LEYENDA DE CLASIFICACIÓN
VERSIÓN PÚBLICA

CONTRATO DE PRESTACIÓN DE SERVICIOS NÚMERO DAGA/099/2022 DE FECHA 02 DE DICIEMBRE DE 2022 QUE CELEBRAN POR UNA PARTE EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C., Y POR LA OTRA PARTE, LA PERSONA MORAL TIC DEFENSE, S.A. DE C.V.

TIPO DE INFORMACIÓN QUE SE CLASIFICA: Confidencial

CONTENIDO DEL DOCUMENTO: 138 fojas útiles (24 del contrato, 42 del anexo técnico, 64 del acta de junta de aclaraciones, 1 de la propuesta económica y 7 del anexo D).

PARTES O SECCIONES CONFIDENCIALES: En las páginas 1, 2, 8, 22, 23 y 24 del contrato.

DATOS IDENTIFICADOS COMO INFORMACIÓN CLASIFICADA: Se testa el contenido de varias líneas por tener datos personales de carácter confidencial como son el Registro Federal de Contribuyentes, nombre de la institución bancaria, clabe interbancaria, número de serie y certificado de firma electrónica.

FUNDAMENTO Y MOTIVACIÓN/PRUEBA DE DAÑO: Los sujetos obligados tienen el deber de guardar la confidencialidad respecto de los datos personales que obren en sus archivos y solo pueden ser tratados para atender la finalidad para la que fueron obtenidos, los cuales no pueden ser objeto de publicidad. Revelar datos personales y de particulares conciernen a una persona identificada e identificable, en consecuencia, se traduce en la vulneración de derechos, en virtud de que se convierte en vulnerable pudiendo transgredir el ámbito privado que puede conllevar a actos de molestia, vulnerabilidad o daño con la publicidad de la información.

FUNDAMENTO LEGAL: Artículos 116, primer y cuarto párrafo, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 113, fracción I y III de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y lo establecido en el capítulo VI de la información confidencial, número Trigésimo Octavo, fracción I, numerales 1, 6 y 10 de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas.

Nombre del Área que Clasifica:	Gerencia de Adquisiciones
Nombre y firma de quien clasifica:	Lic. Karla De Tuya García Gerente de Adquisiciones
Fecha y del Comité de Transparencia donde se aprobó la clasificación de la información	Décima tercera sesión extraordinaria del Comité de Transparencia celebrada el 08 de junio de 2023

CONTRATO ABIERTO PLURIANUAL NÚMERO DAGA/099/2022, PARA LA PRESTACIÓN DE LOS SERVICIOS DE CIBERSEGURIDAD, QUE CELEBRAN, POR UNA PARTE, EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, SOCIEDAD NACIONAL DE CRÉDITO, INSTITUCIÓN DE BANCA DE DESARROLLO, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ " BANOBRAS ", REPRESENTADO EN ESTE ACTO POR LA MAESTRA MARYTELL CASTELLANOS RUEDA , DIRECTORA DE RECURSOS MATERIALES , EN SU CARÁCTER DE REPRESENTANTE LEGAL Y, POR LA OTRA, LA PERSONA MORAL DENOMINADA TIC DEFENSE, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE (TIC DEFENSE SA DE CV), A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PROVEEDOR", REPRESENTADA EN ESTE ACTO POR LA CIUDADANA VALERIA GIORDANO TURRUBIARTE, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIENES EN SU CONJUNTO EN LO SUCESIVO SE LES DENOMINARÁ COMO "LAS PARTES", AL TENOR DE LOS ANTECEDENTES, LAS DECLARACIONES Y LAS CLÁUSULAS SIGUIENTES :

ANTECEDENTES

1. Mediante oficio número DSI/102000/142/2022, de fecha 06 de octubre de 2022, recibido en la Dirección de Recursos Materiales con esa misma fecha, suscrito por el DOCTOR HUMBERTO DAVID ROSALES HERRERA, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, se solicitó iniciar el procedimiento de contratación para los servicios de ciberseguridad.

2. Con fecha 11 de octubre de 2022, se publicó en el Sistema electrónico de información pública gubernamental sobre adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas (CompraNet), la licitación pública nacional electrónica número LA-006G1C001-E157-2022, para la contratación de los servicios de ciberseguridad, al cual en lo sucesivo se le denominará "La Licitación".

3. Con fecha 17 de noviembre de 2022, se emitió el fallo de "La Licitación", en el que, entre otras cosas, el presente contrato fue adjudicado a "El Proveedor".

DECLARACIONES

1. Declara "Banobras" por conducto de su representante legal que:

1.1. Es una Sociedad Nacional de Crédito, legalmente constituida como una entidad, de conformidad con las leyes mexicanas, misma que opera como Institución de Banca de Desarrollo, cuya competencia y atribuciones se señalan en la Ley Orgánica del Banco Nacional de Obras y Servicios Públicos, el Reglamento Orgánico del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo, así como los demás ordenamientos jurídicos vigentes aplicables.

1.2. La MAESTRA MARYTELL CASTELLANOS RUEDA , DIRECTORA DE RECURSOS MATERIALES , con Registro Federal de Contribuyentes (R.F.C.) [redacted] es la servidora pública que tiene conferidas las facultades legales suficientes para celebrar el presente instrumento jurídico, y cuenta con poder general para actos de administración en términos del instrumento público número 143,344 (ciento cuarenta y tres mil trescientos cuarenta y cuatro), libro 3,839 (tres mil ochocientos treinta y nueve), de fecha 13 de enero de 2021, otorgada ante la fe del Licenciado Ricardo Gutiérrez Pérez, Titular de la Notaría Pública número 68 de la Ciudad de México, inscrito en el Registro Público de la Propiedad y de Comercio del Distrito Federal (hoy Ciudad de México) bajo el folio mercantil número 80259, de fecha 19 de abril de 2021.

1.3. De conformidad con lo dispuesto por los artículos 2, fracción III Bis y 84, párrafo octavo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (RLAASSP), así como en términos de lo señalado en el numeral 18 "Administración, Vigilancia del Contrato y Supervisión de las especificaciones y aceptación de los servicios" del documento

Se elimina RFC de persona física, con fundamento en los artículos 116, párrafo primero de la LGTAIP y 113, fracción I de la LFTAIP.

denominado "Anexo Técnico", el DOCTOR HUMBERTO DAVID ROSALES HERRERA , DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN , con R.F.C. [redacted], será el servidor público responsable de administrar, supervisar, vigilar y verificar el cumplimiento del presente contrato, con el apoyo del INGENIERO OMAR MANUEL MATA RUBIO, GERENTE DE SEGURIDAD DE LA INFORMACIÓN 2, o quién (es) en su caso ocupe (n) dicho (s) cargo (s), o quien (es) asuma (n) las atribuciones del (de los) puesto (s).

1.4. Suscribe el presente instrumento jurídico la LICENCIADA KARLA DE TUYA GARCIA , GERENTE DE ADQUISICIONES , con R.F.C [redacted].

1.5. La adjudicación del presente contrato se realizó mediante una LICITACIÓN PÚBLICA , por medio ELECTRÓNICO y de carácter NACIONAL , realizado al amparo de lo establecido, entre otros, el ARTÍCULO 26 FRACCIÓN I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), conforme a lo siguiente:

> La adjudicación del presente instrumento jurídico se realizó mediante "La Licitación", realizada por la Gerencia de Adquisiciones, en su carácter de área contratante, de conformidad con lo dispuesto por el artículo 2, fracción I del RLAASSP, como consta en el ACTA CORRESPONDIENTE A LA CELEBRACIÓN DEL ACTO DE FALLO de fecha 17 de noviembre de 2022, misma que obra en el expediente de contratación correspondiente, con fundamento en lo dispuesto por los artículos 134, párrafo tercero de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), 25, párrafo primero, 26, fracción I, 26 Bis, fracción II, 27, 28, fracción I de la LAASSP y 18 del RLAASSP, en concordancia con el artículo 8 de la Ley Federal de Austeridad Republicana (LFAR), así como en términos de lo señalado en la sección III.7. "De la contratación" de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de BANOBRAS (POBALINES).

1.6. Cuenta con los recursos presupuestarios necesarios y suficientes, así como con la autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, conforme a lo establecido en el artículo 25, párrafo primero de la LAASSP, como se acredita con el documento denominado "Requisición de Bienes, Arrendamientos y Servicios Suficiencia Presupuestal", sellado por la Gerencia de Programación y Control Presupuestal con fecha 30 de agosto de 2022, identificado mediante el número de control interno de la Gerencia de Adquisiciones 124 , con cargo a la partida presupuestal número 33301 "Servicios de informática", clave del Clasificador Único de las Contrataciones Públicas (CUCoP) número 33300001, número de verificación 9353 para el ejercicio fiscal 2022, número de verificación 029 para el ejercicio fiscal 2023 y número de verificación 019 para el ejercicio fiscal 2024.

1.7. Se encuentra debidamente inscrito en el R.F.C. bajo la clave BNO670315CD0

1.8. En cumplimento a lo dispuesto por los artículos 25, párrafos tercero y cuarto de la LAASSP, 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (LFPRH) y 148 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (RLFPRH), así como en términos de lo señalado en las Disposiciones Generales para la Celebración de Contratos Plurianuales del Banco Nacional de Obras y Servicios Públicos, S.N.C., Institución de Banca de Desarrollo, la erogación de los recursos presupuestarios necesarios en el cumplimiento a las obligaciones derivadas del presente contrato fue autorizada por el MAESTRO JUAN JAIME MOLINA VÉLEZ, DIRECTOR GENERAL ADJUNTO DE ADMINISTRACIÓN, mediante oficio número DGAA/190000/291/2022, de fecha 06 de septiembre de 2022, de acuerdo al dictamen efectuado por el DOCTOR HUMBERTO DAVID ROSALES HERRERA, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, a través del oficio número DSI/102000/121/2022, de fecha 1° de septiembre de 2022.

1.9. Para el adecuado cumplimiento y desarrollo de sus actividades cotidianas, requiere contratar los servicios de ciberseguridad.

1.10. Para los fines y efectos legales del presente contrato, señala como su domicilio el ubicado en la Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México.

Se elimina RFC de persona física, con fundamento en los artículos 116, párrafo primero, de la LGTAIP y 113, fracción I, de la LFTAIP.

1.11. Se consultó en el Directorio de Proveedores y Contratistas Sancionados de la página de la Secretaría de la Función Pública (SFP) que "El Proveedor" no se encuentre inhabilitado en los términos de la LAASSP y la Ley de Obras Públicas y Servicios Relacionados con las Mismas (LOPSRM).

2. Declara "El Proveedor" por conducto de su representante legal que:

2.1. Es una persona moral, legalmente constituida conforme a las leyes mexicanas bajo la denominación TIC DEFENSE SA DE CV , tal y como se acredita con la escritura pública número 61,804 (sesenta y un mil ochocientos cuatro), libro 1,801 (mil ochocientos uno), de fecha 29 de noviembre de 2017, otorgada ante la fe del Licenciado Uriel Oliva Sánchez, Titular de la Notaría Pública número 215 de la Ciudad de México, inscrita en el Registro Público de Comercio de la Ciudad de México bajo el número único de documento 20180000372900A8.

■■Dentro de su objeto social se encuentra, entre otros, los relacionados a SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS

2.2. La CIUDADANA VALERIA GIORDANO TURRUBIARTE, en su carácter de representante legal, cuenta con las facultades legales suficientes mismas que, bajo protesta de decir verdad, no le han sido limitadas, modificadas, ni revocadas, en forma alguna para suscribir el presente contrato, y cuenta con poder general para actos de administración en términos del instrumento público número 21,934 (veintiún mil novecientos treinta y cuatro), libro 405 (cuatrocientos cinco), de fecha 15 de noviembre de 2019, otorgada ante la fe del Licenciado Guillermo Aarón Vigil Chapa, Titular de la Notaría Pública número 247 de la Ciudad de México.

2.3. Su representante legal se identifica plenamente mediante credencial para votar expedida a su favor por el Instituto Nacional Electoral (INE).

2.4. Tiene capacidad legal para obligarse en los términos del presente contrato y dispone para ello de los elementos tecnológicos, técnicos, jurídicos, económicos, humanos y materiales, necesarios, adecuados y suficientes, para llevar a cabo la ejecución del mismo.

2.5. Conoce las disposiciones de tipo administrativo, técnico y legal que norman la celebración y ejecución del presente contrato, por lo que acepta someterse a las mismas sin reserva alguna.

2.6. Se encuentra debidamente inscrito en el R.F.C. bajo la clave TDE171130E30

2.7. Manifiesta bajo protesta de decir verdad que, su representante legal, la sociedad, al igual que los socios y/o accionistas integrantes de la misma, o asociados en común, no se encuentran dentro de alguno de los supuestos comprendidos en los artículos 50 y 60 de la LAASSP.

2.8. Manifiesta bajo protesta de decir verdad que, su representante legal, así como los socios y/o accionistas integrantes de la sociedad, no desempeñan un empleo, cargo o comisión en el servicio público, motivo por el cual, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos de lo dispuesto por el artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas (LGRA).

2.9. De conformidad con lo establecido por el artículo 3, fracción III de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa, en términos del artículo 34 del RLAASSP, así como en términos de lo dispuesto en el ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la

Federación el 30 de junio de 2009, manifiesta bajo protesta de decir verdad que, se encuentra constituida conforme a las leyes mexicanas, y con base los criterios (sector, número total de trabajadores y ventas anuales) establecidos en el acuerdo antes citado, tiene un tope máximo combinado de 68.74 (sesenta y ocho punto setenta y cuatro), con base en lo cual, se estratifica como una empresa pequeña.

2.10. Para efectos de lo previsto por el artículo 32-D, párrafos primero, segundo, tercero y cuarto del Código Fiscal de la Federación, presentó a "Banobras", el documento de fecha 18 de noviembre de 2022, con número de folio 22ND6561773, denominado "Opinión del Cumplimiento de Obligaciones Fiscales", expedido por el Servicio de Administración Tributaria (SAT), en el que se emite la opinión positiva respecto del cumplimiento de sus obligaciones fiscales a que alude la regla 2.1.38. de la Resolución Miscelánea Fiscal para 2022, publicada en el Diario Oficial de la Federación el 27 de diciembre de 2021.

2.11. Para efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, así como de conformidad con lo dispuesto en el ACUERDO número ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico en sesión ordinaria de 27 de abril del presente año, por el que se aprobaron las Reglas de carácter general para la obtención de la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social, así como su Anexo Único, publicado en el Diario Oficial de la Federación el 22 de septiembre de 2022, dictado por el H. Consejo Técnico del IMSS, presentó a "Banobras", el documento de fecha 02 de diciembre de 2022, denominado "Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social", expedido por el IMSS, en el que se emite la opinión positiva respecto del cumplimiento de sus obligaciones fiscales en materia de seguridad social.

2.12. Para efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, así como de conformidad con el Anexo Único, numeral 4, incisos a), c) y d) de las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicadas en el Diario Oficial de la Federación el 28 de junio de 2017, emitidas en virtud de la Resolución RCA-5789-01/17, tomada por el H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT), en sesión ordinaria número 790, de fecha 25 de enero de 2017, presentó a "Banobras", el oficio número CGRF/GSRyCF/GCPCyG/0002025202/2022, de fecha 18 de noviembre de 2022, suscrito por el Licenciado Eduardo Jolly Zarazúa, Titular de la Gerencia de Cobro Persuasivo, Coactivo y Garantías del INFONAVIT, del cual se desprende que no se identificaron adeudos ante dicho Instituto, en virtud de que se encuentra al corriente en las obligaciones que señala el artículo 29 de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, respecto de aportar el 5% (cinco por ciento) de los salarios cubiertos a sus trabajadores y de retener y enterar los descuentos para amortizaciones de crédito, hasta el 04 bimestre 2022.

2.13. Señala como su domicilio para cualquier efecto derivado del presente contrato, así como para oír y recibir notificaciones, el ubicado en la calle SENECA 134 PISO 3, COLONIA POLANCO V SECCIÓN, MIGUEL HIDALGO, CIUDAD DE MÉXICO, C.P. 11560

3. Declaran "Las Partes" por conducto de sus respectivas representantes legales que:

3.1. Han revisado y obtenido todas y cada una de las autorizaciones para celebrar el presente contrato, además de que cuentan con las autorizaciones de carácter legal y administrativo necesarias, así como las facultades y capacidades suficientes para tales efectos, mismas que no les han sido modificadas, restringidas, ni revocadas en forma alguna a la fecha de formalización del presente instrumento jurídico.

3.2. Para la celebración del presente contrato, se han conducido en estricto apego a la LGRA, se comprometen a actuar conforme a la misma durante su ejecución, hacia sus contrapartes y a terceros, por lo cual, aceptan expresamente que la transgresión a la presente declaración implica una violación al presente instrumento jurídico.

3.3. En términos de lo dispuesto por la Ley Federal Para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, durante la vigencia del presente contrato, se comprometen a actuar con estricto apego a las siguientes reglas de conducta para combatir la extorsión y el soborno:

-"Banobras" vigilará que los servidores y/o funcionarios públicos que intervengan en la administración, supervisión y/o ejecución del presente contrato cumplan con los compromisos pactados.
-"El Proveedor" actuará siempre con lealtad y mantendrá confidencialidad sobre la información que "Banobras", le haya brindado para la ejecución del presente contrato.
-"El Proveedor" desempeñará con honestidad las actividades que conforman la ejecución del presente contrato, actuando con integridad y profesionalismo, cuidando que no se perjudiquen los intereses de "Banobras".
-"El Proveedor" por sí mismo o a través de interpósita persona, incluyendo a sus empleados y/o representantes, se abstendrá de ofrecer, prometer, dar o aceptar una ganancia pecuniaria indebida para o por los servidores y/o funcionarios públicos de"Banobras", con el fin de obtener o conservar un negocio u otra ventaja impropia.
-"El Proveedor" denunciará ante las autoridades correspondientes los hechos que le consten y que pudiesen ser constitutivos de responsabilidades administrativas y/o penales de los servidores y/o funcionarios públicos de "Banobras" y/o de cualquier tercero que implique violación a la presente declaración.
-"Banobras" exhortará a los servidores y/o funcionarios públicos que por razón de su actividad intervengan en la administración, supervisión y/o ejecución del presente contrato, que cumplan con los compromisos pactados y difundan el presente compromiso entre su personal, así como a terceros que trabajen para "Banobras", que por razones de sus actividades intervengan durante la administración, supervisión y ejecución del presente instrumento jurídico.
-"Banobras" desarrollará sus actividades en la administración, supervisión y ejecución del presente contrato dentro del código de conducta de "Banobras".
-"Banobras" evitará arreglos compensatorios o contribuciones destinadas a favorecer indebidamente a "El Proveedor", por lo que actuará con honestidad y transparencia durante la administración, supervisión y ejecución del presente contrato.

3.4. Comparecen libremente a la celebración del presente instrumento jurídico en los términos consignados, toda vez que es su voluntad celebrarlo; no existe dolo, violencia, lesión, mala fe, ni cualquier otro vicio del consentimiento, además de que se reconocen mutuamente sus respectivas personalidades, aceptando y reconociendo que, en caso de discrepancia entre el contenido del presente contrato, el "Anexo Técnico", la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como la proposición presentada por "El Proveedor", prevalecerá lo establecido en la convocatoria a "La Licitación", en el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022 y en el "Anexo Técnico", de conformidad con lo dispuesto por el artículo 81, fracción IV del RLAASSP, por lo que están de acuerdo en obligarse en los términos y condiciones que se estipulan en las siguientes:

C L Á U S U L A S

PRIMERA. - OBJETO DEL CONTRATO:

"Banobras" encomienda a "El Proveedor" y éste se obliga a proporcionar los SERVICIOS DE CIBERSEGURIDAD, conforme a las características, plazos, términos, condiciones y especificaciones que, de manera enunciativa, más no limitativa, se estipulan en la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, el "Anexo Técnico", elaborado por la Dirección de Seguridad de la Información, en su carácter de área requirente y técnica, de conformidad con lo dispuesto por el artículo 2, fracciones II y III del RLAASSP.

Los anexos que forman parte integral del presente contrato como si a la letra se insertasen se describen a continuación:

-ANEXO A: "Anexo Técnico".

-ANEXO B: ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022.

-ANEXO C: Propuesta económica de "El Proveedor" presentada en "La Licitación".

-ANEXO D: CUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

SEGUNDA. - MONTO Y PRECIO DEL CONTRATO:

El importe de la propuesta económica de "El Proveedor" presentada en "La Licitación", es por la cantidad de $1,799,402.00 (UN MILLÓN SETECIENTOS NOVENTA Y NUEVE MIL CUATROCIENTOS DOS PESOS 00/100 M.N.) , antes del importe que corresponda por concepto del impuesto al valor agregado (I.V.A.), la cual, corresponde a la suma de los precios unitarios mensuales por cada tipo de servicio, misma que forma parte integrante del presente contrato como **ANEXO C.**

Con fundamento en lo dispuesto por los artículos 44, 45, fracciones VI, VII, XIII, 47 de la LAASSP y 85 del RLAASSP, por la prestación de los servicios de ciberseguridad, "Banobras" ejercerá un monto mínimo de $10,796,412.00 (DIEZ MILLONES SETECIENTOS NOVENTA Y SEIS MIL CUATROCIENTOS DOCE PESOS 00/100 M.N.) , más la cantidad de $1,727,425.92 (un millón setecientos veintisiete mil cuatrocientos veinticinco pesos 92/100 M.N.), correspondientes al 16% (dieciséis por ciento) del I.V.A., resultando un monto mínimo total de $12,523,837.92 (doce millones quinientos veintitrés mil ochocientos treinta y siete pesos 92/100) y, un monto máximo de $26,991,030.00 (VEINTISÉIS MILLONES NOVECIENTOS NOVENTA Y UN MIL TREINTA PESOS 00/100 M.N.)

, más la cantidad de $4,318,564.80 (cuatro millones trescientos dieciocho mil quinientos sesenta y cuatro pesos 80/100), correspondientes al 16% (dieciséis por ciento) del I.V.A., resultando un monto máximo total de $31,309,594.80 (treinta y un millones trescientos nueve mil quinientos noventa y cuatro pesos 80/100 M.N.).

Asimismo, los precios unitarios de los SERVICIOS DE CIBERSEGURIDAD, serán los señalados en la propuesta económica de "El Proveedor" presentada en "La Licitación", misma que forma parte integral del presente contrato como si a la letra se insertase como **ANEXO C.**

En este sentido, manifiestan "Las Partes" de común acuerdo, que los precios unitarios de los servicios de ciberseguridad, serán fijos y en moneda nacional, por lo que bajo ninguna circunstancia podrán aumentar durante la vigencia de la relación contractual.

"Banobras" no estará obligado a ejercer el monto máximo del presente contrato.

En cumplimiento a lo dispuesto por los artículos 25, párrafos tercero y cuarto de la LAASSP y 50, fracción IV de la LFPRH, así como lo dispuesto en las Disposiciones Generales para la Celebración de Contratos Plurianuales del Banco Nacional de Obras y Servicios Públicos, S.N.C., Institución de Banca de Desarrollo, los montos mínimos y máximos a ejercer por ejercicio fiscal sin considerar el I.V.A., serán los siguientes:

Ejercicio Fiscal	Monto mínimo	Monto máximo
2022	$1,031,657.15	$2,579,142.87
2023	$8,637,129.60	$21,592,824.00
2024	$1,127,625.25	$2,819,063.13

TERCERA. - FORMA DE PAGO:

Con fundamento en lo dispuesto por los artículos 45, fracción XIV y 51 de la LAASSP, correlativo al artículo 89 del RLAASSP, en términos de lo establecido por la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES y de conformidad con lo señalado en el numeral 14. "Forma de Pago" del "Anexo Técnico", "Banobras" a través de la Dirección de Seguridad de la Información, realizará los pagos que resulten procedentes a "El Proveedor" de manera mensual, por los servicios efectivamente devengados, a entera satisfacción de "Banobras", dentro de los 20 (veinte) días naturales posteriores a la entrega del Comprobante Fiscal Digital (CFDI) respectivo, al correo del Titular de la Dirección de Seguridad de la Información, el cual, le será hecho del conocimiento mediante oficio correspondiente, quien revisará que el CFDI cumpla en cuanto a su contenido con lo estipulado en el presente contrato, el "Anexo Técnico", la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como la proposición de "El Proveedor" presentada en "La Licitación".

El CFDI deberá cumplir con todos los requisitos que marca la normativa vigente, sin limitar, las disposiciones contenidas en los artículos 29, y 29-A del Código Fiscal de la Federación, incluyendo el sello digital correspondiente, por lo que "Banobras" verificará su estructura, contenido y autenticidad.

De conformidad con lo dispuesto por el artículo 90 del RLAASSP, en caso de que el CFDI presente errores o deficiencias, "Banobras" dentro de los 3 (tres) días hábiles siguientes al de su recepción, por conducto del Titular de la Dirección de Seguridad de la Información, le notificará por escrito a través de correo electrónico a "El Proveedor", las observaciones y/o deficiencias detectadas para que realice las aclaraciones pertinentes y, en su caso, cancele y emita el CFDI que sustituya el CFDI que no haya solventado los señalamientos de "Banobras".

El período que transcurre a partir de la entrega del citado escrito y hasta que "El Proveedor" realice las aclaraciones que solventen las observaciones y/o deficiencias detectadas por "Banobras", o bien, sustituya el CFDI que no haya solventado los señalamientos de "Banobras", no se computará para efectos del artículo 51 de la LAASSP.

Dentro del trámite para la aceptación del CFDI que reúna los requisitos fiscales correspondientes, "Banobras" a través de la Dirección de Seguridad de la Información, por conducto de la Gerencia de Seguridad de la Información 2, en su caso, deberá realizar el cálculo y determinación de las penas convencionales y/o deductivas, por lo que, bajo ningún supuesto, podrá suspender dicho trámite o ampliar el plazo para el pago por tal motivo.

Lo anterior sin perjuicio de que "Banobras" proceda al cobro de las penas convencionales y/o deductivas previo al pago correspondiente.

En el supuesto de que sea rescindido el presente contrato, no procederá el cobro de las penas convencionales, ni la contabilización de las mismas, al hacer efectiva la garantía de cumplimento señalada en la cláusula **SÉPTIMA** del presente instrumento jurídico de conformidad con el contenido del artículo 95, párrafo segundo del RLAASSP.

"Banobras" no cubrirá pago alguno a "El Proveedor" respecto de los servicios de ciberseguridad, cuando no cumplan en su totalidad con lo solicitado en el presente contrato, el "Anexo Técnico", la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como la proposición de "El Proveedor" presentada en "La Licitación".

Los pagos que deriven de la relación contractual serán cubiertos por "Banobras" en las oficinas de la Gerencia de Pagos, ubicada en la Avenida Javier Barros Sierra N° 515, Planta Baja, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México, o bien, serán depositados electrónicamente en la cuenta bancaria cuyos datos son CLABE interbancaria [redacted] y nombre de la institución de crédito [redacted].

Posterior a la firma del presente instrumento jurídico, "El Proveedor" deberá enviar al Titular de la Dirección de Seguridad de la Información, así como al Gerencia de Seguridad de la Información 2, la carátula de la cuenta antes señalada, de tal forma que como mínimo deberá contener:

1. Nombre del beneficiario;

2. R.F.C.;

3. CLABE interbancaria de 18 (dieciocho) dígitos;

4. Número de cuenta bancaria;

5. Nombre de la institución de crédito; y

6. Sucursal.

Para el caso de que "El Proveedor" cambie el número de cuenta bancaria, lo hará del conocimiento de "Banobras" por conducto del Titular de la Dirección de Seguridad de la Información y del Titular de la Gerencia de Seguridad de la Información 2, a efecto de que los siguientes pagos sean efectuados a dicha cuenta.

En caso de incumplimiento en los pagos referidos en la presente cláusula, "Banobras" acepta y reconoce que a solicitud de "El Proveedor", deberá pagar gastos financieros conforme a la tasa que será igual a la establecida por la Ley de Ingresos de la Federación en los casos de prórroga para el pago de créditos fiscales.

Dichos gastos se calcularán sobre las cantidades no pagadas y se computarán por días naturales, desde que se venció el plazo pactado hasta la fecha en que las cantidades que correspondan se pongan efectivamente a disposición de "El Proveedor", en la

Se elimina nombre de la institución bancaria y CLABE interbancaria de persona moral con fundamento en los artículos 116, cuarto párrafo, de la LGTAIP y 113, fracción II, de la LFTAIP.

forma y términos prescritos por el artículo 51, párrafo segundo de la LAASSP.

Tratándose de pagos en exceso que haya recibido "El Proveedor", éste deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a lo señalado en el párrafo anterior.

Los intereses se calcularán sobre las cantidades pagadas en exceso en cada caso y se computarán por días naturales, desde la fecha del pago hasta la fecha en que las cantidades que correspondan se pongan efectivamente a disposición de "Banobras", en la forma y términos prescritos por el artículo 51, párrafo tercero de la LAASSP.

Una vez cumplida la totalidad de las obligaciones de "El Proveedor" a entera satisfacción de "Banobras", el Titular de la Dirección de Seguridad de la Información, previa aceptación del Titular de la Gerencia de Seguridad de la Información 2, deberá proceder inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales.

Los pagos señalados en la presente cláusula, quedarán sujetos a que "El Proveedor" entregue en tiempo y forma la garantía de cumplimiento señalada en la cláusula **SÉPTIMA** del presente contrato.

CUARTA. - VIGENCIA DEL CONTRATO:

En cumplimiento a lo dispuesto por el artículo 84, párrafo quinto del RLAASSP y en términos de lo señalado en el numeral 10. "Vigencia del servicio" del "Anexo Técnico", la vigencia del presente contrato será del 18 de noviembre de 2022 (18/11/2022) y hasta el 17 de febrero de 2024 (17/02/2024).

QUINTA. - MODIFICACIONES DEL CONTRATO:

"Las Partes" están de acuerdo en que por necesidades de "Banobras" podrá ampliarse la vigencia de los servicios objeto del presente contrato, de conformidad con lo señalado en el artículo 52 de la LAASSP, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) del monto máximo o cantidad de los conceptos o volúmenes establecidos originalmente.

Asimismo, con fundamento en el artículo 91 del RLAASSP, "El Proveedor" deberá entregar la modificación a la garantía de cumplimiento señalada en la cláusula **SÉPTIMA** del presente contrato.

SEXTA. - CUMPLIMIENTO AL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:

"El Proveedor" se obliga expresamente a conocer y cumplir en todo momento el Manual de Políticas de Seguridad de la Información (MPSI), en la sección III.1. P10 - "Políticas de Seguridad de la Información para la Relación con Proveedores", así como los cambios que deriven durante la vigencia de la relación contractual.

"El Proveedor" se compromete a no incurrir o participar en ningún tipo de actividad sospechosa o dañina para las instalaciones, información y operación de "Banobras".

En caso de que ocurra algún incidente con los activos utilizados (tecnológicos o información), por causas imputables a "El Proveedor", este se obliga a solucionar el problema recobrando en todo momento la operación normal de "Banobras" que se hubiere visto afectada por el incidente.

"El Proveedor" se obliga a cumplir los requerimientos para control de accesos y/o procedimientos de autorización para acceder a los activos de información de "Banobras" (tecnológicos e información), así como a cumplir las cláusulas de restricción para el copiado y acceso a la información que se le indiquen por parte de la Dirección de Seguridad de la Información.

"El Proveedor" en este acto manifiesta bajo protesta de decir verdad, que cuenta con los mecanismos necesarios para asegurar a "Banobras" la protección de virus y/o códigos maliciosos, que pudieran surgir con motivo de la ejecución del presente instrumento jurídico.

"El Proveedor" se obliga a comunicar a su personal, empleados y/o a toda persona que por cualquier causa se encuentre o pudiese estar vinculado a él y al uso de activos de información o a la infraestructura de redes y sistemas de "Banobras", el MPSI, así como los cambios que de éste se deriven durante la vigencia de la relación contractual.

En caso de cualquier incumplimiento a lo establecido en la presente cláusula por parte de "El Proveedor", será motivo de la aplicación de penas convencionales en razón del 3% (tres por ciento) del monto máximo señalado en la cláusula **SEGUNDA** del presente contrato, por cada día natural de atraso en la atención del MPSI que le sean aplicables con motivo de los servicios de ciberseguridad.

Derivado de la naturaleza de los servicios de ciberseguridad, "El Proveedor" deberá cumplir los requerimientos establecidos en el documento denominado CUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, mismo que forma parte integral del presente contrato como si a la letra se insertase en el **ANEXO D**, "Banobras" a través de la Dirección de Seguridad de la Información, supervisará que se dé el debido cumplimiento.

SÉPTIMA. - GARANTÍA DE CUMPLIMIENTO DEL CONTRATO:

Con fundamento en lo dispuesto por los artículos 45, fracción XI, 48, fracción II y 49, fracción II de la LAASSP, correlativos a los artículos 85, fracción III y 103 del RLAASSP, en términos de lo establecido por la sección III.7. "De la contratación" de los POBALINES y de conformidad con lo señalado en el numeral 15. "Garantías" del "Anexo Técnico", "El Proveedor" se obliga a garantizar todas y cada una de las obligaciones contraídas mediante el presente contrato, entregando en un plazo que no exceda de 10 (diez) días naturales contados a partir de la firma del presente instrumento jurídico, una póliza de fianza a favor de " BANOBRAS ", expedida por una institución mexicana autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas, expedida a favor de " BANOBRAS ", o bien, en alguna de las otras formas señaladas en el artículo 79, fracción III del RLFPRH, por un importe equivalente al 10.0% (diez por ciento) del monto máximo antes del I.V.A., señalado en la cláusula **SEGUNDA** del presente contrato, o en su caso, por un importe equivalente al 10% (diez por ciento) del monto por erogar antes del I.V.A. en el ejercicio fiscal 2022, misma que deberá ser renovada dentro de los primeros 10 (diez) días naturales de cada ejercicio fiscal, por un importe equivalente al 10% (diez por ciento) del monto por erogar antes del I.V.A. de dicho ejercicio fiscal, conforme a lo señalado en el artículo 87 del RLAASSP.

En caso de entregarse a través de una póliza de fianza, el texto de la citada póliza, deberá estar redactado conforme a lo dispuesto por los artículos 103, fracción I del RLAASSP y 166 de la Ley de Instituciones de Seguros y de Fianzas, así como en términos de lo establecido en las DISPOSICIONES de carácter general por las que se aprueban los modelos de pólizas de fianzas constituidas como garantía en las contrataciones públicas realizadas al amparo de la LAASSP y la LOPSRM, publicadas en el Diario Oficial de la Federación el 15 de abril de 2022.

A su vez, la mencionada póliza de fianza deberá contar con la especificación por parte de que quien la expida, en caso de que " BANOBRAS " exija el pago de las obligaciones de manera forzosa, el procedimiento de ejecución aplicable será el establecido por el artículo 279 de la Ley de Instituciones de Seguros y de Fianzas, aún para el caso de que procediera el cobro de indemnización por mora, con motivo de pago extemporáneo del importe de la póliza de fianza referida. Para el cobro de indemnización por mora se

estará a lo dispuesto en el artículo 283 de la citada Ley de Instituciones de Seguros y de Fianzas.

■■

"El Proveedor" acepta y reconoce que, la garantía de cumplimiento a que se refiere la presente cláusula, será indivisible, considerando el tipo de obligaciones originadas por los servicios de ciberseguridad y se hará efectiva por el importe total de la obligación garantizada.

La garantía de cumplimiento aludida en la presente cláusula, de ninguna manera será considerada como una limitación de la responsabilidad de "El Proveedor" derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico y de ninguna manera impedirá que "Banobras" reclame la indemnización o el reembolso por cualquier incumplimiento que pudiera exceder el valor de la citada garantía de cumplimiento.

"El Proveedor" se obliga a mantener vigente la garantía de cumplimiento señalada en la presente cláusula, durante la vigencia de la relación contractual o a partir de aquella fecha en que "Banobras" hubiere comunicado la terminación anticipada del presente contrato y la mantendrá vigente durante la sustanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte resolución definitiva por una autoridad competente, salvo que "Las Partes" se otorguen el finiquito correspondiente, en el entendido de que solo podrá ser cancelada mediante autorización expresa de "Banobras", previa solicitud por escrito de "El Proveedor", en la forma y términos señalados por el artículo 81, fracción VIII del RLAASSP, así como lo establecido en la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES.

En tanto "El Proveedor" no entregue la garantía de cumplimiento a que se refiere la presente cláusula a "Banobras", deberá cumplir con todas y cada una de las obligaciones a su cargo contraídas mediante el presente contrato, pero bajo ningún motivo, razón, o circunstancia podrá exigir los derechos a su favor que deriven del presente instrumento jurídico, a su vez que, "Banobras" podrá rescindir administrativamente el presente contrato y remitir el asunto al Órgano Interno de Control en "Banobras" para que determine si se aplican las sanciones estipuladas en el artículo 60, fracción III de la LAASSP.

"El Proveedor" acepta expresamente que, la garantía expedida para garantizar el cumplimiento del presente contrato, se hará efectiva independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o judicial, así como que permanecerá vigente durante la substanciación de los juicios o recursos legales que interpongan con relación al presente contrato, hasta que, sea pronunciada resolución definitiva que cause ejecutoria por parte de una autoridad competente.

En caso de modificación al presente contrato, "El Proveedor" se obliga a actualizar el importe y/o la vigencia de la garantía de cumplimiento, mediante endoso correspondiente, dentro de los 10 (diez) días naturales siguientes a la formalización del convenio modificatorio respectivo, de conformidad con lo señalado en el artículo 91 del RLAASSP, en el entendido de que dichas modificaciones surtirán efectos, únicamente en el supuesto de que quien la expida manifieste su consentimiento, mediante la emisión de los documentos modificatorios o endosos correspondientes, debiendo contener en el citado documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

OCTAVA. - OBLIGACIONES DE "EL PROVEEDOR":

Serán obligaciones de "El Proveedor" las siguientes:

■■■

1. Proporcionar los servicios de ciberseguridad, conforme a las características, plazos, términos, condiciones y especificaciones que, de manera enunciativa, más no limitativa, se estipulan en la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como el "Anexo Técnico".
2. Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el presente contrato.
3. Asumir su responsabilidad ante cualquier situación que pudiera generarse con motivo del presente instrumento jurídico.

4. No difundir a terceros sin autorización expresa de "Banobras" la información que le sea proporcionada, inclusive después de la rescisión o terminación del presente contrato, sin perjuicio de las sanciones administrativas, civiles y/o penales a que haya lugar.
5. Proporcionar la información que le sea requerida por parte de los Órganos Internos de Control, la SFP, la Auditoría Superior de la Federación, así como cualquier otro órgano fiscalizador, supervisor, regulador de "Banobras" o terceros auditores contratados por dichas instancias o el propio "Banobras".■
6. Responder por la calidad de los servicios de ciberseguridad, así como cualquier otra responsabilidad en que incurra, en los términos señalados en el presente instrumento jurídico.
■■

NOVENA. OBLIGACIONES DE "BANOBRAS":

Serán obligaciones de "Banobras" las siguientes:

1. Otorgar todas las facilidades necesarias, a efecto de que "El Proveedor" lleve a cabo en los términos convenidos.
2. Sufragar los pagos correspondientes en tiempo y forma, por el servicio objeto del presente contrato.
3. Extender a "El Proveedor", en caso de que lo requiera, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa del Titular de la Dirección de Seguridad de la Información, previa aceptación del Titular de la Gerencia de Seguridad de la Información 2, para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA. - PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO:

"El Proveedor" manifiesta bajo protesta de decir verdad, que los recursos que componen su patrimonio no provienen de lavado de activos, financiación del terrorismo, narcotráfico, captación ilegal de dinero y en general de cualquier actividad ilícita.

Asimismo, "El Proveedor" manifiesta, que los recursos que se reciban como contraprestación del presente contrato, no serán destinados a ninguna de las actividades antes descritas.

Para efectos de lo anterior, "El Proveedor" autoriza expresamente a "Banobras" para que consulte los listados, sistemas de información y bases de datos a los que haya lugar y de encontrar algún reporte, "Banobras" procederá a adelantar las acciones contractuales y/o legales que corresponda.

En este sentido, "El Proveedor" se obliga a realizar todas las actividades encaminadas a asegurar que todos sus socios, accionistas, administradores, clientes, proveedores, empleados y los recursos de estos, no se encuentren relacionados o provengan de actividades ilícitas, particularmente de las anteriormente enunciadas.

DÉCIMA PRIMERA. - LUGARES DE EJECUCIÓN DE LOS SERVICIOS:

Los lugares para la ejecución de los servicios de ciberseguridad, será en cualquier sitio que por la naturaleza del objeto de los mismos sea requerido por "Banobras", conforme a lo señalado en el "Anexo Técnico".

DÉCIMA SEGUNDA. - INFORMACIÓN Y DOCUMENTACIÓN A INSTANCIAS FISCALIZADORAS:

En términos de lo dispuesto por los artículos 57 de la LAASSP y 107 del RLAASSP, "El Proveedor" acepta expresamente que, en caso de que los Órganos Internos de Control, la SFP, la Auditoría Superior de la Federación, así como cualquier otro órgano fiscalizador, supervisor, regulador de "Banobras" o terceros auditores contratados por dichas instancias o el propio "Banobras", le requiera información y/o documentación con motivo de auditorías, visitas o inspecciones que se practiquen dentro de su ámbito de competencia y con fundamento en la legislación aplicable, relacionadas con el objeto del presente contrato, éste la entregará sin

demora, previo acuse de recibido y comunicarlo de inmediato a "Banobras", mediante carta escrita.

DÉCIMA TERCERA. - ANTICORRUPCIÓN:

"El Proveedor" acepta expresamente que, durante la vigencia de la relación contractual, no ofrecerá, prometerá o dará por sí mismo o por interpósita persona, dinero, objetos de valor o cualquier otra dádiva a servidor y/o funcionario público alguno, que puedan constituir un acto ilícito o incumplimiento sustancial del presente instrumento jurídico.

DÉCIMA CUARTA. - DATOS Y DOCUMENTACIÓN:

"El Proveedor" acepta y reconoce que "Banobras" por conducto de la Dirección de Seguridad de la Información, a través de la Gerencia de Seguridad de la Información 2, le proporcionará los datos y documentación que requiera para la adecuada ejecución de los servicios de ciberseguridad, obligándose "El Proveedor" a guardar absoluta secrecía y confidencialidad en el manejo de la información y a no divulgar a terceros por cualquier causa el contenido de la misma, debiendo tener absoluta cautela de la información y documentación que entregue a su personal para brindar los citados servicios de ciberseguridad, siendo responsable de los daños y perjuicios que ocasione el personal o el mismo a "Banobras" por incumplir con las obligaciones de secrecía y confidencialidad, siempre que estos hayan sido dictaminados por una autoridad competente.

En este sentido, la Dirección de Seguridad de la Información, a través de la Gerencia de Seguridad de la Información 2, se obliga a proporcionar la documentación e información que requiera "El Proveedor" para la adecuada ejecución del presente instrumento jurídico y, por ende, la prestación de los servicios de ciberseguridad.

DÉCIMA QUINTA. - CALIDAD:

"El Proveedor" deberá contar con la infraestructura necesaria, personal técnico especializado en el ramo, herramientas, técnicas y equipos adecuados para proporcionar los servicios de ciberseguridad, a fin de garantizar que sea proporcionado con la calidad, oportunidad y eficiencia requerida para tal efecto, comprometiéndose a realizarlo a satisfacción de "Banobras" y con estricto apego a lo establecido en las cláusulas del presente instrumento jurídico.

"Banobras" no estará obligado a recibir los servicios antes citados cuando estos no cumplan con los requisitos establecidos en el párrafo anterior.

DÉCIMA SEXTA. - TERMINACIÓN ANTICIPADA:

De conformidad con lo previsto en los artículos 54 Bis de la LAASSP y 102 del RLAASSP, "El Proveedor" acepta y reconoce que "Banobras", podrá dar por terminado anticipadamente el presente instrumento jurídico, cuando concurran razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios de ciberseguridad y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionará algún daño o perjuicio al Estado, o se determine la nulidad de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio emitido por la SFP.

En dichos supuestos, "Banobras" reembolsará a "El Proveedor", en su caso, los gastos no recuperables en que haya incurrido, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente instrumento jurídico, limitándose según corresponda, a los conceptos señalados en el artículo 102 del RLAASSP.

DÉCIMA SÉPTIMA. - LICENCIAS, AUTORIZACIONES, PERMISOS, PATENTES, MARCAS Y DERECHOS:

En cumplimiento a lo dispuesto por el artículo 45, fracción XVIII de la LAASSP, durante la vigencia de la relación contractual, "El Proveedor" se obliga a contar con todas las licencias, autorizaciones, concesiones y/o permisos necesarios que, conforme a las

disposiciones legales, administrativas y/o reglamentarias vigentes aplicables, se requieran para proporcionar los servicios de ciberseguridad.

Por otra parte, "El Proveedor" será responsable por el uso de patentes, licencias, derechos de autor y marcas que pudieran corresponder a terceros sobre los procedimientos que utilice y que proporcione para cumplir con los servicios de ciberseguridad.

En caso de infringir dichos conceptos o incurrir en violaciones legales, "El Proveedor" se obliga a resarcir a "Banobras" cualquier gasto comprobable que éste erogue por dichos conceptos o derivado de cualquier responsabilidad que le haya sido imputada por una autoridad competente.

DÉCIMA OCTAVA. - IMPUESTOS Y DERECHOS:

Los impuestos, derechos y gastos que procedan con motivo de la prestación de los servicios objeto del presente contrato, serán pagados por "El Proveedor", mismos que no serán repercutidos a "Banobras".

"Banobras" sólo cubrirá, cuando aplique, lo correspondiente al I.V.A., en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA NOVENA. - CESIÓN:

De conformidad con lo establecido en el artículo 46 de la LAASSP, "El Proveedor" no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso, se deberá de contar con el previo consentimiento y conformidad por escrito de "Banobras", deslindando a éste de toda responsabilidad, mismo que se deberá de solicitar por escrito con 10 (diez) días naturales de anticipación a la fecha estimada de pago, aceptando y reconociendo "El Proveedor" que la falta de cumplimiento a la presente cláusula, constituirá una causal de rescisión, en términos de la cláusula **TRIGÉSIMA** del presente contrato.

"Banobras" está incorporado al programa de cadenas productivas de Nacional Financiera, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (NAFIN).

VIGÉSIMA. - CASO FORTUITO O DE FUERZA MAYOR:

Con fundamento en lo dispuesto por los artículos 55 Bis de la LAASSP 2, fracción IV Bis y 102 del RLAASSP, "Banobras" bajo su responsabilidad podrá suspender la ejecución de los servicios de ciberseguridad, cuando durante la vigencia de la relación contractual, se presente caso fortuito o de fuerza mayor, en cuyo caso, únicamente se pagará la parte proporcional que hubiese sido efectivamente proporcionada, a entera satisfacción de la Dirección de Seguridad de la Información, conforme a lo establecido en el presente contrato, la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como el "Anexo Técnico", debiendo celebrar "Las Partes" el convenio respectivo.

La suspensión de los servicios de ciberseguridad, se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma.

Cuando la suspensión obedezca a causas imputables a "Banobras", previa petición y justificación de "El Proveedor", aquél le reembolsará los gastos no recuperables que se originen durante el tiempo que dure la suspensión.

Dicho pago será procedente, siempre y cuando, los mencionados gastos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, los cuales, estarán limitados, según corresponda, a los conceptos previstos en el artículo 102 del RLAASSP.

"Las Partes" deberán pactar el plazo de suspensión, si al término del mismo no se pudieran reiniciar los servicios de ciberseguridad, podrá iniciarse la terminación anticipada a que se hace referencia en la cláusula **DÉCIMA SEXTA** del presente instrumento jurídico.

"El Proveedor" podrá solicitar a "Banobras" el pago de gastos no recuperables en un plazo máximo de un mes contado a partir de la fecha de suspensión del presente contrato.

Los gastos no recuperables, serán pagados dentro de un término que no podrá exceder de 45 (cuarenta y cinco) días naturales posteriores a la solicitud por escrito, mediante el cual, "El Proveedor" fundamente, documente y motive el pago de dichos gastos no recuperables.

VIGÉSIMA PRIMERA. - CONFIDENCIALIDAD:

"El Proveedor", se obliga a guardar absoluta confidencialidad de toda aquella información marcada como confidencial, la cual, será aquella que de conformidad con la legislación aplicable, deba considerarse como reservada, privilegiada y/o confidencial y que sea propiedad de "Banobras", incluyendo sin limitar, aquella relacionada con sus clientes, proveedores y/o empleados, o bien que pueda considerarse propiedad intelectual en términos de la normatividad aplicable.

"El Proveedor" acepta y reconoce la facultad de "Banobras" de solicitarle, en cualquier momento, la devolución o destrucción de todos los datos e información descrita y las copias que de ella existan, así como todos los medios de soporte en que se encuentre contenida.

"El Proveedor" se obliga a instruir a su personal, empleados, agentes, representantes y/o a toda persona que, por cualquier causa, se encuentre o pudiese estar vinculado a él y a la información de que se trata, respecto del contenido y alcances de la obligación de guardar secrecía y confidencialidad, en los términos y respecto de la información y documentación referenciada en la presente cláusula.

En caso de cualquier incumplimiento a los términos de la presente cláusula, además de aplicarse la rescisión administrativa del presente contrato conforme a las disposiciones de las cláusulas **VIGÉSIMA NOVENA** y **TRIGÉSIMA**, "El Proveedor" deberá sacar en paz y a salvo a "Banobras" de cualquier acción o procedimiento que se inicie en su contra, debiendo además reembolsar los gastos y costos que, en su caso, se generen por la atención de dichas acciones o procedimientos; sin perjuicio del ejercicio por parte de "Banobras" de las demás acciones legales que resulten procedentes por la revelación de secretos en términos de lo dispuesto en el Código Penal Federal y los demás ordenamientos legales vigentes aplicables, así como las acciones que por daños y perjuicios pudieran derivar por las violaciones al secreto bancario, industrial, fiduciario, postal, entre otros, contempladas en las diversas leyes de la materia.

En este sentido, cuando sea necesario, "Banobras" proporcionará a "El Proveedor" la "información reservada o confidencial" que requiera para brindar los servicios de ciberseguridad, siempre que esté relacionado con el objeto de los mismos.

En consecuencia, "Las Partes" expresamente establecen que:

1. "El Proveedor" a partir de la vigencia del presente contrato, se obliga en relación a la "información reservada o confidencial" que le sea proporcionada por "Banobras", a no transmitirla o de alguna otra forma divulgarla o proporcionarla a cualquier persona física o moral, nacional o extranjera, pública o privada, por cualquier medio, aun cuando se trate de incluirla o entregarla en otros documentos como reportes, propuestas, ni en todo ni en parte, por ningún motivo a terceras personas físicas o morales, nacionales o extranjeras, públicas o privadas, presentes o futuras, que no hayan sido autorizadas previamente y por escrito por parte de "Banobras" conforme a lo previsto en el presente instrumento jurídico.

2. De igual forma, "El Proveedor" a partir de la vigencia del presente contrato, con relación a la "información reservada o confidencial", se obliga a no divulgarla o proporcionarla, por cualquier medio, aun cuando se trate de incluirla o entregarla en otros documentos como estudios, reportes, propuestas u ofertas, ni en todo ni en parte, por ningún motivo a sociedades de las cuales "El Proveedor" sea accionista, asesor, asegurador, causahabiente, representante, apoderado, consejero, comisario, tenedor de acciones y, en general, tenga alguna relación de cualquier índole por sí o por terceras personas.

3. La obligación de no transmitir o de alguna otra forma divulgar o proporcionar a cualquier persona física o moral, nacional o extranjera, pública o privada, presente o futura, por cualquier medio, la "información reservada o confidencial" prevista en el presente contrato, se extiende a sus socios, consejeros, representantes/apoderados legales, directivos, gerentes, asesores, dependientes y demás personas físicas o morales que guarden relación con "El Proveedor", por lo que ésta última se obliga a comprometer a las personas referidas en la presente fracción al cumplimiento de la presente cláusula.

4. En virtud de lo anterior, queda entendido que "El Proveedor" debe asegurarse que cada receptor de información mencionado en la fracción inmediata anterior, se adhiera al compromiso de confidencialidad estipulado en el presente contrato.

5. "Banobras" podrá reclamar o solicitar la devolución de la "información reservada o confidencial", en cualquier tiempo, mediante comunicación escrita que haga a "El Proveedor".

"El Proveedor" deberá devolver, dentro de los 15 (quince) días naturales siguientes a la fecha en que reciba el comunicado, los originales, copias y reproducciones de la "información reservada o confidencial" que le haya sido entregada por "Banobras".

"Las Partes" reconocen y convienen que la titularidad de la "información reservada o confidencial" será de exclusiva propiedad de "Banobras" (incluyendo en forma enunciativa, más no limitativa, derechos de autor, marcas o nombres comerciales de la información entregada por "Banobras"), obligándose "El Proveedor" a no ejercitar, sin la autorización de "Banobras", acción alguna concerniente al uso, propiedad o divulgación de la mencionada "información reservada o confidencial".

VIGÉSIMA SEGUNDA. - SUPERVISIÓN DEL CONTRATO:

En términos de lo dispuesto por los artículos 2, fracción III Bis y 84, párrafo octavo del RLAASSP, así como de conformidad con lo señalado en el numeral 18. "Administración, Vigilancia del Contrato y Supervisión de las especificaciones y aceptación de los servicios" del "Anexo Técnico", "Banobras" supervisará las acciones que emprenda "El Proveedor", en la ejecución de los servicios de ciberseguridad, a través del DOCTOR HUMBERTO DAVID ROSALES HERRERA , DIRECTOR DE SEGURIDAD DE LA

INFORMACIÓN , con el apoyo del INGENIERO OMAR MANUEL MATA RUBIO, GERENTE DE SEGURIDAD DE LA INFORMACIÓN 2, o quién (es) en su caso ocupe (n) dicho (s) cargo (s), o quien (es) asuma (n) las atribuciones del (de los) puesto (s), será (n) el (los) servidor (es) público (s) encargado (s) de administrar, supervisar, vigilar y verificar el estricto cumplimiento del presente contrato, por lo que en su caso, deberá (n) girar las instrucciones que considere (n) oportunas, con el apoyo del (de los) servidor (es) público (s) que sea (n) designado (s) para tal efecto, obligándose "El Proveedor" a atender todas las observaciones que se le hicieran por escrito.

VIGÉSIMA TERCERA. - DEDUCTIVAS:

Con fundamento en lo dispuesto por los artículos 53 Bis de la LAASSP y 97 del RLAASSP, así como en términos de lo señalado en la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES, "Banobras" aplicará a "El Proveedor" las deductivas correspondientes, conforme a lo establecido en el numeral 16. "Penas Convencionales y Deductivas" del "Anexo Técnico", en los porcentajes e importes que correspondan.

La suma de dichas deductivas, no podrá exceder del 10.0% (diez por ciento) del monto máximo señalado en la cláusula **SEGUNDA** del presente contrato.

"Banobras" hará efectivas las deductivas que se indican en la presente cláusula, a través de la nota de crédito que emita el "El Proveedor", es decir, sobre el CFDI que corresponda.

"Banobras" tendrá la facultad de verificar que los servicios de ciberseguridad, se están brindando de conformidad con los términos, condiciones y especificaciones de los mismos.

Las deductivas señaladas en la presente cláusula se aplicarán sin incluir el I.V.A.

VIGÉSIMA CUARTA. - PENAS CONVENCIONALES:

Con fundamento en lo dispuesto por los artículos 45, fracción XIX, 53 de la LAASSP, 95 y 96 del RLAASSP, así como en términos de lo señalado en la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES, "Banobras" aplicará a "El Proveedor" las penas convencionales correspondientes, conforme a lo establecido en el numeral 16. "Penas Convencionales y Deductivas" del "Anexo Técnico", en los porcentajes e importes que correspondan.

Dichas penas convencionales serán calculadas por la Dirección de Seguridad de la Información, por conducto de la Gerencia de Seguridad de la Información 2, las cuales, no excederán del 10.0% (diez por ciento) del monto máximo señalado en la cláusula **SEGUNDA** del presente contrato.

Por otra parte, en términos de la cláusula **SEXTA** del presente instrumento jurídico, se aplicará una pena convencional del 3% (tres por ciento) del monto máximo del presente contrato, por cada día natural de atraso en la atención del MPSI que le sean aplicables con motivo de los servicios de ciberseguridad.

Dichas penas convencionales serán calculadas por la Dirección de Seguridad de la Información, por conducto de la Gerencia de Seguridad de la Información 2, las cuales, no excederán del 10% (diez por ciento) del monto máximo señalado en la cláusula **SEGUNDA** del presente contrato.

"Banobras" hará efectivas las penas convencionales que se indican en la presente cláusula, a través de la nota de crédito que emita el "El Proveedor", es decir, sobre el CFDI que corresponda.

"Banobras" tendrá la facultad de verificar que los servicios de ciberseguridad, se están brindando de conformidad con los términos, condiciones y especificaciones de los mismos.

Las penas convencionales señaladas en la presente cláusula se aplicarán sin incluir el I.V.A.

VIGÉSIMA QUINTA. - SANCIONES ADMINISTRATIVAS:

Cuando "El Proveedor" incumpla con sus obligaciones contractuales por causas imputables a éste, y como consecuencia, cause daños y/o perjuicios graves a "Banobras", o bien, proporcione información falsa, actúe con dolo o mala fe en la celebración delpresente contrato o durante la vigencia del mismo, por determinación de la SFP, se podrá hacer acreedor a las sanciones establecidas en los artículos 59, 60 y 61 de la LAASSP, así como del 109 al 115 del RLAASSP.

VIGÉSIMA SEXTA. - RESPONSABILIDAD LABORAL:

"Las Partes" aceptan y reconocen expresamente que no le son aplicables al presente contrato, las disposiciones de la Ley Federal de Trabajo, ni la Ley Federal de los Trabajadores al Servicio del Estado, reglamentaria del apartado "B" del artículo 123 de la CPEUM, motivo por el cual, "Banobras" no adquiere ni reconoce obligación alguna de carácter laboral, obrero patronal, civil, fiscal y/o penal, a favor de "El Proveedor" o de su personal, siendo éste el único y absoluto responsable de las obligaciones patronales del personal que, en su caso, utilice en el cumplimiento de las obligaciones adquiridas mediante el presente instrumento jurídico, liberando expresamente a "Banobras", de cualquier responsabilidad obrero patronal, civil, fiscal y/o penal, siendo así que "Banobras", no tendrá relación alguna de carácter laboral con dicho personal y consecuentemente, queda obligado "El Proveedor" a responder por todas las reclamaciones que sus trabajadores presenten en su contra o en contra de "Banobras", con relación a los ordenamientos en materia de trabajo, higiene y seguridad social. Si "Banobras" llegará a erogar de su peculio cualquier cantidad por los citados conceptos, "El Proveedor" se obliga a reembolsar de inmediato el importe correspondiente.

El personal que se ocupará con motivo de los servicios de ciberseguridad, estará bajo la responsabilidad directa de "El Proveedor" y como consecuencia, en ningún momento se considerará a "Banobras" como patrón sustituto o solidario, ni a "El Proveedor" como intermediario sino como patrón en términos de lo previsto por el artículo 10 de la Ley Federal del Trabajo.

Asimismo, "El Proveedor" brindará los servicios de ciberseguridad de conformidad con lo dispuesto en el Título Décimo, Capítulo II del Libro Cuarto del Código Civil para el Distrito Federal, en forma independiente, es decir, sin subordinación, ni dependencia con "Banobras".

VIGÉSIMA SÉPTIMA. - RESPONSABILIDAD:

"Las Partes" aceptan y reconocen que la idoneidad de "El Proveedor", la razonabilidad del monto de la contraprestación que "Banobras" cubrirá al mismo, así como la correcta ejecución de los servicios de ciberseguridad, quedan bajo la absoluta y exclusiva responsabilidad del DOCTOR HUMBERTO DAVID ROSALES HERRERA, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, así como del INGENIERO OMAR MANUEL MATA RUBIO, GERENTE DE SEGURIDAD DE LA INFORMACIÓN 2, o quién (es), en su caso, ocupe (n) dicho (s) cargo (s), o quién (es) asuma (n) las atribuciones del (de los) puesto (s).

VIGÉSIMA OCTAVA. - RESPONSABILIDAD LEGAL:

Queda expresamente pactado por "Las Partes" que "El Proveedor" es el único y absoluto responsable del cumplimiento de las obligaciones de carácter fiscal, administrativo, civil, laboral y/o penal que le sean imputables y que pudieran derivarse del cumplimiento del presente contrato.

En caso de que "Banobras" llegará a erogar de su peculio cualquier cantidad por los citados conceptos, "El Proveedor" se obliga a reembolsar de inmediato el importe erogado, a su vez que se obliga a sacar en paz y a salvo a "Banobras" de cualquier controversia que pudiera presentarse en caso de que durante la ejecución de los servicios de ciberseguridad, se infrinja cualquiera de las citadas disposiciones legales.

En este sentido, "El Proveedor" responderá por los daños y perjuicios que por inobservancia y/o negligencia de su parte llegue a causar a "Banobras" y/o a terceros, así como de cualquier otra responsabilidad en que hubiera incurrido, con excepción de los que hayan acontecido por caso fortuito o fuerza mayor previstos en la cláusula **VIGÉSIMA** del presente contrato, por lo que, de manera reiterada, se obliga a responder por dichos conceptos, quedando obligado a resarcir a "Banobras" de cualquier gasto o costo que éste erogue por dichos supuestos o pérdidas causadas.

VIGÉSIMA NOVENA. - RESCISIÓN:

En caso de incumplimiento por parte de "El Proveedor" a cualquiera de las obligaciones contraídas mediante el presente contrato y/o en caso de actualizar alguno de los supuestos señalados en la cláusula **TRIGÉSIMA** del mismo, "Banobras" podrá en cualquier momento, rescindir administrativamente el presente instrumento jurídico, bastando para ello la comunicación por escrito en ese sentido, sin necesidad de declaración judicial, de conformidad con lo establecido por los artículos 54 de la LAASSP, 98 y 99 del RLAASSP, así como lo señalado en la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES, conforme al procedimiento siguiente:

1. Se comunicará por escrito a "El Proveedor" el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes;

2. Transcurrido el término a que se refiere el inciso anterior, "Banobras" contará con un plazo de 15 (quince) días para resolver, considerando los argumentos y pruebas que hubiere hecho valer "El Proveedor" o de haber omitido respuesta, debiendo fundar y motivar su determinación de dar por rescindido o no el presente contrato y comunicar por escrito a "El Proveedor", así como a las autoridades competentes, la resolución dentro dicho plazo; y

3. Cuando se rescinda el presente contrato, se formulará y notificará el finiquito correspondiente dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión administrativa, a efecto de hacer constar el pago que deba efectuar "Banobras" por concepto de gastos no recuperables que hubieren sido aceptados a entera satisfacción de la Dirección de Seguridad de la Información, conforme a lo establecido en el presente contrato, hasta el momento de la rescisión administrativa.

De manera previa al inicio de la rescisión administrativa del presente contrato, en cualquier momento, "Las Partes" podrán recurrir al procedimiento de conciliación, establecidos en el Título Sexto, Capítulo Segundo de la LAASSP, por lo que "Banobras" bajo su responsabilidad, podrá suspender el trámite del procedimiento de rescisión administrativa que haya iniciado en su oportunidad.

Si previamente a la determinación de dar por rescindido administrativamente el presente contrato, se brindaran los servicios de ciberseguridad, el procedimiento iniciado quedará sin efecto, previa determinación, aceptación y verificación de "Banobras" de que continúa la necesidad de los mismos, aplicando, en su caso, las penas convencionales y/o deductivas que resulten procedentes.

"Banobras" podrá determinar no dar por rescindido el presente contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, deberá elaborar un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión administrativa del presente instrumento jurídico le resultan más inconvenientes a "Banobras".

Al determinar no rescindir administrativamente el presente contrato, "Banobras" establecerá con "El Proveedor" otro plazo que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión administrativa. El convenio modificatorio que al efecto se celebré deberá atender a las condiciones previstas por los 2 (dos) últimos párrafos del artículo 52 de la LAASSP.

En el caso de que "El Proveedor" se allane a la rescisión o durante su procedimiento, este no podrá suspender la ejecución del presente contrato y por ende los servicios de ciberseguridad, hasta que "Banobras" tenga otro prestador de servicios, obligándose a las medidas de transición que procedan.

Con fundamento en lo dispuesto por el artículo 98, segundo párrafo del RLAASSP, en el caso de que "El Proveedor" decida rescindir el presente contrato, será necesario que acuda ante la autoridad judicial federal y obtenga la declaración correspondiente.

"El Proveedor" será responsable por los daños y perjuicios que le cause a "Banobras".

TRIGÉSIMA. - CAUSALES DE RESCISIÓN:

En cumplimiento a lo establecido por el artículo 45, fracción XVI de la LAASSP y conforme a lo señalado en la sección III.8. "Del seguimiento a los contratos y pedidos" de los POBALINES, en caso de que "El Proveedor" incumpla con las obligaciones pactadas en el presente contrato, "Banobras" podrá en cualquier momento, proceder a la rescisión administrativa del mismo, la cual, se encuentra prevista en la cláusula **VIGÉSIMA NOVENA** del presente instrumento jurídico, sin necesidad de la declaración judicial previa, de conformidad con lo establecido en los artículos 54 de la LAASSP, 98 y 99 del RLAASSP, por una o varias de las siguientes causas imputables a "El Proveedor":

1. Contravenir los términos y condiciones del presente contrato, las disposiciones de la LAASSP, el RLAASSP, así como los demás ordenamientos legales vigentes que resulten aplicables.

2. Brindar los servicios de ciberseguridad con especificaciones diferentes a lo estipulado en el presente contrato, la convocatoria a "La Licitación", el ACTA DE JUNTA DE ACLARACIONES de fecha 31 de octubre de 2022, así como el "Anexo Técnico".

3. Incrementar los precios unitarios del presente contrato, sin la justificación de que dicho incremento fue por una circunstancia económica de tipo general, como resultado de situaciones supervenientes ajenas a la responsabilidad de "Las Partes", que provoquen directamente un aumento en los precios unitarios de los servicios de ciberseguridad.

4. Cuando el importe que se haya deducido por concepto de penas convencionales y/o deductivas, sea igual o superior al 10% (diez por ciento) del monto máximo señalado en la cláusula **SEGUNDA** del presente contrato, es decir, que exceda el importe de la garantía de cumplimiento señalada en la cláusula **SÉPTIMA** del mismo.

5. No reintegrar las cantidades pagadas en exceso y/o indebidos, con los intereses correspondientes derivados del presente contrato, y en su caso, de los convenios modificatorios que se celebren, conforme a lo señalado en la cláusula **TERCERA** del presente instrumento jurídico.

6. No presentar la garantía de cumplimiento señalada en la cláusula **SÉPTIMA** del presente contrato o presentarla de manera apócrifa.

7. Ceder los derechos y obligaciones contraídos mediante el presente instrumento jurídico, en forma total o parcial en favor de otra persona física o moral, así como los derechos de cobro, sin el previo consentimiento de "Banobras", conforme a lo señalado en la cláusula **DÉCIMA NOVENA** del presente instrumento jurídico.

8. No guardar confidencialidad de la información marcada como "información reservada o confidencial", en términos de la cláusula **VIGÉSIMA PRIMERA** del presente instrumento jurídico.

9. Si "Banobras" o cualquier otra autoridad detecta que proporcionó información o documentación apócrifa, alterada o falsa en "La Licitación", para la elaboración del presente contrato y/o durante la ejecución de los servicios de ciberseguridad.

10. Si "Banobras" o cualquier otra autoridad comprueba la falsedad de alguna manifestación contenida en el apartado de declaraciones del presente contrato.

11. Cuando la autoridad competente lo declare en concurso mercantil o sujeto a alguna otra figura análoga, o bien se encuentre en cualquier otra situación que afecte su patrimonio, en forma tal que le impida cumplir con sus obligaciones contraídas en virtud del presente contrato.

12. En general, cualquier incumplimiento de las obligaciones pactadas en el presente instrumento jurídico.

TRIGÉSIMA PRIMERA. - RESPONSABLES POR "LAS PARTES":

"Las Partes" designan como responsables para dar el debido y oportuno cumplimiento a las obligaciones contraídas mediante el presente contrato, así como para vigilar dicho cumplimiento y emitir, en su caso, las conformidades respectivas para que se cubran los pagos que resulten procedentes, a las siguientes personas:

-"Banobras": DOCTOR HUMBERTO DAVID ROSALES HERRERA, DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN e INGENIERO OMAR MANUEL MATA RUBIO, GERENTE DE SEGURIDAD DE LA INFORMACIÓN 2, ambos con domicilio señalado en la Avenida Javier Barros Sierra N° 515, Piso 9, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México.

-"El Proveedor": CIUDADANA VALERIA GIORDANO TURRUBIARTE, en su carácter de representante legal, con domicilio señalado en la CALLE SENECA 134 PISO 3, COLONIA POLANCO V SECCIÓN, MIGUEL HIDALGO, CIUDAD DE MÉXICO, C.P. 11560.

TRIGÉSIMA SEGUNDA. - CAMBIO DE DOMICILIO:

"Las Partes" se obligan en caso de cambiar sus domicilios señalados en la cláusula **TRIGÉSIMA PRIMERA** y en el capítulo de declaraciones del presente contrato, a notificar por escrito a la otra parte, dentro de los 3 (tres) días hábiles siguientes al día quetenga lugar dicho cambio.

TRIGÉSIMA TERCERA. - PROTECCIÓN DE DATOS PERSONALES:

"Las Partes" se comprometen a poner a disposición de los titulares el aviso de privacidad previo al tratamiento de datos y a garantizar la protección de los datos personales de conformidad con las finalidades establecidas en los respectivos avisos deprivacidad, en términos de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En caso de que se modifiquen las finalidades para el tratamiento de los datos personales, "Las Partes" deberán actualizar los avisos de privacidad correspondientes e informar a los titulares de los datos.

TRIGÉSIMA CUARTA. - DENOMINACIÓN DE LAS CLÁUSULAS:

"Las Partes" están de acuerdo en que, las denominaciones utilizadas en las cláusulas del presente contrato, son únicamente para efectos de referencia, por lo que no limitan de manera alguna el contenido y alcance de las mismas, debiendo en todos los casos, estar al contenido pactado por "Las Partes" en dichas cláusulas.

TRIGÉSIMA QUINTA. - NORMATIVA APLICABLE:

"Las Partes" aceptan y reconocen que, para todo lo que no se encuentre expresamente previsto en el presente contrato, se regirá por las disposiciones relativas contenidas en la LAASSP, el RLAASSP y supletoriamente serán aplicables en lo conducente, las disposiciones de la Ley Federal de Procedimiento Administrativo, el Código Civil Federal, las del Código Federal de Procedimientos Civiles, así como por las demás disposiciones legales vigentes que resulten aplicables.

TRIGÉSIMA SEXTA. - JURISDICCIÓN:

"Las Partes" aceptan y reconocen que, en caso de controversia sobre la interpretación y debido cumplimiento del presente contrato, se someten a la jurisdicción y competencia de los Tribunales Federales con residencia en la Ciudad de México, renunciando expresamente al fuero que les pudiera corresponder en razón de su domicilio presente, futuro o por cualquier otra causa.

Por todo lo anteriormente expuesto, habiendo leído "Las Partes", debidamente enteradas, conscientes de su contenido, alcance legal y, toda vez que no existe dolo, violencia, lesión, mala fe, ni cualquier otro vicio del consentimiento, lo ratifican y firman electrónicamente en las fechas especificadas en cada firma electrónica.

BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, SOCIEDAD NACIONAL DE CRÉDITO, INSTITUCIÓN DE BANCA DE DESARROLLO
"BANOBRAS"

NOMBRE	CARGO	R.F.C
MARYTELL CASTELLANOS RUEDA	DIRECTORA DE RECURSOS MATERIALES	[redacted]
HUMBERTO DAVID ROSALES HERRERA	DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN	[redacted]
KARLA DE TUYA GARCIA	GERENTE DE ADQUISICIONES	[redacted]

TIC DEFENSE, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE
"EL PROVEEDOR"

NOMBRE	R.F.C
TIC DEFENSE SA DE CV	TDE171130E30

Se elimina nombre de persona física con fundamento en lo a LFTAIP, artículo 116, párrafo primero, de la LGTAIP y 113, fracción I, c

Contrato: DAGA/099/2022

Cadena original:

c26530757d54442817b5cf24524a42212de45105178484ebf74692656e96580ae7a4504f8a52a10443991f7bcdc630573736bd55b87563b01d7c285ae22da4458fa5342caeb6e60dec9f3774500aa89d058686afc9e9a53941c2

Firmante: KARLA DE TUYA GARCIA
RFC: [redacted]
Número de Serie: [redacted]
Fecha de Firma: 02/12/2022 12:09
Certificado:

[redacted]

Firma:

hVlnyCQY69lWvdmuuUgqDTXnVuUz/gP7DTKDMA7TqfBRnxs1GdQRw0tnH+FbdDHl4M08amwlKQzO1b0hGdARtHJ+M6+wCIdAVbClK6hiomIJnx/bjVlxvrpsenDl4NgbrIl++qERmAjHukQXgvAu5fnCvo2S3rkg
Yh4PnPJH2+R6B0ijOVuULPm8ulJ/EFoh+VGzZ8Ek9n3WEWNV0Qd0olEBjtqSjPp8zYpHCp/hkyox5+p5bCQYTMKqsELe0/mVI87zakBp8OQAtaffA3DOf3e5FL8naqNJg5s3zo1g7evVcG04t0YgSJ2kIxMCK9qn
sNrsw6Z2I5xG+4WJ/0yLjA==

Firmante: HUMBERTO DAVID ROSALES HERRERA
RFC: [redacted]
Número de Serie: [redacted]
Fecha de Firma: 02/12/2022 12:13
Certificado:

[redacted]

Firma:

lmNlM5vF8iC5rrP4ntucVXvloJa9Y2ClG60/fwhCa/MsTO/FrZcALsRX5Db8/lRlBlPs+w7i4u40B7mPXkwm8h4UVuEu5sE6TJp4EbN6qrEJhlZHcNwlyK7ExAPTB3PefVSMHqsgvKeM5TwjvxaL4PGmrAyEpR22
1D0cygcvubqrYDgaSpcUR+3lr5+tBztUiZ5Diu6/ynILNJo8YYP8D4RY6QQaDbm7wKmgRR2j6tRuEuJIHi5KmCmXtwBQgCfNfPDHZD1K5MaFp/lMfkmPVkcsZ7ZaW8I0iqd/Lbt5DYvNoUgfhSu+OY4YOE2la54+
3T9T1UIMzXBotRODee01BQ==

Firmante: MARYTELL CASTELLANOS RUEDA
RFC: [redacted]
Número de Serie: 00001000000508161118
Fecha de Firma: 02/12/2022 12:14
Certificado:

[redacted]

Firma:

Se elimina RFC, números de serie y certificados de firma electrónica de persona física, con fundamento en los artículos 116, párrafo primero, de la LGTAIP y 113, fracción I, de la LFTAIP.

Contrato: DAGA/099/2022

E/FzthxFlWaSeBi0dwlXgSMTXV0qh6cKljtJqby9tQ6bZAlYtA2pLpnsXBefQtHk7GtQB0yAJ9a2piyauAGH4ALiHn0wy4vRQaOXRFJCIsxAfhB2b4FKk43psYx2XXqWt6MBJnxuyt8Ic27mFf06alwL+YavE416
r70lJKdkzEGe3Scy2QMdqYBbLTeEg5+mknoTaa4MQEt4FbH6jFhezD65auI43+/iKidGQGhkU7mbzaQh26ExlRF71q5mWc7D4CP+bdmhD72XDxGi+9K7SaqeJzc33Xhn1u01yW4dTW5GEKXLD0tn9nyedeZpv55f
XmTniIR+HT4ODnV2HXKNaQ==

Firmante: TIC DEFENSE SA DE CV
RFC: TDE171130E30
Certificado:

Número de Serie: [redacted]
Fecha de Firma: 02/12/2022 12:22

[redacted]

Firma:

XAZ/Asm/8N2PRLosXOYxAU0W+XLV5dtClouROAPXTHPthu4T9l/Qx2CC4HESgZwXeZuabIis8VkN65vMf9E+/uaqT5w7wcUA263TVNY7G3OPs9hE/Uh3USKiS2DMr8IUwXx208isP7C65alZOiKHsj/0cwACrdSA
mPPwaRrwQNt6Rnk1OHddxh1qTrRXLb3qP5o6PpQllQDOLTgh7Q0dS0k08cEE4qLL2J517jYMu2S/c7JhDHE83W0HtuUXgAGKKPuYqPJDY91U7E+6vjd2Dnr6OEzysChtB4GbAEUkzzkehZtMRMBKLZm+nzeJgi0n
9OW7qlO+LlpoSoGeaC6C4A==

Se elimina número de serie y certificado de firma electrónica de persona moral, con fundamento en los artículos 116, cuarto párrafo, de la LGTAIP y 113, fracción III, de la LFTAIP.

ANEXO A

001458

BANOBRAS

BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C

ACTDTIC-FI03. ANEXO TÉCNICO

Servicios de Ciberseguridad

ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal. Art,20 y 23

001457

Tabla de Contenido

001455

1. Glosario

Término	Descripción
Aceptación	Acuerdo formal que establece que un servicio de TI, proceso, plan o cualquier otro entregable está completo, es preciso, confiable y cumple con los requerimientos especificados.
Banco	Banco Nacional de Obras y Servicios Públicos S.N.C.
BANOBRAS	Banco Nacional de Obras y Servicios Públicos S.N.C.
BANXICO	Banco de México
BD	Base de Datos.
CNBV	Comisión Nacional Bancaria y de Valores.
Documento	Información y el medio (físico y/o electrónico) en el que está contenida.
Entregable	El producto y/o servicio adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integridad, funcionalidad y capacidades. Documento y/o componente tecnológico a entregar por parte del prestador del servicio.
Infraestructura tecnológica	A la infraestructura de computo, telecomunicaciones, y sistemas.
Licitante Ganador	Institución o empresa que proveerá los servicios para satisfacer los requerimientos del Área Requirente, establecidos en el presente documento.
Riesgo tecnológico	El riesgo tecnológico se define como la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso del hardware, software, sistemas, redes y cualquier otro canal de transmisión de información en la prestación de servicios bancarios a los clientes de la Institución.
SHCP	Secretaría de Hacienda y Crédito Público.
Sistema, Software o Aplicación	Grupo de elementos interrelacionados o que interactúan y que se conforman por un conjunto de componentes o programas construidos con herramientas que habilitan una funcionalidad o digitalizan un proceso, de acuerdo con requerimientos previamente definidos.
SPEI	Sistema de pagos electrónicos interbancarios
BDT	Base de Datos de Transferencias
INDEVAL	Institución para el Depósito de Valores, S.A. de C.V.
Revisión	Determinación de la conveniencia, adecuación o eficacia de un objeto para lograr objetivos
Validación	Confirmación, mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos para una utilización o aplicación específica prevista.
Vulnerabilidad	Debilidad de un control, que puede ser aprovechada por una amenaza y puede permitir la explotación en perjuicio de un sistema.
SIEM	Security Information and Event Management
DLP	Data Loss Prevention

CISSP	Certified Information Systems Security Profesional
NIST	National Institute of Standards and Technology
OWASP	Open web Application Security Project
OSSTM	Open Source Security Testing Methodology Manual
SOC	Centro de Operaciones de Seguridad
IDS	Intrusion Detection Systems
CSIRT	Computer Security Incident Response Team
IPS	Intrusion Prevention Systems
VPN	Virtual Private Network
DNS	Domain Name System
WAF	Web Application Firewall
ETDR	Email Threat Detection and Response
APT	Advanced Persistent Threat
CVE	Common Vulnerabilities and Exposures
Área Requirente	Área que solicite o requiera formalmente la prestación de servicios, o bien aquella que los utilizará, en este caso la DSI
Área Técnica	Área que elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones, las preguntas que sobre estos aspectos realicen los licitantes, en este caso la DTIC
Hardware	Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático
Herramienta	Programas, aplicaciones o instrucciones usadas para efectuar tareas de modo más sencillo.
DTIC	Dirección de Tecnologías de Información y Comunicaciones
DSI	Dirección de Seguridad de la Información
Base de Datos	Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
Servidor	Aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
Posición	Situarse en algún lugar disponiéndose para hacer alguna actividad

2. OBJETIVO

El presente documento tiene como propósito describir a detalle los servicios de ciberseguridad requeridos por el Banco Nacional de Obras y Servicios Públicos, S.N.C., en adelante BANOBRAS, a contratar, así como el alcance detallado de los mismos, sus entregables y términos en los cuales deberán ser entregados.

Estos requerimientos están basados con lo establecido en el Plan Director de Seguridad y la estrategia de seguridad de la información en sus 5 funciones: identificar, proteger, detectar, responder y recuperar mediante los servicios de Ciberseguridad.

001453

3. ALCANCE

Con la finalidad de dar cumplimiento a las iniciativas y proyectos establecidos en el Plan Director de Seguridad, conforme a lo establecido en las Disposiciones de carácter general aplicables a las instituciones de crédito, BANXICO o cualquier otra regulación o normatividad que aplique, se requiere que el alcance del presente anexo conste de los siguientes servicios:

Los servicios deberán ser entregados con base en la descripción de los mismos mencionados en la siguiente sección. Estos deberán ser realizados durante la vigencia del contrato y con estricto apego a las políticas y procedimientos de seguridad de BANOBRAS, las cuales serán dadas a conocer al licitante ganador en la oficina de la DSI, ubicada en Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219, en piso 9, durante los 5 primeros días hábiles después de la notificación del fallo.

El alcance de la Infraestructura Tecnológica consta de:

Alcance	Número aproximado
Infraestructura de telecomunicaciones.	520
Servidores de Aplicaciones	60
Servidores de Base de Datos	350
Activos	406
Aplicaciones o sistemas	60
Muestreo de Equipos de cómputo de usuarios.	1000

4. REQUERIMIENTOS

De los licitantes interesados en presentar los servicios de Ciberseguridad

Los licitantes interesados en presentar los servicios, deberán realizar un ofrecimiento de los mismos por partida completa sin excepción, en el que incluyan todos los requerimientos descritos en este documento.

Los servicios deberán ser cubiertos con personal capacitado y certificado provisto por EL LICITANTE GANADOR a fin de garantizar las capacidades requeridas para la atención de los servicios antes mencionados.

Previo al inicio de cualquiera de los servicios descritos en este documento, EL LICITANTE GANADOR deberá formalizar en conjunto con BANOBRAS el plan de trabajo, alcance específico y por elemento, el calendario y horarios para la ejecución de cada evento, conforme a lo establecido en el numeral 11 "Niveles de Servicio".

EL LICITANTE GANADOR deberá ejecutar los servicios en ambientes controlados y en horarios previamente acordados con la DSI responsable del servicio, conforme a los tiempos establecidos en el numeral 11 "Niveles de Servicio".

EL LICITANTE GANADOR deberá firmar un acuerdo de confidencialidad al día siguiente de la notificación del fallo, el cual debe ser elaborado por BANOBRAS, suficiente para garantizar la integridad, confidencialidad y disponibilidad de la información a la que tendrá acceso.

El personal del LICITANTE GANADOR deberá firmar un acuerdo de confidencialidad personal al día siguiente de la notificación del fallo, el cual debe ser elaborado por BANOBRAS, suficiente para garantizar la integridad, confidencialidad y disponibilidad de la información a la que tendrá acceso.

En caso que en el desarrollo de los servicios, EL LICITANTE GANADOR se encuentre en una situación en la que pueda poner en riesgo algún sistema, base de datos, infraestructura y/o información, deberá reportarlo inmediatamente a la DSI.

Cualquier herramienta, hardware, software o sistema provista por EL LICITANTE GANADOR deberá incluir el licenciamiento, mantenimiento y soporte por la totalidad de la vigencia del contrato, sin costo para BANOBRAS

EL LICITANTE deberá garantizar que en caso de ser adjudicado todas las herramientas, hardware, equipo de cómputo y demás dispositivos provistos por éste, que interactúen directa o indirectamente con la red de BANOBRAS se encuentran libres de virus y cualquier otra amenaza que pueda afectar los principios de seguridad de la información.
Esto por medio de la firma de una cárta compromiso que deberá de integrar a su propuesta técnica en la que se detallará el equipo y herramientas a utilizar en cada interacción con la red de BANOBRAS.

EL LICITANTE GANADOR deberá incluir los recursos informáticos y herramientas asociadas, hardware y/o software que sea requerido para brindar los servicios solicitados. En caso de requerirse la instalación de algún recurso informático, herramienta, hardware y/o software dentro de la Infraestructura Tecnológica de la Institución, se deberá solicitar al Área Requirente en conjunto con la DTIC.

EL LICITANTE GANADOR deberá considerar una etapa de transición de servicio de al menos 1 mes a partir de la finalización del contrato, sin costo adicional, con el fin de permitir a BANOBRAS si fuese el caso, poder iniciar operaciones con un nuevo PROVEEDOR.

Se requiere que el LICITANTE cuente con las certificaciones en las siguientes normas (no será motivo de desechamiento): ISO/IEC 27001:2014, ISO 9001:2015, ISO 22301:2020, ISO/IEC 20000-1 :2020 e ISO 37001 en los siguientes procesos que están directamente relacionados con el objeto del presente Anexo Técnico:
Análisis de Vulnerabilidades y Pruebas de Penetración para Aplicaciones e Infraestructura Tecnológica
Análisis y Monitoreo Externo de la información para el Alertamiento de Riesgos y Ciberamenazas
Centro de Operaciones de Redes y de Seguridad "NOC y SOC" con Detección, Análisis y Respuesta Gestionada "MDR" para la atención con el Equipo de Respuesta ante Emergencias Informáticas
Forense Digital
Gobierno de Seguridad y Cumplimiento Normativo
Inteligencia de Análisis de Información Digital

Es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de Respuesta ante Incidentes de Seguridad Computacional acreditado como CERT ante FIRST (global Forum of Incident Response and Security Teams). (el incumplimiento del punto es motivo de desechamiento)

EL LICITANTE GANADOR deberá considerar y atender cualquier requerimiento o alcance de pruebas durante la vigencia del contrato, así como los plazos para realizarlas conforme a los cumplimientos normativos y/o solicitudes por parte de BANXICO, CNBV, u otra Comisión Regulatoria, sin que genere costo alguno para BANOBRAS.

EL LICITANTE GANADOR deberá garantizar que el personal certificado que brindará los servicios del presente Requerimiento Técnico, sea personal interno contratado dentro de la organización.

SI - Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad

El LICITANTE GANADOR deberá realizar pruebas de análisis de vulnerabilidades a toda la infraestructura tecnológica, en apego a lo indicado en las Disposiciones de carácter general aplicables a las instituciones de Crédito, BANXICO o cualquier otra regulación o normatividad de manera enunciativa más no limitativa.

El LICITANTE GANADOR deberán realizar pruebas de análisis de vulnerabilidades a los componentes de la infraestructura tecnológica y sistemas de BANOBRAS realizando la revisión trimestral de la totalidad de los componentes que almacenen, procesen o transmitan información que sean determinados por BANOBRAS antes de ejecutar el servicio en el mes requerido.

En ambas pruebas de análisis de vulnerabilidades El LICITANTE GANADOR deberá considerar la infraestructura tecnológica incluyendo los sitios primarios y alternos, el DRP, ambientes de desarrollo, pruebas, pre-producción y producción, de manera enunciativa más no limitativa que sean determinados por BANOBRAS antes de ejecutar el servicio.

El LICITANTE GANADOR deberá realizar pruebas de penetración de manera trimestral con personal que cuente con capacidad **técnica comprobable mediante certificaciones especializadas de la industria en la materia**, para la realización de pruebas de penetración en la infraestructura tecnológica y los diferentes sistemas de la Institución con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los clientes y de la propia Institución.

EL LICITANTE GANADOR proporcionará la metodología conforme a lo establecido en el numeral 11 "Niveles de Servicio", la cual deberá estar basada en mejores prácticas y marcos de referencia de seguridad de la información como MITRE ATT&CK, OWASP, OSSTMM, ISSAFF, NIST 800-115, ISO 27001, ISO 31000, misma que deberá ser validada y aprobada por la Dirección de Seguridad de la Información.

EL LICITANTE GANADOR deberá realizar las pruebas en estricto apego a los procesos y políticas de seguridad de BANOBRAS, así como sus metodologías y a la normatividad aplicables, por lo que los reportes deberán contemplar los requerimientos de la normatividad vigente emitida por BANXICO, CNBV o cualquier otra normatividad instruida por escrito por la DSI.

EL LICITANTE GANADOR deberá validar previo a su ejecución el protocolo de pruebas con el Director de Seguridad de la Información, quedando estrictamente prohibido la realización de transacciones, modificación o alteración de datos o pruebas que pudieran afectar la disponibilidad de los sistemas, así como la integridad, disponibilidad y confidencialidad de la información.

Análisis de vulnerabilidades

Las pruebas deberán ser realizadas con un enfoque de caja gris y caja blanca, es decir, se tendrá acceso a la red institucional de BANOBRAS y conectividad a los sistemas, así como usuarios válidos para la ejecución de pruebas dinámicas.

El alcance de las pruebas incluye:

- Infraestructura de telecomunicaciones.
- Servidores de Aplicaciones y base de datos
- Sistemas
- Muestreo de Equipos de cómputo de usuarios.

El detalle de la infraestructura, ambientes, bases de datos y sistemas se dará a conocer únicamente al licitante ganador, durante los 5 primeros días hábiles después de la notificación del fallo.

El servicio deberá ser realizado en las instalaciones de BANOBRAS, para lo que esté proporcionará el espacio físico, facilidades para el acceso a la red y alimentación eléctrica.

Para las pruebas de caja blanca, EL LICITANTE GANADOR deberá garantizar que el canal de comunicación cuente con todos los mecanismos de seguridad, siendo responsable EL LICITANTE GANADOR de cualquier incidente o afectación a BANOBRAS.

EL LICITANTE GANADOR

El servicio deberá permitir la detección oportuna de las vulnerabilidades tecnológicas, el análisis del impacto en caso de explotación y el desarrollo de estrategias de mitigación eficaces para su erradicación.

El servicio solicitado deberá contar de manera enunciativa más no limitativa con:

- Análisis de segregación de flujos
- Análisis de sistemas web y cliente servidor
- Análisis de bases de datos
- Determinación de vulnerabilidades por aplicación
- Análisis de vulnerabilidades de sistemas web, incluyendo pruebas de:
    - SQL Injection, Blind SQL Injection
    - XSS (cross site scripting), CRLF
    - Buffer overflow
    - Ejecución de comandos, LFI, RFI, CSRF
    - XML Injection
    - Pivoteo en sistemas vulnerables
    - Escalación de ataques de la DMZ a la red interna
    - Penetración a los sistemas vulnerables

Pruebas de detección de vulnerabilidades que pudieran desembocar en movimiento lateral, escalación de privilegios o robo de credenciales:

- Riesgo de ataques por Pass-the-hash
- Riesgo de ataques de movimiento lateral
- Riesgo de ataques de escalación de privilegios
- Riesgo de fuga de credenciales de memoria de los equipos

- Esquemas de autenticación en uso, incluyendo:
    - LAN MANAGER
    - NTLM
    - Kerberos

Las vulnerabilidades detectadas deberán ser clasificadas conforme a la metodología establecida por el LICITANTE GANADOR previamente validada por el Director de Seguridad de la Información. La metodología de clasificación deberá incluir la criticidad, probabilidad de ocurrencia e impacto, considerando mapas de calor.

Al finalizar las pruebas de análisis de vulnerabilidad se deberá incluir dentro de los reportes correspondientes los indicadores de las vulnerabilidades detectadas, los cuales deberán incluir de forma enunciativa más no limitativa lo siguiente.

- Información de identificación de elemento TIC vulnerable (IP, host name, mac, identificador, tipo, so, localización, estatus)
- Vulnerabilidades por Impacto.
- Comparación de numero de vulnerabilidades entre eventos.
- Porcentaje de vulnerabilidades mitigadas entre eventos.
- Porcentaje de vulnerabilidades de acuerdo a su causa.

Pruebas de Penetración a la infraestructura tecnológica trimestralmente

Se deberá realizar una evaluación de los niveles de seguridad en la infraestructura tecnológica localizada en el centro de datos y en el perímetro con la finalidad de obtener el nivel de riesgos al que se encuentra.

Se deberán realizar pruebas de Hackeo Ético a la infraestructura tecnológica de BANOBRAS; se considerarán los siguientes servicios:

1. Diagnóstico de caja negra/gris a la infraestructura tecnológica de BANOBRAS desde:
    a. El perímetro de Internet, donde a través de un punto público de inicio se llevará a cabo un descubrimiento de los elementos que conforman la infraestructura expuesta y diagnóstico de vulnerabilidades sobre los mismos considerando como punto de partida el que indique el Director de Seguridad de la Información.
    b. En el interior de BANOBRAS, donde a través de un acceso de red y con cierta información de los dispositivos a evaluar se realizará el diagnóstico de manera enunciativa más no limitativa a: la infraestructura, los servidores, sistemas, bases de datos, usuarios internos, equipos de cómputo y servicios de directorio activo.

Las revisiones del perímetro y del centro de datos comprenderá de manera enunciativa más no limitativa:

a. Los distintos sitios web de BANOBRAS (www.BANOBRAS.gob.mx)
b. Sistemas de BANOBRAS
c. Equipos de Seguridad
d. Servidores y servicios como DNS, Correo, etc.
e. Muestra de equipos de usuario

f. Directorio Activo institucional

En el reporte se deberá incluir de manera enunciativa más no limitativa:

a. Ruta crítica de penetración

Seguridad de la infraestructura de los sistemas

EL LICITANTE GANADOR comprobará la seguridad de la infraestructura de los sistemas que determine BANOBRAS al ejecutar el servicio en busca de problemáticas que pudieran transformarse en fraudes, pérdida del servicio o afectación a la imagen de BANOBRAS, sin entrar en el análisis de los sistemas mismos.

Se deberá realizar a los servidores de BANOBRAS desde internet donde a través de un punto público; EL LICITANTE GANADOR llevará a cabo las pruebas de seguridad y en su caso explotación de vulnerabilidades sobre dicha infraestructura.

1. El diagnóstico de vulnerabilidades y las pruebas de seguridad serán realizadas a partir de la metodología "Open Source Security Testing Methodology Manual" (OSSTMM) del organismo internacional "Institute for Security and Open Methodologies" (ISECOM) en versión 3. Las siguientes actividades son enunciativas más no limitativas:

    a. Escaneo de Puertos
    b. Identificación de Servicios
    c. Identificación de Sistemas
    d. Identificación e investigación de vulnerabilidades
    e. Pruebas y/o Explotación de vulnerabilidades.

2. La DSI en conjunto con la DTIC definiran el inventario de activos.
3. EL LICITANTE GANADOR se compromete a presentar el día hábil siguiente de la notificación del fallo un documento donde se describa la forma o reglas mediante las cuales se llevará a cabo el diagnóstico de vulnerabilidades y pruebas de seguridad, es decir, describir de forma detallada las actividades a realizar, los límites, riesgo, alcances, herramientas a utilizar y resultados esperados, el cual deberá ser aprobado por las áreas correspondientes de BANOBRAS.
4. EL LICITANTE GANADOR deberá realizar un sondeo de la red conforme a lo establecido en el componente S1 "Reporte de Vulnerabilidades", del numeral 11 "Niveles de Servicio", con la finalidad de identificar los servicios de los sistemas, así como generar la búsqueda de vulnerabilidades en la infraestructura tecnológica de BANOBRAS: aplicación de parches, debilidad de contraseñas, permisos de archivos, barridos de puertos, SNMP, RPC, correo electrónico, FTP y servicios habilitados, seguridad del directorio activo, etc.
5. Una vez concluida la búsqueda de vulnerabilidades, EL LICITANTE GANADOR, deberá realizar la documentación de cada una de las vulnerabilidades identificadas; y no importando si las vulnerabilidades fueron o no explotadas, se generarán las recomendaciones que apliquen, conforme a lo establecido en el componente S1, del numeral 11 "Niveles de Servicio".
6. Para cada vulnerabilidad importante identificada, se establecerá el nivel de riesgo que tendría si la vulnerabilidad en cuestión fuera explotada, identificando el impacto al negocio en función del cumplimiento normativo y asignando una calificación de riesgo.

Por tal motivo se considerarán las siguientes actividades de manera enunciativa más no limitativa:

a. Escaneo de Puertos
b. Identificación de Servicios
c. Identificación de Sistemas
d. Identificación e investigación de vulnerabilidades
e. Pruebas y/o Explotación de vulnerabilidades

7. EL LICITANTE GANADOR deberá elaborar un reporte de resultados conforme lo establecido en el componete S1, del numeral 11 "Niveles de Servicio", el cual contendrá al menos lo siguiente: Introducción, Objetivo, Alcance, Resumen de Actividades realizadas, Ambiente evaluado, Hallazgos obtenidos por criticidad (indicando en que equipos se detectó ese hallazgo), resumen por tipo de hallazgos basándose en la escala de la OSSTMM.

Verificación de suficiencia de controles de seguridad

Como parte de las pruebas de vulnerabilidades EL LICITANTE GANADOR deberá proponer los controles eficientes de seguridad aplicables a la Infraestructura Tecnológica.

Verificar y emitir reportes que puedan materializar un riesgo de seguridad, así como la generación de indicadores que permitan el seguimiento y comparación, se enlistas las siguientes actividades de manera enunciativa más no limitativa:

a. Mecanismos de Autenticación de los Usuarios de la Infraestructura Tecnológica.
b. Configuración y controles de acceso a la Infraestructura Tecnológica.
c. Actualizaciones requeridas para los sistemas operativos y software en general, previo a su implementación y una vez implementados.

S2 – Realización periódica de análisis seguridad de sistemas

EL LICITANTE GANADOR del servicio deberá evaluar el nivel de riesgo de los sistemas, en términos de seguridad de la información, emitiendo una opinión que permita identificar y eventualmente con base en esta, permitir a BANOBRAS eliminar la causa raíz del problema, reduciendo el riesgo asociado al proceso que soporta.

Las pruebas se realizarán de forma mensual y se deberá entregar conforme a los reportes establecidos en el componente S2, del numeral "7 Entregables y 11 Niveles de Servicio", durante la vigencia del contrato considerando los nuevos sistemas y/o actualizaciones a los sistemas actuales.

Pruebas estáticas de seguridad del Código

Se deberá realizar un set completo de pruebas para la identificación de vulnerabilidades y pruebas estáticas a los sistemas o cualquier sistema que sea solicitado por la Dirección de Seguridad de la Información de BANOBRAS, detallando su criticidad y el impacto.

Las pruebas de seguridad del código integrarán a **personal certificado** en la revisión de sistemas. El enfoque del servicio es mensual y se deberá entregar conforme a los reportes establecidos en el componente S2, del numeral "7 Entregables y 11 Niveles de Servicio", podrá incluir la revisión de cualquier aplicación y/o módulo nuevo y/o ya existente, asegurando que toda aplicación liberada cumpla con los requerimientos y especificaciones de seguridad.

EL LICITANTE GANADOR del servicio deberá asignar al **personal certificado** para el análisis y deberá analizar el código generado por el grupo de desarrollo por medio de pruebas manuales y pruebas automatizadas (escaneos especializados de seguridad), analizando posibles errores, vulnerabilidades o malas configuraciones que pudieran derivar en un caso de abuso mediante la explotación manual del mismo.

Para cada vulnerabilidad detectada, EL LICITANTE GANADOR del servicio deberá presentar en el reporte de vulnerabilidades e indicadores de vulnerabilidades, establecido en el numeral 11 "Niveles de Servicio", las medidas de mitigación adecuadas a implantar por los equipos de desarrollo, como por ejemplo la elaboración de filtros de limpieza y validación de datos a nivel de expresiones regulares, etc.

Al inicio de la prestación del servicio, BANOBRAS a través de la DSI, deberá priorizar el orden en el que se revisarán los sistemas proporcionando en caso de existir, información al equipo de seguridad de sistemas, tales como:

- Lista de sistemas,
- Ambientes actuales
- Transacciones y uso de sistemas
- Arquitectura tecnológica,
- Código fuente,
- Manuales técnicos de sistemas (Librerías, diccionarios de datos, diagramas de despliegue),
- Documentación de sistemas (documentación de análisis y diseño de los sistemas),
- Documentación de bases de datos, así como la definición de los "Criterios de aceptación de los sistemas".

En caso de no contar con la información antes requerida, BANOBRAS a través de la DTIC deberá proporcionar como mínimo, el código fuente y librerías relacionadas, así como la asignación de personal para asistir a dudas técnicas sobre el código fuente o el aplicativo en cuestión.

EL LICITANTE GANADOR del servicio deberá realizar las pruebas de los sistemas a fin de validar y descartar falsos positivos y determinar su potencial explotación.

Algunos de los tipos de hallazgos que podrían ser detectados y reportados para su corrección de manera enunciativa más no limitativa son:

- Vulnerabilidades del tipo Cross Site Scripting (XSS)
- Vulnerabilidades del tipo SQL Injection, Blind SQL Injection

- Vulnerabilidades del tipo Buffer Overflow
- Vulnerabilidades del tipo Command Injection, etc.
- Manejo pobre de errores y excepciones (poor error handling)
- Uso de bibliotecas vulnerables (libraries).
- Detección de código muerto (Dead code).
- Condiciones de carrera (race conditions), etc.

EL LICITANTE deberá considerar que en caso de resultar ganador deberá realizar el análisis de código fuente (pruebas estáticas) de las aplicaciones y/o módulos que determine BANOBRAS por mes durante la vigencia del contrato.

Pruebas Dinámicas de sistemas

Se evaluará el nivel de riesgo de los sistemas, permitiendo identificar el riesgo asociado al proceso de negocio. Esta revisión proporcionará un reporte detallado de los hallazgos incluyendo medidas de recomendación de mitigación y de solución a los problemas detectados en los diferentes tipos de pruebas, conforme a lo establecido en el componente S2, del numeral 11 "Niveles de Servicio", de manera enunciativa más no limitativa como son:

- Vulnerabilidades inherentes a la arquitectura de la aplicación.
- Riesgos introducidos durante las fases de desarrollo, integración, despliegue y procesos operacionales.
- Vulnerabilidades técnicas inherentes a la plataforma en las diversas capas, incluyendo los servicios de middleware y de bases de datos.
- El riesgo de la aplicación y la infraestructura a diversos ataques como Cross Site Scripting (XSS), SQL Injection, Buffer Overflow, Command Injection, etc.

Las pruebas dinámicas podrán realizarse usando una combinación de herramientas automatizadas y métodos manuales, ejecutando de forma enunciativa más no limitativa:

- Análisis de métodos de autenticación
- Pruebas de seguridad a configuraciones de la aplicación
- Análisis de seguridad de datos de entrada
- Verificación de parámetros
- Pruebas de seguridad conforme a metodología OWASP top 10

Apoyo para solventar vulnerabilidades

Las vulnerabilidades detectadas por el equipo de seguridad del LICITANTE GANADOR, serán documentadas y reportadas a la Dirección de Seguridad de la Información, conforme a los reportes establecidos en el componente S2, del numeral "7 Entregables y 11 Niveles de Servicio".

Se deben realizar los indicadores de seguridad incluyendo de forma enunciativa más no limitativa los siguientes:

- Vulnerabilidades por tipo

- Vulnerabilidades por criticidad

Las recomendaciones de solvencia o mitigación en caso de que no sea posible solventarlas, deberán ser realizadas de forma ejecutiva incluyendo el nivel de riesgo conforme a la metodología establecida incluyendo el mapa de calor de riesgos de seguridad en sistemas, mismo que se actualizará mes con mes. Así mismo se deberá elaborar el reporte técnico con dichas sugerencias, el cual se entregará en la DSI, conforme a lo establecido en el componente S2, del numeral 11 "Niveles de Servicio".

S3 - Reducción de la superficie de ataque del ecosistema de los sistemas.

Este servicio tiene como objetivo la implementación y gestión de una arquitectura de seguridad de Directorio Activo que reduzca el nivel de riesgo. Los trabajos tendrán un alcance Institucional y deberá incluir de manera enunciativa más no limitativa los siguientes objetivos:

Reingeniería y Gestión del riesgo de Ciberseguridad del directorio activo

- ✓ Implementación de una herramienta de Monitoreo y Validación de cambios del directorio activo (descrito en el punto 4.4.2
- ✓ Implementación de un Modelo de seguridad en la arquitectura de Directorio Activo de BANOBRAS.
- ✓ Configuración segura de Domain Controllers.
- ✓ Depuración de cuentas actuales del directorio activo con criterios de seguridad y de riesgo.
- ✓ Definición e implementación de Estrategias de aislamiento de sistemas obsoletos o migración a sistemas modernos.
- ✓ Gestión continua del riesgo, con reportes mensuales según la tabla de entregables.

Herramienta de Monitoreo y Validación de cambios del directorio activo

EL LICITANTE GANADOR deberá instalar una herramienta destinada a efectuar las labores de monitoreo, validación y comprobación de mejoras en la infraestructura del Directorio Activo de la Institución, conforme a lo establecido en el componente S3, del numeral 11 "Niveles de Servicio".

La herramienta deberá cumplir con al menos la siguiente funcionalidad:

- Seguimiento de cambio en las configuraciones de Directorio Activo, incluyendo usuarios, grupos, relaciones de confianza, ACLs, Privilegios, información de usuarios, etc.
- No disruptiva en su operación, a fin de no afectar la operación de la Institución.
- Utilizar un motor de persistencia embebido, transaccional, que almacene datos estructurados en grafos en lugar de en tablas con fines de eficiencia
- Permitir visualizaciones grafica amigable al usuario en un front-end ligero
- Permitir la visualización de las trayectorias más cortas de ataque al directorio Activo
- Permitir la visualización de las trayectorias a los activos valiosos de DA
- Permitir la visualización de los usuarios de kerberos con permisos de DCSync
- Permitir la visualización de las trayectorias más cortas de usuarios sujetos a ataques de Kerberoast
- Permitir la visualización de las trayectorias más cortas a Domain Admins desde usuarios sujetos a ataques de Kerberoast
- Permitir el monitoreo de atributos entre entidades de ACL Edges, incluyendo ACLs que pudieran significar un riesgo al ecosistema de DA de la Institución, tales como:
  - AllExtendedRights
  - AddMember
  - ForceChangePassword

- GenericAll
- GenericWrite

- Capacidad de visualización de relaciones especiales entre entidades que pudieran significar un riesgo al ecosistema de DA de la Institución, tales como:
  - CanRDP
  - ExecuteDCOM
  - AllowedToDelegate
  - AddAllowedToAct
  - AllowedToAct
- Capacidad de exportar datos a formatos de CSV, Excel, etc.
- Capacidad de poder crear queries a la medida, según los requerimientos de la Institución

S4 - Mejora y madurez de los sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365

EL LICITANTE GANADOR del servicio deberá habilitar los procesos de cacería de amenazas de ciberseguridad mediante la oportuna detección de amenazas en los sistemas.

Este servicio tiene como objetivo el proporcionar a BANOBRAS un servicio profesional de excelencia en servicios de ciberseguridad, a fin de cumplir con las prácticas de gestión de riesgo y protección de la información en los sistemas y procesos críticos, así como cumplir con los requerimientos regulatorios de CNBV y de Banxico, o de cualquier otra normatividad que aplique a BANOBRAS.

Personal en sitio en esquema 24x7x365

EL LICITANTE GANADOR de servicios debe incluir personal administrado en equipos de trabajo como equipo de SOC y personal certificado en ciberseguridad designados, cazadores de amenazas, personal certificado ciber forenses especializados, equipo de respuesta a incidentes compuesto por personal certificado en seguridad cibernética.

El LICITANTE GANADOR a través del personal certificado deberá estar listo para atender cada caso de incidentes de seguridad que se presente en BANOBRAS en sitio en un esquema 24x7x365, considerando tener al menos una posición permanente con personas certificadas, permitiendo realizar el monitoreo de la herramienta y la atención de cualquier evento o incidente de seguridad.

El Director de Seguridad de la Información proporcionará accesos y un área física donde asignará al personal externo y sus herramientas a fin de que se acondicione el área de trabajo para brindar el servicio en sitio.

Herramientas de Monitoreo y cacería de amenazas avanzadas de ciberseguridad

EL LICITANTE GANADOR deberá instalar un conjunto de herramientas on-site, cloud o hibrida conforme a lo establecido en el componente S4, del numeral 11 "Niveles de Servicio", destinadas a efectuar las labores de monitoreo y cacería de amenazas en la infraestructura tecnológica de la Institución. Podrán ser una combinación de herramientas basadas en Machine Learning o Redes Neuronales o Inteligencia

Artificial o Procedimientos manuales o Procedimientos automatizados o Sistemas de Análisis de Comportamiento, etc. en la medida que se integren a los servicios entregados.

A continuación se enlistan algunas características principales enunciativas más no limitativas, que se deberá considerar en la herramienta de monitoreo:

Anticipación de Amenazas

La herramienta deberá contar con al menos la siguiente funcionalidad:

- La herramienta debe apoyar la inteligencia de amenazas de terceros y/o externos para ayudar a la respuesta de incidentes trayendo el contexto organizacional y la información interna disponible en el SIEM proporcionado por EL LICITANTE GANADOR y otras fuentes de información de seguridad de BANOBRAS
- La herramienta debe soportar la integración de la inteligencia de amenazas legibles por máquina de diferentes fuentes abiertas y comerciales.
- La herramienta debe soportar la recopilación de noticias de amenazas de lectura humana de diferentes feeds.
- La herramienta debe aplicar la inteligencia de amenazas a los activos de la Institución, el tráfico de red, eventos de seguridad y a los usuarios para proporcionar un informe accionable sobre el probable impacto en cada entidad y recomendar medidas preventivas.
- Se deberán enviar informes preventivos alertando del surgimiento de nuevas amenazas o vulnerabilidades críticas en esquema de 24x7x365.

Cacería de Amenazas y Modelado de Adversario de acuerdo a la Matriz MITRE ATT&CK

- La herramienta debe tener modelos preconstruidos para detectar ataques específicos (ataques desconocidos de actores de amenazas desconocidas).
- La herramienta debe ser capaz de detectar diferentes etapas de la Cyber Kill Chain o de MITRE Attack Matrix (progresión de la cadena de ataque que el atacante debe completar a fin de lograr su objetivo).
- La herramienta debe soportar diferentes categorías de cacería incluyendo la caza de amenazas de la red, caza de amenazas en servidores.
- **La caza de amenazas de red** debe aprovechar las fuentes de red existentes para una mejor detección de ataques avanzados. Las fuentes de red pueden incluir DNS, IPS, VPN, firewall, Directorio Activo/Windows, logs de correo electrónico según lo disponga la Institución.
- La caza de amenazas de red debe soportar diversas fuentes de red y permitir la caza para ataques incluyendo, pero no limitado a, el Movimiento Lateral; Ataques Selectivos de la red, ataques del DNS, ataques a directorio activo, escalación de privilegios, Malware Beaconing, la Exfiltración de Datos etc.
- La herramienta debe ser capaz de buscar de forma proactiva e iterativa a través de una red o el sistema de directorio activo los registros de datos para detectar y aislar las amenazas avanzadas que evaden los sistemas basados en firmas (SIEM, IDS, DLP y otros).
- Deberá utilizarse un modelado de adversario basado en El modelo ATT&CK de MITRE, donde se consideren las diferentes Tácticas y Técnicas de Adversario incluyendo los vectores descritos en la Matriz ATT&CK.
- Deberá aplicarse la metodología de Modelado de Adversario ATT&CK de MITRE detalladas en la Matriz ATT&CK a fin de validar la seguridad de los Sistemas de Pago de BANXICO, tipo SPEI, BDT e INDEVAL incluyendo los requerimientos del Manual de BANXICO más reciente o su última actualización y que incluyan al menos las siguientes pruebas sobre la infraestructura completa e

Infraestructuras de Soporte de SPEI, BDT e INDEVAL y sistemas, incluyendo los sistemas de Directorio Activo:

- ✓ Riesgo de ataques por Pass-the-Hash.
- ✓ Riesgo de ataque por movimiento lateral.
- ✓ Riesgo de ataque por escalación de privilegios.
- ✓ Riesgo de ataque por inyección DLL en memoria.
- ✓ Riesgo de ataque a SMB.
- ✓ Riesgo de ataque a NTLMv2.
- ✓ Riesgo de ataque a Kerberos (Creación y reúso de Golden Tickets).
- ✓ Riesgo de ataque de sincronización de Directorio Activo (DA).
- ✓ Riesgo de abusos de Powershell.
- ✓ Riesgo de ataque a la base de datos de Directorio Activo.
- ✓ Riesgo de volcado masivo de credenciales de RAM o de las bases de datos de DA.
- ✓ Riesgos ante ataque de ransomware y malware de última generación.
- ✓ Riesgos de ataque a cuentas de servicios de AD
- ✓ Riesgo de robo masivo de credenciales, incluyendo el abuso de protocolos LLMNR, NTLMv2, etc.
- ✓ Riesgos de ataques a los sistemas de las nubes Privadas.

Servicio de Analítica de ataques a sistemas

EL LICITANTE GANADOR deberá proporcionar servicios de un personal certificado en el modelado de técnicas de ataque, elaboración de reglas de correlación, detección de ataques reales y amenazas avanzadas, como ransomware, APTs, ataques dirigidos por humanos, malware polimórfico, etc. EL LICITANTE en caso de resultar ganador deberá incluir el personal, equipamiento y herramientas de software necesarias para la habilitación del servicio, así como la infraestructura de soporte.

En este servicio, se requiere que EL LICITANTE GANADOR sea capaz de diseñar e implementar un conjunto de escenarios de ataque generados por los servicios anteriores, buscando recopilar información de los sistemas de manera inteligente, incluyendo información de sistemas, información de consolas de antivirus, información de firewalls, antivirus, end-point, etc. y definir e implementar en una plataforma de analítica de seguridad las trayectorias de ataque más probables, y alertamiento orientadas a la detección de cada patrón de ataque modelado.

Algunos ejemplos de los patrones a modelar, sin ser exhaustivo son los siguientes:

- ✓ Ataques de movimiento lateral con técnicas modernas de ataque como Pass-The-Hash (NTLMV2) y Pass-The Ticket (Kerberos)
- ✓ Ataques de adivinación de contraseñas en diversos servicios
- ✓ Ataques de creación de nuevas cuentas en sistemas
- ✓ Ataques de cambio en configuración de sistemas
- ✓ Ataques de escalación de privilegios en sistemas de directorio activo
- ✓ Robo de credenciales de memoria en sistemas
- ✓ Explotación de ACLs mal configuradas o abuso de permisos y privilegios de cuentas del directorio activo
- ✓ Ataques de reconocimiento de sistemas internos
- ✓ Ataques de acceso a servicios mediante cuentas inusuales
- ✓ Ataques de acceso a recursos críticos como las bases de datos, etc.

Monitoreo permanente de Seguridad

- La herramienta debe proporcionar capacidades para detectar amenazas e incidentes conocidos mediante la aplicación de casos de uso de amplio espectro en bitácoras de varias fuentes.
- La herramienta debe soportar la configuración de patrones de ataque para identificar nuevas amenazas identificadas en un dominio o productos relacionados.
- La herramienta debe crear automáticamente entradas (tickets) para remediación/respuesta basadas en reglas personalizadas definidas y notificar a los usuarios relevantes a través de notificaciones de correo electrónico.
- La herramienta debe tener todo el historial de reglas que se escriben desde el sistema o modelo de entrega.

Análisis de Incidentes

- La herramienta debe apoyar a la Mesa de servicios de BANOBRAS(MSB) con la administración centralizada de incidentes para priorizar y administrar incidentes de seguridad.
- La herramienta debe soportar la ejecución del protocolo de intervención o triaje de las alertas de los productos de seguridad de la red incluyendo SIEM, DLP, IPS, WAF, anti-APT, ETDR.
- La herramienta debe permitir la investigación de alertas de triaje y/o alertas personalizadas consideradas críticas.
- El módulo de investigación debe integrarse con fuentes de bitácoras SIEM bajo pedido para extraer datos relacionados con la alerta investigada. También debe incluir historial y gráficos para analizar los datos.
- La herramienta debe tener características para analizar el impacto del ataque en el activo objetivo, incluyendo configuraciones, indicadores de compromiso (IOCs), conexiones de red externas.
- La herramienta debe admitir características para identificar los atributos del atacante.
- La herramienta debe soportar modelos para construir toda la cadena de ataque, desde la creación de ataques, el progreso del ataque y la propagación al ataque en la red.
- La herramienta debe soportar la integración con fuentes de código abierto o comerciales de IOC, enumerar las fuentes soportadas que se pueden integrar con La herramienta e informar sobre el enfoque de integración.
- La herramienta debe proporcionar funciones de administración de casos para almacenar datos crudos y analizados para una alerta o conjunto de alertas específicos. También debe proporcionar detalles sobre qué artefactos se pueden almacenar relacionados con una investigación.
- La herramienta debe proporcionar libros de ejecución (playbooks) para los pasos de investigación correspondientes a diferentes tipos de ataques.
- La herramienta debe proporcionar características para realizar análisis visuales de las relaciones entre entidades del directorio activo y las posibles trayectorias de ataque.

Respuesta a Incidentes

- La herramienta debe soportar respuesta rápida a un incidente en curso o amenazas graves detectadas en los sistemas.
- El servicio deberá basarse en el Modelo NIST de Ciberdefensa, incluyendo las 5 fases: Identificar, Proteger, Detectar, Responder y Recuperar a las amenazas de ciberseguridad
- Remediación para responder a las amenazas conocidas (por ejemplo, recuperar correos maliciosos de buzones de entrada, bloquear IPs malas en firewall, deshabilitar usuarios ofensores en Directorio activo y otros)

- La herramienta debe admitir varios parámetros de configuración a servidores, equipos de escritorio, incluyendo la eliminación o cambios a servicios, usuarios, ejecución de scripts, claves de registro, software, etc.
- La herramienta debe soportar el flujo de trabajo completo para la coordinación de incidentes.
- La herramienta incluye la elaboración de manuales de procedimientos (playbooks) para los pasos de reacción y respuesta correspondientes a diferentes tipos de ataques, derivar el ataque, detectar el progreso del ataque y la respuesta de contención.
- La herramienta debe apoyar la asignación de actividades a diferentes equipos y el seguimiento para su cierre.
- La herramienta debe soportar flujos de trabajo de escalamiento.
- La herramienta debe admitir el seguimiento de las aprobaciones de excepciones de seguridad para aquellas amenazas e incidentes para los que la remediación no es posible o que hay disponibilidad de controles compensadores.
- La herramienta debe proporcionar detalles de alerta y resultados de investigación vinculados y visibles para los tickets de remediación pertinentes
- La herramienta debe proporcionar la capacidad de mapear el posible incidente contra las diferentes fases del modelo de Matriz ATT&CK de MITRE a fin de mitigar en múltiples niveles a lo largo de la secuencia de adversario.

Investigación de ciber delitos, colección y análisis forense

La aplicación de protocolos y procedimientos en la identificación, fijación y preservación de la evidencia digital se convierten en la clave para garantizar la integridad de esta y evitar duda razonable y en consecuencia su desacreditación ante un incidente con implicaciones legales. Por tal razón, EL LICITANTE GANADOR deberá proporcionar la asistencia como mínimo de un especialista forense, con certificación de **herramientas** y con metodologías y capacidad para realizar la investigación de ciber delitos, efectuar análisis forense en al menos los siguientes casos de uso.

Investigación de ciber delitos

- Fraudes financieros a través de la red.
- Espionaje a través de redes informáticas y/o telecomunicaciones.
- Acceso no autorizado a elementos TIC de la red
- Robo de información
- Pérdida de información
- Perdida de integridad en la información
- Robo de personalidad.
- Alteración de sistemas de bases de datos a través de una red informática

Identificación, fijación y preservación de datos y evidencia con validez legal

- Incluir la posible identificación, fijación y preservación de datos y medios de prueba obtenidos de equipos e infraestructura de almacenamiento de computo, aplicando el procedimiento de cadena de custodia y presentada física y digitalmente a través de un dictamen pericial.
- Identificación, fijación y preservación de datos y medios de prueba obtenidos de dispositivos móviles, aplicando el procedimiento de cadena de custodia y presentada física y digitalmente a través de un dictamen pericial.

- Identificación, fijación y preservación de datos y medios de prueba obtenidos de infraestructura de almacenamiento de computo remota, aplicando el procedimiento de cadena de custodia y presentada física y digitalmente a través de un dictamen pericial.
- Identificación, fijación y preservación de datos y medios de prueba obtenidos de servidores de correo, cuentas de correo electrónico y/o archivos de cuentas de correo electrónico, aplicando el procedimiento de cadena de custodia y presentada física y digitalmente a través de un dictamen pericial.

S5 - Modelado de adversario Blue-Team Red-Team de manera mensual

EL LICITANTE GANADOR deberá proporcionar personal certificado en seguridad de la información para realizar los servicios de Ciberseguridad.

Para efectos de este servicio, se establece que una misión es una actividad para lo cual deberá efectuarse el ciclo completo de la metodología de adversario efectuado por el equipo red-team y se validará contra los procesos de detección y respuesta del grupo de blue-team. El equipo azul es el equipo defensivo. El equipo rojo es el equipo ofensivo.

El servicio de modelado de adversario Blue-Team Red-Team funcionara en la siguiente forma:
Se establecerán objetivos al principio de cada misión entre los 2 grupos: atacantes y defensores. Se definirán los límites de las pruebas, las ventanas de ejecución del servicio y las reglas del juego.

Los servicios deberán ser realizados durante la vigencia del contrato y con estricto apego a las políticas y procedimientos actuales y sus respectivas actualizaciones de BANOBRAS, las cuales serán dadas a conocer al licitante ganador, en la oficina de la DSI, ubicada en Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219, en piso 9, durante los 5 primeros días hábiles después de la notificación del fallo.

Los servicios deberán ser cubiertos con personal capacitado y certificado a fin de garantizar las capacidades requeridas conforme al numeral "5 Personal requerido".

Metodología a utilizar y reglas del servicio

Para cada uno de los escenarios descritos, se deberán efectuar una Metodología que deberá de entregarse conforme a lo establecido en el componente S5, del numeral 11 "Niveles de Servicio", la cual deberá incluir al menos lo siguiente:

Fase preparación

Explicar la Misión en turno y el sentido de la prueba. El sentido del ejercicio es auditar los procesos de detección y respuesta reales mediante la ejecución controlada de un "escenario de incidente" o "misión", analizando los límites de defensa efectiva y los gaps existentes, a fin de mejorarlos, con un sentido preciso de que es lo que funciona y que es lo que no funciona, mapeados contra la clasificación de MITRE ATTACK y poder plantear un plan de mejora efectivo en la seguridad de la institución. EL LICITANTE GANADOR del servicio podrá, en su experiencia, proponer el uso de herramientas automatizadas como MITRE

Caldera, Uber Metta, Atomic Red Team y Endgame RTA, permitiendo a la organización la obtención de métricas repetibles.

- Deberán formarse 2 equipos. El equipo azul es el equipo defensivo. El equipo rojo es el equipo ofensivo.
- Deberán definirse las personas que deban ser incluidos en cada equipo, dependiendo de la misión en turno.
- Nombrar un responsable del equipo azul y un responsable del equipo rojo.
- Identificar los activos bajo prueba.
- Identificar la existencia de algunos controles detectivos de la actividad probada por parte del equipo AZUL.
- Definir los tiempos esperados de TTD (Tiempo de Detección) y TTR (Tiempo de Respuesta) aceptables, acordado con el representante de la Institución. En este caso, algún responsable del negocio o el CISO.
- Identificar la persona responsable de la seguridad de dichos activos. Si es un LICITANTE GANADOR externo, buscar integrarlo al equipo. Si esto no fuera posible, cambiar los activos bajo prueba a otros donde sí se pueda interactuar con el equipo defensivo.
- El responsable del equipo AZUL deberá investigar y explicar la existencia de un conjunto de controles de seguridad que deberían lograr la detección y contención del evento simulado. El responsable del equipo azul deberá comunicar los controles que se encuentren operativos y explicar los límites de efectividad de estos en relación con la misión bajo prueba. De otra forma, el equipo AZUL debería poder declararse no preparado para cubrir este incidente o proponer la adecuación de los controles que hicieran falta, si fuera el caso.
- En cada misión, los elementos aleatorios que se agregarán será que no se revelará el momento exacto de la prueba ni las tácticas y procedimientos utilizados por parte del equipo ROJO, respetando los límites de la prueba nombrados en la sección "Límites Legales de la Metodología".

Durante la ejecución

- EL LICITANTE GANADOR del servicio podrá, en su experiencia, proponer el uso de herramientas automatizadas como MITRE Caldera, Uber Metta, Atomic Red Team y Endgame RTA.
- Cualquier evento importante asociado a la misión bajo análisis deberá ser documentado y guardado como evidencia, incluyendo IOCs.
- En las pruebas de ejecución interna, no se pedirá al equipo ROJO que parta de cero, sino que se ofrecerá al equipo ROJO un usuario interno con los privilegios normales de un usuario interno con acceso a los activos internos normales.
- Ante una detección, ya sea basada en Indicadores de Compromiso (IOC) o indicadores de Ataque (IOA), el equipo AZUL deberá aplicar las políticas de seguridad existentes. Por ejemplo, No se podrá bloquear o eliminar la cuenta ofensora si no es actualmente una política aceptada por la Institución.
- Ante una detección efectiva, se deberá tomar evidencia de su detección, así como de las medidas de contención efectuadas.

Reunión de retroalimentación de cada misión

Al final de cada misión se deberán tener reuniones de trabajo entre ambos grupos, a fin de validar cuales de los procedimientos de ataque fueron exitosamente detectados, bloqueados y contenidos. De igual manera se validarán los procedimientos que fueron exitosos para el atacante a fin de solventar los gaps en los mecanismos de defensa y poder plantear un plan de mejora realista.

- Para dichos análisis se deberá utilizar la metodología de MITRE ATTACK Matrix, identificando para cada fase del ataque, lo que funciona para efectos defensivos y lo que hay que mejorar. A la conclusión de cada ejercicio se deberá establecer un plan claro de mejora, con compromisos reflejados en un Plan de Trabajo por parte del equipo defensivo, conforme a lo establecido en el componente S5, del numeral 11 "Niveles de Servicio".

En esta Etapa se revelarán todos los resultados de ambas partes:

- ✓ Lo que se detectó y se pudo contener
- ✓ Lo que se detectó y no se pudo contener
- ✓ Evidencia del tiempo en el que se detectó y contuvo el incidente por parte del equipo AZUL. Con esto se buscará medir el TTD (Time to Detect) y el TTR (Time to Respond).
- ✓ El equipo ROJO mostrara los alcances de lo que fue posible realizar, evidenciando la falla en los controles de seguridad. En estos casos, se deberá analizar de forma conjunta el escenario de ataque y definir juntos algunas posibles medidas de mejora y controles adicionales, buscando la disminución del riesgo presente.
- ✓ En caso de que no fuera posible la implementación practica de algunos controles adicionales por parte del equipo AZUL, se deberán sugerir medidas de mitigación de riesgo mediante la aplicación de controles de compensación, como aislamiento de sistemas riesgosos, segregación de flujos peligrosos, filtrado de accesos a los activos bajo riesgo, etc.
- ✓ Deberá elaborarse un Calendario de mejora por parte del equipo AZUL, con fechas claras y compromisos a alcanzar.

Reglas de ejecución

Los participantes del equipo de red-team (atacantes) acataran las reglas de comportamiento definidas al principio de cada misión, incluyendo acciones validas, acciones invalidas, límites de las pruebas, etc.

- Por razones obvias, todos los elementos participantes por parte DEL LICITANTE GANADOR en los ejercicios de red-team deberán ser personal con alta especialización y certificaciones de ciberseguridad para la ejecución de las pruebas de seguridad planteadas para los diferentes dominios.

Límites legales de la metodología

Se prohíbe el uso de técnicas que impliquen métodos ilegales.

- ✓ No se pueden simular amenazas a personal por medios telefónicos o electrónicos
- ✓ No se puede usar el chantaje ni la extorsión
- ✓ No se pueden usar técnicas de Sabotaje real
- ✓ No se puede utilizar soborno o coacción del personal
- ✓ No se puede efectuar reclutamiento con fines de Human Intelligence (HUMINT)
- ✓ No se pueden emitir noticias falsas que puedan significar algún riesgo (amenazas de bomba, incendio, etc.)
- ✓ No se puede realizar ataque a dispositivos personales o redes privadas del personal
- ✓ No se pueden usar técnicas de negación de servicio
- ✓ No se puede acceder a información protegida por leyes de privacidad o financiera
- ✓ No se pueden efectuar Intervenciones telefónicas ni ataques de intercepción de llamadas
- ✓ No se puede comprometer a subsidiarias ni afiliadas sin un permiso explicito

- ✓ No se pueden afectar sistemas o procesos productivos
- ✓ No se pueden inyectar datos en bases de datos operacionales, etc.

Retest final de controles

En el mes final del servicio, se efectuarán algunas pruebas de retest a fin de validar el estatus de los posibles controles de mejora comprometidos en misiones anteriores. Se entregará un reporte final a la DSI.

5. Personal requerido

EL LICITANTE GANADOR del servicio deberá asignar a los perfiles el día hábil siguiente a la notificación del fallo requeridos conforme a lo solicitado, a fin de garantizar el nivel de especialización en los servicios y con las certificaciones vigentes.

EL LICITANTE GANADOR deberá brindar los servicios establecidos conforme a la solicitud del perfil requerido. EL LICITANTE GANADOR deberá presentar a todos los recursos que cumplan con el perfil requerido y sus certificaciones respectivamente para brindar los servicios de ciberseguridad.

Componente	Perfil	Requisitos	Cantidad
S1, S2, S3, S4 y S5	Administrador del proyecto	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales o afín. Contar con la certificación PMP (Project Management Professional) y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Senior Lead Auditor • COBIT 5 Foundation Examination, acreditado por ISACA • ITIL V3 o V4 Foundation Certificate in IT Service Management • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	1 recurso
	Especialista en cumplimiento	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones:	1 recurso

Componente	Perfil	Requisitos	Cantidad
		• CISA - Certified Information Systems Auditor • CISM - Certified Information Security Manager • CDPSE - Certified Data Privacy Solutions Engineer y CGEIT - Certified in the Governance of Enterprise IT **ó** TOGAF (The Open Group Arquitecture Framework)	
	Líder técnico de ciberseguridad	Contar con Título o Cédula profesional de ingeniería ó licenciatura en sistemas computacionales, administrción o afín. Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones: Deberá contar con al menos las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager • CISA (Certified Information Systems Auditor) • CISM (Certified Information Security Manager) • CISSP (Certified Information Systems Security Professional)	1 recurso
	Auditor de ciberseguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación PECB Certified ISO 22301 Lead Auditor y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PMP (Project Management Professional)	1 recurso
S2	Líder técnico de seguridad en sistemas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales o afín. Contar con la certificación OSWP (Offensive Security Wireless Professional) y deseable las siguientes certificaciones:	1 recurso

001433

Componente	Perfil	Requisitos	Cantidad
		• CompTIA Security+ ce, EC -Council Certified Ethical Hacker (Master), EC - Council Certified Ethical Hacker (Practical), PECB ISO/IEC 27032 Lead Cybersecurity Manager **ó** EC -Council Certified Ethical Hacker • Certified OSSTMM 3.0 Professional Security Analyst OPSA **ó** CIH (Certified Incident Handler)	
	Especialista en pruebas estáticas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación CompTIA Security+ ce y deseable las siguientes certificaciones: • CISP (Certified Information System Security Professional) • Certified Tester ISTQB (International Software Testing Qualifications Board)	3 recursos
	Especialista en pruebas dinámicas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales o afín. • Contar con la certificación Certified OSSTMM 3.0 Professional Security Analyst (OPSA) y deseable las siguientes certificaciones: • CEH (Certified Ethical Hacker) o CEH (Certified Ethical Hacker) Fundamental • Certificación en programa de Ciberseguridad • Certificación en Celullar Communications Forensics Consultation	1 recurso
S3	Arquitecto de seguridad en arquitecturas de directorio activo	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Deberá contar con cursos en: • Enterprise Security Fundamentals • Directorio Activo	1 recurso

Componente	Perfil	Requisitos	Cantidad
	Auditor de riesgos de seguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación Certified ISO 31000 Risk Manager y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO 22301 Lead Auditor	1 recurso
S4	Analistas de seguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación Certified CSA (Certified SOC Analyst v1) y deseable las siguientes certificaciones: • Certified Incident Handler (CIH)	Al menos 6 recursos
	Líder de operación	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación CNSS (Certifed Network Security Specialist) y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27035 Lead Incident Manager • ITIL v3 o v4 Foundation Certificate in IT Service Management • CSA (Certified SOC Analyst v1) • Certified ISO/IEC 27001	1 recurso
S5	Líder técnico de Red Team	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación GIAC Penetration Tester (GPEN) y deseable las siguientes certificaciones: • GIAC Reverse Engineering Malware (GREM) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Intrusion Analyst	1 recurso

001431

Componente	Perfil	Requisitos	Cantidad
	Especialista de Red Team.	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación Certified Ethical Hacker y deseable las siguientes certificaciones: • Certified OSSTMM 3.0 Professional Security Analyst OPSA • Offensive Security Certified Professional OSCP • CompTIA Security+ ce • GIAC Certified Instrusion Analyst	1 recurso

6. Plan de trabajo

Los servicios entregados por EL LICITANTE GANADOR se deberán apegar al siguiente calendario:

Fase	ID	Actividad	Duración
Planeación Implementación Y puesta a punto	1	Planeación del arranque	Primer mes de inicio de vigencia del contrato
Operación	2	Servicio S1	15 meses
	3	Servicio S2	15 meses
	4	Servicio S3	15 meses
	5	Servicio S4	15 meses
	6	Servicio S5	15 meses
	7	Finalización del contrato	-

7. Entregables

EL LICITANTE GANADOR deberá realizar la entrega de lo siguiente:

Componente	Actividad	Entregable
S1, S2, S3, S4, S5	Planeación del proyecto, única vez, a los 10 días hábiles	Plan de trabajo y Metodología

Componente	Actividad	Entregable
	posteriores de inicio del servicio	
	Definición de metodologías, única vez, a los 15 días hábiles posteriores de inicio del servicio	Documento de definición de metodologías de los servicios dentro del alcance
S1	Evento mensual de toda la infraestructura del SPEI, BDT e INDEVAL de análisis de vulnerabilidades.	Reporte de ejecución de pruebas
	Evento mensual de toda la infraestructura del SPEI, BDT e INDEVAL de análisis de vulnerabilidades.	Reporte de vulnerabilidades
	Evento mensual de toda la infraestructura del SPEI, BDT e INDEVAL de análisis de vulnerabilidades.	Indicadores de vulnerabilidades
	Evento trimestral de análisis de vulnerabilidades y pruebas de penetración.	Reporte de ejecución de pruebas
	Evento trimestral de análisis de vulnerabilidades y pruebas de penetración.	Reporte de vulnerabilidades
	Evento trimestral de análisis de vulnerabilidades y pruebas de penetración	Indicadores de vulnerabilidades
	Evento trimestral de análisis de vulnerabilidades y pruebas de penetración	Reporte de riesgo tecnológico
S2	Análisis de seguridad para sistemas	Reporte mensual de análisis de código estático
	Análisis de seguridad para sistemas	Reporte mensual de análisis dinámico
	Análisis de seguridad para sistemas	Reporte mensual de indicadores de vulnerabilidades de sistemas
S3	Implementación de una herramienta de Monitoreo y validación	Memoria técnica de implementación de la herramienta con las características detalladas en la

Componente	Actividad	Entregable
	de cambios del directorio activo.	sección "Herramienta de Monitoreo y validación de cambios del directorio activo" del numeral anterior.
	Diagnóstico del Riesgo de ciberseguridad del Directorio Activo.	Informe de Riesgo de Ciberseguridad del Directorio Activo.
	Hardening de seguridad a los domain controllers de la Institución.	Recomendaciones de estrategias de hardening de seguridad a los domain controllers de la Institución.
	Validación de implementación de las estrategias de hardening de seguridad a los domain controllers de la Institución.	Reporte de validación en el estatus de implementación de las estrategias de hardening de seguridad a los domain controllers de la Institución.
	Definición de estrategias de aislamiento de sistemas obsoletos o migración a sistemas modernos.	Recomendaciones de estrategias de aislamiento de sistemas obsoletos o migración a sistemas modernos.
	Validación de implementación de las estrategias de aislamiento o actualización en sistemas obsoletos definidos por la Institución.	Reporte de validación en el estatus de implementación de las estrategias de aislamiento o actualización en sistemas obsoletos definidos por la Institución.
	Análisis con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.	Recomendaciones de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.
	Validación de implementación de las estrategias de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.	Reporte de validación en el estatus de implementación de las estrategias de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.

Componente	Actividad	Entregable
	Análisis de cuentas de Directorio Activo, incluyendo permisos, privilegios y ACLs.	Recomendaciones de depuración de cuentas de directorio activo, incluyendo permisos, privilegios y ACLs.
	Validación de implementación de las estrategias de depuración de cuentas de Directorio Activo, incluyendo permisos, privilegios y ACLs.	Reporte de validación del estatus de implementación de las estrategias de depuración de cuentas de Directorio Activo, incluyendo permisos, privilegios y ACLs.
	Sistema de administración de cuentas de administración local para servidores críticos de la Institución.	Memoria técnica de implementación de solución de cuentas de administración local para servidores críticos de la Institución.
	Sistema de accesos privilegiados de administración del directorio activo (PAW).	Memoria técnica de implementación del sistema de accesos privilegiados de administración del directorio activo (PAW).
S4	Implementación del servicio.	Memoria técnica de instalación de soluciones tecnológicas
	Transición del servicio	Memoria técnica de modelado de indicadores de ataque
	Monitoreo y cacería de amenazas	Reporte mensual de actividades sospechosas
	Monitoreo y cacería de amenazas	Reporte mensual de eventos de seguridad
	Respuesta a incidentes, Monitoreo y cacería de amenazas	Reporte mensual de indicadores de seguridad
	Monitoreo y cacería de amenazas	Reporte mensual de indicadores de ataque
S5	Memoria técnica de metodología, descripción de misiones a efectuar y formación de equipos Azul y Rojo	Metodología y detalle de pruebas a ejecutar
	Reporte Técnico de la Misión contra MITRE y recomendaciones de mejora	Reporte mensual de misión de equipos Blue Team y Red Team Plan de trabajo del equipo defensivo

001427

8. Idioma

El LICITANTE deberá entregar su propuesta técnica en idioma español, sin embargo, dada la naturaleza del proyecto y los servicios que se administran, se permitirá el uso de anglicismos en aquellos términos que sean de origen extranjero, o que representen nombres tecnológicos.

9. Propuesta Económica

El LICITANTE deberá presentar la propuesta económica, el valor considerado para cada servicio (S1, S2, S3, S4 y S5), con una vigencia de 15 meses.

La adjudicación del Contrato será por la totalidad de los servicios.

10. Vigencia del servicio

Al día siguiente hábil de la fecha de notificación del fallo, con una vigencia de 15 meses.

11. Niveles de Servicio

En los términos de lo previsto por el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 64 de su reglamento, en esta sección se definen el conjunto mínimo de características que EL LICITANTE GANADOR deberá cumplir para determinar la entera satisfacción por parte de la DSI y la DTIC en el ámbito que corresponda BANOBRAS de la recepción del servicio.

La entera satisfacción de cada uno de los entregables, se definirá en conjunto entre el LICITANTE GANADOR y el **Director de Seguridad de la Información durante el primer mes del servicio**.

La verificación del cumplimiento se hará a través de los esquemas de Evaluación y Control, durante y al final del periodo de vigencia del contrato. En el caso de que el servicio no cumpla con alguna de estas características, se aplicará la pena convencional y /o deducción correspondiente según los términos y el procedimiento definido en la sección Penalizaciones.

Componente	Nivel de Servicio	Entregable
S1, S2, S3, S4, S5	Única vez, a los 10 días hábiles posteriores de inicio del servicio	Plan de trabajo y Metodología
	Única vez, a los 15 días hábiles posteriores de inicio del servicio	Documento de definición de metodologías de los servicios dentro del alcance
S1	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de ejecución de pruebas

Componente	Nivel de Servicio	Entregable
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de vulnerabilidades
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Indicadores de vulnerabilidades
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de riesgo tecnológico
S2	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de análisis de código estático
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de análisis dinámico
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de indicadores de vulnerabilidades de sistemas
S3	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Memoria técnica de implementación de la herramienta con las características detalladas en la sección "Herramienta de Monitoreo y validación de cambios del directorio activo".
	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Informe de Riesgo de Ciberseguridad del Directorio Activo.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Recomendaciones de estrategias de hardening de seguridad a los domain controllers de la Institución.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de validación en el estatus de implementación de las estrategias de hardening de seguridad a los domain controllers de la Institución.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Recomendaciones de estrategias de aislamiento de sistemas obsoletos o migración a sistemas modernos.

Componente	Nivel de Servicio	Entregable
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de validación en el estatus de implementación de las estrategias de aislamiento o actualización en sistemas obsoletos definidos por la Institución.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Recomendaciones de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de validación en el estatus de implementación de las estrategias de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Recomendaciones de depuración de cuentas de directorio activo, incluyendo permisos, privilegios y ACLs.
	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento	Reporte de validación del estatus de implementación de las estrategias de depuración de cuentas de Directorio Activo, incluyendo permisos, privilegios y ACLs.
	Una vez durante el 1 primer mes del servicio	Memoria técnica de implementación de solución de cuentas de administración local para servidores críticos de la Institución.
	Una vez durante los 2 primeros meses del servicio	Memoria técnica de implementación del sistema de accesos privilegiados de administración del directorio activo (PAW).
S4	Única vez, a los 5 días hábiles posteriores al finalizar la	Memoria técnica de instalación de soluciones tecnológicas

Componente	Nivel de Servicio	Entregable
	implementación del servicio	
	Única vez, a los 5 días hábiles posteriores al finalizar la etapa de estabilización del servicio	Memoria técnica de modelado de indicadores de ataque
	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de actividades sospechosas
	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de eventos de seguridad
	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de indicadores de seguridad
	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de indicadores de ataque
	La herramienta de monitoreo deberá contar con una disponibilidad del 99.8 y se deberá entregar una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de disponibilidad del servicio
S5	Única vez, a los 30 días hábiles posteriores de inicio del servicio	Metodología y detalle de pruebas a ejecutar
	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario	Reporte mensual de misión de equipos Blue Team y Red Team Plan de trabajo del equipo defensivo

12. Tipo de Contrato

El contrato que se celebrará será abierto con un monto mínimo y máximo de conformidad con lo establecido en el artículo 47 de la ley de adquisiciones, arrendamientos y servicios del sector público y 85 de su reglamento.

001423

13. Método de Evaluación

Las proposiciones serán evaluadas a través del mecanismo de puntos y porcentajes de acuerdo a lo establecido en el "ACUERDO" por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y relacionados con las mismas.", publicado en el Diario Oficial de la Federación el 09 de septiembre de 2010.

14. Forma de Pago

BANOBRAS pagará al LICITANTE GANADOR el importe de los servicios de acuerdo al costo de cada servicio, conforme al numeral "7 Entregables y 11 Niveles de Servicio" del presente Anexo técnico. una vez que cada una de éstas haya sido concluida, aceptada y proporcionados **los entregables** que la amparen a entera satisfacción de los servicios debidamente devengados, debiendo darse la recepción y aceptación de la factura correspondiente al servicio, acompañada de la documentación soporte que proceda.

El pago de los servicios debidamente proporcionados conforme a contrato, será con la previa validación de los entregables y a entera satisfacción de los servicios debidamente devengados por parte del Director de Seguridad de la Información en el ámbito de sus responsabilidades que se definirá en ese instrumento.

El pago se efectuará **mensualmente** dentro de los veinte días hábiles posteriores a la presentación de la factura respectiva por parte de EL LICITANTE GANADOR, la cual deberá estar debidamente y fiscalmente llenada, previa solicitud de liberación de pago emitida por el Administrador del Contrato.

El pago se realizará contra la factura y la validación a entera satisfacción de los entregables descritos y la validación de los entregables por parte del Director de Seguridad de la Información, estableciendo en su caso las penalizaciones y deductivas cuando se rebase las fechas establecidas en el numeral "6 Plan de trabajo, 7 Entregables y 11 Niveles de Servicio".

15. Garantías

La garantía que deberá proporcionar EL LICITANTE GANADOR, de conformidad con lo dispuesto por el artículo 48 de la LAASSP, se deberá realizar mediante la entrega de una póliza de fianza expedida por una Institución mexicana de fianzas legalmente autorizada, por el 10% del importe total del instrumento contractual, sin considerar el impuesto al valor agregado.

Deberá estar dirigida a: Banco Nacional de Obras y Servicios Públicos, S.N.C.

EL LICITANTE GANADOR se obliga a mantener vigente dicha fianza, en tanto permanezca en vigor el instrumento contractual y si es el caso, durante la substanciación de todos los recursos legales o juicios que se interpongan, hasta que se dicte la resolución definitiva, por autoridad competente, salvo que las partes otorguen el finiquito, o hasta aquella fecha en que BANOBRAS, hubiere comunicado la terminación anticipada del contrato, en el entendido de que sólo podrá ser cancelada mediante autorización por escrito de BANOBRAS, por medio de Representante Legal, previa solicitud por escrito del LICITANTE GANADOR dirigida al Área de Adquisiciones.

EL LICITANTE GANADOR se obliga a mantener vigente dicha fianza, en tanto no se concluyan con las garantías de las **soluciones tecnológicas contra defectos de fabricación, la corrección de cualquier anomalía producto de un defecto en la construcción y/o configuración, mismas que no tendrán costo para BANOBRAS y deberá ser validada y aceptada por el Director de Seguridad de la Información.**

EL LICITANTE GANADOR se compromete a reparar los componentes de la solución contemplados en el presente contrato, que presenten algún defecto, debido a un mal **funcionamiento de la solución desarrollada,** con relación a las especificaciones contenidas en el Documento de Definiciones Funcionales.

Para corregir los posibles defectos EL LICITANTE GANADOR asignará personal para la atención de estos tan pronto como sean detectados, esta garantía será válida dentro de los **6 meses después de haber entregado los servicios para pruebas de aceptación.**

El alcance de la garantía se limita únicamente a tareas de mantenimiento y desarrollo relacionadas con el servicio.

La garantía no aplicará cuando:

a. Los defectos se deban a errores de operación de la solución tecnológica,
b. Los defectos se deban a datos erróneos o incongruentes con el propósito de la solución tecnológica,
c. El código de la solución tecnológica entregada a **BANOBRAS** haya sido alterado por personal ajeno al licitante ganador.

16. Penas Convencionales y Deductivas

Una vez transcurrido el tiempo de entrega sin que los servicios hayan sido recibidos en los términos contractuales y a satisfacción del Director de Seguridad de la Información, proporcionará las constancias de recepción y entrega del servicio, junto con su documentación soporte en la que manifieste el cumplimiento parcial y/o deficiente en que incurrió EL LICITANTE GANADOR, para el cálculo del monto de la pena convencional y/o deductiva, de conformidad con lo establecido en el contrato y sus anexos, iniciando el trámite para que el Área de Pagos la haga efectiva.

El Director de Seguridad de la Información, podrá solicitar en cualquier momento al Área de Pagos la actualización del monto acumulado de penalización, lo cual será con base en la última constancia de recepción y entrega del servicio emitida por el Director de Seguridad de la Información para cada contrato y/o pedido, a efecto de observar que no se rebase el límite máximo de penalización aquí referido.

En el caso de la prestación de servicios donde se conceda el uso y posesión de bienes muebles, la responsabilidad de establecer los mecanismos para la guarda, custodia y control de estos, así como obtener del LICITANTE GANADOR el inventario correspondiente, la actualización de este de conformidad con el clausulado del contrato correspondiente, será a cargo del Director de Seguridad de la Información, para lo cual el LICITANTE GANADOR debe proporcionar una póliza de responsabilidad civil.

El Área de Pagos hará efectivas las deducciones, retenciones, descuentos y/o penas convencionales de contratos, a solicitud expresa del Área de Seguimiento de Contratos o en su caso por parte del Director de Seguridad de la Información.

Para ello se considerarán los costos mensuales especificados para cada uno de los servicios, de la propuesta económica del LICITANTE GANADOR.

Penas Convencionales y deductivas.

001421

Las penas convencionales se constituirán por el retraso en los plazos de ejecución del proyecto y/o por el retraso en la presentación de los entregables de conformidad con lo siguiente:

- Retraso en los plazos de ejecución **con respecto al Plan de Trabajo** por causas ajenas a **BANOBRAS**: 2% del costo total de los servicios no proporcionados a satisfacción por cada día hábil de retraso.
- Retraso en la presentación de los entregables por causas ajenas a **BANOBRAS**: 2% del costo total de los servicios no proporcionados a satisfacción por cada día de retraso, dado que los entregables forman parte integral del servicio, conforme a lo establecidas en el numeral "6 Plan de trabajo, 7 Entregables y 11 Niveles de Servicio".

La aplicación de **deductivas**, será del 1% sobre el importe de los entregables que no cumplan con las especificaciones del servicio o de los servicios que sean prestados de forma parcial o deficientemente.

Nota: La suma de las deductivas y penalizaciones no debe exceder el 10% del importe total del contrato

17. Confidencialidad

EL LICITANTE GANADOR reconoce que con motivo de la prestación de los servicios objeto del presente contrato recibirá de la Dirección de Seguridad de la Información, información de carácter estrictamente confidencial que únicamente puede y podrá ser utilizada por EL LICITANTE GANADOR para los fines de este contrato y en beneficio exclusivo de **BANOBRAS**, por lo que reconoce y acepta la obligación de guardar y mantener total secrecía y confidencialidad respecto de todos los datos e información, de cualquier clase, que **BANOBRAS** le proporcione, o bien, a la que tenga acceso, con motivo de la prestación y el desarrollo de los servicios objeto del presente contrato.

EL LICITANTE en caso de resultar adjudicado, se obliga a instruir a sus funcionarios, personal, incluyendo el subcontratado, empleados, agentes, representantes y/o toda persona que, por cualquier causa, se encuentre o pudiere estar a él vinculada y a la información de que se trata, respecto del contenido y alcances de la obligación de guardar secrecía y confidencialidad, a que se refiere esta Cláusula, siendo EL LICITANTE GANADOR directamente responsable por los daños y perjuicios ocasionados por las violaciones en que incurran las citadas personas de la mencionada obligación. EL LICITANTE GANADOR se obliga, a fin de garantizar el cumplimiento de la presente cláusula, a celebrar contratos de confidencialidad con cada una de las personas antes señaladas.

EL LICITANTE GANADOR reconoce y acepta la facultad de **BANOBRAS** de solicitarle, en cualquier momento, que le sean devueltas o que se destruyan, todos los datos e información descritos en la presente Cláusula, así como toda información, de cualquier naturaleza, que EL LICITANTE GANADOR haya elaborado para **BANOBRAS**, incluyendo resúmenes, hojas de trabajo, extractos, análisis y las copias que de ella existan, así como todos los medios de soporte en que se encuentre contenida. Asimismo, EL LICITANTE GANADOR se obliga a instruir a sus funcionarios, personal, incluyendo el subcontratado, empleados, agentes, representantes y/o toda persona que, por cualquier causa, se encuentre o pudiere estar a él vinculada y a los datos e información de que se trata, de la obligación a que alude este párrafo.

Las partes acuerdan que en caso de que EL LICITANTE GANADOR, sus funcionarios, personal, incluyendo el subcontratado, empleados, agentes, representantes y/o toda persona que, por cualquier causa, se

encuentre o pudiere estar a él vinculada y a los datos e información de que se trata, violen las obligaciones de secrecía y la confidencialidad estipuladas por este contrato, EL LICITANTE GANADOR sus funcionarios, personal, incluyendo el subcontratado, empleados, agentes, representantes y/o toda persona que, por cualquier causa, se encuentre o pudiere estar a él vinculada y a los datos e información de que se trata, responderán en forma solidaria por los daños y perjuicios que tal incumplimiento ocasionare a **BANOBRAS**; esto sin perjuicio del ejercicio de las demás acciones legales procedentes, por el delito de revelación de secretos contemplado en el Código Penal para el Distrito Federal y sus correlativos del Código Federal, así como las acciones y daños y perjuicios que pudieren derivar por las violaciones al Secreto Industrial, contempladas en las diversas leyes de la materia.

Únicamente se considerarán públicos o no confidenciales, aquellos datos e información a los que, por escrito y en forma expresa **BANOBRAS**, otorgue dicho carácter y, por lo tanto, no estarán sujetos a las restricciones estipuladas en la presente Cláusula. EL LICITANTE GANADOR reconoce y acepta que las obligaciones de guardar secreto y confidencialidad asumidas por él, sus funcionarios, personal, incluyendo el subcontratado, empleados, agentes, representantes y/o toda persona que, por cualquier causa, se encuentre o pudiere estar a él vinculada y a los datos e información de que se trata, no cesarán por terminación anticipada, rescisión, cumplimiento del objeto o conclusión de la vigencia de este contrato, quedando a obligados a mantenerla por un periodo indefinido de tiempo

18. Administración, Vigilancia del Contrato y Supervisión de las especificaciones y aceptación de los servicios

Con fundamento en el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como lo dispuesto en el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, en particular al Capítulo III, artículo 42, De las Disposiciones Aplicables a los Procedimientos de Contrataciones de Tecnologías y Seguridad de la Información, el servidor público responsable de administrar el cumplimiento del contrato será el Titular de la Dirección de Seguridad de la Información.

001419

19. Firmas del Área Requirente

Elaboró

Omar Manuel Mata Rubio
Gerente de Seguridad de la Información 2

Revisó

Claudia Galicia Hernández
Gerente de Seguridad de la Información 1

Autorizó

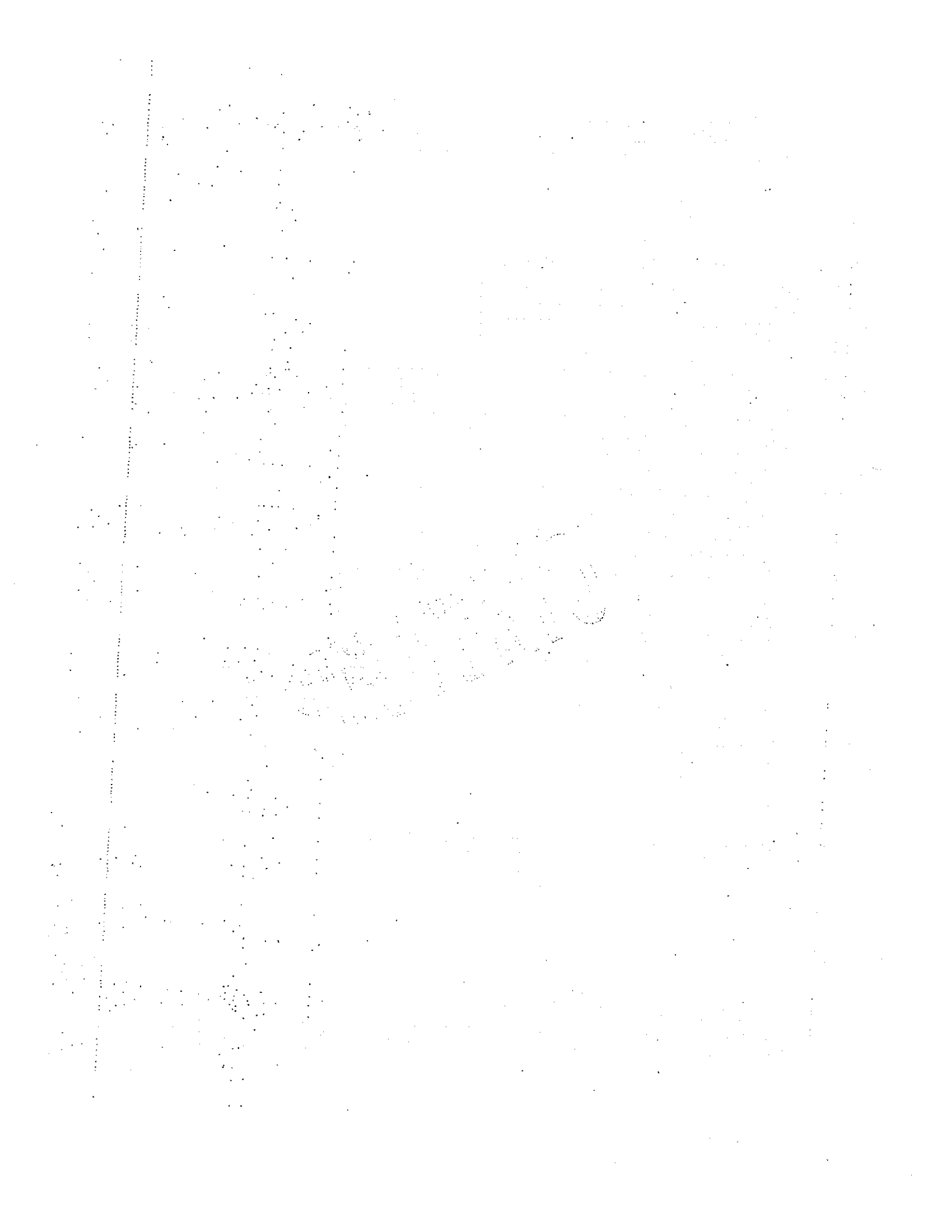
Humberto David Rosales Herrera
Director de Seguridad de la Información

MODELO DE PROPUESTA ECONOMICA: SERVICIOS DE CIBERSEGURIDAD
LICITANTE:
DIRIGIDA A:
NÚMERO DE PROCEDIMIENTO:
FECHA
15 MESES

ID DEL SERVICIO	NOMBRE DEL SERVICIO	ACRÓNIMO	UNIDAD DE MEDIDA (MES)	PRECIO UNITARIO
1	S1-. Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad	S1	1 MES	
2	S2- Realización periódica de análisis de seguridad de sistemas	S2	1 MES	
3	S3- Reducción de la superficie de ataque del ecosistema de los sistemas	S3	1 MES	
4	S4- Sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365	S4	1 MES	
5	S5- Modelado de adversario Blue-Team Red-Team	S5	1 MES	
			Subtotal	
			I.V.A	
			Total	

Anotar con letra, el **subtotal** antes de IV.A
Anotar con letra el importe **total** con I.V.A
Nombre del representante legal
Firma del representante legal del licitante:

*Cualquier diferencia que exista entre la propuesta técnica y la económica será motivo de desechamiento.
*La vigencia de la propuesta deberá ser de al menos 90 días naturales.



ANEXO B

HACIENDA | BANOBRAS

2022 Alfonso Flores Magón

ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD"

En la Ciudad de México, siendo las 10:30 horas del día 31 de octubre de 2022, en la oficina de la Gerencia de Adquisiciones del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (en adelante BANOBRAS), ubicada en el primer piso del edificio sito en Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México, se reunieron los servidores públicos cuyos nombres y firmas aparecen al final de la presente acta, con el objeto de reanudar la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, verificando en el Sistema electrónico de información pública gubernamental sobre adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas (en adelante CompraNet), las solicitudes de aclaración por parte de los licitantes con relación a las respuestas emitida por la convocante mediante el TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES (en adelante TERCER AVISO).

Lo anterior, de acuerdo a lo previsto en los artículos 33, párrafo cuarto, 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 45, y 46, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en la sección III.S. "Procedimientos de contratación" de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de BANOBRAS (en adelante POBALINES), y en términos de lo establecido en el numeral 3. "FORMA, MEDIO Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN" de la convocatoria de mérito.

En atención a las medidas institucionales de BANOBRAS para la prevención y combate de la propagación de la enfermedad generada por el coronavirus SARS-CoV2 (COVID-19), en relación a las medidas implementadas por las autoridades sanitarias federales, a través de los diversos Acuerdos publicados en el Diario Oficial de la Federación (DOF), particularmente correspondientes a los días 14 de mayo y 31 de julio del año 2020, así como sus modificaciones del 30 de septiembre de 2020, 8 de enero, 30 de abril y 30 de julio del año 2021, publicados en el mismo medio de difusión, y en cumplimiento a lo dispuesto en el CRITERIO NORMATIVO DE INTERPRETACIÓN TU 03/2020, emitido por la Ciudadana Titular de la Unidad de Normatividad de Contrataciones Públicas de la Secretaría de Hacienda y Crédito Público, para la celebración de la junta de aclaraciones a la convocatoria del procedimiento de contratación, se habilitó la plataforma *Microsoft Teams*, a efecto de que se guarde la máxima precaución para evitar contagios.

El acto fue presidido por la Licenciada Karla De Tuya García, Gerente de Adquisiciones, servidora pública facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el inciso C) de la sección I.4. "Responsabilidades" de las POBALINES.

Se informa que se cuenta con la asistencia del Ingeniero Moisés Isaac Herrera Ordóñez, Subgerente de Contrataciones, adscrito al área contratante, del Doctor Humberto David Rosales Herrera, Director de Seguridad de la Información y del Ingeniero Omar Manuel Mata Rubio, Gerente de Seguridad de la Información 2, ambos en su carácter de representantes del área requirente y técnica, así como del Licenciado Héctor Javier Gonzalez Galicia, Gerente Jurídico de Asuntos Laborales, Procedimientos y Amparo, representante de la Dirección Jurídica de lo Contencioso y Servicios Institucionales y de la Licenciada Mariana Romero García, representante del Órgano Interno de Control en BANOBRAS (en adelante OIC).

Se hace constar que se cuenta con la participación del Contador Público Certificado Alejandro Frank Díaz, en su carácter de testigo social, designado por la Dirección de Políticas de Fiscalización de la Unidad de Auditoría de

001415

Contrataciones Públicas de la Secretaría de la Función Pública a través del oficio número UACP/DPFCP/257/2022, de fecha 10 de octubre de 2022.

Se hace mención que la representante del OIC, asiste por invitación de la convocante para estar presente en los eventos del procedimiento de contratación, sin prejuzgar de la información que se presenta, siendo estricta responsabilidad de la convocante, cumplir con las disposiciones que regulan su actuar; y de los licitantes la veracidad de la documentación presentada, por lo que el OIC se reserva la facultad de revisar en cualquier momento la documentación que derive del procedimiento de contratación, en términos de la normatividad aplicable.

Se hace constar que de conformidad con lo dispuesto por los artículos 26, párrafo penúltimo de la LAASSP y 45, párrafo quinto del RLAASSP, al acto no asistió ningún representante o persona que manifestara su interés de estar presente en el mismo con calidad de observador.

La servidora pública que preside el acto, informa a los interesados en el procedimiento de contratación que de conformidad con lo dispuesto por el artículo 46, fracción II, párrafo segundo del RLAASSP, a las 11:30 horas del día 25 de octubre de 2022, mediante el TERCER AVISO, se suspendió la junta de aclaraciones a la convocatoria del procedimiento de contratación; con la finalidad de otorgar a los licitantes un plazo de **6 (SEIS) HORAS** contadas a partir de su publicación en el sistema CompraNet, para realizar las solicitudes de aclaración que consideren necesarias únicamente en relación con las respuestas emitidas por la convocante mediante el citado TERCER AVISO, el cual, se adjunta a la presente Acta como **ANEXO 1** para efectos de referencia, precisando que éste fue publicado en el sistema CompraNet a las 11:32 horas del día 25 de octubre de 2022.

De la misma manera, se adjunta a la presente Acta dentro del citado **ANEXO 1**, el PRIMER AVISO AL ACTA DE JUNTA DE ACLARACIONES y el SEGUNDO AVISO AL ACTA DE JUNTA DE ACLARACIONES.

En virtud del plazo otorgado de **6 (SEIS) HORAS** contadas a partir de la publicación del TERCER AVISO en el sistema CompraNet, hasta las 17:32 horas del día 25 de octubre de 2022, fue la fecha y hora límite para que los licitantes enviaran solicitudes de aclaración en relación a las respuestas emitida por la convocante a través del sistema CompraNet, por lo cual, después de haber realizado una verificación al citado sistema, se desprende que **NO** se recibieron solicitudes de aclaración en relación a las respuestas emitidas por la convocante mediante el TERCER AVISO, en tiempo y forma, motivo por el cual, se anexa a la presente acta como **ANEXO 2**, la impresión de pantalla del sistema CompraNet donde se aprecia este último.

Se hace mención que a las 17:40 horas del día 25 de octubre de 2022, fueron recibidas solicitudes de aclaración por parte del licitante SCITUM, S.A. DE C.V., sin embargo, derivado de que hasta las 17:32 horas del día 25 de octubre de 2022, fue la fecha y hora límite para enviar solicitudes de aclaración con relación con las respuestas emitidas por la convocante a través del sistema CompraNet, dichas solicitudes de aclaración fueron recibidas de forma extemporánea, motivo por el cual, con fundamento en lo dispuesto por los artículos 45, último párrafo y 46, fracción II, párrafo segundo del RLAASSP, así como en términos de lo señalado por el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria y lo estipulado en el TERCER AVISO, las citadas solicitudes de aclaración no serán contestadas por la convocante.

Asimismo, se hace constar que a las 23:38 horas del día 25 de octubre de 2022, fueron recibidas solicitudes de aclaración por parte del licitante IQSEC, S.A. DE C.V., sin embargo, derivado de que hasta las 17:32 horas del día 25 de octubre de 2022, fue la fecha y hora límite para enviar solicitudes de aclaración con relación con las respuestas emitidas por la convocante a través del sistema CompraNet, dichas solicitudes de aclaración fueron recibidas de forma extemporánea, motivo por el cual, con fundamento en lo dispuesto por los artículos 45, último párrafo y 46, fracción II, párrafo segundo del RLAASSP, así como en términos de lo señalado por el

numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria y lo estipulado en el TERCER AVISO, las citadas solicitudes de aclaración no serán contestadas por la convocante.

En cumplimiento a lo dispuesto por el artículo 33 Bis, párrafo penúltimo de la LAASSP, se informa a todos los interesados en el procedimiento de contratación, que el acto de presentación y apertura de proposiciones se llevará a cabo a las **13:00 HORAS DEL DÍA 07 DE NOVIEMBRE DE 2022**, de manera electrónica, es decir a través del sistema CompraNet.

En virtud de lo anterior, en términos de lo dispuesto por los artículos 26 Bis, fracción II, 27, 34, párrafo primero, 35 de la LAASSP, 47, párrafo primero y 50 del RLAASSP; así como de conformidad con lo señalado en el numeral 16 del ACUERDO por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet, publicado en el DOF el día 28 de junio de 2011, y en estricto apego a lo establecido en el numeral 3.4. "Presentación y apertura de proposiciones de la licitación" de la convocatoria, las proposiciones de los licitantes deberán ser firmadas electrónicamente, es decir, utilizando la firma electrónica avanzada que emite el Servicio de Administración Tributaria (SAT), por lo que será responsabilidad de los licitantes tener pleno conocimiento del procedimiento correspondiente para firmar dichas proposiciones de manera electrónica.

En términos de lo dispuesto por el artículo 33, párrafo penúltimo de la LAASSP, la presente Acta forma parte integrante de la convocatoria al procedimiento de contratación, debiendo ser considerada por los licitantes en la elaboración de sus proposiciones.

Para efectos de la notificación y en cumplimiento a lo dispuesto por el artículo 37 Bis, párrafo primero de la LAASSP, a partir de esta fecha y por un término no menor a 5 (cinco) días hábiles, se pone a disposición de los interesados, un aviso del lugar donde se encuentra disponible la presente Acta, en la planta baja del edificio ubicado en la Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México.

Asimismo, en términos de lo dispuesto por los artículos 37 Bis, párrafo segundo de la LAASSP y 49, párrafo segundo del RLAASSP, la presente Acta será difundida a través del sistema CompraNet, en la dirección electrónica https://compranet.hacienda.gob.mx/web/login.html, en el claro entendido de que este procedimiento sustituye a la notificación personal.

Después de dar lectura a la presente Acta, se dio por terminado el evento, siendo las 10:48 horas del día 31 de octubre de 2022, firmando al margen y al calce los que en ella intervinieron para dejar constancia, así como los efectos legales a que haya lugar.

La presente Acta y sus anexos constan de 64 (sesenta y cuatro) fojas útiles.

POR EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C.

NOMBRE	CARGO	FIRMA
Lic. Karla De Tuya García	Gerente de Adquisiciones	
Ing. Moisés Isaac Herrera Ordóñez	Subgerente de Contrataciones	

001413

HACIENDA | BANOBRAS

2022 Ricardo Flores Magón

NOMBRE	CARGO	FIRMA
Ph.D. Humberto David Rosales Herrera	Director de Seguridad de la Información	
Ing. Omar Manuel Mata Rubio	Gerente de Seguridad de la Información 2	
Lic. Héctor Javier González Galicia	Gerente Jurídico de Asuntos Laborales, Procedimientos y Amparo	

POR EL ÓRGANO INTERNO DE CONTROL EN EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C.

NOMBRE	FIRMA
Lic. Mariana Romero García	

EL TESTIGO SOCIAL

NOMBRE	FIRMA
C.P.C. Alejandro Frank Díaz (Testigo Social PF 028)	

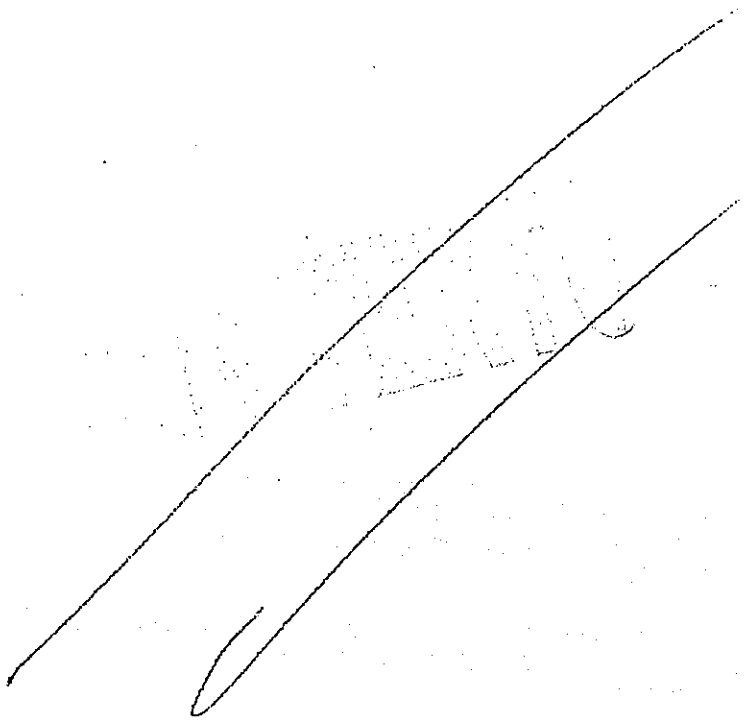
ESTAS FIRMAS FORMAN PARTE INTEGRANTE DEL ACTA DE JUNTA DE ACLARACIONES A LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219, Tel: 5270 1000.
www.gob.mx/banobras

001412

ANEXO 1

ACTA DE JUNTA DE ACLARACIONES A LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

BANOBRAS
BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.

2022 Ricardo Flores Magón Año de

PRIMER AVISO AL ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD"

En la Ciudad de México, siendo las 11:00 horas del día 18 de octubre de 2022, en la oficina de la Gerencia de Adquisiciones del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (en adelante BANOBRAS), ubicada en el primer piso del edificio sita en Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México, se reunieron los servidores públicos designados para intervenir en el presente acto, con el objeto de iniciar la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, de acuerdo a lo previsto en los artículos 33, párrafo cuarto, 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 45 y 46, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en la sección III.5. "Procedimientos de contratación" de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de BANOBRAS (en adelante POBALINES), y en términos de lo establecido en el numeral 3. "FORMA, MEDIO Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN" de la convocatoria de mérito.

En atención a las medidas institucionales de BANOBRAS para la prevención y combate de la propagación de la enfermedad generada por el coronavirus SARS-CoV2 (COVID-19), en relación a las medidas implementadas por las autoridades sanitarias federales, a través de los diversos Acuerdos publicados en el Diario Oficial de la Federación (DOF), particularmente correspondientes a los días 14 de mayo y 31 de julio del año 2020, así como sus modificaciones del 30 de septiembre de 2020, 8 de enero, 30 de abril y 30 de julio del año 2021, publicados en el mismo medio de difusión, y en cumplimiento a lo dispuesto en el CRITERIO NORMATIVO DE INTERPRETACIÓN TU 03/2020, emitido por la Ciudadana Titular de la Unidad de Normatividad de Contrataciones Públicas de la Secretaría de Hacienda y Crédito Público, para el inicio de la junta de aclaraciones a la convocatoria del procedimiento de contratación, se habilitó la plataforma *Microsoft Teams*, a efecto de que se guarde la máxima precaución para evitar contagios.

El acto fue presidido por la Licenciada Karla De Tuya García, Gerente de Adquisiciones, servidora pública facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el inciso C) de la sección I.4. "Responsabilidades" de las POBALINES.

La que preside el acto hace constar lo siguiente:

Derivado del número de solicitudes de aclaración recibidas en tiempo y forma por parte de los licitantes, así como del tiempo que se requiere emplear en darles contestación, se informa que siendo las 11:05 horas del día 18 de octubre de 2022, se suspende la junta de aclaraciones a la convocatoria antes citada, para reanudarse a las **11:00 horas del día 24 de octubre de 2022**, de conformidad con lo dispuesto por el artículo 46, fracción V del RLAASSP, así como lo señalado en el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria en mención.

El presente Primer Aviso al Acta de Junta de Aclaraciones, consta de 2 (dos) fojas útiles.

POR EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C.

NOMBRE	CARGO	FIRMA
Lic. Karla De Tuya García	Gerente de Adquisiciones	
Ing. Moisés Isaac Herrera Ordóñez	Subgerente de Contrataciones	

ESTAS FIRMAS FORMAN PARTE INTEGRANTE DEL PRIMER AVISO AL ACTA DE JUNTA DE ACLARACIONES A LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

----------FIN DEL AVISO----------

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

0014 JM

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

BANOBRAS
BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.

2022 Ricardo Flores Magón Año de

SEGUNDO AVISO AL ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD"

En la Ciudad de México, siendo las 11:00 horas del día 24 de octubre de 2022, en la oficina de la Gerencia de Adquisiciones del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (en adelante BANOBRAS), ubicada en el primer piso del edificio sita en Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México, se reunieron los servidores públicos designados para intervenir en el presente acto, con el objeto de reanudar la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, de acuerdo a lo previsto en los artículos 33, párrafo cuarto, 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 45 y 46, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en la sección III.5. "Procedimientos de contratación" de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de BANOBRAS (en adelante POBALINES), y en términos de lo establecido en el numeral 3. "FORMA, MEDIO Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN" de la convocatoria de mérito.

En atención a las medidas institucionales de BANOBRAS para la prevención y combate de la propagación de la enfermedad generada por el coronavirus SARS-CoV2 (COVID-19), en relación a las medidas implementadas por las autoridades sanitarias federales, a través de los diversos Acuerdos publicados en el Diario Oficial de la Federación (DOF), particularmente correspondientes a los días 14 de mayo y 31 de julio del año 2020, así como sus modificaciones del 30 de septiembre de 2020, 8 de enero, 30 de abril y 30 de julio del año 2021, publicados en el mismo medio de difusión, y en cumplimiento a lo dispuesto en el CRITERIO NORMATIVO DE INTERPRETACIÓN TU 03/2020, emitido por la Ciudadana Titular de la Unidad de Normatividad de Contrataciones Públicas de la Secretaría de Hacienda y Crédito Público, para la celebración de la junta de aclaraciones a la convocatoria del procedimiento de contratación, se habilitó la plataforma *Microsoft Teams*, a efecto de que se guarde la máxima precaución para evitar contagios.

El acto fue presidido por la Licenciada Karla De Tuya García, Gerente de Adquisiciones, servidora pública facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el Inciso C) de la sección I.4. "Responsabilidades" de las POBALINES.

La que preside el acto hace constar lo siguiente:

Derivado del número de solicitudes de aclaración recibidas en tiempo y forma por parte de los licitantes, así como del tiempo que se requiere emplear en darles contestación, se informa que siendo las 11:05 horas del día 24 de octubre de 2022, se suspende la junta de aclaraciones a la convocatoria antes citada, para reanudarse a las **10:30 horas del día 25 de octubre de 2022**, de conformidad con lo dispuesto por el artículo 46, fracción II del RLAASSP, así como lo señalado en el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria en mención.

El presente Segundo Aviso al Acta de Junta de Aclaraciones, consta de 2 (dos) fojas útiles.

POR EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C.

NOMBRE	CARGO	FIRMA
Lic. Karla De Tuya García	Gerente de Adquisiciones	
Ing. Moisés Isaac Herrera Ordóñez	Subgerente de Contrataciones	

ESTAS FIRMAS FORMAN PARTE INTEGRANTE DEL SEGUNDO AVISO AL ACTA DE JUNTA DE ACLARACIONES A LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006GIC001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

----------FIN DEL AVISO----------

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

BANOBRAS
BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.

2022 Ricardo Flores Magón
Año de

TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD"

En la Ciudad de México, siendo las 10:30 horas del día 25 de octubre de 2022, en la oficina de la Gerencia de Adquisiciones del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (en adelante BANOBRAS), ubicada en el primer piso del edificio sita en Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México, se reunieron los servidores públicos designados para intervenir en el presente acto, con el objeto de reanudar la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, de acuerdo a lo previsto en los artículos 33, párrafo cuarto, 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 45, y 46, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en la sección III.5. "Procedimientos de contratación" de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de BANOBRAS (en adelante POBALINES), y en términos de lo establecido en el numeral 3. "FORMA, MEDIO Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN" de la convocatoria de mérito.

En atención a las medidas institucionales de BANOBRAS para la prevención y combate de la propagación de la enfermedad generada por el coronavirus SARS-CoV2 (COVID-19), en relación a las medidas implementadas por las autoridades sanitarias federales, a través de los diversos Acuerdos publicados en el Diario Oficial de la Federación (DOF), particularmente correspondientes a los días 14 de mayo y 31 de julio del año 2020, así como sus modificaciones del 30 de septiembre de 2020, 8 de enero, 30 de abril y 30 de julio del año 2021, publicados en el mismo medio de difusión, y en cumplimiento a lo dispuesto en el CRITERIO NORMATIVO DE INTERPRETACIÓN TU 03/2020, emitido por la Ciudadana Titular de la Unidad de Normatividad de Contrataciones Públicas de la Secretaría de Hacienda y Crédito Público, para la celebración de la junta de aclaraciones a la convocatoria del procedimiento de contratación, se habilitó la plataforma *Microsoft Teams*, a efecto de que se guarde la máxima precaución para evitar contagios.

El acto fue presidido por la Licenciada Karla De Tuya García, Gerente de Adquisiciones, servidora pública facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el inciso C) de la sección I.4. "Responsabilidades" de las POBALINES.

Se informa que se cuenta con la asistencia del Ingeniero Moisés Isaac Herrera Ordóñez, Subgerente de Contrataciones, adscrito al área contratante, del Doctor Humberto David Rosales Herrera, Director de Seguridad de la Información y del Ingeniero Omar Manuel Mata Rubio, Gerente de Seguridad de la Información 2, ambos en su carácter de representantes del área requirente y técnica, así como del Licenciado Héctor Javier González Galicia, Gerente Jurídico de Asuntos Laborales, Procedimientos y Amparo, representante de la Dirección Jurídica de lo Contencioso y Servicios Institucionales y de la Licenciada Mariana Romero García, representante del Órgano Interno de Control en BANOBRAS (en adelante OIC).

Se hace constar que se cuenta con la participación del Contador Público Certificado Alejandro Frank Díaz, en su carácter de testigo social, designado por la Dirección de Políticas de Fiscalización de la Unidad de Auditoría de Contrataciones Públicas de la Secretaría de la Función Pública a través del oficio número UACP/DPFCP/257/2022, de fecha 10 de octubre de 2022.

Se hace mención que la representante del OIC, asiste por invitación de la convocante para estar presente en los eventos del procedimiento de contratación, sin prejuzgar de la información que se presenta, siendo estricta responsabilidad de la convocante, cumplir con las disposiciones que regulan su actuar; y de los licitantes la

veracidad de la documentación presentada, por lo que el OIC se reserva la facultad de revisar en cualquier momento la documentación que deriva del procedimiento de contratación, en términos de la normatividad aplicable.

Se hace mención que de conformidad con lo dispuesto por los artículos 26, párrafo penúltimo de la LAASSP y 45, párrafo quinto del RLAASSP, al acto no asistió ningún representante o persona que manifestara su interés de estar presente en el mismo con calidad de observador.

La servidora pública que preside el acto comunicó a los servidores públicos asistentes que de conformidad con lo dispuesto por los artículos 33 Bis, párrafos tercero y cuarto de la LAASSP, 45 y 46, fracción VI del RLAASSP, así como en términos de lo señalado en el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria, solamente se atenderán las solicitudes de aclaración de las personas que hayan presentado a través del Sistema electrónico de información pública gubernamental sobre adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas (en adelante CompraNet), por sí o en representación de un tercero, el escrito de interés en participar en el procedimiento de contratación y cuyas solicitudes de aclaración se hayan recibido con al menos 24 (veinticuatro) horas de anticipación a la fecha y hora establecida para la celebración de la junta de aclaraciones, es decir, a más tardar a las 11:00 horas del día 17 de octubre de 2022, que cumplan en tiempo y forma con lo señalado en el numeral de la convocatoria antes mencionado.

Se informa que fueron recibidas con 24 (veinticuatro) horas de anticipación a la fecha establecida para la celebración de la junta de aclaraciones, solicitudes de aclaración por parte del licitante SBEL SYSTEM GROUP, S.A. DE C.V., sin embargo, dichas solicitudes de aclaración no fueron acompañadas del escrito de interés en participar en el procedimiento de contratación, de tal forma que este fue recibido de forma extemporánea, motivo por el cual, con fundamento en lo dispuesto por los artículos 33 Bis, párrafo tercero de la LAASSP y 45, párrafos tercero y cuarto del RLAASSP, así como en términos de lo señalado por el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria, dichas solicitudes de aclaración no serán contestadas por la convocante.

Se hace constar que fueron recibidas con 24 (veinticuatro) horas de anticipación a la fecha establecida para la celebración de la junta de aclaraciones, solicitudes de aclaración por parte del licitante CAD & LAN MÉXICO, S.A. DE C.V., sin embargo, el escrito de interés en participar en el procedimiento de contratación con el que fueron acompañadas dichas solicitudes de aclaración no señala el nombre, denominación o razón social del licitante, de tal forma que este fue corregido de forma extemporánea, motivo por el cual, con fundamento en lo dispuesto por los artículos 33 Bis, párrafo tercero de la LAASSP y 45, párrafos tercero y cuarto del RLAASSP, así como en términos de lo señalado por el numeral 3.2. "Junta de aclaraciones de la licitación" de la convocatoria, dichas solicitudes de aclaración no serán contestadas por la convocante.

Se hace mención que fue recibido de forma extemporánea el escrito de interés en participar en el procedimiento de contratación por parte de los licitantes SERVICIOS ADMINISTRADOS MEXIS, S.A. DE C.V. y MICRONET DE MÉXICO, S.A. DE C.V., respectivamente, sin embargo, dichos licitantes no formularon solicitud de aclaración alguna.

En virtud de lo anterior, se dará respuesta a las solicitudes de aclaración de los siguientes licitantes:

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE	NÚMERO DE SOLICITUDES DE ACLARACIÓN
ECLIPSE TELECOMUNICACIONES, S. A. DE C.V.	5
CONSULTORÍA ESTRATÉGICA Y COACHING, S. DE R.L. DE C.V.	19
TIC DEFENSE, S. A. DE C.V.	21

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

SCITUM, S.A. DE C.V.	47
PG RANHTOE SERVICIOS ADMINISTRATIVOS, S.A. DE C.V.	2
DELOITTE ASESORÍA EN RIESGOS, S.C.	30
TOTAL DE SOLICITUDES DE ACLARACIÓN RECIBIDAS EN TIEMPO Y FORMA:	124

Las respuestas a las solicitudes de aclaración enviadas por los licitantes, mismas que fueron atendidas por el área requirente y técnica, así como el área contratante, en el ámbito de sus respectivas competencias, forman parte integral del presente TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES como **ANEXO A**.

La que preside el acto, dio lectura a las solicitudes de aclaración recibidas en tiempo y forma, así como sus respectivas respuestas, señalando que ha sido solventada por la convocante en su totalidad, informando que con fundamento en lo dispuesto por el artículo 46, fracción II, párrafo segundo del RLAASSP, las respuestas son publicadas y puestas a disposición de los interesados a través del sistema CompraNet, con la finalidad de que, en su caso, los licitantes se encuentren en la posibilidad de realizar las solicitudes de aclaración que consideren necesarias únicamente en relación con las respuestas emitidas, por lo que contarán con un plazo de **6 (SEIS) HORAS** contadas a partir de la publicación de las respuestas en el sistema CompraNet, para formular dichas solicitudes de aclaración, precisando que se tomará como hora de recepción la que registre el citado sistema al momento de su envío.

Las solicitudes de aclaración que no cumplan con este requisito no serán contestadas por la convocante, por lo que no se dará respuesta a las solicitudes de aclaración que se reciban con posterioridad a la hora señalada, con la finalidad de no generar desigualdad entre los participantes y motivar la libre participación.

Con fundamento en lo dispuesto por el artículo 33 de la LAASSP y en términos de lo señalado en el numeral 3.3. "Forma, modificaciones y aclaraciones que podrán efectuarse a la convocatoria", se adjunta al presente TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES como **ANEXO B**, las modificaciones a los aspectos establecidos en la convocatoria del procedimiento de contratación.

En cumplimiento a lo dispuesto por el artículo 49, párrafo segundo del RLAASSP, se incorpora al sistema CompraNet el presente TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES.

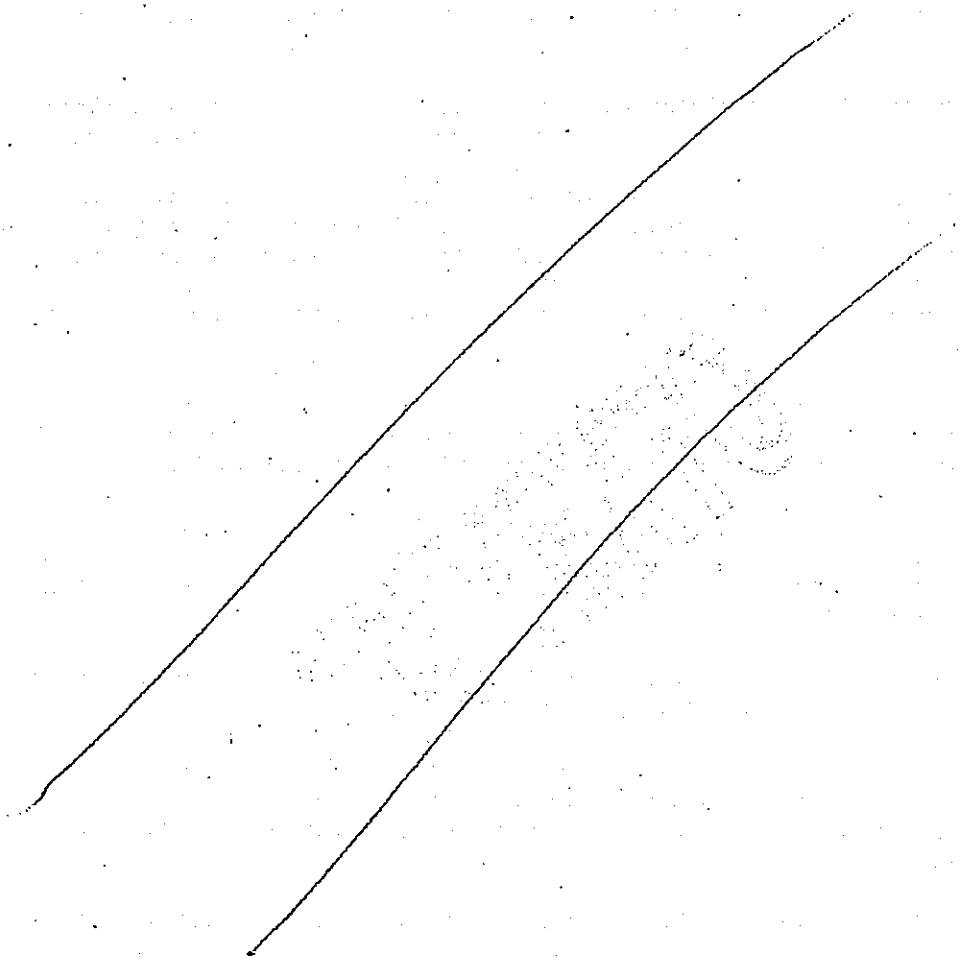
La que preside el acto, procedió a preguntar a los servidores públicos asistentes, si existe algún comentario, no existiendo comentarios, se suspende la junta de aclaraciones a la convocatoria del procedimiento de contratación, siendo las 11:30 horas del día 25 de octubre de 2022, para reanudarse a las **10:30 HORAS DEL DÍA 31 DE OCTUBRE DE 2022.**

El presente TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES y sus anexos constan de 52 (cincuenta y dos) fojas útiles.

POR EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C.

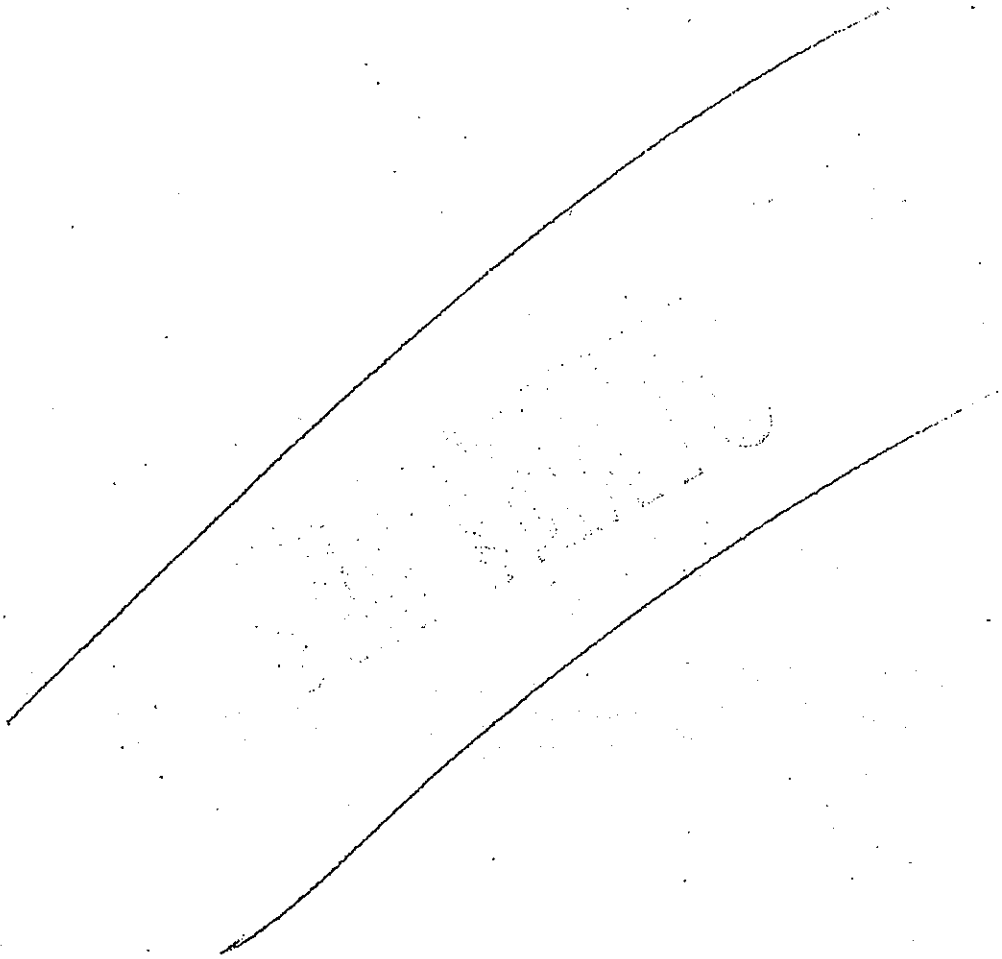
NOMBRE	CARGO	FIRMA
Lic. Karla De Tuya García	Gerente de Adquisiciones	
Ing. Moisés Isaac Herrera Ordóñez	Subgerente de Contrataciones	

----------FIN DEL AVISO----------



ANEXO A

TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES DE LA CONVOCATORIA A LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006GYN001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD"

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: ECLIPSE TELECOMUNICACIONES, S. A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"

Nº.	NÚMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	DICE: Es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de respuesta ante Incidentes de Seguridad Computacional acreditado como CERT ante FIRST (Global Forum of Incidente Response and Security Temas). (el incumplimiento del punto es motivo de desechamiento). La Universidad de Carnegie Mellon propietario de la Marca CERT ha decidido descontinuar su práctica de otorgar licencias de la marca CERT a nivel internacional. Como nos fue expresado por en el correo del año 2020 del cual anexa la impresión para conocimiento exclusivo de la Convocante. Se solicita amablemente a la Convocante no sea considerada como causa de desechamiento de la propuesta el no presentar la certificación CERT ante FIRST, y esta certificación sea considerada como opcional. ya que esta certificación no puede ser obtenida por los participantes en México, y sólo algunas empresas obtuvieron dicha certificación cuando fue emitida en México, lo anterior resulta en la limitación de la libre participación en la presente licitación y sólo favorece a algunas empresas. Y sólo sea considerada la evaluación por puntuación descrita en el anexo 16 en la página 8 inciso 3.B que a la letra dice "Al licitante que presente la evidencia documental de contar con el Certificado de membresía FIRST (Forum of Incidente Response and Security Temas): Se le otorgarán 1 punto. ¿Se acepta nuestra solicitud?	Se aclara que el certificado de afiliación al FIRST (Global Forum of Incidente Response and Security Temas) no establece limitación de adhesión en ningún país para ninguna organización pública o privada que lo desee hacer en cualquier momento, evidenciando en su publicación a través de su sitio web que en los últimos 2 (dos) meses del presente año se han acreditado empresas en México, por lo que no se acepta su solicitud, todos los licitantes deberán cumplir con lo establecido en los requerimientos del numeral 4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD", del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria.

001403

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

2	"MODELO DE PROPUESTA ECONÓMICA: SERVICIOS DE CIBERSEGURIDAD"	¿Es correcto entender que sólo se deberán cotizar los servicios de manera mensual, sin tener que realizar la totalización por los 15 meses del servicio de ciberseguridad objeto de la presente licitación? Lo anterior debido a que en el formato de la Propuesta Económica que hay que alimentar en el sistema de Compranet está indicado como cantidad 15 meses. Favor de Clarificar el formato de la Propuesta Económica para que sea congruente con lo solicitado en la página de Compranet.	Para efectos de la propuesta económica, misma que se encuentra señalada en el numeral 4.2. "Propuesta económica" de la convocatoria, no se debe de realizar la totalización por los 15 (quince) meses de servicio. El licitante únicamente deberá de señalar el precio unitario (mensual) de cada uno de los servicios y realizar la sumatoria para obtener un importe total mensual de los servicios objeto de la licitación. Para efectos del sistema CompraNet, el licitante deberá insertar el precio unitario (mensual) conforme a las cifras que se encuentren en su propuesta económica y el sistema automáticamente realizará una multiplicación por los 15 (quince) meses de servicio.
3	OTRO (PÁGINA DE COMPRANET)	En la página de Compranet en el inciso 1.1 PROPUESTA TÉCNICA - Sección de Parámetro Se solicita lo siguiente: *La propuesta técnica, misma que deberá cumplir con todos los requisitos, condiciones y especificaciones técnicas mencionadas en el Anexo Técnico, contenido en el ANEXO 1 de la presente convocatoria, así como los documentos requeridos en el mismo, por lo que los Licitantes deberán presentar toda la documentación en el mismo orden que se solicita en el citado Anexo Técnico. (INDISPENSABLE) Para llevar a cabo la evaluación a través del mecanismo de PUNTOS Y PORCENTAJES, se solicita a los Licitantes presentar la documentación señalada en el ANEXO 16 de la presente convocatoria. También en la página de Compranet en el inciso 1.4 DOCUMENTOS PARA LA EVALUACIÓN A TRAVÉS DE PUNTOS Y PORCENTAJES - Sección de Parámetro. Se solicitan sean cargado de manera individual los anexos del 1.4.1 al 1.4.14. Los documentos solicitados son los mismos en los dos puntos, lo cual implica que se deberán cargar dos veces, es decir, en el inciso 1.1. PROPUESTA TÉCNICA y en el inciso 1.4 DOCUMENTOS PARA LA EVALUACIÓN A TRAVÉS DE PUNTOS Y PORCENTAJES.	No es correcto su entendimiento, para efectos de la propuesta técnica, misma que se encuentra señalada en el numeral 4.1. "Propuesta técnica" de la convocatoria, esta deberá de ser cargada por el licitante en el apartado habilitado para tal efecto del sistema CompraNet. La documentación señalada en el ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES" de la convocatoria, deberá ser cargada por el licitante en los apartados habilitados para tal efecto del citado sistema CompraNet. En este sentido, la documentación no deberá ser duplicada a menos que la misma sea requerida para ambos. Asimismo, es importante mencionar que los licitantes deberán elaborar sus proposiciones en la forma que estimen conveniente a efecto de cumplir en su totalidad con lo solicitado por la convocante para el procedimiento de contratación. En caso de que las proposiciones de los licitantes no contengan la totalidad de las especificaciones y requisitos solicitados, será causa de desechamiento de las mismas.

001402

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		¿Es correcto nuestro entendimiento, caso contrario favor de especificar?	
NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: ECLIPSE TELECOMUNICACIONES, S. A. DE C.V.			
SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"			
N°	RUBRO ESPECÍFICO DEL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES".	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	GENERAL	¿Es correcto entender que aunque el Documento se encuentra con el título "Anexo 2 CRITERIO DE EVALUACIÓN" debe ser ANEXO 16 MATRIZ DE PUNTOS Y PORCENTAJES?	Es correcto su entender. Se procede a realizar la modificación correspondiente a la convocatoria. Para efectos de lo anterior, consultar la MODIFICACIÓN 7 de las modificaciones a la convocatoria.
2	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 1.- Experiencia en asuntos relacionados con la materia del servicio por parte del personal	El Licitante deberá acreditar con el Curriculum Vitae por lo menos del siguiente personal requerido para la prestación del servicio objeto de la presente contratación: Todos los perfiles. Dice: Asimismo deberá adjuntar la(s) constancia(s) laborales emitidas a favor de la persona, en la que se indique el nombre de la empresa, domicilio de la empresa, período en el que laboró, puesto y/o funciones que desempeñó, fecha y firma del emisor, a fin de acreditar los años de experiencia requeridos. Hacemos del conocimiento de la Convocante que por lo general las constancias laborales son emitidas por las empresas indicando el período laboral y el puesto desempeñado por el empleado. El solicitar las constancias laborales de esta forma tan específica es limitativo para la libre participación en la presente licitación, y pueden inducir la idea de que existe una tendencia a favorecer a algún licitante que tiene ya preparada la documentación exactamente como la solicitan. Con base en lo anterior y con la finalidad de no limitar la libre participación, solicitamos a la Convocante que sean aceptadas las Constancias Laborales más comúnmente emitidas que incluyen nombre del empleado, el período laboral y el puesto desempeñado emitidas por la empresa en la que se elaboró. ¿Se acepta nuestra solicitud?	Para demostrar la veracidad en la acreditación de la experiencia en asuntos relacionados con objeto del servicio por parte del personal, se requiere la emisión de constancia(s) laborales emitidas a favor de la persona, teniendo la(s) constancia(s) la siguiente información: nombre escrito o logotipo oficial de la empresa y/o institución, domicilio escrito en texto o a través de la plantilla institucional del emisor, periodo en el que laboró, puesto y/o funciones que se desempeñó, fecha y firma del emisor, este último puede ser jefe inmediato o departamento de recursos humanos o persona facultada para emitirla, lo anterior es la mínima información requerida dejando como opcional el teléfono directo y/o correo electrónico del emisor, de acuerdo a lo anterior NO SE ACEPTA su solicitud.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

001401

19

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: CONSULTORÍA ESTRATÉGICA Y COACHING, S. DE R.L. DE C.V.			
SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"			
Nº	NUMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	Dice: Es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de Respuesta ante Incidentes de Seguridad Computacional acreditado como CERT ante FIRST (global Forum of Incident Response and Security Teams). (el incumplimiento del punto es motivo de desechamiento). Se solicita amablemente a la convocante aclarar que la asignación de puntos en la Matriz de Puntos y Porcentajes sea de 1 punto si presenta la certificación, y si no la presenta será desechada su propuesta. ¿Es correcta nuestra apreciación?	Se confirma lo establecido en el numeral 4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD", del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, en donde se establece que es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de Respuesta ante Incidentes de Seguridad Computacional acreditado como CERT ante FIRST (global Forum of Incident Response and Security Teams). El incumplimiento del punto es motivo de desechamiento, y lo establecido en el ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES" de la convocatoria, en el apartado CAPACIDAD DE EQUIPAMIENTO es en donde se establece que se le otorgará 1 punto al licitante que presente el certificado.
2	5. "PERSONAL REQUERIDO"	En el perfil de Administrador de Proyectos, se solicitan las siguientes Certificaciones: Contar con la certificación PMP (Project Management Professional) y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Senior Lead Auditor • COBIT 5 Foundation Examination, acreditado por ISACA • ITIL V3 o V4 Foundation Certificate in IT Service Management • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, ya que la función principal de un Administrador de Proyectos es la gestión de actividades de todos los involucrados en el servicio y no participa en actividades operartivas. ¿Se acepta nuestra solicitud?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
3	5. "PERSONAL REQUERIDO"	En el perfil de Especialista en cumplimiento, se solicitan las siguientes Certificaciones: Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones:	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		• CISA - Certified Information Systems Auditor • CISM - Certified Information Security Manager • CDPSE - Certified Data Privacy Solutions Engineer y CGEIT - Certified in the Governance of Enterprise IT ó TOGAF (The Open Group Arquitecture Framework) ¿Es correcto entender que las certificaciones deseables son opcionales?	
4	5. "PERSONAL REQUERIDO"	En el perfil de Administrador de Proyectos, se solicitan las siguientes Certificaciones: Contar con la certificación PMP (Project Management Professional) y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Senior Lead Auditor • COBIT 5 Foundation Examination, acreditado por ISACA • ITIL V3 o V4 Foundation Certificate in IT Service Management • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, ya que la función principal de un Administrador de Proyectos es la gestión y no necesariamente se requiere la especialización de un Líder Auditor en ISO 27001, por mencionar un ejemplo. ¿Se acepta nuestra solicitud?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
5	5. "PERSONAL REQUERIDO"	En el perfil de Especialista en cumplimiento, se solicitan las siguientes Certificaciones: Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones: • CISA - Certified Information Systems Auditor • CISM - Certified Information Security Manager • CDPSE - Certified Data Privacy Solutions Engineer y CGEIT - Certified in the Governance of Enterprise IT ó TOGAF (The Open Group Arquitecture Framework) Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, y así permitir la libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas.	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

001356

		¿Se acepta nuestra solicitud?	
6	5. "PERSONAL REQUERIDO"	En el perfil de Líder Técnico de Ciberseguridad, se solicitan las siguientes Certificaciones: Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager • CISA (Certified Information Systems Auditor) • CISM (Certified Information Security Manager) • CISSP (Certified Information Systems Security Professional) Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, y así permitir la libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas. ¿Se acepta nuestra solicitud?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
7	5. "PERSONAL REQUERIDO"	En el perfil de Líder Técnico de Ciberseguridad, se solicitan las siguientes Certificaciones: Contar con la certificación CRISC - Certified in Risk and IS Control y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager • CISA (Certified Information Systems Auditor) • CISM (Certified Information Security Manager) • CISSP (Certified Information Systems Security Professional) Al respecto, se solicita amablemente a la convocante, que acepte la Certificación ISO/IEC 27001 Lead Auditor y la ISO/IEC 27032 Lead Cybersecurity Manager emitidas por un organismo certificador distinto al PECB, ya que de no ser así, se estaría limitando la libre participación de los proveedores. ¿Se acepta nuestra solicitud?	La convocante aclara que, se puede presentar la Certificación ISO/IEC 27001 Lead Auditor y la ISO/IEC 27032 Lead Cybersecurity Manager emitidas por un organismo certificador distinto al PECB.
8	5. "PERSONAL REQUERIDO"	En el perfil de Auditor de Ciberseguridad, se solicitan las siguientes Certificaciones:	La convocante aclara que, se puede presentar la Certificación ISO/IEC 27001 Lead Auditor emitidas por un organismo certificador distinto al PECB.

001398

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		Contar con la certificación PECB Certified ISO 22301 Lead Auditor y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PMP (Project Management Professional) Al respecto, se solicita amablemente a la convocante, que acepte la Certificación ISO/IEC 27001 Lead Auditor emitida por un organismo certificador distinto al PECB, ya que de no ser así, se estaría limitando la libre participación de los proveedores. ¿Se acepta nuestra solicitud?	
9	5. "PERSONAL REQUERIDO"	En el perfil de Especialista en Pruebas Estáticas, se solicitan las siguientes Certificaciones: Contar con la certificación CompTIA Security+ ce y deseable las siguientes certificaciones: • CISSP (Certified Information Systems Security Professional) • Certified Tester ISTQB (International Software Testing Qualifications Board) Al respecto, se solicita amablemente a la convocante, que acepte al menos una de las certificaciones deseables, y así permitir la libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas. ¿Se acepta nuestra solicitud?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
10	5. "PERSONAL REQUERIDO"	En el perfil de Especialista en Pruebas Dinámicas, se solicitan las siguientes Certificaciones: Contar con la certificación OSSTMM 3.0 Professional Security Analyst (OPSA) y deseable las siguientes certificaciones: • CEH (Certified Ethical Hacker) o CEH (Certified Ethical Hacker) Fundamental • Certificación en programa de Ciberseguridad • Certificación en Cellular Communications Forensics Consultation Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, y así permitir la	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

0013

		libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas. ¿Se acepta nuestra solicitud?	
11	5. "PERSONAL REQUERIDO"	En el perfil de Auditor de Riesgos de Seguridad, se solicitan las siguientes Certificaciones: Contar con la certificación ISO 31000 Risk Manager y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO 22301 Lead Auditor Al respecto, se solicita amablemente a la convocante, que acepte la Certificación ISO/IEC 27001 Lead Auditor y la ISO 22301 Lead Auditor emitida por un organismo certificador distinto al PECB, ya que de no ser así, se estaría limitando la libre participación de los proveedores. ¿Se acepta nuestra solicitud?	La convocante aclara que, se puede presentar la Certificación Certificación ISO/IEC 27001 Lead Auditor y la ISO 22301 Lead Auditor emitidas por un organismo certificador distinto al PECB.
12	5. "PERSONAL REQUERIDO"	En el perfil de Líder de Operación, se solicitan las siguientes Certificaciones: Contar con la certificación CNSS (Certifed Network Security Specialist) y deseable las siguientes certificaciones: • PECB Certified ISO/IEC 27035 Lead Incident Manager • ITIL v3 o v4 Foundation Certificate in IT Service Management • CSA (Certified SOC Analyst vl) • Certified ISO/IEC 27001 Al respecto, se solicita amablemente a la convocante, que acepte la Certificación ISO/IEC 27035 Lead Incident Manager emitida por un organismo certificador distinto al PECB, ya que de no ser así, se estaría limitando la libre participación de los proveedores. ¿Se acepta nuestra solicitud?	La convocante aclara que, se puede presentar la Certificación ISO/IEC 27035 Lead Incident Manager emitidas por un organismo certificador distinto al PECB.
13	5. "PERSONAL REQUERIDO"	En el perfil de Líder de Operación, se solicitan las siguientes Certificaciones: Contar con la certificación CNSS (Certifed Network Security Specialist) y deseable las siguientes certificaciones:	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

001396

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		• PECB Certified ISO/IEC 27035 Lead Incident Manager • ITIL v3 o v4 Foundation Certificate in IT Service Management • CSA (Certified SOC Analyst v1) • Certified ISO/IEC 27001 Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, y así permitir la libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas. ¿Se acepta nuestra solicitud?	
14	5. "PERSONAL REQUERIDO"	En el perfil de Especialista en Read Team, se solicitan las siguientes Certificaciones: Contar con la certificación Certified Ethical Hacker y deseable las siguientes certificaciones: • Certified OSSTMM 3.0 Professional Security Analyst OPSA • Offensive Security Certified Professional OSCP • CompTIA Security+ ce • GIAC Certified Instrusion Analyst Al respecto, se solicita amablemente a la convocante, que acepte al menos dos de las certificaciones deseables, y así permitir la libre participación de los proveedires, debido a que en el mercado difícilmente se encuentran recursos que tengan dichas certificaciones juntas. ¿Se acepta nuestra solicitud?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: CONSULTORÍA ESTRATÉGICA Y COACHING, S. DE R.L. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"

Nº	RUBRO ESPECÍFICO DEL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	I).- RUBRO CAPACIDAD DEL LICITANTE B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE	En la tabla de puntos y porcentajes especifica la siguiente distribución, para un total de 12 puntos: I | B) SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO, POR PARTE DEL LICITANTE. | 12 1.- CAPACIDAD DE LOS RECURSOS ECONÓMICOS | 2 2.- CAPACIDAD DE EQUIPAMIENTO | 10	La convocante aclara que para la asignación de la puntos del B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE deberá referirse a la MODIFICACIÓN 9 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

001355

		Se solicita atenatamente a la convocante indicar cual es la asignación correcta de puntos en el subrubro?, ya que en el detalle tiene una distribución de 2 puntos a la Capacidad de los Recursos Económicos, 9 puntos a la Capacidad de Equipamiento y 1 punto a la Certificación del FIRST.	
2	I).- RUBRO CAPACIDAD DEL LICITANTE B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	En este Subrubro se solicita que el licitante deberá acreditar en su propuesta técnica lo siguiente: • Si acredita el total del equipamiento obtendrá 2 puntos: ▪ Licenciamiento de análisis de vulnerabilidades ▪ Licenciamiento de Inteligencia de amenazas ▪ Licenciamiento de un HelpDesk especializado en atención de incidentes de ciberseguridad ▪ Licenciamiento de EDR (Endpoint Detection and Response) Al respecto, dichas licencias no se especifican como un requerimiento dentro del Anexo 1 - Anexo Técnico. En este sentido, es correcto entender que en la Matriz de Puntos y Porcentajes no se deben solicitar componentes para evaluación si no están descritos claramente en el Anexo 1 - Anexo Técnico. ¿Es correcta nuestra apreciación?	El licitante deberá acreditar en su propuesta técnica que cuenta con el equipo suficiente para la prestación del servicio.
3	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Administrador del proyecto	Dice: Contar con las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Senior Lead Auditor • COBIT 5 Foundation Examination, acreditado por ISACA • ITIL V3 o V4 Foundation Certificate in IT Service Management • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
4	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con	Dice: Contar con las siguientes certificaciones: • CISA - Certified Information Systems Auditor • CISM - Certified Information Security Manager	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

001394

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	los conocimientos académicos o profesionales del personal TABLA B Especialista en cumplimiento	• CDPSE - Certified Data Privacy Solutions Engineer y CGEIT - Certified in the Governance of Enterprise IT ó TOGAF (The Open Group Arquitecture Framework) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	
5	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Líder técnico de ciberseguridad	Dice: Contar con las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager • CISA (Certified Information Systems Auditor) • CISM (Certified Information Security Manager) • CISSP (Certified Information Systems Security Professional) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
6	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Auditor de ciberseguridad	Dice: Contar con las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PMP (Project Management Professional) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
7	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con	Dice: Contar con las siguientes certificaciones: • CompTIA Security+ ce, EC -Council Certified Ethical Hacker (Master), EC -Council Certified Ethical Hacker (Practical),	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200: www.gob.mx/banobras

	los conocimientos académicos o profesionales del personal TABLA B Líder técnico de seguridad en sistemas	PECB ISO/IEC 27032 Lead Cybersecurity Manager ó EC - Council Certified Ethical Hacker • Certified OSSTMM 3.0 Professional Security Analyst OPSA ó CIH (Certified Incident Handler) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	
8	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Especialista en pruebas estáticas	Dice: Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con la certificación CompTIA Security+ ce y deseable las siguientes certificaciones: • CISP (Certified Information System Security Professional) • Certified Tester ISTQB (International Software Testing Qualifications Board) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
9	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Especialista en pruebas dinámicas	Dice: Contar con las siguientes certificaciones: • CEH (Certified Ethical Hacker) o CEH (Certified Ethical Hacker) Fundamental • Certificación en programa de Ciberseguridad • Certificación en Celullar Communications Forensics Consultation Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

001392

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

10	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Auditor de riesgos de seguridad	Dice: Contar con las siguientes certificaciones: • PECB Certified ISO/IEC 27001 Lead Auditor • PECB Certified ISO 22301 Lead Auditor Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
11	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Analistas de seguridad	Dice: Contar con las siguientes certificaciones: Certified Incident Handler (CIH) Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación? ¿Es correcta nuestra apreciación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
12	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Líder de operación	Dice: Contar con las siguientes certificaciones: • PECB Certified ISO/IEC 27035 Lead Incident Manager • ITIL v3 o v4 Foundation Certificate in IT Service Management • CSA (Certified SOC Analyst v1) • Certified ISO/IEC 27001 Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
13	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal	Dice: Contar con las siguientes certificaciones: • GIAC Reverse Engineering Malware (GREM) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Intrusion Analyst	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

0013

26

	TABLA B Líder técnico de Red Team	Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación?	
14	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Líder técnico de Red Team	Dice: Contar con las siguientes certificaciones: • Certified OSSTMM 3.0 Professional Security Analyst OPSA • Offensive Security Certified Professional OSCP • CompTIA Security+ ce • GIAC Certified Instrusion Analyst Al respecto y conforme a lo indicado en el anexo técnico como certificaciones deseables, ¿es correcto entender que se cumple este perfil con al menos una certificación?	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
15	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal	Dice: No se otorgará puntaje cuando: • El Licitante omita presentar la documentación requerida. • La documentación sea entregada de forma parcial, ilegible o su contenido no permita acreditar el dominio de herramientas relacionadas con el servicio, solicitado por la convocante. • La documentación presentada se encuentre a nombre de otra persona. • *Un recurso humano cubra 2 o más perfiles.* Al respecto, se solicita amablemente a la convocante, que acepte que un recurso humano pueda cubrir más de dos perfiles. ¿Se acepta nuestra solicitud?	NO SE ACEPTA SU SOLICITUD, No es posible que un recurso humano cubra 2 perfiles, ya que cada recurso con su perfil esta asignado a un servicio en particular (S1, S2, S3, S4 y S5), el cubrir un recurso 2 perfiles implica tener una persona participando en 2 servicios lo que implicaría una degradación en el servicio y no cumpliría con lo establecido en el Anexo Técnico numeral "5. Personal Requerido".

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: TIC DEFENSE, S. A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"

Nº	NÚMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	5. "PERSONAL REQUERIDO", COMPONENTE S1, S2, S3, S4 Y S5, PERFIL "ADMINISTRADOR DEL PROYECTO"	LA CONVOCANTE solicita contar con la certificación PMP (Project Management Professional), se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación SCRUM MASTER derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, NO SE ACEPTA SU SOLICITUD, derivado a que el nivel de especialización y enfoques de la metodología de ambas certificaciones son diferentes.

001390

2	5. "PERSONAL REQUERIDO", COMPONENTE S1, S2, S3, S4 Y S5, PERFIL "ESPECIALISTA EN CUMPLIMIENTO"	LA CONVOCANTE solicita contar con la certificación CRISC - Certified in Risk and IS Control, se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación CISSP (Certified Information Systems Security Professional) derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, NO SE ACEPTA SU SOLICITUD, derivado a que el nivel de especialización de las certificaciones es diferente.
3	5. "PERSONAL REQUERIDO", COMPONENTE S1, S2, S3, S4 Y S5, PERFIL "AUDITOR DE CIBERSEGURIDAD"	LA CONVOCANTE establece como una de las certificaciones deseables la certificación: PECB Certified ISO/IEC 27001 Lead Auditor, se solicita amablemente a LA CONVOCANTE que pueda considerar para el cumplimiento del perfil no solo la certificación PECB Certified ISO/IEC 27001 Lead Auditor sino también aceptar para su cumplimiento la certificación PECB Certified ISO 22301 Lead Implementer, derivado a que la certificación principal requerida del perfil pertenece al área de especialidad de la ISO 22301 continuidad del negocio y por lo tanto se fortalece incluso la especialización de ciberseguridad requerida en el perfil. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación PECB Certified ISO/IEC 27001 Lead Auditor ó la certificación PECB Certified ISO 22301 Lead Implementer.
4	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS"	LA CONVOCANTE establece las siguientes certificaciones deseables del perfil: - CompTIA Security+ ce, EC -Council Certified Ethical Hacker (Master), EC - Council Certified Ethical Hacker (Practical), PECB ISO/IEC 27032 Lead Cybersecurity Manager ó EC -Council Certified Ethical Hacker Es correcto entender que solo la certificación PECB ISO/IEC 27032 Lead Cybersecurity Manager puede ser cumplida y/o sustituida de igual manera por la certificación EC - Council Certified Ethical Hacker y no todas las anteriores. FAVOR DE PRONUNCIARSE AL RESPECTO	La convocante aclara que para las certificaciones deseables se podrá presentar alguna de las siguientes certificaciones: CompTIA Security+ ce, EC -Council Certified Ethical Hacker (Master), EC -Council Certified Ethical Hacker (Practical), PECB ISO/IEC 27032 Lead Cybersecurity Manager ó EC -Council Certified Ethical Hacker Y para las siguientes certificaciones deseables alguna de las siguientes certificaciones: Certified OSSTMM 3.0 Professional Security Analyst OPSA ó CIH (Certified Incident Handler)
5	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "ESPECIALISTA EN PRUEBAS ESTÁTICAS"	LA CONVOCANTE solicita contar con la certificación CompTIA Security+ ce, se solicita amablemente a LA CONVOCANTE que pueda considerar para el cumplimiento del perfil no solo la certificación CompTIA Security+ ce sino también aceptar la certificación CompTIA Network+ ce, derivado a que ambas pertenecen a la misma rama de especialización y ven áreas de seguridad similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación CompTIA Security+ ce ó la certificación CompTIA Network+ ce.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México. 01219. Tel: 5270 1200. www.gob.mx/banobras

6	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "ESPECIALISTA EN PRUEBAS DINÁMICAS"	LA CONVOCANTE solicita contar con la certificación Certified OSSTMM 3.0 Professional Security Analyst (OPSA), se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación Certified ISO/IEC 27001 Lead Auditor derivado a que ambas certificaciones tienen como marco rector la seguridad de la información. ¿ACEPTA LA CONVOCANTE?	No se acepta respuesta, las dos certificaciones ven especialidades distintas y esto puede decrementar la especialización del servicio.
7	5. "PERSONAL REQUERIDO", COMPONENTE S3, PERFIL "AUDITOR DE RIESGOS DE SEGURIDAD"	Se entiende que, en el Título o Cédula al referirse como área de especialización a la administración, se entiende que se puede cumplir con áreas administrativas de la licenciatura y no necesariamente áreas técnicas. ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	La convocante aclara que los perfiles del personal propuesto deberán contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Es correcto su entendimiento, pueden ser áreas administrativas o técnicas.
8	5. "PERSONAL REQUERIDO", COMPONENTE S4, PERFIL "ANALISTAS DE SEGURIDAD"	LA CONVOCANTE solicita contar con la certificación Certified CSA (Certified SOC Analyst vl) para el perfil, se solicita a LA CONVOCANTE que pueda considerar amablemente para el cumplimiento del perfil no solo aceptar la certificación Certified CSA (Certified SOC Analyst vl) sino también se pueda aceptar la certificación CEH (Certified Ethical Hacker) para el cumplimiento del perfil, derivado a que ambas certificaciones consideran áreas de seguridad similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación Certified CSA (Certified SOC Analyst vl) ó la certificación CEH (Certified Ethical Hacker).
9	5. "PERSONAL REQUERIDO", COMPONENTE S4, PERFIL "LÍDER DE OPERACIÓN"	LA CONVOCANTE solicita contar con la certificación CNSS (Certifed Network Security Specialist), se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación CEH (Certified Ethical Hacker) derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	No se acepta la propuesta, las certificaciones no son equivalentes en especialidad y esto puede comprometer la especialización del servicio

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: TIC DEFENSE, S. A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"

Nº	RUBRO ESPECÍFICO DEL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 1.- Experiencia en asuntos relacionados con la materia del servicio por parte del personal Especialista en cumplimiento	Se solicita a LA CONVOCANTE acepte que la experiencia del perfil sea cumplida desde los 3 años de experiencia y no solo a partir de los 4 años. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, que se podrá presentar una experiencia de 4 (cuatro) años o más.

091338

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

2	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Administrador del proyecto	LA CONVOCANTE solicita contar con la certificación PMP (Project Management Professional), se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación SCRUM MASTER derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, NO SE ACEPTA SU SOLICITUD, derivado a que el nivel de especialización y enfoques de la metodología de ambas certificaciones son diferentes.
3	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Especialista en cumplimiento	LA CONVOCANTE solicita contar con la certificación CRISC - Certified in Risk and IS Control, se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación CISSP (Certified Information Systems Security Professional) derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, NO SE ACEPTA SU SOLICITUD, derivado a que el nivel de especialización de las certificaciones es diferente.
4	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Especialista en pruebas estáticas	LA CONVOCANTE solicita contar con la certificación CompTIA Security+ ce, se solicita amablemente a LA CONVOCANTE que pueda considerar para el cumplimiento del perfil no solo la certificación CompTIA Security+ ce sino también aceptar la certificación CompTIA Network+ ce, derivado a que ambas pertenecen a la misma rama de especialización y ven áreas de seguridad similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación CompTIA Security+ ce ó la certificación CompTIA Network+ ce.
5	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Especialista en pruebas dinámicas	LA CONVOCANTE solicita contar con la certificación Certified OSSTMM 3.0 Professional Security Analyst (OPSA), se solicita amablemente a LA CONVOCANTE aceptar en sustitución la certificación Certified ISO/IEC 27001 Lead Auditor derivado a que ambas certificaciones tienen como marco rector la seguridad de la información. ¿ACEPTA LA CONVOCANTE?	No se acepta respuesta, las dos certificaciones ven especialidades distintas y esto puede decrementar la especialización del servicio.
6	I).- RUBRO CAPACIDAD DEL LICITANTE	Se entiende que, en el Título o Cédula al referirse como área de especialización a la administración, se entiende que se puede	La convocante aclara que los perfiles del personal propuesto deberán contar con Título o Cédula profesional de Ingeniería

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

05138

	A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Auditor de riesgos de seguridad	cumplir con áreas administrativas de la licenciatura y no necesariamente áreas técnicas. ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	o licenciatura en sistemas computacionales, administración o afín. Es correcto su entendimiento, pueden ser áreas administrativas o técnicas.
7	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Analistas de seguridad	LA CONVOCANTE requiere contar con la certificación Certified CSA (Certified SOC Analyst VI) para el perfil, se solicita a LA CONVOCANTE *que pueda considerar amablemente para el* cumplimiento del perfil no solo aceptar la certificación Certified CSA (Certified SOC Analyst VI) sino también se pueda aceptar la certificación CEH (Certified Ethical Hacker) para el cumplimiento del perfil, derivado a que ambas certificaciones consideran áreas de seguridad similares. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación Certified CSA (Certified SOC Analyst VI) ó la *certificación CEH (Certified Ethical Hacker).*
8	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Líder de operación	LA CONVOCANTE solicita contar con la certificación CNSS (Certifed Network Security Specialist), se solicita amablemente a LA CONVOCANTE aceptar en su sustitución la certificación CEH (Certified Ethical Hacker) derivado a que ambas certificaciones son similares. ¿ACEPTA LA CONVOCANTE?	No se acepta la respuesta, las certificaciones no son equivalentes en especialidad y esto puede comprometer la especialización del servicio.
9	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Auditor de ciberseguridad	LA CONVOCANTE establece como una de las certificaciones deseables la certificación: PECB Certified ISO/IEC 27001 Lead Auditor, se solicita amablemente a LA CONVOCANTE *que* pueda considerar para el cumplimiento del perfil no solo la certificación PECB Certified ISO/IEC 27001 Lead Auditor sino también aceptar para su cumplimiento la certificación PECB Certified ISO 22301 Lead Implementer, derivado a que la certificación principal requerida del perfil pertenece al área de especialidad de la ISO 22301 continuidad del negocio y por lo tanto se fortalece incluso la especialización de ciberseguridad requerida en el perfil. ¿ACEPTA LA CONVOCANTE?	La convocante aclara que, para este perfil se podrá presentar la certificación PECB Certified ISO/IEC 27001 Lead Auditor ó la *certificación PECB Certified ISO 22301 Lead Implementer..*
10	I).- RUBRO CAPACIDAD DEL LICITANTE	LA CONVOCANTE establece las siguientes certificaciones deseables del perfil:	La convocante aclara que para las certificaciones deseables se podrá presentar alguna de las siguientes certificaciones:

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Líder técnico de seguridad en sistemas	• CompTIA Security+ ce, EC - Council Certified Ethical Hacker (Master), EC -Council Certified Ethical Hacker (Practical), PECB ISO/IEC 27032 Lead Cybersecurity Manager ó EC - Council Certified Ethical Hacker Es correcto entender que solo la certificación PECB ISO/IEC 27032 Lead Cybersecurity Manager puede ser cumplida y/o sustituida de igual manera por la certificación EC -Council Certified Ethical Hacker y no por todas las anteriores. FAVOR DE PRONUNCIARSE AL RESPECTO	CompTIA Security+ ce, EC -Council Certified Ethical Hacker (Master), EC -Council Certified Ethical Hacker (Practical), PECB ISO/IEC 27032 Lead Cybersecurity Manager ó EC -Council Certified Ethical Hacker. Y para la siguiente certificación deseable alguna de las siguientes certificaciones: Certified OSSTMM 3.0 Professional Security Analyst OPSA ó CIH (Certified Incident Handler).
11	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B Especialista en pruebas estáticas	LA CONVOCANTE solicita contar con la certificación CompTIA Security+ ce, esta ya se solicita en el mismo perfil en la TABLA A, favor de aclarar si con el cumplimiento de la tabla A respecto a esta certificación se cumple, independientemente de cumplir con las certificaciones deseables. FAVOR DE PRONUNCIARSE AL RESPECTO	La convocante aclara que, para este perfil de la Tabla B queda de la siguiente manera: Contar con las siguientes certificaciones: •CISP (Certified Information System Security Professional) •Certified Tester ISTQB (International Software Testing Qualifications Board)
12	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B	LA CONVOCANTE no establece los criterios de evaluación ni la asignación de puntos de la TABLA B FAVOR DE PRONUNCIARSE AL RESPECTO	Se procede a realizar la modificación correspondiente a la convocatoria. Para efectos de lo anterior, consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: SCITUM, S.A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON LA CONVOCATORIA

Nº	NÚMERAL ESPECÍFICO DE LA CONVOCATORIA	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	1.5. Idioma en que se deberán presentar las proposiciones	Se solicita atentamente a la Convocante, permita que, para el caso de certificados de empresa o personal, sean presentados en copia simple tal y como se emiten por las casas certificadoras sin necesidad de una traducción. ¿Se acepta nuestra propuesta?	La convocante acepta que sean presentadas en copia simple las certificaciones tal y como son emitidas por los entes certificadores.
2	ANEXO 11 MANIFESTACIÓN DE LA ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES)	Se solicita atentamente a la Convocante, que, para el caso del escrito de estratificación Anexo 12, los licitantes que no están catalogados en el segmento de MIPYME, basta que presenten dicho anexo con la manifestación de que son una empresa GRANDE. De lo contrario favor de aclarar.	Se acepta su solicitud.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

32

3	GENERAL	Se solicita a la convocante compartir los documetnos de bases y respuesta de Junta de Aclaraciones en formato Word. ¿Se acepta nuestra propuesta?	No se acepta su propuesta, toda la documentación que derive de la junta de aclaraciones a la convocatoria del procedimiento de contratación será puesta a disposición de los interesados en formato *PDF*, ya que la misma forma parte integrante del acta/aviso con las firmas y rúbricas autógrafas de los asistentes.

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: SCITUM, S.A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"

Nº	NÚMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	4. "REQUERIMIENTOS", "S1 - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD"	¿Podría especificar la convocante si es correcto inferir que los analisis de vunerabilidades ejecutados de manera trimestral será realizado a la infraestructura definida en la tabla descrita dentro del alcance?	Es correcto su entender, sin embargo, la infraestructura tecnológica de Banobras puede ser sustituida, actualizada o incrementada en volumen por lo que la tabla solo es enunciativa más no limitativa en su alcance.
2	4. "REQUERIMIENTOS", "S1 - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD"	¿Podria especificar la convocante la cantidad de estimada de objetivos (Sistemas de banobras, equipos de seguridad, servidores, etc.) que se tienen que considerar por prueba, tanto para la prueba en el perímetro de internet como la prueba en el interior de BANOBRAS?	La convocante comparte un aproximado de la información solicitada, sin embargo, la información completa será proporcionada al licitante ganador. **Objetivo** — **Cantidad Aproximada** Servidores — 498 Base de Datos — 313 WAN — 147 LAN — 266 Equipos de cómputo — 1,736
3	4. "REQUERIMIENTOS", "S2 – REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD DE SISTEMAS", "PRUEBAS ESTÁTICAS DE SEGURIDAD DEL CÓDIGO" Y "PRUEBAS DINÁMICAS DE SISTEMAS"	Se le solicita la convocante precise y aclare: ¿Cuántas aplicaciones y sistemas deben ser considerados para realizar la pruebas estaticas y dinamicas? ¿Cuál es la periodicidad en la cual serán ejecutas las pruebas estaticas y dinamicas?	La convocante aclara que serán 60 (sesenta) aplicaciones aproximadamente, y las pruebas estáticas y dinámicas se realizan de forma mensual.
4	4. "REQUERIMIENTOS", "S2 – REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD DE SISTEMAS", "PRUEBAS ESTÁTICAS DE SEGURIDAD DEL CÓDIGO" Y "PRUEBAS DINÁMICAS DE SISTEMAS"	Con la finalidad de que todos los participantes tengan claridad y puedan dimensionar el esfuerzo correspondiente, se le solicita a la convocante precise y aclare: ¿Cuál es la cantidad promedio de lineas de codigo que se deben analizar? ¿Cuál es la cantidad promedio de vistas que deberán ser consideradas para las pruebas dinamicas?	La convocante aclara que esta información será proporcionada al licitante ganador conforme se realicen las pruebas mensuales, ya que cada aplicación varía en el número de líneas de código.
5	4. "REQUERIMIENTOS", "S3 - REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL ECOSISTEMA DE LOS	Con la finalidad de que todos los participantes tengan claridad y puedan dimensionar los servicios requeridos, se le solicita a la convocante precise y aclare, ¿Cuántos servidores de directorio activo deben ser monitoreados?	La convocante aclara que son 4 (cuatro) controladoras de dominio.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	SISTEMAS", "HERRAMIENTA DE MONITOREO Y VALIDACIÓN DE CAMBIOS DEL DIRECTORIO ACTIVO"		
6	4. "REQUERIMIENTOS", "S3 - REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL ECOSISTEMA DE LOS SISTEMAS", "HERRAMIENTA DE MONITOREO Y VALIDACIÓN DE CAMBIOS DEL DIRECTORIO ACTIVO"	¿Podría especificar la convocante si es correcto inferir que en caso de que se requiera instalar un agente para realizar el monitoreo y validación de cambios en el directorio activo la convocante brindará las facilidades para instalarlo?	La convocante aclara que es correcto su entender.
7	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365", "HERRAMIENTAS DE MONITOREO Y CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD"	Se le solicita a la convocante precise y aclare, ¿es correcto inferir que la herramienta actual es propiedad de su proveedor actual?	La convocante aclara que, no se cuenta actualmente con un proveedor que preste el servicio del objeto de esta licitación ni con el licenciamiento mencionado.
8	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365", "HERRAMIENTAS DE MONITOREO Y CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD"	En caso de que la convocante requiera que el licitante ganador provea e implemente una solución de SIEM o XDR, solicitamos precise y aclare, ¿Cuál es la cantidad de de eventos por segundo que se deben considerar, así como la cantidad de fuentes de información que deben ser integradas a dichas soluciones propuestas?	La convocante aclara que, la cantidad es superior a 100,000 (cien mil) eventos por segundo, consumiendo diferentes fuentes de indicadores de compromiso y de mitre att&ck.
9	4. "REQUERIMIENTOS", "S5 - MODELADO DE ADVERSARIO BLUE-TEAM RED-TEAM DE MANERA MENSUAL"	¿Podría especificar la convocante si es correcto inferir que de manera mensual se deberán ejecutar diferentes misiones por cada mes, considerando 15 meses?	La convocante aclara que es correcto su entender.
10	4. "REQUERIMIENTOS", "S3 - REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL ECOSISTEMA DE LOS SISTEMAS" Y "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA	Con la finalidad de que todos los participantes tengan claridad de los tiempos de implementación de las herramientas, se le solicita a la convocante precise y aclare ¿Cuántos días se tienen para realizar la implementación de las herramientas solicitadas en el punto S3 - Reducción de la superficie de ataque del ecosistema de los sistemas y S4 - Mejora y madurez de los	La convocante aclara que se contará con un periodo de 15 (quince) días hábiles para su instalación, configuración y puesta en operación.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365"	sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365?	
11	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365"	¿Podría especificar la convocante si es correcto inferir que los participantes deberán de realizar la desinstalación del EDR actual?	La convocante aclara que el sistema de antivirus no lo administra el área de seguridad, por lo que no es parte de la presente licitación.
12	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365", "CACERÍA DE AMENAZAS Y MODELADO DE ADVERSARIO DE ACUERDO A LA MATRIZ MITRE ATT&CK"	¿Podria precisar la convocante la cantidad de vlan´s actuales de la red interna que se deben considerar para la caza de amenazas en la red?	la convocante aclara que, esta información será proporcionada al licitante ganador.
13	5. "PERSONAL REQUERIDO"	¿Podria especifcar la convocante si es correcto inferir que el personal listado debe estar operando y desempeñando sus funciones en las instalaciones de la convocante?	La convocante aclara que, solo el personal requerido en el apartado S4 - Mejora y madurez de los sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365 en donde se establece el Personal en sitio en esquema 24x7x365.
14	5. "PERSONAL REQUERIDO"	¿Podría especificar la convocante las adecuaciones que otorgara como tal la convocante al personal en sitio (por ejemplo silla, nodo de red, monitor, diadema, etc.)?	La convocante aclara que, solo se asignará espacio físico y suministro eléctrico, todo el inmueble y equipo tecnológico necesario para prestar el servicio en óptimas condiciones deberá ser suministrador por el licitante ganador.
15	4. "REQUERIMIENTOS", "S1 - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD", "ANÁLISIS DE VULNERABILIDADES"	La convocante describe: El alcance de las pruebas incluye: · Infraestructura de telecomunicaciones. · Servidores de Aplicaciones y base de datos · Sistemas · Muestreo de Equipos de cómputo de usuarios. Se solicita a la convocante compartir un número aproximado de dispositivos de cada rubro. Esto con el objetivo de poder hacer un dimensionamiento costo-beneficio lo más adecuado posible.	La convocante comparte un aproximado de la información solicitada, sin embargo, la información completa será proporcionada al licitante ganador. **Objetivo** / **Cantidad Aproximada** Servidores: 498 Base de Datos: 313 WAN: 147 LAN: 266 Equipos de cómputo: 1,736

00136

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

16	4. "REQUERIMIENTOS", "S2 – REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD DE SISTEMAS", "APOYO PARA SOLVENTAR VULNERABILIDADES"	Se solciita a la convicante aclarar si es que las remedicaicón de vulnerabilidades debe ser considerada y realizada por el licitante o las realizará la convocante.	La convocante aclara que será realizada por Banobras.
17	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365", "PERSONAL EN SITIO EN ESQUEMA 24X7X365"	La convocante describe: "al menos una posición permanente con personas certificadas, permitiendo realizar el monitoreo de la herramienta y la atención de cualquier evento o incidente de seguridad." Se solicita a la convocante precisar el horario laboral requerido para la persona en sitio solicitada.	La convocante aclara que el personal en sitio deberá estar en un esquema 24x7x365, pudiendo ingresar en los horarios de 7:00 a 23:00 horas.
18	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365", "SERVICIO DE ANALÍTICA DE ATAQUES A SISTEMAS"	La convicante describe: "EL LICITANTE en caso de resultar ganador deberá incluir el personal, equipamiento y herramientas de software necesarias para la habilitación del servicio, así como la infraestructura de soporte." Se solicita a la convocante precisar y aclarar si es que la licitante debe considerar racks y cableado dentro de su propuesta para la instalación de la infraestructura considerada o los racks y cableado serán provistos por la convocante.	La convocante aclara que el licitante ganador deberá incluir el personal, equipamiento y herramientas de software necesarias para la habilitación del servicio, incluyendo la instalación de infraestructura, racks, cableado y todo equipamiento y accesorios para presentar el servicio en las condiciones requeridas.
19	5. "PERSONAL REQUERIDO", COMPONENTE S2, S3, S4 Y S5	Se solicita a la convocante permitir el cumplimiento de las certificaciones de cada perfil con la suma de más de 1 recurso humano.	No se acepta su solicitud, la convocante aclara que se deberá cumplir con lo establecido en el numeral 5. "PERSONAL REQUERIDO" del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria.
20	9. "PROPUESTA ECONÓMICA"	La convocante describe: El LICITANTE deberá presentar la propuesta económica, el valor considerado para cada servicio (S1, S2, S3, S4 y S5), con una vigencia de 15 meses. Se solicita ala convocante especificar el tipo de moneda requerida para la presentación de la propuesta.	La convocante aclara que, la propuesta económica deberá ser en moneda nacional (pesos mexicanos).

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: SCITUM, S.A. DE C.V.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"

Nº	RUBRO ESPECÍFICO DEL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS	Dice: asimismo deberá adjuntar la(s) constancia(s) laborales emitidas a favor de la persona, en la que se indique el nombre de la empresa, domicilio de la empresa, periodo en el que	La convocante aclara que, no se acepta su solicitud, la solicitud del requerimiento es una forma de verificar la experiencia laboral que se comparte en el curriculum vitae.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

36

	l.- Experiencia en asuntos relacionados con la materia del servicio por parte del personal Administrador del proyecto Especialista en cumplimiento Líder técnico de ciberseguridad Auditor de ciberseguridad Líder técnico de seguridad en sistemas Especialista en pruebas estáticas Especialista en pruebas dinámicas Arquitecto de seguridad en arquitecturas a directorio activo Auditor de riesgos de seguridad Analistas de seguridad Líder de operación Líder técnico de Red Team Especialista de Red Team	laboró, puesto y/o funciones que desempeñó, fecha y firma del emisor, a fin de acreditar los años de experiencia requeridos. Se solicita a la convocante aceptar que esta información este plasmada en el CV del perfil solicitado sin necesidad de una constancia laboral ya que muchas empresas consideran esa información confidencial y no otorgan constancias laborales. De lo contrario favor de aclarar.	
2	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A TABLA B	¿Es correcto interpretar que la Tabla A y la Tabla B se refieren a los mismos perfiles pero diferentes certificaciones? De lo contrario favor de aclarar.	Es correcta su interpretación, la Tabla A y la Tabla B se refieren a los mismos perfiles, pero diferentes certificaciones.
3	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A TABLA B	¿Es correcto interpretar que la asignación máxima de puntos para los perfiles, será al cubrir el título o cédula y la certificación solicitada en la Tabla A? De lo contrario favor de aclarar.	Favor de consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
4	I).- RUBRO CAPACIDAD DEL LICITANTE	¿Es correcto interpretar que las certificaciones de la Tabla B son deseables; como lo dice el Anexo Técnico, sin embargo, no son	La convocante aclara que las certificaciones deseables establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA B	obligatorias ni se otorgarán puntos adicionales si se presentan? De lo contrario favor de aclarar.	convocatoria, son opcionales para este proceso de licitación, y para su evaluación consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
5	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 3. Dominio de herramientas relacionado con el servicio por parte del personal	¿Es correcto interpretar que las certificaciones o diplomas pueden ser de cualquier entidad especialista en estas soluciones? De lo contrario favor de aclarar.	La convocante aclara que, las certificaciones o diplomas pueden ser de cualquier entidad que pueda emitirlas, siempre y cuando sean similares.
6	I).- RUBRO CAPACIDAD DEL LICITANTE B). - SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	¿Es correcto interpretar que la información como precios o costos, u otra información confidencial podrá ser testada? De lo contrario favor de aclarar.	La convocante aclara que, la información para acreditar la propiedad del equipo y/o herramientas será con copia simple de las facturas o instrumento contractual que acredite su uso, goce y disfrute con el que garantice que cubre el periodo de la vigencia del servicio, así mismo, podrá ser testada la información de precios o costos.
7	I).- RUBRO CAPACIDAD DEL LICITANTE B). - SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	Dice: Al licitante que presente la evidencia documental de contar con el Certificado de membresia FIRST (Forum of Incident Response and Security Teams). Se le otorgarán 1 punto. ¿Es correcto interpretar que este punto es independiente al del equipo suficiente para la prestación del servicio? De lo contrario favor de aclarar.	Favor de consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
8	I).- RUBRO CAPACIDAD DEL LICITANTE C). - SUBRUBRO PARTICIPACIÓN DE PERSONAS CON DISCAPACIDAD O EMPRESAS QUE CUENTEN CON TRABAJADORES CON DISCAPACIDAD	¿Es correcto interpertar que en caso de que mi representada no cuente con personas con discapacidad bastará con una carta en la que se constate?	La convocante aclara que, para acreditar si cuenta o no con personal con discapacidad será a través de una carta donde se incluya la evidencia solicitada en el 1).- RUBRO CAPACIDAD DEL LICITANTE, C). SUBRUBRO PARTICIPACIÓN DE PERSONAS CON DISCAPACIDAD O EMPRESAS QUE CUENTEN CON TRABAJADORES CON DISCAPACIDAD.
9	II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE A). - SUBRUBRO EXPERIENCIA	¿Es correcto interpretar que de acuerdo con los "lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas" emitido	La convocante aclara que, para garantizar que el licitante cuente y demuestre la experiencia, la especialidad y las competencias requeridas en los servicios y soluciones

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

32

	B). – SUBRUBRO ESPECIALIDAD	el 9 de septiembre de 2010 en el Diario Oficial de la Federación, se pueden presentar contratos cuya vigencia no supere los 10 años de antigüedad? De lo contrario favor de aclarar.	establecidas en el ANEXO TÉCNICO, es necesario cumplir con lo establecido en el II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE, A). - SUBRUBRO EXPERIENCIA y B). – SUBRUBRO ESPECIALIDAD Por lo que solo se considerarán los contratos en el periodo establecido en el II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE.
10	IV) RUBRO CUMPLIMIENTO DE CONTRATOS A). - CUMPLIMIENTO SATISFACTORIO DE CONTRATOS	¿Es correcto interpretar que de acuerdo con los "lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas" emitido el 9 de septiembre de 2010 en el Diario Oficial de la Federación, se pueden presentar contratos cuya vigencia no supere los 10 años de antigüedad? De lo contrario favor de aclarar.	La convocante aclara que, para garantizar que el licitante cuente y demuestre la experiencia, la especialidad y las competencias requeridas en los servicios y soluciones establecidas en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, es necesario cumplir con lo establecido en el IV) RUBRO CUMPLIMIENTO DE CONTRATOS, A). - CUMPLIMIENTO SATISFACTORIO DE CONTRATOS. Por lo que solo se considerarán los contratos en el periodo establecido en el IV) RUBRO CUMPLIMIENTO DE CONTRATOS.
11	II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE A). - SUBRUBRO EXPERIENCIA B). – SUBRUBRO ESPECIALIDAD	¿Es correcto interpretar que se aceptarán convenios modificatorios de los contratos? De lo contrario favor de aclarar	La convocante aclara que, es correcto su entender, siempre y cuando se presente formalizado como un instrumento contractual.
12	IV) RUBRO CUMPLIMIENTO DE CONTRATOS A). - CUMPLIMIENTO SATISFACTORIO DE CONTRATOS	¿Es correcto interpretar que se aceptarán convenios modificatorios de los contratos? De lo contrario favor de aclarar.	La convocante aclara que, es correcto su entender, siempre y cuando se presente formalizado como un instrumento contractual.
13	II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE A). - SUBRUBRO EXPERIENCIA B). – SUBRUBRO ESPECIALIDAD	¿Es correcto entender que en caso de contar con contratos con convenios modificatorios que se encuentren en el periodo solicitado podrá ser contabilizado como 1 contrato, aunque su suscripción haya sido antes del 2018? De lo contrario favor de aclarar.	La convocante aclara que, es correcto su entender, solo se contabilizarán los meses que se encuentren dentro del periodo requerido, aunque la formalización del contrato sea antes del mismo.
14	IV) RUBRO CUMPLIMIENTO DE CONTRATOS A). - CUMPLIMIENTO SATISFACTORIO DE CONTRATOS	¿Es correcto entender que en caso de contar con contratos con convenios modificatorios que se encuentren en el periodo solicitado podrá ser contabilizado como 1 contrato, aunque su suscripción haya sido antes del 2018? De lo contrario favor de aclarar.	La convocante aclara que, es correcto su entender, solo se contabilizarán los meses que se encuentren dentro del periodo requerido, aunque la formalización del contrato sea antes del mismo.
15	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con	Se solicita a la convocante permita presentar certificados ISO de otra entidad certificadora distinta a PECB, toda vez que tienen validez y reconocimiento a nivel internacional, ¿Se acepta nuestra propuesta?	La convocante aclara que, se podrán presentar certificados ISO de otras entidades certificadoras.

GG13736

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	los conocimientos académicos o profesionales del personal TABLA A TABLA B		
16	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A TABLA B	Se solicta a la convicante otorgar el máximo de puntos en los perfiles presentando únicamente las certificaciones mencionadas en la tabla A y dejando como desables las de la tabla B, como se menciona en el anexo técnico. ¿Se acepta nuestra propuesta?	La convocante aclara que, no se acepta su propuesta, favor de referirse a la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
17	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A TABLA B	De ser negativa la respuesta anterior, se solicita presentar solo una certificación por perfil de la tabla B. ¿Se acepta nuestra propuesta?	La convocante aclara que, no se acepta su propuesta, favor de referirse a la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
18	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 1.- Experiencia en asuntos relacionados con la materia del servicio por parte del personal	La convicante describe: "deberá adjuntar la(s) constancia(s) laborales emitidas a favor de la persona, en la que se indique el nombre de la empresa, domicilio de la empresa, periodo en el que laboró, puesto y/o funciones que desempeñó, fecha y firma del emisor, a fin de acreditar los años de experiencia requeridos.". Se solicita a la convocante eliminar este requerimineto y pueda ser cubierto con la entrega de CV y la descripción de los puestos que el personal ha ocupado. Esto porque a razón de que el personal no cuente con dicha constancia; su solicitud, aprobación y firma puede superar el tiempo de entrega de propuestas.	La convocante aclara que, no se acepta su solicitud, la solicitud del requerimiento es una forma de verificar la experiencia laboral.
19	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal	Certificación OSWP (Offensive Security Wireless Professional). Se solicita a la convocante aceptar certificaciones que pueden ser equivalentes o similares.	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	TABLA A Líder técnico de seguridad en sistemas		
20	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Analistas de seguridad	Certificación CSA (Certified SOC Analyst). Se solicita a la convocante aceptar certificaciones que pueden ser equivalentes o similares.	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.
21	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal TABLA A Líder de operación	Certificación CNSS (certified Network Security Specialist). Se solicita a la convocante aceptar certificaciones que pueden ser equivalentes o similares.	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.
22	I).- RUBRO CAPACIDAD DEL LICITANTE B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	La convocante describe: "Al licitante que presente la evidencia documental de las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 9001:2015 o versión superior, ISO 22307:2020 o versión superior, ISO/IEC 20000-1:2018 o versión superior e ISO 37001". Se solicita a la convocante aceptar evidencia de cumplimiento que pueden ser los certificados y/o cartas de cumplimiento de las normas, emitidas por las entidades certificadoras.	La convocante aclara que, solo deberá presentar copia simple de las certificaciones ISO solicitadas.
23	II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE A). - SUBRUBRO EXPERIENCIA	La convocante describe: "se considerará el o los contratos o pedidos celebrados con entes gubernamentales y/o empresas privadas durante el periodo del 2018 al 2022". ¿Es correcto interpretar que la convocante acepta contratos terminados y/o vigentes durante este periodo de tiempo, en el entendido de que la sumatoria de experiencia será a la fecha de presentación de propuestas?	La convocante aclara que, la sumatoria de experiencia con contratos terminados y/o vigentes será a la fecha de presentación de propuesta.
24	II) RUBRO EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE B). - SUBRUBRO ESPECIALIDAD	La convocante describe: "Presentando contratos y/o pedidos con instituciones públicas de carácter federal, estatal o municipal y/o empresas privadas durante el año 2018 al 2022 que acredite la prestación de servicios de la misma naturaleza del objeto de la presente contratación".	La convocante aclara que, la sumatoria de experiencia con contratos terminados y/o vigentes será a la fecha de presentación de propuesta.

001376

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		¿Es correcto interpretar que la convocante acepta contratos terminados y/o vigentes durante este periodo de tiempo, en el entendido de que la sumatoria de experiencia será a la fecha de presentación de propuestas?	
NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: PG RANHTOE SERVICIOS ADMINISTRATIVOS, S.A. DE C.V.			
SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"			
Nº.	NÚMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	Es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de Respuesta ante incidentes de Seguridad Computacional acreditado como CERT ante FIRST (global Fórum of Incident Response and Security Teams). En virtud de la relevancia de Banobras y su estado de seguridad, se menciona que los licitantes cuenten con un equipo de respuesta incidentes de Seguridad Computacional, acreditado como CERT ante el FIRST, sin embargo; los integrantes del FIRST para su acreditación, requieren no sólo de la verificación de sus procesos; si no te la invitación por parte de miembros, lo que excluye de su participación a otros equipos. Se sugiere a la licitante tomar como equiparable, al homólogo de la Universidad de Carnegie Mellón para su verificación; proceso que evalúa los mismos puntos para su acreditación; sin embargo, no requiere de una invitación. Lo que genera un proceso más abierto para que cualquier equipo en condiciones de postularse, sea acreditado. Así mismo, se recomienda evaluar el cumplimiento con la norma ISO:IEC 27001:2013, la cual incluye dentro de sus dominios, los puntos de verificación listados por el Common Body Knowledge del FIRST ¿Acepta LA CONVOCANTE nuestra sugerencia?, De lo contrario, favor de justificar la negativa.	Se aclara que el certificado de afiliación al FIRST (Global Forum of Incidente Response and Security Temas) no establece limitación de adhesión en ningún país para ninguna organización pública o privada que lo desee hacer en cualquier momento, evidenciando en su publicación a través de su sitio web que los últimos 2 (dos) meses del presente año se han acreditado empresas en México, por lo que NO SE ACEPTA su solicitud, todos los licitantes deberán cumplir con lo establecido en los requerimientos del numeral 4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD", del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria. Adicionalmente se hace del conocimiento a los licitantes que la Universidad de Carnegie Mellón comunicó lo siguiente: "CERT" es una marca registrada propiedad de la Universidad Carnegie Mellon. CMU ha decidido descontinuar su práctica de otorgar licencias de la marca CERT a nivel internacional. Como resultado, ya no buscaremos acuerdos de licencia fuera de los Estados Unidos. Los equipos de respuesta a incidentes de seguridad informática (CSIRT), dentro de los Estados Unidos, que comparten el compromiso de SEI de mejorar la seguridad de las redes conectadas a Internet pueden solicitar autorización para usar la marca "CERT" en sus nombres" Link de referencia: https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/index.cfm
2	5. "PERSONAL REQUERIDO"	Dentro del componente S1, S2,S3,S4,S5.- Perfil Especialista en cumplimiento, requiere lo siguiente: Contar con la certificación CRISC -Certified in Risk and IS Control y deseable las siguientes certificaciones:	No se acepta su solicitud, los licitantes deberán cumplir con lo establecido en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

0013

		• CISA - Certified Information Systems Auditor • CISM - Certified Information Security Manager • CDPSE- Certified Data Privacy Solutions Engineer • CGEIT- Certified in the Governance of Enterprise IT ó TOGAF (The Open Group Arquitecture Framework) Podría la convocante aceptar la documentación que avale la experiencia profesional en el desarrollo de las actividades soportadas por la certificación CRISC?	

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: DELOITTE ASESORÍA EN RIESGOS, S.C.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 1 "ANEXO TÉCNICO"

Nº	NUMERAL ESPECÍFICO DEL ANEXO 1 "ANEXO TÉCNICO"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	3. "ALCANCE"	En la tabla dentro de la sección 3. Alcance se especifica que hay 406 Activos. ¿Podría la Convocante especificar o detallar a que designa como "Activo" dentro de la tabla de el alcance de la Infraestructura Tecnológica?	La convocante aclara que, todo aquel componente tecnológico tangible e intangible que forma parte de las operaciones de Banobras.
2	3. "ALCANCE"	¿Existen redes inalámbricas incluidas? ¿En caso de ser afirmativo, cuantos SSID y ubicaciones físicas deberíamos considerar?	La convocante aclara que, esta información será proporcionada al licitante ganador.
3	3. "ALCANCE"	¿El muestreo se debe definir sobre los 1000 equipos de usuario final? ¿O 1000 activos es el muestreo definido por la convocante?	La convocante aclara que, 1736 (mil setecientos treinta y seis) activos es el muestreo aproximado, la información completa será proporcionada al licitante ganador.
4	3. "ALCANCE"	Podría indicar sobre las aplicaciones o sistemas: 1. ¿Tipo de aplicaciones (web, cliente-servidor, móviles)? 2. Cuántos módulos, servicios web y entradas de datos cuenta cada una? 3. Las aplicaciones se probarán con un enfoque de caja negra o se proporcionarán usuarios de acceso?	La convocante aclara que: 1.- Cliente-Servidor, Web de manera enunciativa más no limitativa. 2.- Esta información será proporcionada al licitante ganador. 3.- Se proporcionan usuarios de acceso para las pruebas dinámicas.
5	3. "ALCANCE"	¿Las pruebas se realizarán en sitio o es posible colocar un equipo del proveedor al que podamos acceder vía remota para la ejecución de las pruebas?	La convocante aclara que, las pruebas deberán realizarse en sitio, no se permiten equipos con acceso vía remota para la ejecución de las pruebas.
6	4. "REQUERIMIENTOS", "SI - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD", "ANÁLISIS DE VULNERABILIDADES"	¿Cuándo se refiere al análisis de vulnerabilidades a toda la infraestructura tecnológica, se refiere a los activos mencionados en el alcance? ¿O que universo debemos considerar?	La convocante aclara que, se refiere tánto a los activos mencionados en el ANEXO 1 "ANEXO TÉCNICO" de la convocatoria y a todos aquellos activos pertenecientes a Banobras que sean notificados durante la ejecución del servicio, siendo el alcance enunciativo más no limitativo.
7	4. "REQUERIMIENTOS", "SI - ANÁLISIS DE VULNERABILIDADES,	En caso de no poder proporcionar la información anterior, ¿se espera que en la propuesta económica se determine un umbral	La convocante aclara que, es incorrecto su entender, en la propuesta económica se deberá cotizar la totalidad del servicio sin umbrales.

Av. Javier Barros Sierra 515. Lomas de Santa Fe, Ciudad de México. 01219. Tel: 5270 1200. www.gob.mx/banobras

GU1374

	PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD", "ANÁLISIS DE VULNERABILIDADES"	de activos que permitan definir un modelo de costos de la ejecución de estos análisis de vulnerabilidades?	
8	4. "REQUERIMIENTOS", "SI - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD", "ANÁLISIS DE VULNERABILIDADES"	¿La convocante estaría en posibilidad de proporcionar un espacio de virtualización para la implementación de las herramientas de análisis? O debemos considerar el ingreso de equipos físicos y/o "appliance" para la ejecución de las pruebas?	La convocante aclara que, el licitante en caso de resultar ganador deberá incluir el personal, equipamiento y herramientas de software necesarias para la habilitación del servicio, así como la infraestructura de soporte.
9	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	Se dice:" EL LICITANTE deberá garantizar que en caso de ser adjudicado todas las herramientas, hardware, equipo de cómputo y demás dispositivos provistos por éste, que interactúen directa o indirectamente con la red de BANOBRAS se encuentran libres de virus y cualquier otra amenaza que pueda afectar los principios de seguridad de la información. Esto por medio de la firma de una carta compromiso que deberá de integrar a su propuesta técnica en la que se detallará el equipo y herramientas a utilizar en cada interacción con la red de BANOBRAS." ¿Esta carta compromiso que se debe integrar a la propuesta técnica, tiene la Convocante algún modelo de esta carta o será de libre texto a consideración del Licitante y no será causa de desechamiento de propuesta?	La convocante aclara que, la carta será de libre texto a consideración del licitante siempre y cuando enuncie lo solicitado por Banobras, su omisión será causa de desechamiento de la propuesta.
10	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	Se dice: "Se requiere que el LICITANTE cuente con las certificaciones en las siguientes normas (no será motivo de desechamiento): ISO/IEC 27001:2014, ISO 9001:2015, ISO 22301:2020, ISO/IEC 20000-1 :2020 e ISO 37001 en los siguientes procesos que están directamente relacionados con el objeto del presente Anexo Técnico". a. ¿Se puede cumplir con este requerimiento si mi representada cuenta con las certificaciones ISO/IEC 27001:2013 e ISO 22301:2019? b. Al ser esta una licitación de servicios de ciberseguridad ¿Podría la Convocante solamente considerar para la evaluación de puntos y porcentajes que la empresa Licitante tenga las certificaciones ISO 27001 y/o ISO 22301 que tienen que ver con la gestión de seguridad de la información y la gestión de continuidad de negocio?	La convocante aclara que, no se acepta su solicitud, se deberá cumplir conforme a lo establecido en el numeral 4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD", del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria, la omisión o la entrega parcial de este requisito no será motivo de desechamiento.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México. 01219. Tel: 5270 1200. www.gob.mx/banobras

11	4. "REQUERIMIENTOS", "DE LOS LICITANTES INTERESADOS EN PRESENTAR LOS SERVICIOS DE CIBERSEGURIDAD"	Se dice: "Es indispensable que todos los licitantes participantes sin excepción alguna cuenten con un equipo de Respuesta ante Incidentes de Seguridad Computacional acreditado como CERT ante FIRST (global Forum of Incident Response and Security Teams)". Al pertenecer a una Red Global dentro de Deloitte y contar con un Equipo de Respuesta ante Incidentes de Seguridad en México, estamos registrados como miembros ante el FIRST (global Forum of Incident Response and Security Teams) como Deloitte ECC, en el cual uno de los países de este 'Team' es México y cuya referencia se podrá consultar en la siguiente liga: https://www.first.org/members/teams/deloitte_ecc . ¿La Convocante nos podrá confirmar que con esto damos cabal cumplimiento a este requisito?	SE ACEPTA SU SOLICITUD, la convocante aclara que, se deberá presentar copia simple del certificado.
12	4. "REQUERIMIENTOS", "S1 - ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD"	Se dice: "El servicio deberá ser realizado en las instalaciones de BANOBRAS, para lo que esté proporcionará el espacio físico, facilidades para el acceso a la red y alimentación eléctrica. Para las pruebas de caja blanca, EL LICITANTE GANADOR deberá garantizar que el canal de comunicación cuente con todos los mecanismos de seguridad, siendo responsable EL LICITANTE GANADOR de cualquier incidente o afectación a BANOBRAS." Con esto, es factible también el de poder ejecutar este servicio S1 a través de un equipo del Licitante instalado físicamente en las instalaciones y red de BANOBRAS y que pueda ser accesado remotamente por personal del Licitante para este servicio a través de un canal de comunicación segura o VPN autorizado por BANOBRAS?	La convocante aclara que, las pruebas deberán realizarse en sitio, no se permiten equipos con acceso vía remota para la ejecución de las pruebas.
13	4. "REQUERIMIENTOS", "S2 – REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD DE SISTEMAS"	a. ¿Es correcto interpretar que el alcance de este servicio S2 - Realización periódica de análisis seguridad de sistemas será hacia las 60 Aplicaciones o Sistemas declarados en la sección 3. Alcance? b. Si no fuera así, ¿Podría amablemente la Convocante de cuantos Sistemas sería el alcance? c. ¿De cuantas líneas de código sería el análisis de cada uno de estos Sistemas o rango de líneas de código por Sistema a analizar de manera mensual?	La convocante aclara que, serán 60 (sesenta) aplicaciones aproximadamente; la información completa será proporcionada al licitante ganador.
14	4. "REQUERIMIENTOS", "S3 - REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL	Se dice: "Implementación de una herramienta de Monitoreo y Validación de cambios del directorio activo (descrito en el punto 4.4.2"	Favor de consultar la MODIFICACIÓN 6 de las modificaciones a la convocatoria.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	ECOSISTEMA DE LOS SISTEMAS"	Podría amablemente la Convocante aclarar en donde se encuentra descrito este punto 4.4.2 para la ""Implementación de una herramienta de Monitoreo y Validación de cambios del directorio activo".	
15	4. "REQUERIMIENTOS", "S4 - MEJORA Y MADUREZ DE LOS SISTEMAS DE PREVENCIÓN, CACERÍA DE AMENAZAS AVANZADAS DE CIBERSEGURIDAD EN ESQUEMA DE 24X7X365"	Se solicita un conjunto de "Herramientas de Monitoreo y cacería de amenazas avanzadas de ciberseguridad" ya sea on-site, cloud o de forma híbrida. a. Para el cumplimiento de los diferentes servicios y características de las herramientas contempladas en este punto "S4 – Mejora y madurez de los sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365", ¿La Convocante puede aceptar el cumplimiento de las características solicitadas a través de la integración de soluciones comerciales, de open source y de herramientas desarrolladas por el propio Licitante, así como de los propios servicios que proporciona en esta materia, para dar cumplimiento a cada característica o funcionalidad solicitada? b. ¿Es correcto interpretar que una de las herramientas principales para este servicio y que debe de proporcionar el Licitante Ganador es un SIEM en el cual se integre la Infraestructura tecnológica de BANOBRAS?	La convocante aclara que, es correcto su entender, pero no está acotado a un SIEM, el licitante puede proponer cualquier tecnología XDR, SIEM, SOAR, THREAT HUNTING, etc., que sea necesaria para el cabal cumplimiento de los requerimientos establecidos en el numeral S4 del ANEXO 1 "ANEXO TÉCNICO" de la convocatoria.
16	4. "REQUERIMIENTOS", "S5 - MODELADO DE ADVERSARIO BLUE-TEAM RED-TEAM DE MANERA MENSUAL"	¿Es correcto interpretar que el equipo rojo o equipo ofensivo está conformado por personal diferente al equipo azul o defensivo, que es el que proporciona los servicios del "S4 – Mejora y madurez de los sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365"?	La convocante aclara que el personal que conforma al equipo Rojo y Azul son diferentes.
17	5. "PERSONAL REQUERIDO"	¿Es posible que una persona pueda cumplir con uno o más perfiles, si cumple los requisitos solicitados por cada perfil?	No se acepta respuesta, porque el licitante podría entonces llevar un solo recurso que haga todo aunque cumpla el servicio, se debe garantizar la totalidad de los recursos de la tabla de perfiles como se establece en el anexo técnico con su nivel de especialización y experiencia.
18	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "OWSP (Offensive Security Wireless Profesional)" que solamente cubre una parte de lo solicitado para el servicio "S2 - Realización periódica de análisis seguridad de sistemas", el que este requisito de certificación se cubra con algunas de las certificaciones deseables que solicitan también para este perfil y que son: CompTIA Security+ ce, o EC -Council Certified Ethical Hacker (Master), o EC - Council Certified Ethical Hacker (Practical), o PECB ISO/IEC 27032 Lead Cybersecurity Manager, ó EC -	La convocante no acepta su solicitud, sin embargo, se aclara que las certificaciones pueden ser de cualquier entidad que pueda emitirlas, siempre y cuando sean similares.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		Council Certified Ethical Hacker, o Certified OSSTMM 3.0 Professional Security Analyst OPSA ó CIH (Certified Incident Handler) y que esto cuente también para el cumplimiento del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	
19	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "ESPECIALISTA EN PRUEBAS ESTÁTICAS"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "CompTIA Security+ ce", se cumpla este requisito de certificación con algunas de las certificaciones deseables que solicitan también para este perfil y que son: CISP (Certified Information System Security Professional), o Certified Tester ISTQB (International Software Testing Qualifications Board), o con la certificación del fabricante de alguna de las herramientas para el análisis de pruebas estáticas y que esto cuente también para el cumplimiento del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.
20	5. "PERSONAL REQUERIDO", COMPONENTE S2, PERFIL "ESPECIALISTA EN PRUEBAS DINÁMICAS"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "Certified OSSTMM 3.0 Professional Security Analyst (OPSA)", se cumpla este requisito de certificación con algunas de las certificaciones deseables que solicitan también para este perfil y que son: CEH (Certified Ethical Hacker) o CEH (Certified Ethical Hacker) Fundamental, o Certificación en programa de Ciberseguridad, o Certificación en Celular Communications Forensics Consultation y que esto cuente también para el cumplimiento del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.
21	5. "PERSONAL REQUERIDO", COMPONENTE S4, PERFIL "ANALISTAS DE SEGURIDAD"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "Certified CSA (Certified SOC Analyst v1", se cumpla este requisito de certificación con algunas de las certificaciones: Certified Incident Handler (CIH), o Certified Ethical Hacker, o con una carta bajo protesta de decir verdad firmada por representante legal que dicho profesional ha estado laborando como Analista de Seguridad en el SOC del Licitante y que esto cuente también para el cumplimiento del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	La convocante no acepta su solicitud, sin embargo, se aclara que las certificaciones pueden ser de cualquier entidad que pueda emitirlas, siempre y cuando sean similares.
22	5. "PERSONAL REQUERIDO", COMPONENTE S4, PERFIL "LÍDER DE OPERACIÓN"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "CNSS (Certifed Network Security Specialist", se cumpla este requisito de certificación con algunas de las certificaciones deseables para este perfil: PECB Certified ISO/IEC 27035 Lead Incident Manager, o ITIL v3 o v4 Foundation Certificate in IT Service Management, o CSA (Certified SOC Analyst v1), o Certified ISO/IEC 27001; ó ISO 31000 Risk Manager y que esto cuente también para el cumplimiento	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

		del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	
23	5. "PERSONAL REQUERIDO", COMPONENTE S5, PERFIL "LÍDER TÉCNICO DE RED TEAM"	¿La Convocante puede aceptar que para el cumplimiento de este perfil, en lugar de la certificación "GIAC Penetration Tester (GPEN)", se cumpla este requisito de certificación con algunas de las certificaciones deseables para este perfil: GIAC Reverse Engineering Malware (GREM), o GIAC Certified Forensic Analyst (GCFA), o GIAC Certified Intrusion Analyst; ó Offensive Security Certified Professional (OSCP) y que esto cuente también para el cumplimiento del criterio de evaluación del perfil en la matriz de puntos y porcentajes?	No se acepta la solicitud, existen certificaciones como CISA, CISM, CISSP, CEH, OSWP, entre otras, que su casa certificadora es la que desarrolló su estándar y metodología a nivel global y son estas entidades las más reconocidas y referenciadas por todos los gobiernos del mundo, no se pueden aceptar otras certificaciones similares porque no siguen los procesos estandarizados de seguridad implementados por estas casas certificadoras.
24	11. "NIVELES DE SERVICIO", COMPONENTE S3	Del primer entregable del servicio S3 que es sobre la "Memoria técnica de implementación de la herramienta con las características detalladas en la sección 'Herramienta de Monitoreo y validación de cambios del directorio activo'." Se establece que el nivel de servicio es: "Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento". ¿Esta memoria técnica se tiene que entregar cada mes o solamente es de una sola vez después de haber hecho la implementación de la herramienta?	La convocante aclara que, el entregable "Memoria técnica de implementación de la herramienta con las características detalladas en la sección 'Herramienta de Monitoreo y validación de cambios del directorio activo', deberá ser entregado una vez después de haber hecho la implementación de la herramienta por parte del licitante.
25	16. "PENAS CONVENCIONALES Y DEDUCTIVAS"	¿Es correcto interpretar que para el "Retraso en los plazos de ejecución con respecto al Plan de Trabajo por causas ajenas a BANOBRAS: 2% del costo total de los servicios no proporcionados a satisfacción por cada día hábil de retraso.", esta pena convencional por este concepto solamente se aplicaría con referencia al monto mensual del servicio que haya incurrido en este retraso?	La convocante aclara que, es correcta su interpretación.
26	16. "PENAS CONVENCIONALES Y DEDUCTIVAS"	¿Es correcto interpretar que para el "Retraso en la presentación de los entregables por causas ajenas a BANOBRAS: 2% del costo total de los servicios no proporcionados a satisfacción por cada día de retraso, dado que los entregables forman parte integral del servicio, conforme a lo establecidas en el numeral "6 Plan de trabajo, 7 Entregables y 11 Niveles de Servicio.", esta pena convencional por este concepto solamente se aplicaría con referencia al monto mensual del servicio que haya incurrido en este retraso?	La convocante aclara que, es correcta su interpretación.

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE: DELOITTE ASESORÍA EN RIESGOS, S.C.

SOLICITUDES DE ACLARACIÓN RELACIONADAS CON EL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"

Nº	RUBRO ESPECÍFICO DEL ANEXO 16 "MATRIZ DE PUNTOS Y PORCENTAJES"	SOLICITUD DE ACLARACIÓN	RESPUESTA
1	I).- RUBRO CAPACIDAD DEL LICITANTE	Se solicita adjuntar por cada perfil la(s) constancia(s) laborales emitidas a favor de la persona, en la que se indique el nombre de la empresa, domicilio de la empresa, periodo en el que	La convocante aclara que, no se acepta su solicitud, la solicitud del requerimiento garantiza la certeza de que realmente el personal cuenta con la experiencia requerida.

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

	A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 1.- Experiencia en asuntos relacionados con la materia del servicio por parte del personal.	laboró, puesto y/o funciones que desempeñó, fecha y firma del emisor, a fin de acreditar los años de experiencia requeridos. Si la persona ha trabajado previamente en otras empresas diferentes a las del Licitante ¿Adicional a la constancia laboral que emita el área de recursos humanos del Licitante, la Convocante podría aceptar como constancia el curriculum vitae firmado por este profesional en donde establezca bajo protesta de decir verdad los datos de la(s) empresa(s) donde ha trabajado anteriormente a la del Licitante y se indique el nombre de la empresa, domicilio de la empresa, periodo en el que laboró, puesto y/o funciones que desempeñó?	
2	I).- RUBRO CAPACIDAD DEL LICITANTE A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS 2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal	La asignación de puntos solo especifica cómo llegar a 3.0 puntos y no a los 6.0 puntos de este rubro. ¿Podría amablemente la Convocante aclarar cómo se pueden obtener los 6.0 puntos de este requisito?	Favor de consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.
3	I).- RUBRO CAPACIDAD DEL LICITANTE B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	Se solicita que "El licitante deberá acreditar en su propuesta técnica que cuenta con el equipo suficiente para la prestación del servicio. Debiendo acreditar la propiedad del equipo con copia simple de las facturas o instrumento contractual que acredite su uso, goce y disfrute con el que garantice que cubre el periodo de la vigencia del instrumento". Dado que el licenciamiento que se compraría por parte de la Licitante en caso de ser ganadora de esta licitación ¿La Convocante podría aceptar para cumplir este requisito el presentar cartas de los fabricantes de tecnología en la que acrediten que la Licitante es canal o partner de ellas y que puede comprar su licenciamiento para este tipo de proyectos o licitaciones?	La convocante aclara que, no se acepta su solicitud, el licitante debe garantizar que cuenta con su propia infraestructura disponible para prestar el servicio requerido.
4	I).- RUBRO CAPACIDAD DEL LICITANTE B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE 2.- CAPACIDAD DE EQUIPAMIENTO	a. ¿Podría amablemente la Convocante distribuir proporcionalmente los 7 puntos de acuerdo a la evidencia documental de cumplir con 5, ó 4, ó 3, ó 2, ó 1 de las Certificaciones requeridas? b. ¿Y que éstas certificaciones sean a la empresa Licitante de manera general para todos sus procesos de negocio y no de manera particular los 5 procesos particulares que solicitan y que limitarían la participación de empresas Licitantes en esta Licitación?	La convocante aclara que, ambas solicitudes no se aceptan, derivado a que se evaluará la especialización de procesos en ciberseguridad y no de procesos generales. Consultar la MODIFICACIÓN 8 de las modificaciones a la convocatoria.

001366

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

----------FIN DEL TEXTO----------

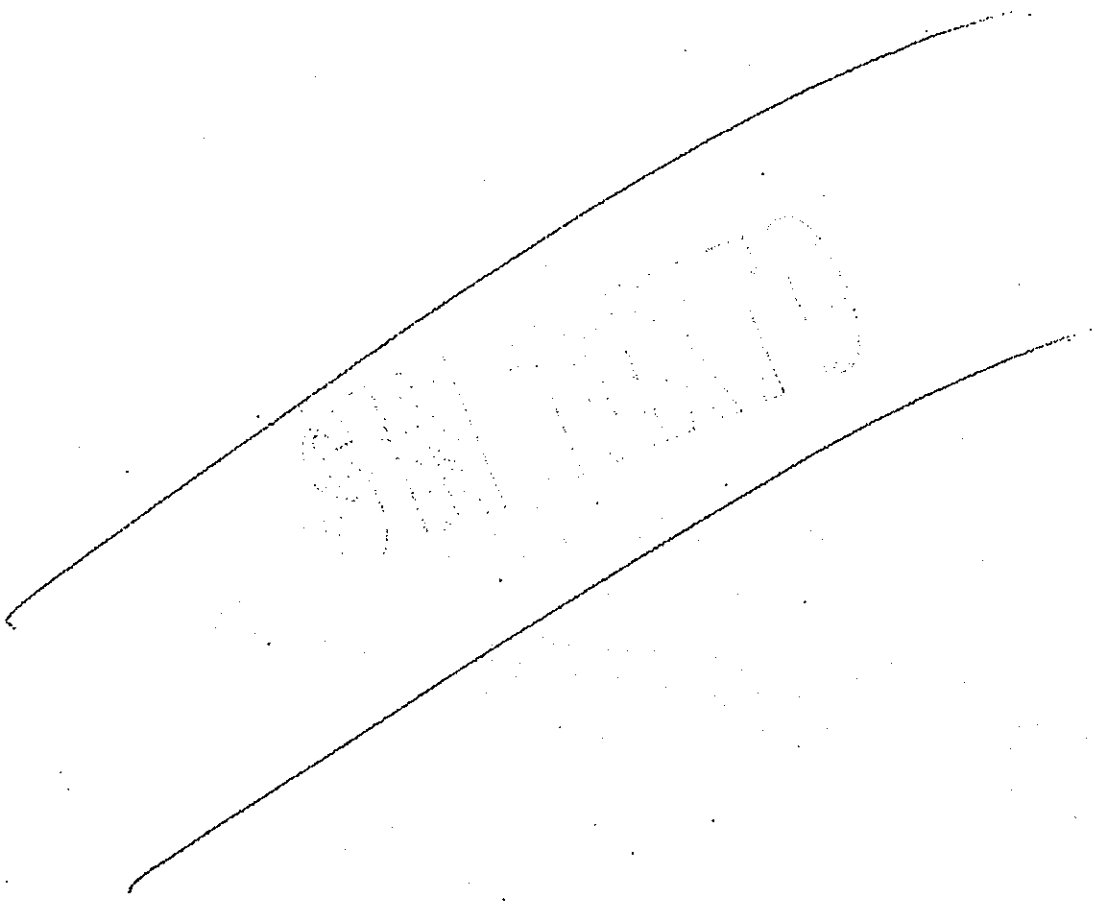
001367

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

58

ANEXO B

TERCER AVISO AL ACTA DE JUNTA DE ACLARACIONES DE LA CONVOCATORIA A LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".



HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

BANOBRAS
BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.

2022 Ricardo Flores Magón
Año de

MODIFICACIONES A LA CONVOCATORIA

LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

MODIFICACIÓN 1

DICE:

1.8. Difusión de la convocatoria

En cumplimiento a lo señalado en el artículo 30 de la **LAASSP**, la presente convocatoria se difundirá a través del sistema **CompraNet**, en la dirección electrónica https://compranet.hacienda.gob.mx, así como en la página de Internet de **BANOBRAS** y se publicará un resumen de la misma en el Diario Oficial de la Federación.

DEBE DECIR:

1.8. Difusión de la convocatoria

En cumplimiento a lo señalado en el artículo 30 de la **LAASSP**, la presente convocatoria se difundirá a través del sistema **CompraNet**, en la dirección electrónica https://compranet.hacienda.gob.mx y se publicará un resumen de la misma en el Diario Oficial de la Federación.

MODIFICACIÓN 2

DICE:

3.1. Fecha, hora y lugar de los eventos de la licitación

La **Licitación** dará lugar a los eventos conforme al calendario que a continuación se señala:

Fecha de publicación en **CompraNet**: **11 de octubre de 2022**.

EVENTO	FECHA	HORA	LUGAR
JUNTA DE ACLARACIONES	18/10/2022	11:00 A.M.	A TRAVÉS DEL SISTEMA COMPRANET
PRESENTACIÓN Y APERTURA DE PROPOSICIONES	01/11/2022	01:00 P.M.	
FALLO	08/11/2022	05:00 P.M.	
FIRMA DEL CONTRATO	Dentro de los 15 (quince) días naturales posteriores a la notificación del fallo de conformidad con lo dispuesto en el artículo 46 de la **LAASSP**.		A TRAVÉS DEL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS (MFIJ)

(...)

DEBE DECIR:

3.1. Fecha, hora y lugar de los eventos de la licitación

La **Licitación** dará lugar a los eventos conforme al calendario que a continuación se señala:

Fecha de publicación en **CompraNet**: **11 de octubre de 2022**.

EVENTO	FECHA	HORA	LUGAR
JUNTA DE ACLARACIONES	18/10/2022	11:00 A.M.	

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

57

001384

PRESENTACIÓN Y APERTURA DE PROPOSICIONES	**07/11/2022**	**01:00 P.M.**	**A TRAVÉS DEL SISTEMA COMPRANET**
FALLO	**10/11/2022**	**01:00 P.M.**	
FIRMA DEL CONTRATO	Dentro de los 15 (quince) días naturales posteriores a la notificación del fallo de conformidad con lo dispuesto en el artículo 46 de la **LAASSP.**		**A TRAVÉS DEL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS (MFIJ)**

(...)

MODIFICACIÓN 3

DICE:

ANEXO 2
MODELO DE CONTRATO

(...)

DECLARACIONES

(...)

II. Declara **"El Proveedor"** por conducto de su representante legal que:

II.I. a II.IX. (...)

II.X. Para efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, así como de conformidad con lo dispuesto en el ACUERDO ACDO.SA1.HCT.101214/281.P.DIR y su Anexo Único, dictado por el H. Consejo Técnico del Instituto Mexicano del Seguro Social (IMSS), relativo a las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015, y que entró en vigor el 03 de marzo de 2015, reformado mediante ACUERDO ACDO.SA1.HCT.250315/62.P.DJ, relativo a la autorización para modificar la Primera de las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 03 de abril de 2015, así como ACUERDO ACDO.AS1.HCT.260220/64.P.DIR, relativo a modificar la Primera de las Reglas y adicionar tres párrafos a la Tercera de las Reglas para la obtención de la opinión de cumplimiento de obligaciones fiscales en materia de seguridad social, publicado en el Diario Oficial de la Federación el 30 de marzo de 2020, ambos dictados por el H. Consejo Técnico del IMSS, presentó a **"Banobras"**, el documento de fecha __ de _____ de 2022, denominado "Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social", con número de folio _____, expedido por el IMSS, en el que se emite la opinión positiva respecto del cumplimiento de sus obligaciones fiscales en materia de seguridad social.

(...)

DEBE DECIR:

ANEXO 2
MODELO DE CONTRATO

(...)

DECLARACIONES

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

3

(...)

II. Declara **"El Proveedor"** por conducto de su representante legal que:

II.I. a II.IX. (...)

II.X. Para efectos de lo previsto por el artículo 32-D del Código Fiscal de la Federación, así como de conformidad con lo dispuesto en el ACUERDO número ACDO.AS2.HCT.270422/107.P.DIR dictado por el H. Consejo Técnico en sesión ordinaria de 27 de abril del presente año, por el que se aprobaron las Reglas de carácter general para la obtención de la opinión del cumplimiento de obligaciones fiscales en materia de seguridad social, así como su Anexo Único, publicado en el Diario Oficial de la Federación el 22 de septiembre de 2022, dictado por el H. Consejo Técnico del IMSS, presentó a **"Banobras"**, el documento de fecha __ de _____ de 2022, denominado "Opinión de Cumplimiento de Obligaciones en Materia de Seguridad Social", con número de folio _____, expedido por el IMSS, en el que se emite la opinión positiva respecto del cumplimiento de sus obligaciones fiscales en materia de seguridad social.

(...)

MODIFICACIÓN 4

DICE:

ANEXO 2
MODELO DE CONTRATO

(...)

DECLARACIONES

(...)

II. Declara **"El Proveedor"** por conducto de su representante legal que:

II.I. a II.XVI. (...)

DEBE DECIR:

ANEXO 2
MODELO DE CONTRATO

(...)

DECLARACIONES

(...)

II. Declara **"El Proveedor"** por conducto de su representante legal que:

II.I. a II.XVI. (...)

II.XVII. Para efectos de lo señalado en el artículo 14 de la Ley Federal del Trabajo, el personal que prestará los servicios de ciberseguridad en el sitio donde se realizarán las actividades designadas por **"Banobras"**, será de aproximadamente __ (____) elementos.

MODIFICACIÓN 5

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

SC4

DICE:

ANEXO 2
MODELO DE CONTRATO

(...)

CLÁUSULAS

(...)

SÉPTIMA. - GARANTÍA DE CUMPLIMIENTO DEL CONTRATO: Con fundamento en lo dispuesto por los artículos 45, fracción XI, 48, fracción II y 49, fracción II de la LAASSP, correlativos a los artículos 85, fracción III y 103 del RLAASSP, en términos de lo establecido por la sección III.7. "De la contratación" de los POBALINES y de conformidad con lo señalado en el numeral 15. "Garantías" del **"Anexo Técnico"**, **"El Proveedor"** se obliga a garantizar todas y cada una de las obligaciones contraídas mediante el presente contrato, entregando en un plazo que no exceda de 10 (diez) días naturales contados a partir de la firma del presente instrumento jurídico, una póliza de fianza a favor de **"Banobras"**, expedida por una institución mexicana autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas, o bien, en alguna de las otras formas señaladas en el artículo 79, fracción III del RLFPRH, por un importe equivalente al 10% (diez por ciento) del monto máximo antes del I.V.A., señalado en la cláusula **CUARTA** del presente contrato, o en su caso, por un importe equivalente al 10% (diez por ciento) del monto por erogar antes del I.V.A. en el ejercicio fiscal 2022, misma que deberá ser renovada dentro de los primeros 10 (diez) días naturales de cada ejercicio fiscal, por un importe equivalente al 10% (diez por ciento) del monto por erogar antes del I.V.A. de dicho ejercicio fiscal, conforme a lo señalado en el artículo 87 del RLAASSP.

DEBE DECIR:

ANEXO 2
MODELO DE CONTRATO

(...)

CLÁUSULAS

(...)

SÉPTIMA. - GARANTÍA DE CUMPLIMIENTO DEL CONTRATO: Con fundamento en lo dispuesto por los artículos 45, fracción XI, 48, fracción II y 49, fracción II de la LAASSP, correlativos a los artículos 85, fracción III y 103 del RLAASSP, en términos de lo establecido por la sección III.7. "De la contratación" de los POBALINES y de conformidad con lo señalado en el numeral 15. "Garantías" del **"Anexo Técnico"**, **"El Proveedor"** se obliga a garantizar todas y cada una de las obligaciones contraídas mediante el presente contrato, entregando en un plazo que no exceda de 10 (diez) días naturales contados a partir de la firma del presente instrumento jurídico, una póliza de fianza a favor de **"Banobras"**, expedida por una institución mexicana autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas, o bien, en alguna de las otras formas señaladas en el artículo 79, fracción III del RLFPRH, por un importe equivalente al 10% (diez por ciento) del monto máximo antes del I.V.A., señalado en la cláusula **CUARTA** del presente contrato, o en su caso, por un importe equivalente al 10% (diez por ciento) del monto máximo por erogar antes del I.V.A. en el ejercicio fiscal 2022, misma que deberá ser renovada dentro de los primeros 10 (diez) días naturales de cada ejercicio fiscal, por un importe equivalente al 10% (diez por ciento) del monto máximo por erogar antes del I.V.A. de dicho ejercicio fiscal, conforme a lo señalado en el artículo 87 del RLAASSP.

MODIFICACIÓN 6

DICE:

ANEXO 1
ANEXO TÉCNICO

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

(...)

4. REQUERIMIENTOS

(...)

S3 – Reducción de la superficie de ataque del ecosistema de los sistemas.

(...)

Reingeniería y Gestión del riesgo de Ciberseguridad del directorio activo

- ✓ Implementación de una herramienta de Monitoreo y Validación de cambios del directorio activo (descrito en el punto 4.4.2

(...)

DEBE DECIR:

ANEXO 1
ANEXO TÉCNICO

(...)

4. REQUERIMIENTOS

(...)

S3 – Reducción de la superficie de ataque del ecosistema de los sistemas.

(...)

Reingeniería y Gestión del riesgo de Ciberseguridad del directorio activo

- ✓ Implementación de una herramienta de Monitoreo y Validación de cambios del directorio activo (descrito en el apartado de **Herramienta de Monitoreo y Validación de cambios de directorio activo**).

(...)

MODIFICACIÓN 7

DICE:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

ANEXO 2
CRITERIO DE EVALUACIÓN

(...)

DEBE DECIR:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

(...)

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

MODIFICACIÓN 8

DICE:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

I).- RUBRO CAPACIDAD DEL LICITANTE

(...)

A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS

(...)

2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal

(...)

Asignación de Puntos:
La asignación de puntaje será de manera individual por cada tabla:

Tabla A
- No presenta certificaciones ni título y/o cédula del personal propuesto para cada perfil solicitado por la convocante: **0 PUNTOS**
- Presenta certificaciones y título y/o cédula del personal propuesto para cada perfil solicitado por la convocante: **3.0 PUNTOS**

Tabla B

DEBE DECIR:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

I).- RUBRO CAPACIDAD DEL LICITANTE

(...)

A).- SUBRUBRO CAPACIDAD DE LOS RECURSOS HUMANOS

(...)

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

2.- Competencia o habilidades en el trabajo de acuerdo con los conocimientos académicos o profesionales del personal

(...)

Asignación de Puntos:
La asignación de puntaje será de manera individual por cada tabla y solo aplica lo solicitado en la **Tabla B** si se cumple primero lo solicitado para la **Tabla A**.

Tabla A

- No presenta certificaciones ni título y/o cédula del personal propuesto para cada perfil solicitado por la convocante: **0 PUNTOS**
- Presenta certificaciones y título y/o cédula del personal propuesto para cada perfil solicitado por la convocante: **3.0 PUNTOS**

Tabla B

- Cumple de 7 a 13 perfiles solicitados por la convocante: **3 PUNTOS**
- Cumple de 5 a 6 perfiles solicitados por la convocante: **2 PUNTOS**
- Cumple de 3 a 4 perfiles solicitados por la convocante: **1 PUNTO**
- Cumple de 2 o menos perfiles solicitados por la convocante: **0 PUNTOS**

Para el cumplimiento de cada perfil se va a considerar de la siguiente manera:

NO	PERFIL	CANTIDAD DE CERTIFICACIONES OPCIONALES
1	Administrador del proyecto	4
2	Especialista en cumplimiento	3
3	Líder técnico de ciberseguridad	5
4	Auditor de ciberseguridad	2
5	Líder técnico de seguridad en sistemas	2
6	Especialista en pruebas estáticas	2
7	Especialista en pruebas dinámicas	3
8	Arquitecto de seguridad en arquitecturas de directorio activo	0
9	Auditor de riesgos de seguridad	2
10	Analistas de seguridad	1
11	Líder de operación	4
12	Líder técnico de Red Team	3
13	Especialista de Red Team	4

MODIFICACIÓN 9

DICE:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

I).- RUBRO CAPACIDAD DEL LICITANTE

(...)

B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

58

1.- CAPACIDAD DE LOS RECURSOS ECONÓMICOS (2 puntos).- A fin de conocer y evaluar la capacidad económica del licitante, se evaluarán los ingresos económicos del licitante a través de la presentación de su declaración anual correspondiente al ejercicio fiscal 2021 y la última declaración fiscal provisional del impuesto sobre la renta del ejercicio fiscal 2022, presentada ante la Secretaría de Hacienda y Crédito Público (SHCP) a la que se encuentre obligado, con las cuales deberá acreditar ingresos equivalentes al 10% del subtotal sin I.V.A. del importe máximo referencial por los meses estimados del servicio, de conformidad con la **PROPUESTA ECONÓMICA**.

En este sentido y tomando como base su propuesta económica y los ingresos que acrediten a través de sus declaraciones fiscales que presenten. Se asignarán puntos en los siguientes términos:

- Acredita el 10% o más de ingresos, obtendrá **2 puntos.**
- Acredita del 6% y hasta un 9.99% de ingresos obtendrá, **1.5 puntos.**
- Acredita el 5% y hasta el 5.99% de ingresos obtendrá **1 punto.**
- Acredita menos del 5% de ingresos, obtendrá **0 puntos.**

La formalidad que será susceptible de verificación en este subrubro, será la siguiente:

- Las declaraciones señaladas anteriormente deberán ser legibles y contener el sello digital del Servicio de Administración Tributaria (SAT)

- **2.- CAPACIDAD DE EQUIPAMIENTO (9 PUNTOS). -** El licitante deberá acreditar en su propuesta técnica que cuenta con el equipo suficiente para la prestación del servicio. Debiendo acreditar la propiedad del equipo con copia simple de las facturas o instrumento contractual que acredite su uso, goce y disfrute con el que garantice que cubre el periodo de la vigencia del instrumento contractual que para este servicio formalizaría con BANOBRAS, ya que en caso contrario no se asignarán puntos por este concepto. En este sentido se otorgarán puntos en los términos siguientes:

En este sentido y tomando como base su propuesta, se asignarán puntos en los siguientes términos:

- Si acredita el total del equipamiento obtendrá **2 punto:**
  - Licenciamiento de análisis de vulnerabilidades
  - Licenciamiento de inteligencia de amenazas
  - Licenciamiento de un HelpDesk especializado en atención de incidentes de ciberseguridad
  - Licenciamiento de EDR (Endpoint Detection and Response)

- Al licitante que presente la evidencia documental de las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 9001:2015 o versión superior, ISO 22301:2020 o versión superior, ISO/IEC 20000-1:2018 o versión superior e ISO 37001 se le otorgará **7 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 9001:2015 o versión superior, ISO 22301:2020 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **6.5 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 22301:2020 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **2 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **1 punto.** Si el licitante solo presenta la certificación de la norma ISO/IEC 27001:2014 o versión superior se le otorgará **0.5 puntos**, para otorgarse los puntos deberán acreditar las certificaciones solicitadas de al menos cinco de los siguientes procesos:
  - Análisis de Vulnerabilidades y Pruebas de Penetración para Aplicaciones e Infraestructura Tecnológica
  - Análisis y Monitoreo Externo de la información para el Alertamiento de Riesgos y Ciberamenazas
  - Centro de Operaciones de Redes y de Seguridad "NOC y SOC" con Detección, Análisis y Respuesta Gestionada "MDR" para la atención con el Equipo de Respuesta ante Emergencias Informáticas
  - Forense Digital
  - Gobierno de Seguridad y Cumplimiento Normativo
  - Inteligencia de Análisis de Información Digital

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

Al licitante que presente la evidencia documental de contar con el Certificado de membresía FIRST (Forum of Incident Response and Security Teams). Se le otorgarán **1 punto.**

DICE:

ANEXO 16
MATRIZ DE PUNTOS Y PORCENTAJES

(...)

I).- RUBRO CAPACIDAD DEL LICITANTE

(...)

B).- SUBRUBRO CAPACIDAD DE LOS RECURSOS ECONÓMICOS Y DE EQUIPAMIENTO POR PARTE DEL LICITANTE

1.- CAPACIDAD DE LOS RECURSOS ECONÓMICOS (2 puntos).- A fin de conocer y evaluar la capacidad económica del licitante, se evaluarán los ingresos económicos del licitante a través de la presentación de su declaración anual correspondiente al ejercicio fiscal 2021 y la última declaración fiscal provisional del impuesto sobre la renta del ejercicio fiscal 2022, presentada ante la Secretaría de Hacienda y Crédito Público (SHCP) a la que se encuentre obligado, con las cuales deberá acreditar ingresos equivalentes al 10% del subtotal sin I.V.A. del importe máximo referencial por los meses estimados del servicio, de conformidad con la **PROPUESTA ECONÓMICA.**

En este sentido y tomando como base su propuesta económica y los ingresos que acrediten a través de sus declaraciones fiscales que presenten. Se asignarán puntos en los siguientes términos:

- Acredita el 10% o más de ingresos, obtendrá **2 puntos.**
- Acredita del 6% y hasta un 9.99% de ingresos obtendrá; **1.5 puntos.**
- Acredita el 5% y hasta el 5.99% de ingresos obtendrá **1 punto.**
- Acredita menos del 5% de ingresos, obtendrá **0 puntos.**

La formalidad que será susceptible de verificación en este subrubro, será la siguiente:

- Las declaraciones señaladas anteriormente deberán ser legibles y contener el sello digital del Servicio de Administración Tributaria (SAT)

2.- CAPACIDAD DE EQUIPAMIENTO (10 PUNTOS). - El licitante deberá acreditar en su propuesta técnica que cuenta con el equipo suficiente para la prestación del servicio. Debiendo acreditar la propiedad del equipo con copia simple de las facturas o instrumento contractual que acredite su uso, goce y disfrute con el que garantice que cubre el periodo de la vigencia del instrumento contractual que para este servicio formalizaría con BANOBRAS, ya que en caso contrario no se asignarán puntos por este concepto. En este sentido se otorgarán puntos en los términos siguientes:

En este sentido y tomando como base su propuesta, se asignarán puntos en los siguientes términos:

- Si acredita el total del equipamiento obtendrá **2 punto**:
  - Licenciamiento de análisis de vulnerabilidades
  - Licenciamiento de inteligencia de amenazas
  - Licenciamiento de un HelpDesk especializado en atención de incidentes de ciberseguridad
  - Licenciamiento de EDR (Endpoint Detection and Response)

- Al licitante que presente la evidencia documental de las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 9001:2015 o versión superior, ISO 22301:2020 o versión superior, ISO/IEC 20000-1:2018 o versión superior e ISO 37001 se le otorgará **7 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 9001:2015 o versión superior, ISO 22301:2020 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **5.6 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior, ISO 22301:2020 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **4.2 puntos.** Si el licitante solo presenta las certificaciones de las normas ISO/IEC 27001:2014 o versión superior e ISO/IEC 20000-1:2018 o versión superior se le otorgará **2.8**

Av. Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219. Tel: 5270 1200. www.gob.mx/banobras

puntos. Si el licitante solo presenta la certificación de la norma ISO/IEC 27001:2014 o versión superior se le otorgará **1.4 puntos**, para otorgarse los puntos deberán acreditar las certificaciones solicitadas de al menos cinco de los siguientes procesos:

- Análisis de Vulnerabilidades y Pruebas de Penetración para Aplicaciones e Infraestructura Tecnológica
- Análisis y Monitoreo Externo de la información para el Alertamiento de Riesgos y Ciberamenazas
- Centro de Operaciones de Redes y de Seguridad "NOC y SOC" con Detección, Análisis y Respuesta Gestionada "MDR" para la atención con el Equipo de Respuesta ante Emergencias Informáticas
- Forense Digital
- Gobierno de Seguridad y Cumplimiento Normativo
- Inteligencia de Análisis de Información Digital

o Al licitante que presente la evidencia documental de contar con el Certificado de membresía FIRST (Forum of Incident Response and Security Teams). Se le otorgarán **1 punto.**

NOTA

Por la naturaleza del servicio, la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como minimizar riesgos de vulnerabilidad, el licitante que resulte adjudicado en el procedimiento de contratación para los servicios de "CIBERSEGURIDAD" de esta Institución Bancaría, no podrá contar, al momento del fallo, con otro contrato vigente con BANOBRAS en materia de tecnologías de la información y comunicaciones.

Las presentes modificaciones se realizan con fundamento en lo establecido por el artículo 33 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en términos de lo señalado en el numeral 3.3. "Forma, modificaciones y aclaraciones que podrán efectuarse a la convocatoria" de la convocatoria a la licitación pública nacional electrónica número LA-006G1C001-E157-2022, cuyo objeto es la contratación de los "Servicios de Ciberseguridad".

----------**FIN DEL TEXTO**----------

001355

ANEXO 2

ACTA DE JUNTA DE ACLARACIONES A LA CONVOCATORIA DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA NÚMERO LA-006G1C001-E157-2022, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

Volver a la Lista | Publicación DOF | Duplicar Procedimiento | Modificar fecha de apertura | ...

Procedimiento : 1116287 - SERVICIOS DE CIBERSEGURIDAD

Vigente

Expediente:2519712- SERVICIOS DE CIBERSEGURIDAD

Fecha y hora de apertura de proposiciones: 07/11/2022 01:00:00 p. m.

Administración del Procedimiento | Monitoreo de Licitantes | Grupo de Evaluación | Fallo | Discusiones | Mensajes Unidad Compradora / Licitantes

Crear Mensaje | Mensajes Recibidos | Mensajes Enviados | Borrador de Mensajes | Mensajes Adjuntados

Mensajes Recibidos

Crear Elemento ...

Introduzca Filtro (escriba para iniciar

	Remitente	Fecha	Asunto	Fecha de Mi Consulta	Fecha de Consulta en la UC	Respuesta
1	IQSEC SA DE CV	25/10/2022 11:38 p. m.	MANIFIESTO DE INTERES Y PLIEGO DE PREGUNTAS	26/10/2022 09:32 a. m.	26/10/2022 09:32 a. m.	
2	IQSEC SA DE CV	25/10/2022 05:47 p. m.	FALLAS EN PLATAFORMA COMPRANET	25/10/2022 05:53 p. m.	25/10/2022 05:50 p. m.	
3	SCITUM SA DE CV	25/10/2022 05:40 p. m.	Aclaración de Re-preguntas Scitum S.A. de C.V.	25/10/2022 05:41 p. m.	25/10/2022 05:41 p. m.	
4	SCITUM SA DE CV	25/10/2022 05:34 p. m.	Repreguntas Scitum S.A. de C.V.	25/10/2022 05:39 p. m.	25/10/2022 05:39 p. m.	
5	MICRONET DE MEXICO SA DE CV	24/10/2022 09:37 p. m.	Escrito Interés Participación	25/10/2022 09:06 a. m.	25/10/2022 09:06 a. m.	
6	CAD & LAN MEXICO SA DE CV	17/10/2022 06:45 p. m.	Interés en participar en licitación	18/10/2022 12:07 p. m.	18/10/2022 12:07 p. m.	
7	SBEL SYSTEMS GROUP SA DE CV	17/10/2022 05:45 p. m.	ESCRITO DE INTERES	18/10/2022 03:49 p. m.	18/10/2022 12:58 p. m.	
8	SERVICIOS ADMINISTRADOS MEXIS SA DE CV	17/10/2022 11:11 a. m.	ANEXO 3	17/10/2022 11:23 a. m.	17/10/2022 11:23 a. m.	
9	SCITUM SA DE CV	17/10/2022 10:52 a. m.	Preguntas JA Parte 2	17/10/2022 11:44 a. m.	17/10/2022 11:43 a. m.	
10	DELOITTE ASESORIA EN RIESGOS SC	17/10/2022 10:46 a. m.	Se envían preguntas de Deloitte así como el manifiesto de interés por participar	17/10/2022 11:43 a. m.	17/10/2022 11:34 a. m.	
11	PG RANHTOE SERVICIOS ADMINISTRATIVOS SA DE CV	17/10/2022 10:45 a. m.	Anexo 4.- Junta de Aclaraciones	17/10/2022 11:40 a. m.	17/10/2022 11:40 a. m.	
12	CAD & LAN MEXICO SA DE CV	17/10/2022 10:43 a. m.	Envío de Información	17/10/2022 11:41 a. m.	17/10/2022 11:41 a. m.	
13	PG RANHTOE SERVICIOS ADMINISTRATIVOS SA DE CV	17/10/2022 10:43 a. m.	Anexo 4.- Junta de Aclaraciones	17/10/2022 11:40 a. m.	17/10/2022 11:40 a. m.	
14	PG RANHTOE SERVICIOS ADMINISTRATIVOS SA DE CV	17/10/2022 10:41 a. m.	ANEXO 3.- ESCRITO DE INTERES EN PARTICIPAR EN LA LICITACIÓN	17/10/2022 11:40 a. m.	17/10/2022 11:40 a. m.	
15	SBEL SYSTEMS GROUP SA DE CV	17/10/2022 10:12 a. m.	PREGUNTAS SBEL	17/10/2022 11:40 a. m.	17/10/2022 11:40 a. m.	
16	SCITUM SA DE CV	17/10/2022 06:40 a. m.	Preguntas Junta de Aclaraciones	17/10/2022 09:18 a. m.	17/10/2022 09:18 a. m.	
17	SCITUM SA DE CV	17/10/2022 06:38 a. m.	Escrito de Interés	17/10/2022 09:17 a. m.	17/10/2022 09:17 a. m.	
18	TIC DEFENSE SA DE CV	16/10/2022 09:32 p. m.	JUNTA DE ACLARACIONES	16/10/2022 09:37 p. m.	16/10/2022 09:37 p. m.	
19	CONSULTORIA ESTRATEGICA Y COACHING S DE RL DE CV	16/10/2022 02:16 p. m.	Fe de erratas Escrito de Interés y preguntas	16/10/2022 09:36 p. m.	16/10/2022 09:36 p. m.	
20	CONSULTORIA ESTRATEGICA Y COACHING S DE RL DE CV	16/10/2022 01:56 p. m.	Escrito de interés y preguntas	16/10/2022 09:35 p. m.	16/10/2022 09:35 p. m.	

Total 21 Página 1 de 2 1 2 > >>

63

← Volver a la Lista | Publicación DOF | Duplicar Procedimiento | Modificar fecha de apertura | ...

Procedimiento : 1116287 - SERVICIOS DE CIBERSEGURIDAD

Vigente

Expediente:2519712- SERVICIOS DE CIBERSEGURIDAD

Fecha y hora de apertura de proposiciones: 07/11/2022 01:00:00 p. m.

Administración del Procedimiento | Monitoreo de Licitantes | Grupo de Evaluación | Fallo | Discusiones | Mensajes Unidad Compradora / Licitantes

Crear Mensaje | Mensajes Recibidos | Mensajes Enviados | Borrador de Mensajes | Mensajes Adjuntados

Mensajes Recibidos

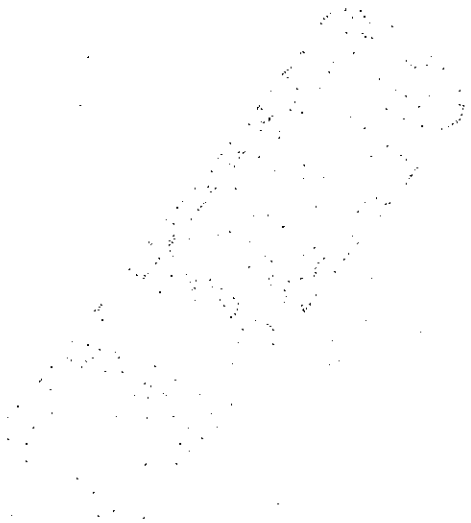
Crear Elemento ...

Introduzca Filtro (escriba para iniciar

	Remitente	Fecha	Asunto	Fecha de Mi Consulta	Fecha de Consulta en la UC	Respuesta
21	ECLIPSE TELECOMUNICACIONES SA DE CV	14/10/2022 05:28 p. m.	Envio Dudas e Interés de Participación	14/10/2022 07:53 p. m.	14/10/2022 07:53 p. m.	

Total 21 Página 2 de 2 << < 1 2

ANEXO C



TICDEFENSE
CYBERSECURITY.

001351

PROPUESTA ECONÓMICA

Ciudad de México, a 07 de noviembre de 2022

Lic. Karla De Tuya García
Gerente de Adquisiciones en
Banobras, S.N.C.
Presente

El suscrito en mi carácter de Representante Legal de la Empresa **TIC DEFENSE, S.A. DE C.V.**, manifiesto que mi Representada, en caso de resultar adjudicada del procedimiento de contratación que instrumente Banobras a partir de la Licitación Pública Nacional Electrónica N° **LA-006G1C001-E157-2022**, mantendrá fijo el Costo del Servicio y los demás ofertados antes de I.V.A., hasta la conclusión de la vigencia de la relación contractual, cuya Proposición Económica del ***"Servicio de Ciberseguridad"*** a continuación se presenta:

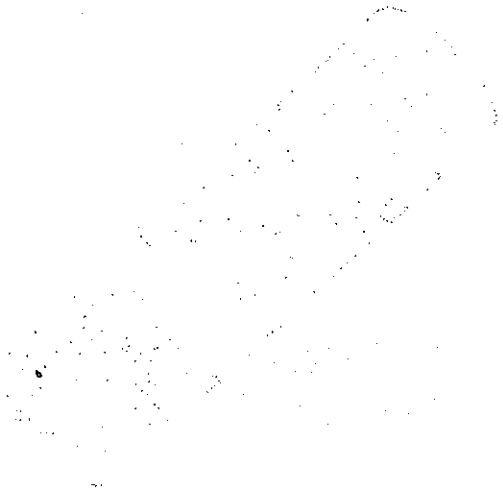
MODELO DE PROPOSICIÓN ECONÓMICA: SERVICIOS DE CIBERSEGURIDAD				
LICITANTE: TIC DEFENSE, S.A. DE C.V.				
DIRIGIDA A: Banobras, S.N.C.				
NÚMERO DE PROCEDIMIENTO: Licitación Pública Nacional Electrónica Número. LA-006G1C001-E157-2022				
FECHA: 07 de noviembre de 2022				
12 MESES				
ID DEL SERVICIO	**NOMBRE DEL SERVICIO**	**ACRÓNIMO**	**UNIDAD DE MEDIDA (MES)**	**PRECIO UNITARIO**
1	S1-Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad	S1	1 MES	$285,451.00
2	S2-Realización periódica de análisis de seguridad de sistemas	S2	1 MES	$278,785.00
3	S3-Reducción de la superficie de ataque del ecosistema de los sistemas	S3	1 MES	$448,237.00
4	S4-Sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365	S4	1 MES	$499,599.00
5	S5-Modelado de adversario Blue-Team Red-Team	S5	1 MES	$287,330.00
			Subtotal	**$1,799,402.00**
			I.V.A.	**$287,904.32**
			Total	**$2,087,306.32**
Anotar con letra, el **subtotal** antes de IV.A.: UN MILLÓN SETECIENTOS NOVENTA Y NUEVE MIL CUATROCIENTOS DOS PESOS 00/100 MXN				
Anotar con letra el **importe total** con I.V.A., incluido: DOS MILLONES OCHENTA Y SIETE MIL TRESCIENTOS SEIS CON TREINTA Y DOS CENTAVOS 32/100 MXN				
Nombre del representante legal **Valeria Giordano Turrubiarte**				
Firma del representante legal del licitante:				

*Cualquier diferencia que exista entre la Proposición técnica y la económica será motivo de desechamiento.
*La vigencia de la Proposición es de 90 días naturales.
*Los precios serán fijos durante la vigencia del contrato.
*Precios establecidos en pesos mexicanos

Atentamente

Valeria Giordano Turrubiarte
Representante Legal
TIC DEFENSE, S.A. DE C.V.

ANEXO D



CUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

"El Proveedor" se obliga a conocer y cumplir en todo momento las "Políticas de Seguridad de la Información" y los cambios que de éstas se deriven, durante el periodo de vigencia del contrato y/o pedido y guardar confidencialidad sobre la información a que tiene acceso permanentemente, durante y después de finalizar el contrato.

"El Proveedor" se obliga a comunicar a su personal, empleados y/o toda persona que por cualquier causa se encuentre o pudiese estar vinculado a él y al uso de activos de información o a la infraestructura de redes y sistemas de **"Banobras"**, las "Políticas de Seguridad de la Información" y los cambios que de éstas se deriven, durante el periodo de vigencia del contrato. A continuación, se enlistan las Políticas de Seguridad de la Información, mismas que son de carácter enunciativo mas no limitativo:

- Manual de Seguridad de la Información.

1. Políticas para la Organización de la Seguridad de la Información.
2. Políticas de Seguridad de la Información en los Recursos Humanos.
3. Políticas de Seguridad de la Información para la Gestión de Activos.
4. Políticas de Seguridad de la Información para el Control de Accesos.
5. Políticas de Seguridad de la Información para el Cifrado.
6. Políticas de Seguridad de la Información para la Seguridad Física y Ambiental.
7. Políticas de Seguridad de la Información para las Operaciones.
8. Políticas de Seguridad de la Información para las Comunicaciones.
9. Políticas de Seguridad de la Información para la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
10. Políticas de Seguridad de la Información para la Relación con Proveedores.
11. Políticas de Seguridad de la Información para la Gestión de Incidentes de Seguridad de la Información.
12. Políticas de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
13. Políticas de Seguridad de la Información para el Cumplimiento.

AUDITORÍA SOBRE EL CUMPLIMIENTO DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTREGA DE LOS SERVICIOS CONTRATADOS.

"Banobras" tiene la facultad de supervisar y/o auditar periódicamente, por sí mismo o a través de un tercero, que los productos y/o servicios materia del presente contrato y/o pedido cumplen con lo establecido en las "Políticas de Seguridad de la Información" de **"Banobras"** y los cambios que de éstas se deriven, durante el periodo de vigencia del contrato y/o pedido. **"El Proveedor"** tiene la obligación de otorgar los accesos y elementos requeridos para llevar a cabo cada una de las supervisiones o auditorías a ser realizadas.

"Banobras" puede solicitar, de así requerirlo, dictámenes de los controles internos en materia de seguridad de la información del **"El Proveedor"** sobre los procesos relacionados con los productos y servicios que entrega a sus clientes, realizado por un despacho de auditoría independiente y reconocido.

CONFIDENCIALIDAD DE LA INFORMACIÓN.

Para garantizar la Confidencialidad de la información de **"Banobras"**, **"El Proveedor"** deberá entender las definiciones y categorías de clasificación de la información de acuerdo a lo establecido en las Políticas de Seguridad de la Información. Considerando que la información incluye formato electrónico, físico y comunicación verbal.

"El Proveedor" al dar tratamiento a información confidencial, clasificada por **"Banobras"**, está obligado a:

a) Mantenerla en estricta reserva y no revelar ningún dato de la información a ninguna otra parte, relacionada o no, sin el consentimiento previo escrito de **"Banobras"**.

b) Instruir al personal que estará encargado de recibir la información confidencial, debiendo suscribir el correspondiente acuerdo de confidencialidad si fuere necesario, de su obligación de recibir, tratar y usar la información recibida, clasificada como confidencial y destinada únicamente al propósito del presente, en los términos que se estipula.

c) Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la estructura de **"El Proveedor"** y de **"Banobras"**.

d) Tratar confidencialmente toda la información recibida directa o indirectamente del **"Banobras"**, y no utilizar la información de forma distinta al objeto de este contrato y/o pedido.

RESPONSABILIDADES DEL PERSONAL DEL PROVEEDOR.

Para garantizar el cumplimiento de los requisitos referentes a la responsabilidad de los empleados, de **"El Proveedor"**, éste deberá:

Certificar que todos los dispositivos utilizados por los empleados de **"El Proveedor"** o sus subcontratistas que estén conectados al ambiente de procesamiento de **"Banobras"**, cumplan y sigan cumpliendo los siguientes requisitos:

a) Deben aplicarse y estar al día los paquetes de actualizaciones (service pack) más recientes y todos los parches de seguridad aplicables a todos los sistemas operativos y software residentes en los dispositivos.

b) Los dispositivos deben tener el software estándar de la industria contra programas maliciosos (malware) instalado, funcionando y actualizado con el último archivo de firma; y el dispositivo debe tener instalado y activo un producto de seguridad tipo cortafuego (firewall) personal y estándar de la industria.

c) Deben asegurar que los computadores utilizados para el procesamiento de datos suministrados por **"Banobras"** no cuentan con accesos habilitados a puertos USB.

d) Garantizar que los datos de clientes suministrados por **"Banobras"** no serán tratados a través de dispositivos móviles, celulares, tabletas, etc.

e) **"El Proveedor"** acepta que periódicamente sus equipos pueden ser objeto de revisiones de cumplimiento por parte de **"Banobras"**.

SEGURIDAD DE LOS SERVIDORES.

Para asegurar la integridad, confidencialidad y disponibilidad de todos los servidores utilizados para procesar la información y datos de **"Banobras"**, y para mitigar la amenaza, riesgo e impacto del uso indebido y abusos externos o internos de las plataformas de servidores, **"El Proveedor"** deberá:

1. Proteger el acceso a todos los servidores, como mínimo, mediante una combinación de la identificación (ID) del usuario y la contraseña.

2. Cambiar todas las contraseñas de los servidores que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente en función a las Políticas de Seguridad de la Información establecidas.

3. Asegurar que los servidores se encuentren ubicados en zonas físicamente seguras.

4. Reforzar la seguridad de todos los servidores utilizados para procesar, almacenar o transmitir datos e información de **"Banobras"**, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores.

5. Implementar herramientas de análisis de la seguridad de los servidores para informar periódicamente sobre el estado de cada servidor y verificar que todas las configuraciones, parámetros y opciones estén conformes con el estado de reforzamiento acordado para ese dispositivo y para detectar cambios no autorizados a partir de la línea base de la configuración aprobada del servidor.

6. Registrar toda la actividad de acceso del servidor y almacenar los datos de dicha actividad de una manera apropiada, en función a las Políticas de Seguridad de la Información establecidas y revisar periódicamente (al menos una vez al año) todos los controles de seguridad del servidor definidos anteriormente para asegurarse de que todavía estén vigentes.

7. **"El Proveedor"** periódicamente deberá realizar análisis de vulnerabilidades sobre los servidores asociados a la prestación de servicios objeto de éste contrato y/o pedido.

8. **"Banobras"**, tendrá la facultad para realizar periódicamente revisiones de cumplimiento sobre la seguridad en los servidores asociados a la prestación de servicios objeto de éste contrato y/o pedido.

DESARROLLO DEL SOFTWARE.

Para garantizar el cumplimiento de los requisitos de **"Banobras"** para los códigos seguros, **"El Proveedor"** deberá:

a) Documentar la arquitectura; componentes internos y externos, controles de seguridad, arquitectura (aplicación, seguridad, etc.).

b) Análisis de vulnerabilidades por un tercero; incorporar el análisis Estático y Dinámico de los códigos de seguridad en el ciclo de vida del desarrollo del software.

c) Mitigar los problemas de seguridad identificados, durante el análisis Estático y Dinámico de los códigos antes de pasarlos al entorno de producción.

d) Cumplir con lo establecido en la política de gestión de identidades y accesos.

e) Establecer una gestión de sesiones acorde a las necesidades del Banco.

f) Evitar que la aplicación permita el registro de datos maliciosos.

g) Uso de elementos criptográficos sobre datos sensibles.

h) Adecuada gestión de errores.

SEGURIDAD DE LOS ARCHIVOS DE DATOS Y BASES DE DATOS.

Para asegurar la integridad, confidencialidad y seguridad en general de todas las bases de datos y archivos de datos utilizados para almacenar información y datos de **"Banobras"**, **"El Proveedor"** deberá:

1. Almacenar la información "Confidencial" de **"Banobras"** (por ejemplo, contraseñas, datos de los clientes, etc.) en un formato cifrado de conformidad con las mejores prácticas de la industria; y acorde al estándar de criptografía aprobado por **"Banobras"**.

2. Ubicar todos los servidores de bases de datos, servidores de archivos y repositorios que contengan datos de **"Banobras"** en un área físicamente segura.

3. Restringir todo el acceso físico y lógico a las bases de datos, archivos de datos e información y datos almacenados en éstos, así como a cualquier sistema o componente de la red relacionado con el procesamiento de transacciones según un esquema basado solo en la "necesidad de conocer o usar" de la Institución.

4. Proteger todos los accesos a las bases de datos y archivos de datos utilizando, como mínimo, una combinación de la identificación del usuario y la contraseña.

5. Cambiar todas las contraseñas de las bases de datos que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente en función a las Políticas de Seguridad de la Información establecidas.

6. Registrar toda la actividad de acceso a las bases de datos y archivos de datos, y almacenar los datos de dicha actividad de una manera apropiada, en función a las Políticas de Seguridad de la Información establecidas.

7. Implementar herramientas de análisis de la seguridad de las bases de datos para revisar periódicamente las configuraciones de las bases de datos y garantizar el cumplimiento de las configuraciones base esperadas.

8. Eliminar y destruir de una manera adecuada y segura todas las instancias de cualquier información o datos de **"Banobras"** y material impreso conexo para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas.

9. Revisar en forma periódica (al menos una vez al año) todos los controles de seguridad de la base de datos definidos anteriormente para asegurar que continúan vigentes.

SEGURIDAD DE LA RED.

Para mitigar la amenaza, riesgo e impacto de intrusiones, abuso o uso indebido del sistema o la red, **"El Proveedor"** deberá:

a) Instalar, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración y ataques por denegación de servicio.

b) Instalar cortafuegos (firewall) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (gateways) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet.

c) Registrar toda la actividad de los cortafuegos y puertas de enlace y almacenar los datos de dicha actividad.

d) Proteger los datos contra la divulgación no autorizada durante su tránsito a través de redes públicas a **"Banobras"**, o sus agentes autorizados, o sus clientes, para garantizar la seguridad de los datos que sean propiedad de **"Banobras"** o estén relacionados con **"Banobras"**.

PROTECCIÓN CONTRA PROGRAMAS MALICIOSOS (MALWARE).

Para mitigar la amenaza, riesgo e impacto de los virus informáticos, gusanos, troyanos y otros tipos de software malicioso, colectivamente llamado "malware", **"El Proveedor"** deberá:

1. Instalar, configurar, activar y mantener actualizado un software antivirus y antiespías (antispyware) basado en las mejores prácticas de la industria, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen las transacciones y cualquier otro dato de **"Banobras"**.

2. Configurar dicho software anti-malware para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado.

VULNERABILIDADES DE LA SEGURIDAD E INSTALACIÓN DE PARCHES DE SEGURIDAD.

Para mitigar la amenaza, riesgo e impacto de las vulnerabilidades de la seguridad en el sistema o red, **"El Proveedor"** deberá:

a) Desarrollar e implementar un proceso para investigar continuamente las fuentes fiables de advertencias sobre vulnerabilidades de la seguridad emergentes.

b) Identificar vulnerabilidades específicas que puedan impactar los ambientes operativos o plataformas utilizados por **"El Proveedor"** y **"Banobras"**.

c) Evaluar la criticidad de una vulnerabilidad en relación con las operaciones generales de **"El Proveedor"** y **"Banobras"**, a fin de determinar la conveniencia de instalar el correspondiente parche de seguridad.

d) Probar e instalar oportunamente los parches de seguridad.

ALERTA Y ESCALAMIENTO DE PROBLEMAS Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

En el caso de pérdida, acceso no autorizado, o divulgación no autorizada de la Información Confidencial de **"Banobras"**, datos personales tratados por **"Banobras"**, u otros datos de **"Banobras"**, (cada uno de ellos una "Violación de Seguridad de la información"), **"El Proveedor"** inmediatamente y tan pronto como sea posible, después de determinar que se le ha producido una Violación de la Seguridad de la Información deberá:

1. Investigar la violación de seguridad de la información y proporcionar a **"Banobras"** la información detallada sobre la violación de seguridad de la información.

2. **"El Proveedor"** de forma inmediata, después de determinar que ha ocurrido la Violación de la Seguridad de los Datos: deberá Notificar a **"Banobras"** de las violaciones de seguridad de los datos a los siguientes correos electrónicos: mesa.servicio@banobras.gob.mx y banseg@banobras.gob.mx

CONTROL DE CAMBIOS.

Para garantizar el cumplimiento de los requisitos de **"Banobras"** y de las mejores prácticas de la industria para el control de cambios, **"El Proveedor"** deberá:

1. Desarrollar, probar y documentar cada cambio de conformidad con la gestión de cambios, preservando la integridad, lógica continua de los datos, programas y rastros de auditoría.

RESPALDO Y RECUPERACIÓN.

Para garantizar el cumplimiento de los requisitos de **"Banobras"** y de las mejores prácticas de la industria para el respaldo y la recuperación, **"El Proveedor"** deberá:

a) Implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema.

b) Facilitar la reanudación de las aplicaciones críticas y actividades de negocios de una manera oportuna después de una emergencia o desastre.

c) Mantener un plan de recuperación de desastres documentado para cada sistema crítico relacionado con **"Banobras"** y probarlo anualmente.

"El Proveedor" se compromete a no incurrir o participar en ningún tipo de actividad sospechosa o dañina para las instalaciones, información y/o operación de **"Banobras"**.

En caso de ocurrir algún incidente con los activos utilizados (tecnológicos o información) por causas imputables a **"El Proveedor"**, este se obliga a solucionar el problema recobrando en todo momento la operación normal de **"Banobras"** que se hubiere visto afectada por el incidente.

"El Proveedor" se obliga a cumplir los requerimientos para control de accesos y/o procedimientos de autorización para acceder a los activos de información de **"Banobras"** (tecnológicos e información), así como a cumplir las cláusulas de restricción para el copiado y acceso a la información que se le indiquen por parte del área requirente del servicio.

"El Proveedor" en este acto manifiesta bajo protesta de decir verdad que cuenta con los mecanismos necesarios para asegurar a **"Banobras"** la protección de virus y código malicioso, que pudieran surgir con motivo de la prestación de los servicios objeto de este instrumento.

DEVOLUCIÓN DE INFORMACIÓN.

En cualquier momento, ante solicitud escrita de **"Banobras"**, **"El Proveedor"** devolverá toda o parte de la Información según se requiera, así como las copias que se encuentren en su poder cualquiera sea su formato. A requerimiento de **"Banobras"**, **"El Proveedor"** deberá destruir la Información y proporcionar prueba de su destrucción.

INCUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Será motivo de la aplicación de la pena convencional más alta establecida en el contrato y/o pedido por cada día natural de atraso en la atención de las "Políticas de Seguridad de la Información", que le sean aplicables con motivo de la prestación del servicio objeto del presente contrato y/o pedido.