el personal asignado por el proveedor y su perfil, a fin de garantizar que las horas estimadas en la propuesta del prestador de servicios, así como los perfiles del personal corresponden con las actividades ejecutadas.

4. Contrato DAGA/084/2016 "Servicio de Aseguramiento de la Calidad para la Implementación del Sistema Integral Bancario y Administrativo (SIBA)"

Con el análisis del contrato número DAGA/084/2017 celebrado con DELOITTE CONSULTING GROUP, SC. y GALAZ, YAMAZAKI, RUIZ URQUIZA, S.C., mediante el procedimiento de licitación pública mixta nacional número LA-006G1C001-E105-2016, con objeto de recibir el "Servicio de Aseguramiento de la Calidad para la Implementación del Sistema Integral Bancario y Administrativo (SIBA)", vigente del 4 de junio de 2016 al 31 de agosto de 2018; por un monto de 57,611.0 miles de pesos; con fecha de 4 de enero de 2017 se celebró un convenio modificatorio para adicionar el servicio de "recepción y elaboración del plan integral del proyecto", ampliar el costo de los servicios a un monto de 64,281.0 miles de pesos, así como el monto de la fianza, se determinó lo siguiente:

Alcance

El alcance del contrato consistió en la revisión de la calidad en las actividades realizadas por un tercero para la implementación del Sistema Integral Bancario y Administrativo (SIBA), emitir las observaciones relevantes y realizar las validaciones correspondientes para mantener la utilización estándar del producto e identificar eventos que pongan en riesgo la garantía del mismo, para así maximizar el aprovechamiento de dicha inversión. En este sentido, se proporcionaron los siguientes servicios:

- S1. Recepción y elaboración del plan integral del proyecto.
- S2. Monitoreo y control del proyecto.
- S3. Planeación de la calidad.
- S4. Control de la calidad.

Proceso de contratación

Se identificó que la investigación de mercado IM/238/2015 fue elaborada el 3 de noviembre de 2015; sin embargo, el contrato se celebró en junio de 2016, por lo que la investigación de mercado no se actualizó conforme a la situación del mercado al momento de contratar los servicios.

Pagos

Se realizaron pagos a enero de 2017 por un monto de 14,428.5 miles de pesos.

Terminación Anticipada

Debido a la terminación anticipada del contrato DAGA/050/2014 en diciembre de 2016, el Banco decidió el 27 de enero de 2017 también terminar anticipadamente el contrato celebrado con el proveedor DELOITTE CONSULTING GROUP, SC. y GALAZ, YAMAZAKI, RUIZ URQUIZA, S.C., debido a que el objeto de este contrato era proporcionar asesoría y garantizar la calidad de los servicios ejecutados en el contrato DAGA/050/2014, por lo que no se contaba con la necesidad que dio origen a la adjudicación.

Por lo anterior, el proveedor ejecutó únicamente los servicios:

- S1. Recepción y elaboración del plan integral del proyecto.
- S2. Monitoreo y control del proyecto.
- S3. Planeación de la calidad.

El Banco proporcionó el dictamen de la terminación anticipada, oficio de su solicitud y notificación al proveedor, en cumplimiento de lo estipulado en el artículo 54 bis de la LAASSP, así como de la cláusula sexta del contrato DAGA/084/2016.

Cumplimiento técnico y funcional

- Se carece de la documentación que garantice que el Banco dio atención a los hallazgos emitidos por el proveedor, respecto a la documentación del contrato DAGA/050/204, en el entregable "S1.E1. Inventario de la documentación existente del proyecto", en el cual el prestador de servicios identificó documentos duplicados, nombre de documentos incorrectos, archivos no organizados correctamente en carpetas, documentos sin firma; así como recomendaciones relacionadas con la estructura de las carpetas y la nomenclatura correcta de los archivos.

  De igual manera, no entregó evidencia que asegure que los archivos identificados por el proveedor como faltantes en el repositorio del proyecto, se encuentren actualmente dentro de dicho repositorio.
- Por la terminación anticipada del contrato DAGA/050/2014, se identificó:

  - Los siguientes entregables, estipulados en el contrato, no fueron utilizados en su totalidad por BANOBRAS:
    - S1.E2. "Plan de Trabajo Integral del proyecto de implementación del SIBA,
    - S1.E3. Los mecanismos de gobierno, seguimiento y control del proyecto,

- S3.E2. Plan de Calidad,
- S3.E3. Bitácora de entregables y
- S3.E4. Calendario de revisiones.

- El proveedor no generó los entregables correspondientes al servicio S4. Control de la Calidad.

- Se carece de la documentación que acredite que el proveedor instruyó al personal que participó en el proyecto a guardar secrecía y confidencialidad sobre los activos e información requerida para la prestación de los servicios, conforme a lo establecido en el Anexo Técnico en su numeral 12. Confidencialidad; así como de la evidencia que garantice que el Banco haya verificado su cumplimiento.

Se concluye que existieron algunas deficiencias en la administración y seguimiento a las actividades definidas en el contrato DAGA/084/2016, debido a que el Banco no implementó acciones correctivas ni dio seguimiento a los hallazgos, recomendaciones, planes y observaciones identificados por el prestador de servicios en el entregable "S1.E1. Inventario de la documentación existente del proyecto", a fin de garantizar la calidad en las tareas de implementación del Sistema Integral Bancario y Administrativo (SIBA), lo cual fue el objeto de llevar a cabo la contratación.

2017-2-06G1C-15-0092-01-006 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. de seguimiento a los hallazgos, recomendaciones, planes y observaciones identificados por terceros, a fin de corregir y garantizar la calidad en las tareas de implementación del Sistema Integral Bancario y Administrativo (SIBA).

5. Ciberseguridad

Con la revisión de la información proporcionada por el Banco Nacional de Obras y Servicios Públicos S.N.C. (BANOBRAS), relacionada con la administración y operación de los controles de Ciberseguridad para el Sistema de Pagos Electrónicos Interbancarios (SPEI), se analizaron las directrices, infraestructura y herramientas informáticas en esta materia; para lo cual se solicitó información al Banco conforme a lo establecido en la circular 14/2017 "Reglas Del Sistema De Pagos Electrónicos Interbancarios (SPEI)" de fecha 4 de julio de 2017, así como al Apéndice M "Requisitos de Seguridad Informática y de Gestión del Riesgo Operacional" del Manual de Operación del SPEI definido por el Banco de México (BANXICO).

Se utilizó como referencia el documento "CIS Controls IS Audit/Assurance Program", emitido de manera compartida por Control of Internet Security (CIS) e ISACA, en el cual se establecen 20 controles de ciberdefensa, integrados por 149 actividades de control para llevar a cabo la evaluación e identificación de las estrategias, políticas, procedimientos y controles de ciberdefensa implementados en el Banco y definir su nivel de madurez.

Para efectuar la revisión, se realizó una conciliación entre los controles definidos en la circular 14/2017 y los establecidos en el documento CIS Controls IS Audit/Assurance Program, verificando los siguientes:

- Inventario de dispositivos autorizados y no autorizados.
- Inventario de software autorizado y no autorizado.
- Configuraciones de seguridad para hardware y software en dispositivos móviles, laptops, estaciones de trabajo y servidores.
- Evaluación continua de vulnerabilidades y remediación.
- Uso controlado de privilegios administrativos.
- Mantenimiento, monitoreo y análisis de registros de auditoría.
- Protecciones de correo electrónico y navegador web.
- Defensas contra malware.
- Limitación y control de puertos de red, protocolos y servicios.
- Capacidad de recuperación de datos.
- Configuraciones de seguridad en dispositivos de red (Firewalls, Routers y Switches).
- Defensa perimetral.
- Protección de la Información.
- Control del acceso según la necesidad de información.
- Control del acceso inalámbrico.
- Supervisión y control de cuentas.
- Capacitación en Seguridad de la Información.
- Seguridad del software de aplicación.
- Respuesta y gestión de los incidentes.
- Pruebas de penetración.

En la revisión efectuada, se identificaron áreas de oportunidad en los controles de ciberdefensa implementados en el Banco, las cuales fueron dadas a conocer a BANOBRAS para su remediación y robustecer las acciones llevadas a cabo en esta materia.

Por lo anterior, la ASF emite las siguientes recomendaciones:

- Evaluar herramientas para identificar automáticamente a los equipos que se conectan a la red, enlistar y controlar el software que se ejecuta en la infraestructura tecnológica, con la finalidad de contar con un inventario de equipos preciso, asegurar la integridad de los archivos, el control de cambios al software, así como disminuir los riesgos que pudieran impactar en la óptima operación y manejo de la información en el Banco.

- Ejecutar análisis de riesgos, de vulnerabilidades y pruebas de penetración periódicamente, a fin de identificar posibles amenazas que pudieran ocasionar una afectación a la confidencialidad, la disponibilidad e integridad de la información del SPEI; así como implementar mecanismos para remediar las incidencias detectadas en dichos ejercicios para el sistema.

- Instrumentar acciones para resguardar, monitorear y vigilar las actividades de las cuentas administrativas, así como monitorear y analizar periódicamente los registros de auditoría con una adecuada segregación de funciones; con la finalidad de evitar el mal uso de las cuentas de usuario por parte de personal no autorizado, así como documentar las incidencias de la revisión de las bitácoras y mitigar los riesgos que sean identificados.

- Definir e implantar una política en donde se establezcan los puertos y protocolos seguros que deben ser ejecutados en el SPEI, así como la línea base de configuración de seguridad para los equipos de comunicaciones como son Firewalls, Routers y Switches; con la finalidad de prevenir vulnerabilidades asociadas con los puertos y fortalecer las configuraciones de la infraestructura tecnológica para mitigar los impactos de las posibles amenazas.

- Incorporar en el procedimiento de gestión de incidentes del SPEI, un apartado en donde se consideren los incidentes de seguridad; así como evaluar la viabilidad de implementar una herramienta automatizada que permita llevar a cabo la definición, clasificación, seguimiento y atención de los incidentes de seguridad del SPEI. Identificar y suprimir los eventos maliciosos y establecer los métodos de comprobación de la solución del problema, para minimizar el impacto del riesgo y mejorar los tiempos de servicio.

- Implementar el análisis y estudio de la Segregación de Funciones en las actividades operativas y sustantivas del Gerente de Operación de Tecnologías de la Información y las funciones ejecutadas como encargado de "Seguridad Informática del servicio SPEI", para resolver o mitigar las situaciones con posibilidad de fraude, irregularidades en los procesos, en el procesamiento de transacciones y duplicidad de funciones.

- Definir e implementar políticas y procedimientos para llevar a cabo la clasificación de la información del SPEI, así como de seguridad de las redes inalámbricas (Wireless), a fin de mitigar el riesgo de que personal no autorizado tenga acceso a información confidencial y existan filtraciones de datos, lo que vulneraría la privacidad e integridad de la información contenida en el SPEI.

2017-2-06G1C-15-0092-01-007 **Recomendación**

Para que el Banco Nacional de Obras y Servicios Públicos, S.N.C. evalúe herramientas para identificar automáticamente a los equipos que se conectan a la red; ejecute análisis de riesgos, de vulnerabilidades y pruebas de penetración periódicamente; instrumente acciones para resguardar, monitorear y vigilar las actividades de las cuentas administrativas y registros de auditoría; defina e implemente una política en donde se establezcan los puertos y protocolos seguros que deben ser ejecutados en el Sistema de Pagos Electrónicos Interbancarios (SPEI), así como la línea base de configuración de seguridad para los equipos

de comunicaciones; establezca el procedimiento de gestión de incidentes de seguridad del SPEI y evalúe la viabilidad de implementar una herramienta automatizada para la gestión de los mismos; implemente el análisis y estudio de la Segregación de Funciones en las actividades operativas y sustantivas de los responsables de administración del SPEI; defina e implemente políticas y procedimientos para llevar a cabo la clasificación de la información del SPEI, así como de seguridad de las redes inalámbricas; y ejecute el monitoreo y supervisión del cumplimiento de las disposiciones normativas relacionadas con Ciberseguridad.

Resumen de Observaciones y Acciones

Se determinaron 5 observaciones las cuales generaron: 7 Recomendaciones.

Dictamen

Con base en los resultados de la auditoría practicada, cuyo objetivo consistió en fiscalizar la gestión financiera de las TIC, su adecuado uso, operación, administración de riesgos y aprovechamiento, así como evaluar la eficacia y eficiencia de los recursos asignados en procesos y funciones. Asimismo, verificar que las erogaciones, los procesos de adjudicación, contratación, servicios, recepción, pago, distribución, registro presupuestal y contable, entre otros, se realizaron conforme a las disposiciones jurídicas y normativas aplicables, y específicamente respecto de la muestra revisada por 87,587.3 miles de pesos; se concluye que, en términos generales, el Banco Nacional de Obras y Servicios Públicos, S.N.C. cumplió con las disposiciones legales y normativas que son aplicables en la materia, excepto por los aspectos observados siguientes:

- Del contrato número DAGA/097/2017 (para prestar los servicios de continuidad operativa del Sistema Integral Bancario y Administrativo [SIBA]), celebrado con la empresa SAP MÉXICO, S.A. DE C.V.; se determinó lo siguiente:
    - No fue posible identificar la validación realizada, por personal del Banco, para determinar la cantidad de horas prestadas por el personal asignado por el proveedor, su perfil, así como el costo por hora; a fin de verificar que éstas corresponden a lo estimado en la cotización presentada por el proveedor, así como a los servicios efectuados.
    - Se carece de la definición y evaluación de los Acuerdos de operación (OLA's) mediante los cuales se realizaría la medición de la disponibilidad del módulo de prevención contra el lavado de dinero y el financiamiento al terrorismo (PLD/FT); no se verificó el cumplimiento del nivel de disponibilidad del 99.5% del SIBA.
    - No se ejecutó un análisis de vulnerabilidades antes de la liberación del módulo PLD/FT en el ambiente de producción; por lo que existe el riesgo de que no se puedan detectar deficiencias en la seguridad de la información que pudieran ocasionar una afectación a la operación del SIBA.

- Se identificaron deficiencias en el proceso de supervisión por parte de los administradores de los contratos en revisión, debido a que no se identificó la

documentación soporte que confirme las actividades de monitoreo realizadas por la Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC).

- No se verificó los recursos del proveedor que participaron en la ejecución de los servicios contratados contaran con la experiencia, conocimientos y certificaciones requeridas para llevar a cabo las actividades.

- Se identificaron áreas de oportunidad en la administración y operación de los controles de Ciberseguridad para el Sistema de Pagos Electrónicos Interbancarios (SPEI) implementados en el Banco, las cuales fueron dadas a conocer a BANOBRAS para su remediación y robustecer las acciones llevadas a cabo en esta materia.

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

El presente dictamen se emite el 15 de octubre de 2018, fecha de conclusión de los trabajos de auditoría correspondientes a la Cuenta Pública 2017, la cual se practicó sobre la información proporcionada por la entidad fiscalizada y de cuya veracidad es responsable.

Servidores públicos que intervinieron en la auditoría:

Director de Área	Director General
Mtro. Roberto Hernández Rojas Valderrama	Ing. Alejandro Carlos Villanueva Zamacona

Comentarios de la Entidad Fiscalizada

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

Apéndices

Procedimientos de Auditoría Aplicados

1. Verificar que las cifras reportadas en la Cuenta Pública correspondan con las registradas en el estado del ejercicio del presupuesto y que estén de conformidad con las disposiciones y normativas aplicables; análisis del gasto ejercido en materia de TIC en los capítulos contables de la Cuenta Pública fiscalizada.

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

3. Verificar que el proceso de contratación, cumplimiento de las especificaciones técnicas y distribución del bien o servicio se realizó 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; analizar la documentación de las contrataciones para descartar asociaciones indebidas, subcontrataciones en exceso, adjudicaciones sin fundamento, transferencia de obligaciones, suscripción de los contratos (facultades para la suscripción, cumplimiento de las obligaciones fiscales, fianzas), entre otros.

4. Comprobar que los pagos realizados por los trabajos contratados están debidamente soportados, cuentan con controles que permitan 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 en caso de incumplimientos.

5. Analizar los contratos y anexos técnicos relacionados con la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados vinculados a la infraestructura tecnológica, telecomunicaciones y aplicativos sustantivos para verificar: antecedentes; investigación de mercado; adjudicación; beneficios esperados; análisis de entregables (términos, vigencia, entrega, resguardo, operación, penalizaciones y garantías); pruebas de cumplimiento y sustantivas; implementación y post-Implementación.

6. Evaluación del riesgo inherente en la administración de proyectos, desarrollo de soluciones tecnológicas, administración de procesos y servicios administrados, así como el plan de mitigación para su control, manejo del riesgo residual y justificación de los riesgos aceptados por la entidad.

7. Evaluar los controles y procedimientos aplicados en la administración de los mecanismos de ciberdefensa, en las acciones fundamentales que cada entidad debe

implementar para mejorar la protección de sus activos de información, tales como el inventario y autorización de dispositivos y software; configuración del hardware y software en dispositivos móviles, laptops, estaciones y servidores; evaluación continua de vulnerabilidades y su remediación; controles en puertos, protocolos y servicios de redes; protección de datos; controles de acceso en redes inalámbricas; seguridad del software aplicativo; entre otros; verificar que el personal del área de seguridad de la información cuente con las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación, experiencia y capacitación.

Áreas Revisadas

La Dirección General de Tecnologías de la Información y Comunicaciones (DGTIC) del Banco Nacional de Obras y Servicios Públicos, S.N.C. (BANOBRAS).

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 por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, artículos 10 fracción I, 18, 26 y 27;

Manual Administrativo de Aplicación General en Materia de Tecnologías de Información y Comunicaciones y Seguridad de la Información, Proceso II.C Administración de la Seguridad de la Información (ASI) Objetivo general; Proceso III.D Operación de Controles de Seguridad de la Información y del ERISC (OPEC) Objetivo general; III.C Proceso de Administración de la Operación (AOP), actividad AOP 1 factor crítico 5.E; II.B. Proceso de Administración de la Configuración (ACNF), actividad ACNF 1, factor crítico 3.D; III.B. Proceso De Administración de Proveedores (APRO), actividades APRO 1, APRO 2 y APRO3;

Lineamientos de Seguridad de la Información e Informática para la Operación del SPEI;

Directrices de Gestión de Cuentas de Usuarios, numerales II.2, II.2.6, II.3, II.4 y II.5;

Contrato DAGA/003/2017, Cláusula séptima, décima cuarta;

Anexo Técnico del contrato DAGA/003/2017, numerales 4, 5.1.1, 7, 10, 12;

Contrato DAGA/097/2017, cláusula tercera, vigésima;

Anexo técnico del contrato DAGA/097/2017, numerales 5.2.1, 5.2.7, 5.2.9, 5.2.12.1, 5.2.14, 5.3, 6.1, 6.1.3, 9.1, 10.2, 10.3 y 18;

Proceso de Administración de Incidentes de BANOBRAS, numeral 6;

Políticas Generales de Seguridad de la Información de BANOBRAS, numerales II.8.6, 11.5.1 11.5.2;

Contrato número DAGA/084/2016, cláusula décima sexta;

Anexo técnico del contrato número DAGA/084/2016, numeral 5;

Bases de Colaboración para la ejecución del Programa para un Gobierno Cercano y Moderno 2014-2018, apartados 4.5.3, 4.5.4 y 4.5.5;

Fundamento Jurídico de la ASF para Promover Acciones

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.