Anexo Técnico

I. Introducción

El Banco Nacional de Obras y Servicios Públicos (Banobras), es una Institución de Banca de Desarrollo que se tipifica como empresa pública con participación estatal mayoritaria; cuenta con personalidad jurídica y patrimonio propios.

Banobras como parte del Sistema Financiero Mexicano, se obliga al cumplimiento de la normativa emitida por las Autoridades Financieras.

En este sentido, con fundamento en el Art. 160, fracciones I, II y III; Art. 164, fracción V, incisos e), f), g) y h), y Anexo 52 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito (Disposiciones), y en apego a lo establecido en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información (MAAGTICSI), y en a lo establecido en el documento de Políticas Generales de Seguridad de la Información de Banobras, se formula el presente Anexo Técnico, con la finalidad de contratar los servicios de auditoría para evaluar el cumplimiento relativo a "Seguridad de la Información en la Infraestructura Tecnológica, Telecomunicaciones y en el procesamiento de Información", y demás normatividad, vigente aplicable en este tema, con el propósito de validar el adecuado establecimiento y vigilancia de los mecanismos que permitan la administración de la seguridad de la información de la Institución; así como, disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución.

II. Solicitud

El presente documento se elabora con el propósito de integrar los requerimientos para que un auditor externo independiente lleve a cabo la revisión a que se refieren el art. 160, fracciones I, II y III, Art. 164, fracción V, incisos e), f), g) y h), y Anexo 52 de las Disposiciones, y en apego al Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, y al documento de Políticas Generales de Seguridad de la Información de Banobras.

III. Objetivo del servicio

Llevar a cabo una auditoría por un Auditor Externo independiente, con el propósito de verificar el cumplimiento a la regulación vigente en materia de "Seguridad de la Información en la infraestructura tecnológica, telecomunicaciones y en el procesamiento de información".

IV. Datos, universo y alcance

El universo y alcance de revisión, son los incisos del e) al h), de la fracción V. del Art. 164 y Anexo 52 de las Disposiciones; así como, los procesos ASI (II.C. Proceso de administración de la seguridad de la información) y OPEC (III.D. Proceso de operación de los controles de seguridad de la información y del ERISC), en materia de Tecnologías de la Información y Comunicaciones (TIC) y de Seguridad de la

Información del MAAGTICSI, y al documento de Políticas Generales de Seguridad de la Información de Banobras.

Para la información proporcionada por las áreas (operaciones, actividades y equipos), de los procedimientos señalados en el presente Anexo Técnico, apartado V.. el auditor externo independiente, determinará la muestra estadística representativa.

Disposiciones

Artículo 164. La Dirección General será la responsable de la debida implementación del Sistema de Control Interno; lo anterior, en el ámbito de las funciones que correspondan a dicha dirección.

En la implementación deberá procurarse que su funcionamiento sea acorde con las estrategias y fines de la Institución, aplicando las medidas preventivas y correctivas necesarias para subsanar cualquier deficiencia detectada.

Al efecto, a la Dirección General, en adición a lo señalado en estas disposiciones, le corresponderá llevar a cabo las actividades siguientes:

V. Prever las medidas que se estimen necesarias a fin de que los sistemas informáticos que utilicen las Instituciones para realizar sus operaciones y para la prestación de servicios al público, cumplan con lo siguiente:

e) Cuenten con controles tanto de seguridad que protejan la confidencialidad de la información, como de acceso para garantizar la integridad de los sistemas y de la información generada, almacenada y transmitida por éstos. Dichas medidas serán acordes con el grado de criticidad de la información.

f) Minimicen el riesgo de interrupción de la operación con base en mecanismos de respaldo y procedimientos de recuperación de la información; así como, de la infraestructura tecnológica para su procesamiento.

g) Mantengan registros de auditoría, incluyendo la información detallada de la operación o actividad efectuadas por los usuarios, acorde con lo señalado en el Capítulo IV del Título Segundo de las presentes disposiciones, en particular en lo relativo a la administración del riesgo tecnológico; así como, los procedimientos para su revisión periódica.

h) Contemplen, incluyendo toda su infraestructura tecnológica, la realización de pruebas tendientes a detectar vulnerabilidades de los medios electrónicos, de telecomunicaciones y equipos automatizados, que prevengan el acceso y uso no autorizado. Dichas pruebas se realizarán cuándo menos una vez al año o cuando efectúen modificaciones sustantivas en la infraestructura tecnológica.

Anexo Técnico

Anexo 52 Lineamientos Mínimos de Operación y Seguridad para la Contratación de Servicios de Apoyo Tecnológico.

I. Aspectos en materia de operación.

a) Esquemas de redundancia o mecanismos alternos en las telecomunicaciones de punto a punto que permitan contar con enlaces de comunicación que minimicen el riesgo de interrupción en el servicio de telecomunicaciones.

b) Estrategia de continuidad en los servicios informáticos que proporcionen a la Institución la capacidad de procesar y operar los sistemas en caso de contingencia, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo centrales y otros que estén involucrados en el servicio de procesamiento de información de operaciones o servicios.

c) Mecanismos para establecer y vigilar la calidad en los servicios de información, así como los tiempos de respuesta de los sistemas y aplicaciones.

d) Esquema de soporte técnico, a fin de solucionar problemas e incidencias, con independencia, en su caso, de las diferencias en husos horarios y días hábiles.

II. Aspectos en materia de seguridad.

a) Medidas para asegurar la transmisión de la Información Sensible del Usuario en forma cifrada punto a punto y elementos o controles de seguridad en cada uno de los nodos involucrados en el envío y recepción de datos.

b) Establecimiento de funciones del oficial de seguridad. Para efectos de que la Institución contratante se mantenga enterada del acceso y uso de la información, deberá designar a una persona que se desempeñe como oficial de seguridad en la Institución, quien gozará de independencia respecto de las áreas operativas, de auditoría y de sistemas, y cuya función consistirá, entre otras cosas, en administrar y autorizar los accesos. Dichos accesos deberán corresponder a la necesidad de conocer la información de acuerdo a las funciones documentadas del puesto.

Asimismo, el oficial de seguridad deberá contar en todo momento con los registros de todo el personal que tenga acceso a la información relacionada con las operaciones de la Institución, incluso de aquél ubicado fuera del territorio nacional, en cuyo caso el personal autorizado para acceder a dicha información deberá ser autorizado por el responsable de las funciones de contraloría interna señaladas en la fracción V del Artículo 166 de las presentes disposiciones.

c) Esquema mediante el cual se mantendrá en una oficina de la institución de crédito contratante, la bitácora de acceso a la información por el personal debidamente autorizado.

III. Auditoría y Supervisión.

a) Mecanismos de acceso al ambiente tecnológico, incluyendo información, bases de datos y configuraciones de seguridad, desde las instalaciones de la Institución en territorio nacional.

MAAGTICSI

II. Procesos de organización.
II.C Proceso de Administración de la Seguridad de la Información (ASI).

III. Procesos de entrega.
III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (Equipo de Respuesta a Incidentes de Seguridad TIC en la Institución) (OPEC).

Políticas Generales de Seguridad de la Información en Banobras

Sección II. Políticas

1. Política de Seguridad de Información
2. Organización para la Seguridad de la Información
3. Seguridad en los Recursos Humanos
4. Gestión de Activos
5. Control de Accesos
6. Cifrado
7. Seguridad física y ambiental
8. Política de seguridad en las operaciones
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información
11. Relación con proveedores
12. Gestión de incidentes en la seguridad de la información
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
14. Cumplimiento

V. Periodo de revisión

1. De octubre del 2017 a septiembre del 2018.

VI. Procedimientos

A continuación se definen los procedimientos sujetos a revisión, establecidos en las Disposiciones, en el MAAGTICSI y en las Políticas Generales de Seguridad de la Información de Banobras.

Anexo 52 Infraestructura, Controles y Operación del Centro de Datos Primario:

1. Validar los esquemas de redundancia o mecanismos alternos en las telecomunicaciones de punto a punto que permitan contar con enlaces de comunicación que minimicen el riesgo de interrupción en el servicio de telecomunicaciones.

2. Revisar la estrategia de continuidad en los servicios informáticos que proporcionen la capacidad de procesar y operar los sistemas en caso de contingencia, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo centrales y otros que estén involucrados en el servicio de procesamiento de información de operaciones o servicios.

3. Validar los mecanismos para establecer y vigilar la calidad en los servicios de información, así como los tiempos de respuesta de los sistemas y aplicaciones.

4. Validar el esquema de soporte técnico, a fin de solucionar problemas e incidencias, con independencia, en su caso, de las diferencias en husos horarios y días hábiles.

5. Revisar las medidas para asegurar la transmisión de la Información Sensible del Usuario en forma cifrada punto a punto y elementos o controles de seguridad en cada uno de los nodos involucrados en el envío y recepción de datos.

6. Validar el establecimiento de funciones del oficial de seguridad. Para efectos de que la Institución se mantenga enterada del acceso y uso de la información, designación de una persona que se desempeñe como oficial de seguridad en la Institución, quien gozará de independencia respecto de las áreas operativas, de auditoría y de sistemas, y cuya función consistirá, entre otras cosas, en administrar y autorizar los accesos. Dichos accesos deberán corresponder a la necesidad de conocer la información de acuerdo a las funciones documentadas del puesto.

7. Revisar que el oficial de seguridad cuente en todo momento con los registros de todo el personal que tenga acceso a la información relacionada con las operaciones de la Institución, en cuyo caso el personal autorizado para acceder a dicha información deberá ser autorizado por el responsable de las funciones de contraloría interna señaladas en la fracción V del Artículo 166 de las Disposiciones.

8. Revisar el esquema mediante el cual se mantendrá en una oficina de la institución de crédito contratante, la bitácora de acceso a la información por el personal debidamente autorizado.

9. Validar los mecanismos de acceso al ambiente tecnológico, incluyendo información, bases de datos y configuraciones de seguridad:

   I. Seguridad Física
      a) Control de acceso.
      b) Pruebas de mecanismos de detección y alarma.
      c) Acceso de mercancías y personal de proveedores.
      d) Seguridad perimetral.
      e) Gestión de energía y continuidad.

   II. Seguridad Lógica
      a) Actualización de los sistemas.
      b) Configuración y operación de seguridad.
      c) Segregación de entornos.
      d) Datos reales en entornos no controlados.
      e) Cifrado.
      f) Segmentación y gestión de la red.
      g) Accesos privilegiados.
      h) Accesos remotos de terceras partes.

Disposiciones y Proceso de Administración de la Seguridad de la Información (ASI):

10. Verificar que se cuenten con controles tanto de seguridad que protejan la confidencialidad de la información, como de acceso para garantizar la integridad de los sistemas y de la información generada, almacenada y transmitida por éstos. Dichas medidas serán acordes con el grado de criticidad de la información. Así como, los procesos:

    a) Revisar la designación del responsable de la seguridad de la información y el establecimiento del grupo de trabajo encargado de la implementación y adopción del modelo de gobierno de seguridad de la información en la Institución, en apego a lo establecido en el proceso ASI1.

    b) Revisar que la institucionalización de las prácticas, aseguren la implementación, seguimiento y control de la seguridad de la información en la Institución, y se encuentren conforme a lo establecido en el ASI2.

    c) Revisar que la definición de los objetivos y el diseño, en proceso, de las directrices para establecer el SGSI en la Institución, se encuentren conforme a lo establecido en el ASI3.

11. Verificar que se minimice el riesgo de interrupción de la operación con base en mecanismos de respaldo y procedimientos de recuperación de la información, así como de la infraestructura tecnológica para su procesamiento. Así como, el proceso:

    a) Revisar se elabore y mantenga actualizado un catálogo de infraestructuras de información esencial y, en su caso, críticas, a fin de facilitar la definición de los controles que se requieran para protegerlas, conforme a lo establecido en el ASI4.

12. Revisar que se mantengan registros de auditoría, incluyendo la información detallada de la operación o actividad efectuadas por los usuarios, acorde con lo señalado en el Capítulo IV del Título Segundo de las presentes disposiciones, en particular en lo relativo a la administración del riesgo tecnológico (Artículo 86 Fracción III inciso b)), incluyendo los procedimientos para su revisión periódica. Así como, los procesos:

    a) Revisar la identificación, clasificación y priorización de los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, de manera que se obtengan las matrices de análisis de riesgos, conforme a lo establecido en el ASI5.

    b) Revisar que se hayan definido los controles mínimos de seguridad de la información e integrarlos al SGSI, para su implementación a través de los diversos procesos de la UTIC y aquellos procesos de la Institución que contengan activos de TIC y TO, activos de información e infraestructuras de información esenciales y, en su caso, críticas, conforme a lo establecido en el ASI6.

    c) Revisar las mejoras de seguridad de la información, a través de la aplicación de acciones preventivas y correctivas derivadas de las revisiones que se efectúen al SGSI, conforme a lo establecido en el ASI7.

Disposiciones y Proceso de operación de los controles de seguridad de la información y del ERISC (OPEC).

    d) Revisar la designación del servidor público como responsable de la supervisión de la adecuada implementación de los controles de seguridad de la información definidos en el SGSI y de aquellos resultantes del análisis de riesgos conforme a lo establecido en el OPEC1.

    e) Revisar el establecimiento de la operación del ERISC (Equipo de Respuesta a Incidentes de Seguridad en TIC); así como, la guía técnica de atención a incidentes, conforme a lo establecido en el OPEC2.

    f) Revisar la ejecución de las acciones necesarias para atender un incidente de seguridad de la información de acuerdo a la guía técnica elaborada y de conformidad a los procedimientos establecidos en el OPEC3.

13. Verificar que se contemplen, incluyendo toda su infraestructura tecnológica, la realización de pruebas tendientes a detectar vulnerabilidades de los medios electrónicos, de telecomunicaciones y equipos automatizados, que prevengan el acceso y uso no autorizado. Dichas pruebas se realizarán cuando menos una vez al año o cuando efectúen modificaciones sustantivas en la infraestructura tecnológica.

14. Verificar las Políticas Generales de Seguridad de la Información en Banobras, las cuales contienen:

    a) Política de Seguridad de Información.
    b) Organización para la Seguridad de la Información.
    c) Seguridad en los Recursos Humanos.
    d) Gestión de Activos.
    e) Control de Accesos.
    f) Cifrado.
    g) Seguridad física y ambiental.
    h) Política de seguridad en las operaciones.
    i) Seguridad de las comunicaciones.
    j) Adquisición, desarrollo y mantenimiento de los sistemas de información.
    k) Relación con proveedores.
    l) Gestión de incidentes en la seguridad de la información.
    m) Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
    n) Cumplimiento.

VII. Requisitos del Auditor

El auditor externo deberá cumplir con las siguientes características:

1. Acreditar la capacidad técnica del grupo de trabajo que realizará la revisión, mediante curriculum donde plasme su experiencia profesional en materia de Auditoria en Sistemas de Información y en Seguridad de la Información;. No se aceptaran pasantes para el análisis de información.
2. Proporcionar copia de certificación vigente, en materia de Auditoría en Sistemas de Información y de Seguridad de la Información (ej.: ISO/IEC 27001, CISM, CISA) del equipo de trabajo;

Para dar cumplimiento al numeral 1 y 2, deberá integrar al currículum, referencias de las auditorías en materia de Seguridad de la Información, en los últimos 5 años, para lo cual deberán incorporar en el currículum la siguiente información: ente auditado, fecha, nombre del contacto, teléfono, domicilio, correo electrónico y un extracto apropiado del contrato de prestación de servicios.

VIII. Vigencia

La vigencia del contrato es a partir de la firma del contrato hasta el 27 de noviembre de 2018 y la prestación del servicio de auditoria es del 01 de octubre al 27 de noviembre de 2018, período en el cual

deberá considerar la revisión de la documentación en sitio, entrevistas presenciales, elaboración de productos entregables, entre otras actividades.

IX. Forma de pago

La forma de pago se efectuará contractualmente, a la entrega y aceptación de los siguientes entregables:

No.	Entregable	Periodo	Porcentaje del Pago
1.	Plan de trabajo	A más tardar el 9 de octubre de 2018	5%
2.	Observaciones	A más tardar el 12 de noviembre de 2018	30%
3.	Proyecto de informe	A más tardar el 20 de noviembre de 2018	30%
4.	Informe Final y papeles de trabajo	A más tardar el 27 de noviembre de 2018	35%

X. Entregables

Derivado de las necesidades y de los beneficios que Banobras espera recibir con la contratación de este servicio, deberá considerarse la entrega de los siguientes documentos con las características que se señalan a continuación:

- Plan de trabajo de la Auditoría: Deberá considerar la fecha compromiso de la conclusión de cada procedimiento del apartado VI. de este anexo; así como, fecha de emisión de observaciones y/o recomendaciones, de emisión del proyecto de informe, de entrega de papeles de trabajo y del informe final, respectivamente.

- Observaciones: En caso de existir observaciones y/o recomendaciones, se deberá especificar por cada una, la situación encontrada y el fundamento legal que determine el incumplimiento, y en caso de recomendación, la mejor practica y el plan de acción sugerido para corregir o implementar la observación o recomendación; así como, la clasificación de su importancia en alto, medio bajo o recomendación, considerando lo siguiente:

Alto:	Son observaciones que representan un hecho pasado que causarán daño patrimonial, robo o fraude, riesgo de reputación.
Medio:	Son observaciones que representan un hecho pasado que causarán que pone en riesgo el patrimonio de la Institución.
Bajo:	Son observaciones que representan un hecho pasado cuya materialización no pone en riesgo el patrimonio de la institución.
Recomendación:	Son sugerencias del Auditor que tienen el propósito de mejorar el ambiente de control actual.

- Proyecto de informe de auditoría, deberá contener lo siguiente:
  - Antecedentes
  - Objetivo
  - Alcance
  - Criterios y procedimientos de evaluación
  - Validación del cumplimiento en materia de seguridad de la información, establecido en el apartado VI. de este anexo, describiendo:
  - Observaciones y/o recomendaciones para mitigar los hallazgos identificados
  - Conclusiones y opinión sobre el estado actual considerando los elementos evaluados
  - Anexos (Observaciones y/o Recomendaciones; Glosario)

- Informe final, deberá contener las correcciones sugeridas por la Dirección de Auditoria Interna y lo siguiente:
  - Antecedentes
  - Objetivo
  - Alcance
  - Criterios y procedimientos de evaluación
  - Validación del cumplimiento en materia de seguridad de la información, incluyendo lo establecido en el apartado VI. de este anexo, describiendo:
    - Observaciones y/o recomendaciones para mitigar los hallazgos identificados
    - Conclusiones y opinión sobre el estado actual considerando los elementos evaluados
  - Anexos (Observaciones y/o Recomendaciones; Glosario)

  Las observaciones y/o recomendaciones del informe final, deberán estar referenciados con índices, marcas y fuente de información, conforme a los documentos de análisis elaborados por los auditores y de la información soporte.

  El informe deberá ser entregado en papel membretado por la empresa con la que se firmó el contrato, y firmado por el auditor externo certificado, en original y tres tantos.

- Papeles de trabajo: Deben estar integrados por los documentos de análisis elaborados por el auditor, los cuales deberán describir el trabajo desarrollado de cada procedimiento del apartado VI. de este anexo, por la información soporte entregada por las diferentes áreas del Banco, por las observaciones e informe final. Los papeles de trabajo y documentos que los soporten deberán estar debidamente indexados y contar con marcas, fuente de información y foliados.

  Es importante mencionar que el informe y documentos generados son para uso interno, en su caso se podrán fotocopiar y turnar a las entidades fiscalizadoras y a las autoridades financieras que lo soliciten, sin requerir autorización del despacho ganador.

XI. Penalizaciones y deductivas

Penas

En caso de que los entregables no se reciban por Banobras en las fechas establecidas en el plan de trabajo del licitante ganador, éste se hará acreedor a la siguiente penalización:

a) 2% del valor del entregable contractual, por día de atraso.

Deductivas

En los términos de lo previsto por el artículo 53 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, Banobras aplicará al licitante que resulte ganador una deductiva del 2% del valor del entregable por cumplimiento parcial o deficiente del mismo, por cada día de atraso contractual, con base en la fecha establecida en el plan de trabajo, y a entera satisfacción de la Dirección de Auditoría Interna, de acuerdo con las características señaladas en el apartado X de este anexo.