



CONTRATO DAGA/083/2026

CONTRATO CERRADO NÚMERO **DAGA/083/2026**, CORRESPONDIENTE A LA PRESTACIÓN DE LOS **"SERVICIOS DE CIBERSEGURIDAD"**, EN ADELANTE **"EL SERVICIO"**, CON CARÁCTER **NACIONAL**, QUE CELEBRAN, POR UNA PARTE, EL BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS, S.N.C., I.B.D., EN LO SUCESIVO **"BANOBRAS"**, REPRESENTADA POR LA SERVIDORA PÚBLICA MARYTELL CASTELLANOS RUEDA, PERSONA TITULAR DE LA DIRECCIÓN DE RECURSOS MATERIALES, EN SU CARÁCTER DE REPRESENTANTE LEGAL, Y, POR LA OTRA, **TIC DEFENSE, S.A. DE C.V.**, EN LO SUCESIVO **"EL PROVEEDOR"**, REPRESENTADA POR VALERIA GIORDANO TURRUBIARTE, EN SU CARÁCTER DE REPRESENTANTE LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

Se elimina RFC de persona física, con fundamento en el Artículo 115, párrafo primero de la LGTAIP.

1. **"BANOBRAS"** declara 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. Conforme a lo dispuesto por las Políticas Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios de **"BANOBRAS"**, en lo sucesivo las **"POBALINES"**, la servidora pública Marytell Castellanos Rueda, persona Titular de la Dirección de Recursos Materiales, con R.F.C. [REDACTED] es quien tiene conferidas las facultades legales suficientes para celebrar el presente contrato, y cuenta con poder general para actos de administración en términos de la escritura pública número 147,852 (ciento cuarenta y siete mil ochocientos cincuenta y dos), libro 3,153 (tres mil ciento cincuenta y tres), de fecha 17 de noviembre de 2023, otorgada ante la fe del Licenciado José Ángel Villalobos Magaña, Titular de la Notaría Pública número 9 de la Ciudad de México, inscrita en el Registro Público de Comercio de la Ciudad de México, bajo el folio mercantil electrónico número 80259, de fecha 23 de mayo de 2024, quien podrá ser sustituida en cualquier momento en su cargo o funciones, sin que por ello, sea necesario celebrar un convenio modificatorio.
 - 1.3. De conformidad con lo dispuesto por los artículos 2, fracción IV, y 129, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (**"RLAASSP"**), así como en términos de lo señalado en el numeral **"19. Denominación del área administradora y técnica del Contrato"**, del documento denominado **"ANEXO TÉCNICO"**, la persona Titular de la Dirección de Seguridad de la Información, a cargo del servidor público, Humberto David Rosales Herrera, con R.F.C. [REDACTED] o quien en su caso ocupe dicho cargo, o quien asuma las atribuciones del puesto, o a quien designe expresamente, será el servidor público encargado de administrar, supervisar, vigilar y verificar el cumplimiento del presente contrato, así como el que dará seguimiento y verificará el cumplimiento de las obligaciones que deriven del presente contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito firmado por la persona servidora pública facultada para ello, informando de manera inmediata al nuevo administrador, a **"EL PROVEEDOR"**, al Órgano Interno de Control de **"BANOBRAS"**, a la Unida de Administración de **"BANOBRAS"**, así como a las demás áreas competentes, para los efectos del presente contrato.
 - 1.4. Suscribe el presente contrato la servidora pública Karla De Tuya García, persona Titular de la Gerencia Ejecutiva de Adquisiciones, con R.F.C. [REDACTED] como responsable del procedimiento de contratación.
 - 1.5. La adjudicación del presente contrato se realizó mediante el procedimiento de licitación pública nacional, con número asignado por la Plataforma Digital de Contrataciones Públicas (COMPRAS MX) **LA-06-G1C-006G1C001-N-68-2026**, al cual





CONTRATO DAGA/083/2026

en lo sucesivo se le denominará **"LA LICITACIÓN"**, como consta en el ACTA CORRESPONDIENTE A LA CELEBRACIÓN DEL ACTO DE FALLO, de fecha 14 de julio del 2026, misma que obra en el expediente de contratación correspondiente, realizado por la persona Titular de la Gerencia Ejecutiva de Adquisiciones, en su carácter de área contratante, de conformidad con lo dispuesto por el artículo 2, fracción I del **"RLAASSP"**, con fundamento en lo dispuesto por los artículos 134, párrafos quinto y sexto de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), 35 fracción I, 39 fracción I, y 67 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público **"LAASSP"**, 18 del **"RLAASSP"**, así como en términos de lo señalado en el numeral III.7. "De la contratación", de los **"POBALINES"**.

- 1.6. **"BANOBRAS"** cuenta con los recursos necesarios y suficientes, así como con la autorización para ejercerlos en el cumplimiento de las obligaciones derivadas del presente contrato, conforme a lo establecido en el artículo 33, párrafo primero de la **"LAASSP"**, como se acredita con el documento denominado "Requisición de Bienes, Arrendamientos y Servicios Suficiencia Presupuestal", sellado por la persona Titular de la Gerencia de Programación y Control Presupuestal con fecha 08 de junio de 2026, identificado mediante el número de control interno de la Gerencia Ejecutiva de Adquisiciones 085, con número de folio 26-02254 de la Gerencia de Programación y Control Presupuestal, con cargo a la partida presupuestal número 33301 y clave del Clasificador Único de las Contrataciones Públicas (CUCoP) número 33300001.
- 1.7. Cuenta con el Registro Federal de Contribuyentes N° **BNO670315CD0**.
- 1.8. Tiene establecido su domicilio en Avenida Javier Barros Sierra N° 515, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México mismo que señala para los fines y efectos legales del presente contrato.
- 1.9. Cuenta con una Política de Género cuyos principios buscan potenciar los impactos positivos de género, la cual es aplicable al personal, proveedores y directrices internas de la Institución; y una Política Ambiental y Social, así como una Estrategia de Banco Sostenible, que impulsa el desarrollo de proyectos que contribuyen al bienestar social, y busca respetar el medio ambiente y la conservación de los ecosistemas, igualmente aplicable al personal de esta Institución y extensiva a clientes de **"BANOBRAS"**.
- 1.10. Se consultó en el Directorio de Proveedores y Contratistas Sancionados de la página de la Secretaría Anticorrupción y Buen Gobierno que **"EL PROVEEDOR"** no se encontró inhabilitado en los términos de la **"LAASSP"** y la Ley de Obras Públicas y Servicios Relacionados con las Mismas (LOPSRM).
2. **"EL PROVEEDOR"** declara que:
 - 2.1. Es una Sociedad Anónima de Capital Variable, constituida conforme a la legislación mexicana, según consta en el testimonio de la escritura número 61,804 (Sesenta y un mil ochocientos cuatro), Libro 1801 (Mil ochocientos uno), de fecha 29 de noviembre de 2017, otorgada ante la fe del Lic. 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 folio mercantil electrónico número N-2018001411, de fecha 11 de enero de 2018, denominada como **TIC DEFENSE, S.A. DE C.V.**

Mediante escritura pública número 246 (Doscientos cuarenta y seis), Libro 6 (Seis), de fecha 11 de mayo de 2023, otorgada ante la Fe del Lic. Agustín Gerardo Saldaña Villarreal, Titular de la Notaría Pública número 41, de la Ciudad de Torreón, del Estado de Coahuila de Zaragoza; donde se protocolizó la Asamblea General Extraordinaria de Accionistas,



CONTRATO DAGA/083/2026

donde se acordó lo siguiente: I.- Propuesta, discusión y, en su caso, aprobación para decretar un aumento de capital social en la parte variable; II.- Designación de delegado especial ejecutor que formalice las resoluciones que se adopten; inscrita en el Registro Público de Comercio de la Ciudad de México, bajo el folio mercantil electrónico número N-2018001411, de fecha 10 de noviembre de 2025.

Dentro de su objeto social está entre otros, "... a) *El diseño, desarrollo, implantación, comercialización, importación y exportación de productos y servicios de tecnologías y sus derivados de seguridad de la información y ciberseguridad a personas físicas y morales, derecho público o privado, nacionales o extranjeras, empresas de participación estatal, la federación, los gobiernos de los estados, el gobierno de la Ciudad de México, Municipios, organismos descentralizados, desconcentrados y paraestatales; así como en la participación en concursos y licitaciones de cualquier índole...*"; mismo que se encuentra señalado en la escritura pública 61,804.

- 2.2. Valeria Giordano Turrubiarte, en su carácter de Representante Legal, cuenta con las facultades legales suficientes, las cuales a la fecha no le han sido limitadas, modificadas ni revocadas, en forma alguna, para obligar a su representada en los términos y condiciones establecidos en el presente contrato, según consta en la escritura pública número 21,934 (Veintiún mil novecientos treinta y cuatro), Libro 405 (Cuatrocientos cinco), de fecha 15 de noviembre del año 2019, otorgada ante la Fe de la Lic. Guillermo Aarón Vigil Chapa, Titular de la Notaría número 247 de la Ciudad de México.
- 2.3. Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.
- 2.4. Cuenta con su Registro Federal de Contribuyentes **TDE171130E30**.
- 2.5. Manifiesta bajo protesta de decir verdad que, el que suscribe, la persona que representa, 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 71 y 90 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- 2.6. Manifiesta bajo protesta de decir verdad que conocen el contenido del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas, especificando que ni el Representante Legal legal, así como ninguno de los socios y/o accionistas quienes ejercen el control de la sociedad, mencionadas en su escrito, desempeñan 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.
- 2.7. 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 57 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, por lo que manifiesta que su representada se estratifica como una empresa **PEQUEÑA**.
- 2.8. Su Representante Legal se identifica plenamente mediante credencial de elector expedida a su favor por el Instituto Nacional Electoral.



CONTRATO DAGA/083/2026

- 2.9. Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones Patronales y Entero de Descuentos, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.
- 2.10. Tiene establecido su domicilio en: Prolongación Paseo de la Reforma No 799, Piso 15, Oficina VIP 02, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, C.P. 01219, Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.
3. **Declaran "LAS PARTES":**
- 3.1. Han revisado y obtenido todas y cada una de las autorizaciones para celebrar el presente contrato, además de que sus representantes cuentan con las autorizaciones de carácter legal y administrativo necesarias, así como con las facultades y capacidad legal suficientes para tales efectos, mismas que no les han sido modificadas, restringidas ni revocadas en forma alguna, a la fecha de formalización del presente contrato.
- 3.2. Para la celebración del presente contrato se han conducido con apego a la LGRA; se comprometen a actuar conforme a las mismas durante su ejecución, hacia sus contrapartes y terceros; **"LAS PARTES"** aceptan expresamente que la transgresión a esta declaración implica una violación del presente contrato.
- 3.3. Durante la vigencia del contrato y en términos de lo dispuesto por la Ley Federal Para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, se comprometen a actuar con estricto apego a las siguientes reglas de conducta para combatir la extorsión y el soborno:
- **"BANOBRAS"** vigilará que las personas servidoras públicas 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 las personas servidoras públicas 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 las personas servidoras públicas de **"BANOBRAS"** y/o de cualquier tercero que implique violación a la presente declaración.
 - **"BANOBRAS"** exhortará a las personas servidoras públicas 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/o ejecución del presente contrato.
 - **"BANOBRAS"** desarrollará sus actividades en la administración, supervisión y/o ejecución del presente contrato dentro del código de conducta de **"BANOBRAS"**.



CONTRATO DAGA/083/2026

- **"BANOBRAS"** evitará arreglos compensatorios o contribuciones destinadas a favorecer indebidamente a **"EL PROVEEDOR"**; de esta forma, actuará con honestidad y transparencia durante la administración, supervisión y/o ejecución del presente contrato.

- 3.4. Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

"EL PROVEEDOR" acepta y se obliga a proporcionar a **"BANOBRAS"**, **"EL SERVICIO"** conforme a las características, plazos, términos y condiciones, que, se indican en el documento denominado **"ANEXO TÉCNICO" (ANEXO A)**, elaborado por el área requirente y que es parte integrante del presente contrato como si a la letra se insertase, lo señalado en el documento denominado **"CUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN" (ANEXO B)**, así como lo señalado en el **ACTA DE JUNTA DE ACLARACIONES (ANEXO C)**.

SEGUNDA. MONTO DEL CONTRATO.

"BANOBRAS" pagará a **"EL PROVEEDOR"**, como contraprestación objeto de este contrato, la cantidad de **\$19,275,433.12 (DIECINUEVE MILLONES DOSCIENTOS SETENTA Y CINCO MIL CUATROCIENTOS TREINTA Y TRES PESOS 12/100 M.N.)**, más la cantidad de **\$3,084,069.29 (TRES MILLONES OCHENTA Y CUATRO MIL SESENTA Y NUEVE PESOS 29/100 M.N.)** correspondiente al 16% (Dieciséis por ciento) del Impuesto al Valor Agregado (I.V.A.), dando un total de **\$22,359,502.41 (VEINTIDOS MILLONES TRESCIENTOS CINCUENTA Y NUEVE MIL QUINIENTOS DOS PESOS 41/100 M.N.)**.

Por lo que respecta al mes de **julio de 2026**, y considerando que la vigencia del presente contrato comienza el **15** de dicho mes, se pagará la parte proporcional.

Los precios unitarios mensuales ofertados por **"EL PROVEEDOR"** son los siguientes:

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	\$428,954.00
2	S2.- Realización periódica de análisis de seguridad de sistemas.	S2	1 MES	\$368,142.00
3	S3.- Reducción de la superficie de ataque del ecosistema de los sistemas.	S3	1 MES	\$677,345.00
4	S4.- Sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365	S4	1 MES	\$1,576,243.00
5	S5.- Modelado de adversario Blue-Team Red-Team	S5	1 MES	\$432,828.00

Los precios unitarios mensuales ofertados por **"EL PROVEEDOR"** serán fijos y en moneda nacional (PESO MEXICANO) hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación de **"EL SERVICIO"**, por lo que **"EL PROVEEDOR"** no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.



TERCERA. ANTICIPO.

Para el presente contrato **"BANOBRAS"** no otorgará anticipo a **"EL PROVEEDOR"**.

CUARTA. FORMA Y LUGAR DE PAGO.

"BANOBRAS" realizará el o (los) pago (s) que resulte (n) procedente (s) a **"EL PROVEEDOR"**, de forma mensual conforme a lo señalado en el numeral **"13.2. Forma de pago"** del **ANEXO TÉCNICO**, una vez que se haya recibido **"EL SERVICIO"** a entera satisfacción de **"BANOBRAS"**, a través de la persona Titular de la Dirección de Seguridad de la Información, dentro de los 17 (diecisiete) días hábiles posteriores a la entrega del comprobante fiscal digital (CFDI) respectivo, el cual, le será hecho del conocimiento mediante oficio correspondiente, previa emisión de la Constancia de Aceptación de los Servicios emitida por la persona Titular de la Dirección de Seguridad de la Información, quien revisará que el CFDI cumpla, en cuanto a su contenido, con lo estipulado en el presente contrato, el **"ANEXO TÉCNICO"** y la oferta económica de **"EL PROVEEDOR"**.

El cómputo del plazo para realizar el pago se contabilizará a partir del día hábil siguiente de la aceptación del CFDI o factura electrónica, y ésta reúna los requisitos fiscales que establece la legislación en la materia, el desglose de **"EL SERVICIO"** prestado, el monto, se verifique su autenticidad, no existan aclaraciones al importe y vaya acompañada con la documentación soporte de la prestación de los servicios facturados.

De conformidad con el artículo 135 del **"RLAASSP"**, en caso de que el CFDI o factura electrónica entregado presente errores, la persona servidora pública administradora del presente contrato o a quien ésta designe por escrito, dentro de los 3 (tres) días hábiles siguientes de su recepción, indicará a **"EL PROVEEDOR"** las deficiencias que deberá corregir; por lo que, el procedimiento de pago reiniciará en el momento en que **"EL PROVEEDOR"** presente el CFDI y/o documentos soporte corregidos y sean aceptados.

El tiempo que **"EL PROVEEDOR"** utilice para la corrección del CFDI y/o documentación soporte entregada, no se computará para efectos de pago, de acuerdo con lo establecido en el artículo 73 de la **"LAASSP"**.

El CFDI o factura electrónica deberá ser presentada al correo de la persona Titular de la Dirección de Seguridad de la Información, revisará que el o los CFDI cumplan en cuanto a su contenido con lo estipulado en el presente instrumento jurídico.

El CFDI o factura electrónica se deberá presentar desglosando el impuesto cuando aplique.

"EL PROVEEDOR" manifiesta su conformidad que, hasta en tanto no se cumpla con la verificación, supervisión y aceptación de la prestación de **"EL SERVICIO"**, no se tendrán como recibido o aceptado por la persona servidora pública administradora del presente contrato.

Para efectos de trámite de pago, **"EL PROVEEDOR"** deberá ser titular de una cuenta bancaria, en la que se efectuará la transferencia electrónica de pago, respecto de la cual deberá proporcionar toda la información y documentación que le sea requerida por **"BANOBRAS"**, para efectos del pago.

"EL PROVEEDOR" deberá presentar la información y documentación que **"BANOBRAS"** le solicite para el trámite de pago, atendiendo a las disposiciones legales e internas de **"BANOBRAS"**.



CONTRATO DAGA/083/2026

El pago de la prestación de **"EL SERVICIO"**, recibido, quedará condicionado proporcionalmente al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales y, en su caso, deductivas. **"BANOBRAS"** no cubrirá pago alguno respecto de **"EL SERVICIO"** proporcionado por **"EL PROVEEDOR"**, que no cumpla en su totalidad con los requisitos fiscales y los solicitados en el presente contrato y en el **"ANEXO TÉCNICO"**.

El o 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 aparecen en la carátula de cuenta proporcionada por **"EL PROVEEDOR"**, la cual, será enviada a la persona Titular de la Dirección de Seguridad de la Información, posterior a la firma del presente instrumento jurídico, de tal forma que como mínimo contendrá: la Clabe interbancaria de 18 (dieciocho) dígitos, número de cuenta, nombre de la institución de crédito, sucursal y nombre del cuentahabiente.

Para el caso de que **"EL PROVEEDOR"** cambie el número de cuenta bancaria, lo hará del conocimiento de **"BANOBRAS"** por conducto de la persona Titular de la Dirección de Seguridad de la Información, para que los siguientes pagos sean efectuados a dicha cuenta.

En caso de incumplimiento en el o 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 forma y términos prescritos por el artículo 73, 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 73, párrafo tercero de la **"LAASSP"**.

Una vez cumplida la totalidad de las obligaciones de **"EL PROVEEDOR"** a entera satisfacción de **"BANOBRAS"**, mediante la aceptación de la persona Titular de la Dirección de Seguridad de la Información, deberá proceder inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales.

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE **"EL SERVICIO"**.

La prestación de **"EL SERVICIO"** se realizará conforme a los plazos, condiciones y entregables establecidos por **"BANOBRAS"** en el **"ANEXO TÉCNICO"** y del presente contrato.

El lugar para la entrega de la prestación de **"EL SERVICIO"** será en los lugares señalados en el numeral **"6.4. Lugar para la prestación de Servicios"**, del **"ANEXO TÉCNICO"**.



CONTRATO DAGA/083/2026

En los casos que derivado de la verificación se detecten defectos o discrepancias en la prestación de **"EL SERVICIO"** o incumplimiento en las especificaciones técnicas, **"EL PROVEEDOR"** deberá realizar la sustitución o corrección, conforme lo indica el **"ANEXO TÉCNICO"** sin costo adicional para **"BANOBRAS"**.

SEXTA. VIGENCIA.

"LAS PARTES" convienen en que la vigencia del presente contrato será tal y como se señala en el numeral **6.1. "Vigencia"** del **"ANEXO TÉCNICO"**, la cual será del **15 de julio de 2026** hasta el **31 de diciembre de 2026**.

SÉPTIMA. MODIFICACIONES DEL CONTRATO.

"LAS PARTES" están de acuerdo que **"BANOBRAS"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad de **"EL SERVICIO"**, de conformidad con el artículo 74 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el **20% (veinte por ciento)** de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"BANOBRAS", podrá ampliar la vigencia del presente contrato, siempre y cuando, no implique incremento del monto contratado o de la cantidad de **"EL SERVICIO"**, siendo necesario que se obtenga el previo consentimiento de **"EL PROVEEDOR"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"BANOBRAS"**, se podrá modificar el plazo del presente contrato, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES"**.

En los supuestos previstos en los dos párrafos anteriores, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse a través de la Plataforma Digital de Contrataciones Públicas (Compras MX), por el servidor público de **"BANOBRAS"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PROVEEDOR"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 136, último párrafo del Reglamento de la **"LAASSP"**, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"BANOBRAS" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un **"PROVEEDOR"** comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS

Para la prestación de **"EL SERVICIO"**, materia del presente contrato, no se requiere que **"EL PROVEEDOR"** presente garantía por la calidad de **"EL SERVICIO"** contratado.

NOVENA. GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

Conforme a los artículos 66, fracción XI, 69, fracción II y 70, fracción II de la **"LAASSP"**, correlativos al artículo 130, fracción III y



CONTRATO DAGA/083/2026

151 del **"RLAASSP"**, y de conformidad con lo señalado en el numeral **16.- "Garantía de Anticipo/Garantía de cumplimiento/Excepción de la presentación de la Garantía de Cumplimiento"** del **"ANEXO TÉCNICO"**, **"EL PROVEEDOR"** se obliga a constituir una garantía indivisible por el cumplimiento fiel y exacto de todas las obligaciones derivadas de este contrato, así mismo 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 siguientes a la formalización del presente contrato, 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 Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria (LFPRH), por un importe equivalente al **10% (diez por ciento) del monto total** antes del I.V.A., señalado en la cláusula **SEGUNDA** del presente contrato.

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 151, fracción I del **"RLAASSP"** y 166 de la Ley de Instituciones de Seguros y de Fianzas; así como, 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 ley de adquisiciones, arrendamientos y servicios del sector público y la ley de obras públicas y servicios relacionados con las mismas publicado en el diario oficial de la federación el día 15 de abril de 2022.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PROVEEDOR"** incumpla con la entrega de la garantía en el plazo establecido, **"BANOBRAS"** podrá rescindir el contrato y dará vista al Órgano Interno de Control de **"BANOBRAS"** para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PROVEEDOR"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"BANOBRAS"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PROVEEDOR"** se obliga a entregar a **"BANOBRAS"** **dentro de los 10 (diez días) naturales siguientes** a la formalización del mismo, de conformidad con el último párrafo del artículo 136 del **"RLAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **"EL PROVEEDOR"** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **"BANOBRAS"** a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda.

Una vez cumplidas las obligaciones a satisfacción, el servidor público facultado por **"BANOBRAS"** procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía de cumplimiento del contrato, lo que comunicará a **"EL PROVEEDOR"**.

DÉCIMA. OBLIGACIONES DEL "PROVEEDOR".

"EL PROVEEDOR", se obliga a:



CONTRATO DAGA/083/2026

- a) Prestar **"EL SERVICIO"** en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.
- b) Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.
- c) Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"BANOBRAS"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
- d) Proporcionar la información que le sea requerida por la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control, de conformidad con el artículo 156 del Reglamento de la **"LAASSP"**.
- e) Mantener al corriente sus obligaciones fiscales durante la vigencia del presente contrato.

DÉCIMA PRIMERA. OBLIGACIONES DE **"BANOBRAS"**.

"BANOBRAS", se obliga a:

- a) Otorgar todas las facilidades necesarias, a efecto de que **"EL PROVEEDOR"** lleve a cabo en los términos convenidos en la prestación de **"EL SERVICIO"** objeto del contrato.
- b) Realizar el pago correspondiente en tiempo y forma.
- c) Extender a **"EL PROVEEDOR"**, por conducto de la persona servidora pública facultada, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicha persona servidora pública, para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA SEGUNDA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE **"EL SERVICIO"**.

"BANOBRAS" designa como administrador del presente contrato al servidor público Humberto David Rosales Herrera, persona Titular de la Dirección de Seguridad de la Información, quien dará seguimiento y verificará el cumplimiento de los derechos y obligaciones establecidos en este contrato.

"EL SERVICIO" se tendrá por recibido previa revisión de la persona servidora pública administradora del presente contrato, la cual consistirá en la verificación del cumplimiento de las especificaciones establecidas y en su caso en los anexos respectivos, así como las contenidas en la propuesta técnica de **"EL PROVEEDOR"**.

"BANOBRAS" a través de la persona servidora pública administradora del contrato, rechazará **"EL SERVICIO"**, que no cumplan las especificaciones establecidas en este contrato, y en el **"ANEXO TÉCNICO"** y **JUNTA DE ACLARACIONES**, obligándose **"EL PROVEEDOR"** en este supuesto a entregarlo nuevamente bajo su responsabilidad y sin costo adicional para **"BANOBRAS"**, sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondiente.

"BANOBRAS", a través de la persona servidora pública administradora del contrato, podrá aceptar **"EL SERVICIO"** que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en el **"ANEXO TÉCNICO"**, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición de **"EL SERVICIO"**, cuando la naturaleza propia de éstos lo permita.



DÉCIMA TERCERA. DEDUCCIONES.

"BANOBRAS" aplicará deducciones al pago por el incumplimiento parcial o deficiente en **"EL SERVICIO"** o entrega no oportuna de los consumibles, en que incurra **"EL PROVEEDOR"**, conforme a lo señalado en el apartado **III.8. "Del seguimiento a los contratos"** en el numeral **III.8.6. "Aplicación de Deducciones"** de las **"POBALINES"** y conforme a los supuestos señalados en el numeral **"9.2. Deducciones al Pago"**, del **"ANEXO TÉCNICO"**, por conducto de la persona Titular de la Dirección de Seguridad de la Información se aplicará a **"EL PROVEEDOR"** una deductiva del 1% (uno por ciento) 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 deficiente.

En ningún caso las deducciones al pago podrán negociarse en especie.

Independientemente de la aplicación de las deducciones mencionadas, **"BANOBRAS"** a través de la Dirección de Seguridad de la Información podrá en cualquier momento optar por la rescisión del contrato por incumplimiento

Las cantidades a deducir se aplicarán en el CFDI o factura electrónica que **"EL PROVEEDOR"** presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pagos pendientes, se requerirá a **"EL PROVEEDOR"** que realice el pago de la deductiva, a través de la Nota de Crédito, en el momento en el que emita el comprobante de ingreso (factura o CFDI de ingreso) por concepto de **"EL SERVICIO"**, en términos de las disposiciones jurídicas aplicables.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir impuestos.

La notificación y cálculo de las deducciones correspondientes las realizará el administrador del contrato de **"BANOBRAS"**, por escrito o vía correo electrónico, por incumplimiento parcial o deficiente.

La suma de dichas deductivas, no podrán exceder del **10% (diez por ciento)** del monto total antes de I.V.A. señalado en la cláusula **SEGUNDA** del presente contrato.

DÉCIMA CUARTA. PENAS CONVENCIONALES.

En caso de que **"EL PROVEEDOR"** incurra en atraso en el cumplimiento conforme a lo pactado para la prestación de **"EL SERVICIO"**, objeto del presente contrato, conforme a lo establecido en el apartado **III.8.5. "Aplicación de Penas Convencionales"** de las **"POBALINES"**, **"BANOBRAS"** aplicará a **"EL PROVEEDOR"** las penas convencionales correspondientes conforme a los supuestos señalados en el numeral **"9.1. Penas convencionales"**, **"BANOBRAS"** aplicará penas convencionales de acuerdo a los siguientes supuestos:

- Retraso en los plazos de ejecución con respecto al Plan de Trabajo por causas ajenas a **"BANOBRAS"**: **2% (Dos por ciento)** 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% (Dos por ciento)** del costo total de los servicios no proporcionados a satisfacción por cada día de retraso, dado que los entregables forman parte integral del servicio.



CONTRATO DAGA/083/2026

Las penas convencionales serán determinadas, calculadas y notificadas por escrito al licitante adjudicado por la Dirección de Seguridad de la Información a través del administrador del contrato.

En ningún caso las penas convencionales podrán negociarse en especie.

Independientemente de la aplicación de las penas mencionadas, **"BANOBRAS"** a través de la Dirección de Seguridad de la Información podrá en cualquier momento optar por la rescisión del contrato, por incumplimiento.

El pago de **"EL SERVICIO"** quedará condicionado, proporcionalmente, al pago que se le deba efectuar a **"EL PROVEEDOR"** por concepto de penas convencionales por atraso; en el supuesto que el contrato sea rescindido en términos de lo previsto en la **CLÁUSULA VIGÉSIMA CUARTA**, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena convencional podrá efectuarse a través de la Nota de Crédito, en el momento en el que emita el comprobante de ingreso (factura o CFDI de ingreso) por concepto de **"EL SERVICIO"**, en términos de las disposiciones jurídicas aplicables.

El importe de la pena convencional, no podrán exceder del **10% (Diez por ciento)** del monto total antes de I.V.A. señalado en la cláusula **SEGUNDA** del presente contrato.

DÉCIMA QUINTA. LICENCIAS Y AUTORIZACIONES Y PERMISOS.

"EL PROVEEDOR" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA SEXTA. PÓLIZA DE RESPONSABILIDAD CIVIL.

Para la prestación de **"EL SERVICIO"**, materia del presente contrato, no se requiere que **"EL PROVEEDOR"** presente póliza de Responsabilidad Civil.

DÉCIMA SÉPTIMA. TRANSPORTE.

"EL PROVEEDOR" se obliga bajo su costa y riesgo en caso de ser aplicable, a contar con transporte para poder prestar **"EL SERVICIO"**, desde su lugar de origen, hasta las instalaciones de **"BANOBRAS"**.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS.

Los impuestos, derechos y gastos que procedan con motivo de la prestación de **"EL SERVICIO"**, objeto del presente contrato, serán pagados por **"EL PROVEEDOR"**, mismos que no serán repercutidos a **"BANOBRAS"**.

"BANOBRAS" sólo cubrirá, cuando aplique, lo correspondiente al Impuesto al Valor Agregado (IVA), en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.



CONTRATO DAGA/083/2026

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

"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 contar con la conformidad previa y por escrito de **"BANOBRAS"**.

Se exceptúa de lo anterior en el caso de fusión, escisión, o transformación de sociedades, siempre que la nueva sociedad que resulte cuente con la solvencia técnica, jurídica y económica exigidas al adjudicarse el contrato, cumpla con lo dispuesto en el Reglamento de la **"LAASSP"** y no se encuentre en los supuestos de impedimento previstos en la **"LAASSP"**.

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

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.

"EL PROVEEDOR" se hace responsable de daños directos determinados por autoridad judicial competente en la materia, por lo que no se hace responsable de daños a terceros, y si será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional, con motivo del cumplimiento de las obligaciones del presente contrato.

De presentarse alguna reclamación en contra de **"BANOBRAS"**, por cualquiera de las causas antes mencionadas, **"EL PROVEEDOR"**, se obliga a salvaguardar los derechos e intereses de **"BANOBRAS"** de cualquier controversia, liberándola de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

En caso de que **"BANOBRAS"** tuviese que erogar recursos por cualquiera de estos conceptos, **"EL PROVEEDOR"** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.

"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratará de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en las disposiciones vigentes en materia de transparencia y acceso a la información pública y de protección de datos personales.

Para el tratamiento de los datos personales que **"LAS PARTES"** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **"EL PROVEEDOR"** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

"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.



CONTRATO DAGA/083/2026

"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 la disposición de la cláusula **VIGÉSIMA CUARTA**, **"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 **"EL SERVICIO"** objeto del presente contrato, siempre que esté relacionado con el objeto del mismo. En consecuencia, **"Las Partes"** expresamente establecen que:

- I. **"EL PROVEEDOR"** a partir de la vigencia del presente contrato, se obliga en relación con 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 contrato.
- II. 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.
- III. 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.



CONTRATO DAGA/083/2026

- IV. 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.
- V. **"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. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE "EL SERVICIO".

Con fundamento en el artículo 80 de la **"LAASSP"**, y 150, fracción II, del **"RLAASSP"**, **"BANOBRAS"** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de **"EL SERVICIO"**, de manera temporal, quedando obligado a pagar a **"EL PROVEEDOR"**, aquellos servicios que hubiesen sido efectivamente prestados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **"BANOBRAS"** así lo determina; y en caso de que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

"BANOBRAS" cuando concurran razones de interés general, de común acuerdo, o bien, cuando por causas justificadas se extinga la necesidad de requerir los bienes arrendados originalmente y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"BANOBRAS"**, 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, emitida por la Secretaría Anticorrupción y Buen Gobierno, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"BANOBRAS"**.

Cuando **"BANOBRAS"** determine dar por terminado anticipadamente el contrato, lo notificará a **"EL PROVEEDOR"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen que precise las razones o las causas justificadas que le dieron origen a la misma, una vez notificada la terminación anticipada, se extinguirá el contrato, lo que dará lugar a formalizar el finiquito entre las partes.

En el finiquito se harán constar los pagos que, en su caso, deba efectuar **"BANOBRAS"** por concepto de los bienes arrendados hasta el momento de la terminación anticipada, además, en su caso, pactará en el mismo el reembolso al proveedor de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.



VIGÉSIMA CUARTA. RESCISIÓN.

"BANOBRAS" podrá iniciar en cualquier momento el procedimiento de rescisión, cuando **"EL PROVEEDOR"** incurra en alguna de las siguientes causales:

- a) Contravenir los términos pactados para la prestación de **"EL SERVICIO"**, establecidos en el presente contrato.
- b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual.
- c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"BANOBRAS"**.
- d) Suspender total o parcialmente y sin causa justificada la prestación de **"EL SERVICIO"** del presente contrato.
- e) No realizar la prestación de **"EL SERVICIO"** en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos.
- f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen.
- g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio.
- h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato.
- i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo.
- j) Cuando la suma de las penas convencionales exceda el monto total de la garantía de cumplimiento del contrato.
- k) Cuando la suma de las deducciones al pago, excedan el límite establecido para las deducciones.
- l) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"BANOBRAS"** en los términos de lo dispuesto en la **CLÁUSULA VIGÉSIMA PRIMERA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES** del presente instrumento jurídico.
- m) Impedir el desempeño normal de labores de **"BANOBRAS"**.
- n) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **"BANOBRAS"**, cuando sea extranjero.
- o) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.
- p) No presentar la opinión favorable de sus obligaciones fiscales, de manera bimestral al administrador del contrato durante la vigencia del presente contrato.

Para el caso de optar por la rescisión del contrato, **"BANOBRAS"** comunicará a través de la Plataforma (COMPRAS MX), a **"EL PROVEEDOR"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **"BANOBRAS"**, en un plazo de 10 (diez) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PROVEEDOR"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PROVEEDOR"** dicha determinación dentro del citado plazo. Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"BANOBRAS"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PROVEEDOR"**.

Iniciado un procedimiento de conciliación **"BANOBRAS"** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se realiza la prestación de **"EL SERVICIO"**, el procedimiento



CONTRATO DAGA/083/2026

iniciado quedará sin efecto, previa aceptación y verificación de **"BANOBRAS"** de que continúa vigente la necesidad de la prestación de **"EL SERVICIO"**, aplicando, en su caso, las penas convencionales correspondientes.

"BANOBRAS" podrá determinar no dar por rescindido el 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, **"BANOBRAS"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **"BANOBRAS"** establecerá con **"EL PROVEEDOR"**, otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 74 de la **"LAASSP"**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"BANOBRAS"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PROVEEDOR"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 73, párrafo cuarto, de la **"LAASSP"**.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"BANOBRAS"**.

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL.

"EL PROVEEDOR" reconoce y acepta ser el único patrón de todos y cada una de las trabajadoras y/o trabajadores que intervienen en la prestación de **"EL SERVICIO"**, deslindando de toda responsabilidad a **"BANOBRAS"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PROVEEDOR" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"BANOBRAS"**, así como en la ejecución de **"EL SERVICIO"**.

Para cualquier caso no previsto, **"EL PROVEEDOR"** exime expresamente a **"BANOBRAS"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"BANOBRAS"** reciba una demanda laboral por parte de trabajadores de **"EL PROVEEDOR"**, en la que se demande la solidaridad y/o sustitución patronal a **"BANOBRAS"**, **"EL PROVEEDOR"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS.

"LAS PARTES" convienen que, en caso de discrepancia entre la convocatoria a **"LICITACIÓN"**, la **JUNTA DE ACLARACIONES** de



CONTRATO DAGA/083/2026

"LA LICITACIÓN", y el Contrato, prevalecerá lo establecido en los dos primeros documentos, de conformidad con el artículo 126, fracción IV del **"RLAASSP"**.

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 109, 111 y 112 de la **"LAASSP"**, y 186 al 196 del **"RLAASSP"**.

VIGÉSIMA OCTAVA. DOMICILIOS.

"LAS PARTES" señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal.

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE.

"LAS PARTES" se obligan a sujetarse estrictamente para la prestación de **"EL SERVICIO"** objeto del presente contrato a todas y cada una de las cláusulas que lo integran, sus anexos que forman parte integral del mismo, a la **"LAASSP"**, su **"RLAASSP"**; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles y/o Código Nacional de Procedimientos Civiles y Familiares; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

TRIGÉSIMA. JURISDICCIÓN.

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

TRIGÉSIMA PRIMERA. CUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

"EL PROVEEDOR" se obliga expresamente a conocer y cumplir en su caso, con el documento denominado **"Cumplimiento a las Políticas de Seguridad de la Información" (ANEXO B)**, así como los cambios y actualizaciones 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



CONTRATO DAGA/083/2026

para el copiado y acceso a la información que se le indiquen por parte de la persona Titular de la Dirección de Seguridad de la Información, encargado de administrar, supervisar, vigilar el cumplimiento del contrato.

"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 contrato.

"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 Manual de Políticas de Seguridad de la Información (**"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 total máximo **"EL SERVICIO"** 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 **"EL SERVICIO"** objeto del presente contrato.

Derivado de la naturaleza de **"EL SERVICIO"** objeto del presente contrato, en caso de que **"EL PROVEEDOR"** deba 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 B**, **"BANOBRAS"** a través de la Dirección de Seguridad de la Información, supervisará que se dé el debido cumplimiento.

TRIGÉSIMA SEGUNDA. 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 **"EL SERVICIO"** objeto del presente contrato, se infrinja cualquiera de las citadas disposiciones legales.

En este sentido, **"EL PROVEEDOR"** responderá por los daños directos determinados por autoridad judicial competente en la materia que llegue a causar a **"BANOBRAS"**.

TRIGÉSIMA TERCERA. 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.



CONTRATO DAGA/083/2026

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.

TRIGÉSIMA CUARTA. INFORMACIÓN Y DOCUMENTACIÓN A INSTANCIAS FISCALIZADORAS.

En términos de lo dispuesto por los artículos 87 y 88 de la **"LAASSP"** y 156 del **"RLAASSP"**, **"EL PROVEEDOR"** acepta expresamente que, en caso de que los Órganos Internos de Control, la Secretaría Anticorrupción y Buen Gobierno, 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.

TRIGÉSIMA QUINTA. 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 la persona servidora pública alguna, que puedan constituir un acto ilícito o incumplimiento sustancial del presente contrato.

TRIGÉSIMA SEXTA. RESPONSABLE 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" a: El servidor público Humberto David Rosales Herrera, persona Titular de la Dirección de Seguridad de la Información, con domicilio señalado en: Avenida Javier Barros Sierra N° 515, PH, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, Código Postal 01219, Ciudad de México.

"EL PROVEEDOR" a: La Ciudadana Valeria Giordano Turrubiarte, en su carácter de Representante Legal, con domicilio ubicado en: Prolongación Paseo de la Reforma No 799, Piso 15, Oficina VIP 02, Colonia Lomas de Santa Fe, Alcaldía Álvaro Obregón, C.P. 01219, Ciudad de México.

FIRMANTES O SUSCRIPCIÓN.

Por lo anterior expuesto, **"BANOBRAS"** y **"EL PROVEEDOR"**, manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente contrato contiene, por lo que lo ratifican y firman electrónicamente en las fechas especificadas en cada firma electrónica.





CONTRATO DAGA/083/2026

Se elimina RFC de persona física, con fundamento en el Artículo 115, párrafo primero de la LGTAIP.

POR: "BANOBRAS"

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

POR: "EL PROVEEDOR"

NOMBRE	R.F.C
TIC DEFENSE, S.A. DE C.V.	TDE171130E30

REVISÓ: Moisés Isaac Herrera Ordóñez
ELABORÓ: Tania Paulina Romero Jiménez

Subgerente de Contrataciones
Experto Técnico



Se elimina RFC, números de serie y certificados de firma electrónica de personas físicas, con fundamento en el Artículo 115, párrafo primero de la LGTAIP.

Cadena original:

4b3e27c8a5508cdf7d62f7d8239f3405abe19c36d76fd09edb260480e81fab1a

Firmante: KARLA DE TUYA GARCIA
RFC: [REDACTED]

Número de Serie: [REDACTED]
Fecha de Firma: 28/07/2026 13:42

Certificado:



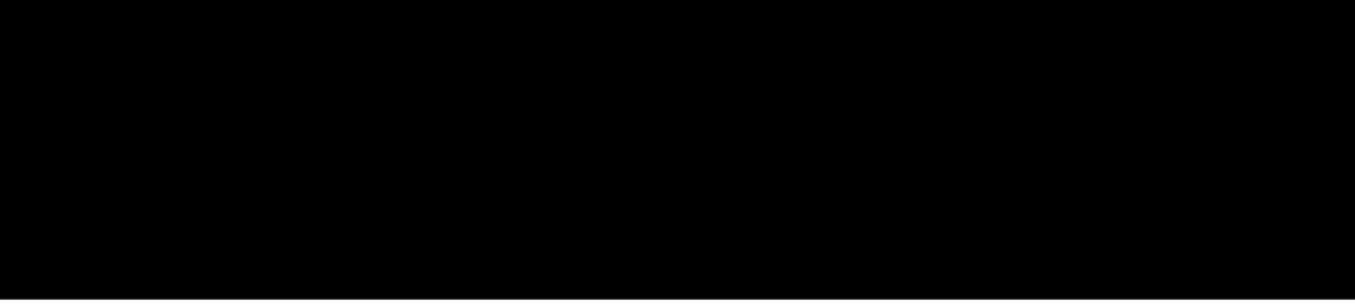
Firma:

E6+r1g3Hq1w9hJ1DTo6v1rSX9jDt21QhpjM7V1NyOJxaJA5rW0dqB/X6sBIGvcWe1C2MJgAUVvEp0pfjB6r1XjzbpP3Rn+Yo6aBOIwMNYw/dO6aCkx3KK97OaLY2ECfAZCwsvDeVnqo1JR6obBW9b8t/5GZwouiM
KLXnwhNkuFJg2g1RY632rbe0HFEONUOSMS3mywV+27Ar1IoLaQ6spt7XDDfXeGXnR/DIQ2C5h2jXeRnwVJDRiD5yMN5IgbzOBJodmEgRFIHSATbv/DhRUaTLF06/oFkM/s2ef+V+vLGh3kgBSZUNgCJ0fhNrw1R
IgeeJTk8o7ekFWaXln2Jg==

Firmante: MARYTELL CASTELLANOS RUEDA
RFC: [REDACTED]

Número de Serie: [REDACTED]
Fecha de Firma: 28/07/2026 13:47

Certificado:



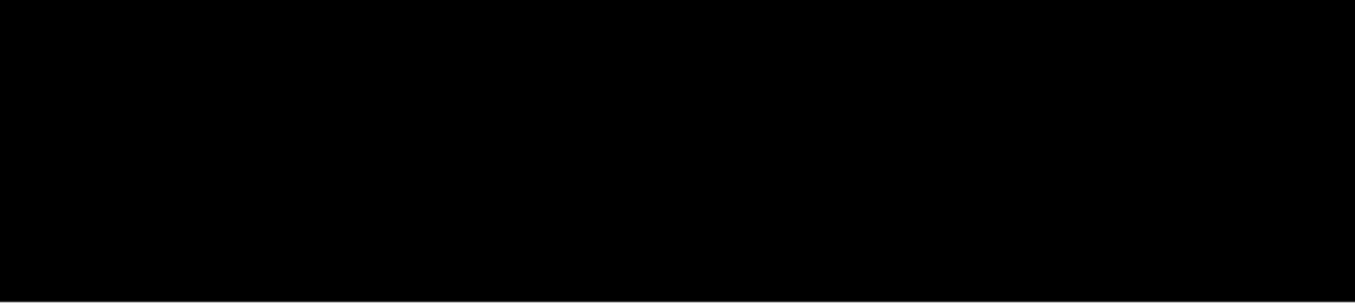
Firma:

JfGeFNUa2x2vwji20j9rpu2RqaLxepJbyBH5FG6N1gmDevImh7yqvD0xUNAV9o2ecBBLy/ns1l51Ne6FgVZBy1o2udTNKb9cWk0ANcb7gt/qbS0xtfkoa07ohm++dC7vPRhQt2+gp/kc+sJIqSINbwS9nRAOBAR
ZjwHjSi7mR82sNFPsEPOMU3mkLjaxLmshr4X2kuoZ5KINsey4xDDfMEWY4HYCJBrYyXbaE0MHhb1zS172TKo0Z8GAXCzy84vPSibKM0vdJQqUZV1HZfHHoi5rdyygFpEbrf1PXXLTJ5jH38rShD6wD4gU45qV0/
EEX3CCvhr26FndoBr3nHyw==

Firmante: HUMBERTO DAVID ROSALES HERRERA
RFC: [REDACTED]

Número de Serie: [REDACTED]
Fecha de Firma: 28/07/2026 14:30

Certificado:



Firma:

Se elimina número de serie y certificado de firma electrónica de persona moral,
con fundamento en el Artículo 115, párrafo cuarto de la LGTAIP.

LpQcYPe+EQnsM0GLZ8SOYjQF4UyAjAcXPu7UtleLAhfP5sqTrZjyi3n+OSMNqM3UoUEHXFMDUQG0xwNte0aVNxOgfeVgKvhnqJUV/2mZGVJKRBPMQwFBXE+KPbFjlcA+GM66uvQ2hckiOZSEwNJR XOilpntuMERI
YerfJBigyC LUWUr2Rjpd2WCe8htAtDRYGBR7+YEUsvGMKgnDKLuFyaLKa6nuoihtwPAtyq1kZeYwyBSrCB184aUH3YEUkcAZM1vp4ExixIW rNJ9hc9Cr1DrpiNt21XEmO9oxJHboB14y07ULXTBa1PTvEVB YvM1
w1mgW2DCyRU8+N7UqyUy0w==

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

Número de Serie: [REDACTED]
Fecha de Firma: 28/07/2026 14:40



Firma:
odSTyVMezen57EY8H/69IN0zjnJwezgoZ5IQGoKVNwpqUUn8L1IK9IGY6wr3tqILctq9ISf7c69YKPS3YkgU+T77t7bTu5KLsUIgtDW5UKXHYN7K/xXQfkLVGxqyI13/NEvqiVZAQqZCRiftl3GbJsBvxVcWJoygV
0uCAJyXkbuHi+f58CP/0GxK6V9z2DdOKdkW/6zVn+rElWtG2C7gbIVbksD9FYvd4+UKfQl0ZawkDgh0Xi v7hkuXbOk5fjvv6iXGSd6UQ1NqQTh7fbuQnKzIGteEp38XTIAZXj4+vCXe2jKlGK7xv62BxfsiY7bdZ
CdDTlmr5M7wzeAbcm1jqzw==



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

ID BANOBRAS-2026-O-000505

ACTDTIC-FI03. ANEXO TÉCNICO

Estrategia Institucional de Contrataciones

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

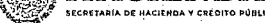
carls
X

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	2 de 86
		De ini de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico

1. Tabla de Contenido

1.	GLOSARIO.....	6
2.	OBJETIVO GENERAL.....	8
3.	OBJETIVOS ESPECÍFICOS	8
4.	SITUACIÓN ACTUAL.....	9
4.1.	ARQUITECTURA ACTUAL.....	9
4.2.	LÍNEA BASE	9
4.3.	PERSONAL.....	10
4.4.	UBICACIÓN	21
4.5.	HERRAMIENTAS TECNOLÓGICAS.....	21
5.	NECESIDAD A SER CUBIERTA	24
5.1.	BENEFICIOS ESPERADOS	24
5.2.	REQUERIMIENTOS Y/ O SERVICIOS GENERALES	25
5.3.	APLICACIONES Y/O PROCESOS DE NEGOCIO INVOLUCRADOS EN EL SERVICIO	50
5.4.	ARQUITECTURA PROPUESTA.....	52
6.	ALCANCE.....	53

2-125

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	3 de 86
		De ini de elaboración	06/11/2025
		Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico

6.1. VIGENCIA	53
6.2. ROLES Y RESPONSABILIDADES	53
6.3. CALIDAD	58
6.4. LUGAR PARA LA PRESTACIÓN DE SERVICIOS	58
6.5. FORMA Y TÉRMINOS EN QUE SE REALIZARÁ LA VERIFICACIÓN Y ACEPTACIÓN DEL SERVICIO	59
6.6. CRONOGRAMA.....	59
7. REQUERIMIENTOS Y/O SERVICIOS ESPECÍFICOS.....	60
7.1.1. OPERACIÓN DEL SERVICIO.....	60
7.1.1.1. PUESTA A PUNTO DEL SERVICIO.....	60
7.1.2. ENTREGABLES	61
7.1.2.1. ENTREGABLES DE ÚNICA VEZ.....	61
7.1.2.2. ENTREGABLES PERIÓDICOS.....	63
7.1.3. CUMPLIMIENTO NORMATIVO.....	71
7.1.3.1. CUMPLIMIENTO NORMATIVO	71
7.2. REQUERIMIENTOS OPERATIVOS.....	72
7.2.1. DERECHO DE USO Y SOPORTE.....	72
7.2.2. TIEMPOS DE RESPUESTA DE SOPORTE Y SERVICIO	72



	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	4 de 86
		De ini de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

8. ACUERDOS DE NIVELES DE SERVICIOS Y OPERACIONALES 72

8.1. ACUERDOS DE NIVEL DE SERVICIOS (SLA ´S)..... 72

8.2. ACUERDOS DE NIVELES DE OPERACIÓN ENTRE CONTRATOS (OLA ´S) 75

9. PENAS CONVENCIONALES Y DEDUCCIONES AL PAGO. 75

9.1. PENAS CONVENCIONALES..... 75

9.2. DEDUCCIONES AL PAGO 76

10. CONFIDENCIALIDAD..... 77

11. LICENCIAS, AUTORIZACIONES Y PERMISOS. 77

12. AUDITORÍA..... 78

13. MODELO DE PROPUESTA ECONÓMICA Y FORMA DE PAGO 78

13.1. MODELO DE PROPUESTA ECONÓMICA..... 78

13.2. FORMA DE PAGO 80

14. PROPUESTA TÉCNICA 81

14.1. PRESENTACIÓN DE LA PROPUESTA TÉCNICA..... 81

14.1.1. LENGUAJE 81

14.1.2. DIAGRAMAS..... 82

14.2. DOCUMENTACIÓN REQUERIDA PARA LA ENTREGA DE LA PROPUESTA TÉCNICA..... 82

2-12

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	5 de 86
		De ini de elaboración	06/11/2025
		Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico

15.CRITERIO DE EVALUACIÓN..... 83

16.GARANTÍA DE ANTICIPO / GARANTÍA DE CUMPLIMIENTO / EXCEPCIÓN DE LA PRESENTACIÓN DE LA GARANTÍA DE CUMPLIMIENTO..... 83

17.NORMAS DE CALIDAD (ISO), NORMAS OFICIALES, NORMAS MEXICANAS, NORMAS INTERNACIONALES..... 84

18.TIPO DE CONTRATO..... 84

19.DENOMINACIÓN DEL ÁREA ADMINISTRADORA Y TÉCNICA DEL CONTRATO..... 84

20. FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN..... 86

[Handwritten signature]
[Handwritten signature]
[Handwritten signature]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	6 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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.

X

21/11/25

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	7 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

Término	Descripción
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

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	8 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

Término	Descripción
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 General

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.

3. Objetivos Específicos

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:

- S1 - Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.
- S2 - Realización periódica de análisis seguridad de sistemas.
- S3 - Reducción de la superficie de ataque del ecosistema de los sistemas.

(Handwritten mark)

(Handwritten mark)

(Handwritten mark)

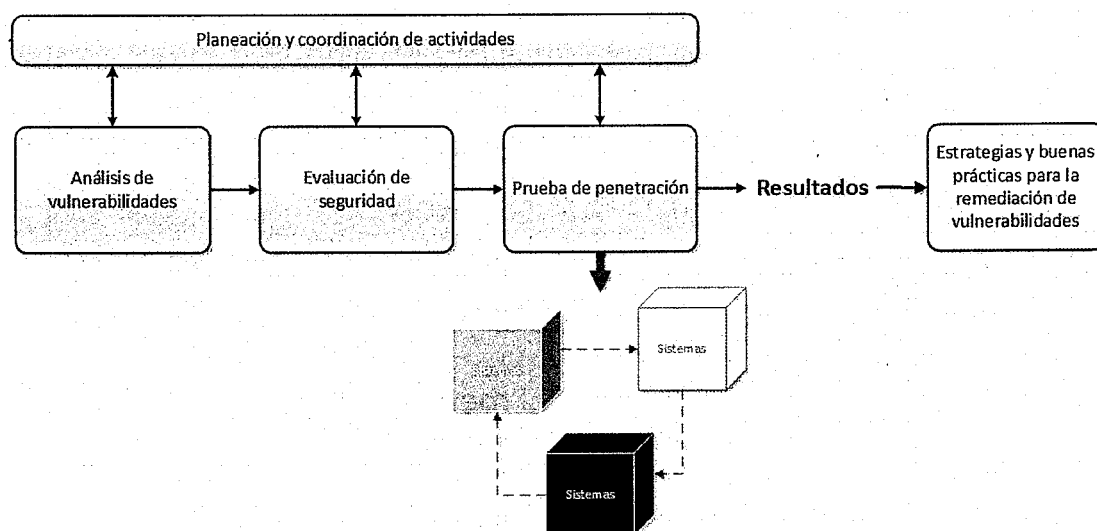
	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	9 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

- S4 –Sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365.
- S5 - Modelado de adversario Blue-Team Red-Team.

4. Situación actual

A través de la implementación de los servicios de ciberseguridad, se han identificado un gran número de vulnerabilidades en la infraestructura tecnológica y los aplicativos de BANOBRAS, por lo que, es de suma importancia dar continuidad a los servicios de ciberseguridad para evitar que las vulnerabilidades identificadas o por identificar, se conviertan en una amenaza a algún activo de información y se materialice en un riesgo o posible incidente de seguridad para BANOBRAS. Adicionalmente, es importante mencionar que el contar con la contratación de estos servicios, ha permitido dar cumplimiento a las regulaciones que aplican a BANOBRAS, principalmente en el cumplimiento de las disposiciones establecidas por Banco de México, la Comisión Nacional Bancaria y de Valores (CNBV) y la Unidad de Gobierno Digital.

4.1. Arquitectura actual



4.2. Línea Base

El alcance de la Infraestructura Tecnológica consta de:

Alcance	Número aproximado
Infraestructura virtual	648

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	10 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

Infraestructura física	523
Aplicaciones o sistemas	63
Estaciones de trabajo	1516

4.3. Personal

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.

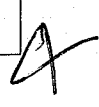
EL LICITANTE GANADOR deberá brindar los servicios establecidos conforme a la solicitud del perfil requerido. EL LICITANTE GANADOR deberá presentar a todos los recursos que cumplan con el perfil requerido y sus certificaciones respectivamente para brindar los servicios de ciberseguridad.

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 al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: PMP (Project Management Professional)	1 recurso

[Handwritten signature and initials]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	11 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

Componente	Perfil	Requisitos	Cantidad
		Certificaciones Opcionales: • 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 • CISM - Certified Information Security Manager • Líder Auditor ISO/IEC 27001 • Líder Auditor ISO/IEC 22301 • Líder Auditor ISO/IEC 27002 • Líder Auditor ISO/IEC 27701	
	Especialista en cumplimiento	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • Certified Fraud Examiner - ACFE	1 recurso


Componente	Perfil	Requisitos	Cantidad
		Certificaciones Opcionales: • CISA - Certified Information Systems Auditor. • CISM - Certified Information Security Manager • CRISC - Certified in Risk and IS Control • CDPSE - Certified Data Privacy Solutions Engineer y CGEIT - Certified in the Governance of Enterprise IT	
	Líder técnico de ciberseguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • CISSP (Certified Information Systems Security Professional) Certificaciones Opcionales:	1 recurso

X

21/12/25

Componente	Perfil	Requisitos	Cantidad
		- Certified ISO/IEC 27001 Lead Auditor - Certified ISO/IEC 27032 Lead Cybersecurity Manager - CRISC - Certified in Risk and IS Control - CISA (Certified Information Systems Auditor) - CISM (Certified Information Security Manager)	
	Auditor de ciberseguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: - ISO 22301 Lead Auditor Certificaciones Opcionales: - Líder Auditor ISO/IEC 27001 - Líder Auditor ISO/IEC 22301 - Líder Auditor ISO/IEC 27002 - Líder Auditor ISO/IEC 27701	1 recurso

[Handwritten signature]

[Handwritten signature]

Componente	Perfil	Requisitos	Cantidad
S2	Líder técnico de seguridad en sistemas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: - OSWP (Offensive Security Wireless Professional) Certificaciones Opcionales: - CompTIA Security+ ce - Certified Ethical Hacker (Master) - ISO/IEC 27032 Lead Cybersecurity Manager - Certified OSSTMM 3.0 Professional Security Analyst OPSA - Offensive Security Certified Professional (OSCP) - GIAC Penetration Tester Certification (GPEN) - GIAC Web Application Penetration Tester (GWAPT) - Red Team Operator	1 recurso

6

X

2/12

Componente	Perfil	Requisitos	Cantidad
	Especialista en pruebas estáticas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • CompTIA Security+ ce Certificaciones Opcionales: • Líder Auditor ISO/IEC 27001	3 recursos
	Especialista en pruebas dinámicas	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil.	1 recurso

[Handwritten signature]

[Handwritten signature]

Componente	Perfil	Requisitos	Cantidad
		Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: - Certified OSSTMM 3.0 Professional Security Analyst (OPSA) Certificaciones Opcionales: - Certified Ethical Hacker (Master) - CompTIA Security +	
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. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas.	1 recurso

(Handwritten mark)

(Handwritten mark)

(Handwritten mark)

Componente	Perfil	Requisitos	Cantidad
		Deberá contar con cursos en: - Enterprise Security Fundamentals - Directorio Activo	
	Auditor de riesgos de seguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: - CCISO – Chief Information Security Officer Certificaciones Opcionales: - Certified ISO/IEC 27001 Lead Auditor - Certified ISO 22301 Lead Auditor	1 recurso

Componente	Perfil	Requisitos	Cantidad
S4	Analistas de seguridad	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • CompTIA Security+ o Certified Incident Handler (CIH) Certificaciones Opcionales: • Líder Auditor ISO/IEC 27002 • Líder Auditor ISO/IEC 27701	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 al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil.	1 recurso

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	19 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

Componente	Perfil	Requisitos	Cantidad
		Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • CNSS (Certified Network Security Specialist) Certificaciones Opcionales: • ITIL v3 o v4 Foundation Certificate in IT Service Management • Certified ISO/IEC 27001	
S5	Líder técnico de Red Team	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus	1 recurso

[Handwritten signature]

[Handwritten signature]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	20 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

Componente	Perfil	Requisitos	Cantidad
		últimos empleos con organizaciones distintas. Certificación Obligatoria: • GIAC Penetration Tester (GPEN) Certificaciones Opcionales: • GIAC Cloud Threat Detection (GCTD) • GIAC Continuous Monitoring Certification (GMON) • GIAC Cyber Threat Intelligence (GCTI)	
	Especialista de Red Team	Contar con Título o Cédula profesional de ingeniería o licenciatura en sistemas computacionales, administración o afín. Contar con al menos 3 años de experiencia en proyectos similares, demostrados en CV el cual deberá ser firmado por el perfil. Presentar identificación oficial legible. Presentar al menos 3 cartas de recomendación de sus últimos empleos con organizaciones distintas. Certificación Obligatoria: • Certified Ethical Hacker	1 recurso

[Handwritten signature]

[Handwritten mark]

[Handwritten initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	21 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

Componente	Perfil	Requisitos	Cantidad
		Certificaciones Opcionales: • Certified OSSTMM 3.0 Professional Security Analyst OPSA • CompTIA Security+ ce • CHFI Computer Haking Forensic Investigator • EC-Council Certified Incident Handler	

4.4. Ubicación

Avenida Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219, en piso 9

4.5. Herramientas tecnológicas

Se enlistan las herramientas de manera enunciativa más no limitativa que podrán emplearse:

SERVICIO S1

DNS Dumpster, ROBTEX, NIKTO, CURL, FEROXBUSTER, OWASP ZAP, NESSUS, ACUNETIX, BURPSUITE, DIRP, BLOODHOUND, NPAM, en conjunto con LDAPDomainDump, nbtscan, nmblookup, snmpbrute.py, snmpwalk, snmp-check, ntpdc, ntpq, dnsrecon, DNSenum, fierce, hydra, PICUS, smbmap, crackmapexec, cualquier otra herramienta que cumpla con lo solicitado en el servicio

SERVICIO S2

Deesrcaner, SonarQUBE, Burpsuite y OWASPZAP, cualquier otra herramienta que cumpla con lo solicitado en el servicio

SERVICIO S3

ADAudit Plus / Manage Engine, ADManager Plus / Manage Engine y PowerShell/Windows, cualquier otra herramienta que cumpla con lo solicitado en el servicio

[Handwritten signatures and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	22 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

SERVICIO S4

Elastic Stack, Elasticsearch, Kibana, Wazuh, Suricata, cualquier otra herramienta que cumpla con lo solicitado en el servicio

Herramientas de cacería de amenazas:

Pignus PinkShark, Night Guard Dark Web, Fire Tank, dnsrecon, dnsenum, theHarvester, Spiderfoot, nmap, cualquier otra herramienta que cumpla con lo solicitado en el servicio

Buscadores especializados:

Google, Yahoo!, Duck Duck Go, Bing, Yandex y Tor, cualquier otra herramienta que cumpla con lo solicitado en el servicio

SERVICIO S5

MITRE CALDERA, ATOMIC RED TEAM, BURPSUITE, PICUS o cualquier otra herramienta que cumpla con lo solicitado en el servicio

4.6 Aplicaciones y /o Procesos de Negocio involucrados en el Servicio

Se enlistan las aplicaciones de manera enunciativa más no limitativa:

- Roles y Facultades
- Portal FONADIN
- Portal Intranet Banobras
- Sistema de Contabilidad Financiera
- Módulo de Contingencia en SPEI
- Sistema de Reportes TRANSFINT
- Sistema de Información Crediticia a Buró de Crédito
- Sistema de Planeación y Control
- Sistema de Control de Gestión Documental
- Fideicomiso 1936 FONADIN
- Sistema de Seguimiento, Supervisión y Alertamientos de los Reportes Regulatorios de Banobras
- Sistema de Administración y Actualización del Inventario de Procesos de Banobras
- Herramienta de Reportes para Módulo de Rentabilidad en SICOFIN
- Sistema de Control de Viáticos
- Módulo de Análisis de Crédito
- Sistema Var Mercados
- Sistema de Administración de Riesgos de Crédito
- Sistema Fiduciario Yatla





	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	23 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

- Sistema Integral de Cartera
- Consulta a la Base de Datos de Transferencias
- Sistema de Consulta de Comprobante Electronico de Pagos
- Portal de Consulta de Comprobantes Fiscales Digitales
- Portal de Transparencia
- Enlace Financiero IndevaI
- Enlace Financiero SPEI
- Registro Nacional de Población
- Sistema de Requerimientos de Capital
- Portal Proyectos México
- Banobras Hoy
- Sistema para Seguimiento y Clasificación del Crédito
- Sistema de Consulta y Descarga de Expediente Electronico de Crédito
- Sistema de Administración de Clientes
- Sistema de Administración de Originación de Crédito
- Sistema de Prevención de Lavado de Dinero y Financiamiento al Terrorismo de Banobras
- Almacén de datos Operativos
- Sistema de Recursos Humanos LOBO-RH/Intra LOBO
- Sistema de Recursos Humanos LOBO-RH (Activos)
- Sistema de Recursos Humanos LOBO-RH (Jubilados)
- Sistema de Recursos Humanos LOBO-RH (Citrix)
- Capacitación de Recursos Humanos
- Registro de Eventos de Riesgos Operativos
- Gestión Integral de Riesgo Operacional
- Sistema de Control de Gestión del Área de Presupuesto
- "Sistema de Mercados Financieros
- IKOSNET"
- "Sistema de Mercados Financieros
- CASHNET"
- Interfaz P&L-SIMEFIN
- ESB Enterprise Service BUS
- Calificadoras
- Portales de Colaboración 2022
- Portales de Colaboración 2016
- Portal de Contabilidad (WEBCONTA)
- XVAS Derivados
- Tableros de Información de la DTIC (QLIK)
- Portal de Operación de la DTIC
- Portal Institucional
- "Sistema de Pérdida Crediticia Esperada para Cuentas por Cobrar
- PCE CXC"
- Sistema de Pérdida Crediticia Esperada para Instrumentos Financieros PCE IF
- PCC Plataforma Integral de Calificación de Cartera
- Conciliación de Corros
- REPOFIDU Sistema Contenedor Documental de Instrucciones de Pago de Fideicomisos
- Seguimiento de Reportes Regulatorios
- PCE IF Módulo de Cálculo de Perdida Crediticia para Instrumentos Financieros
- PCE CXC Módulo de Cálculo de Perdida Crediticia para Cuentas por Cobrar





	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	24 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

5. Necesidad a ser cubierta

BANOBRAS tiene el compromiso de proteger y asegurar niveles adecuados de confidencialidad, disponibilidad e integridad de la información, apoyándose en controles de seguridad de la información, con la finalidad de salvaguardar la información de los clientes, mantener la continuidad de negocio, evitar daños a los activos y reputación del Banco.

Por otra parte, se requiere contar con los “Servicios de Ciberseguridad”, con la finalidad de dar cumplimiento a las iniciativas y proyectos establecidos en el Plan Director de Seguridad, conforme se establece en los artículos 168 Bis 12 y 14, fracción I y II respectivamente, de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito.

Se requiere realizar pruebas de análisis de vulnerabilidades a toda la infraestructura tecnológica (incluyendo SPEI, BDT e INDEVAL) en apego a lo indicado en las “Disposiciones de carácter general aplicables a las instituciones de crédito, Artículo 168 Bis 12, numeral III” y a lo establecido por “Banco de México”.

Asimismo, se debe contratar a un tercero independiente, 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 los diferentes sistemas y aplicativos 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, en apego a lo indicado en las “Disposiciones de carácter general aplicables a las instituciones de crédito, Artículo 168 Bis 12, numeral IV”.

Adicionalmente, BANOBRAS no cuenta con una herramienta que proporcione la capacidad para detectar y dar respuesta rápida ante posibles amenazas o incidentes de seguridad, y tampoco cuenta con personal certificado en un esquema de 24x7x365 para el monitoreo y la atención de cualquier evento, amenaza o incidente de seguridad.

5.1. Beneficios esperados

- Minimizar los riesgos tecnológicos de seguridad que pudieran atentar contra la integridad, disponibilidad y confidencialidad de la información de BANOBRAS.

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	25 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

- Mitigar de forma efectiva las vulnerabilidades identificados.
- Proteger la información sensible y los servicios de Banobras ante ataques, robo y pérdida de información.
- Reducir a niveles aceptables la atención de incidentes de seguridad derivados del establecimiento de mecanismos de respuesta a incidentes de seguridad, así como la comunicación y colaboración.
- Reducir la superficie de ataque asegurando las capacidades de la infraestructura.

5.2.Requerimientos y/ o Servicios Generales

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 8.1 "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 8.1 "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.

①

4

2025

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	26 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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 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.

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 Requiriente 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.

"EL LICITANTE" deberá incluir como parte de su propuesta, escrito en hoja membretada en el que se manifieste que en los últimos seis años y hasta la fecha de emisión de la propuesta técnica, que ninguno de sus clientes en el orden de Gobierno Federal, Estatal o Municipal, ha sido vulnerado y/o expuesto de manera pública y que la información de sus clientes no ha sido expuesta públicamente (en medios de comunicación, Redes Sociales, Dark Web, o plataformas digitales) a raíz de incidentes de seguridad informática y que la imagen pública de sus clientes no fue afectada durante ese periodo, cuando se han prestado SERVICIOS DE

(Handwritten mark)

(Handwritten mark)

(Handwritten mark)

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	27 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03, Anexo Técnico	

CIBERSEGURIDAD o similares a los de este anexo bajo contrato. En el caso de participación conjunta, el presente escrito deberá ser presentado por cada uno de los participantes. Lo anterior para acreditar las capacidades de "EL LICITANTE" para evitar la exposición de información sensible de BANOBRAS, y/o datos de orden gubernamental y financiero; además de no verse afectado el daño reputacional de la imagen institucional de BANOBRAS.

"EL PRESTADOR DE SERVICIOS" que actualmente tenga vigente un contrato de servicio de Tecnologías de la Información con BANOBRAS específicamente referente al servicio de centro de datos y/o fábrica de software, no podrá participar en esta licitación, lo anterior con la finalidad de garantizar la objetividad del servicio para evitar que el mismo proveedor se autoevalúe en la infraestructura que proporciona y/o administra para BANOBRAS.

Es indispensable que todos LOS LICITANTES participantes cuenten con las certificaciones en las siguientes normas: ISO/IEC 27001:2022 o superior, ISO 9001:2015 o superior, ISO/IEC 22301:2019 o superior, ISO/IEC 20000-1: 2018 o superior e ISO 37001:2016 o superior (*el incumplimiento del punto es motivo de desechamiento*).

Se debe contar con al menos cinco (5) de los siguientes procesos certificados en todas las normas ISO antes mencionadas:

- Forense Digital.
- Centro de Operaciones de Seguridad "SOC".
- Inteligencia de Análisis de Información Digital.
- Mesa de Ayuda Especializada en la Atención y Gestión de Incidentes de Seguridad de la información.
- Análisis y Monitoreo Externo de la Información para el Alertamiento de Riesgos y Ciber amenazas.
- Gobierno de Seguridad y Cumplimiento Normativo.
- Protección Digital de la Identidad Corporativa mediante el Análisis de Ciber amenazas.

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) con una antigüedad de

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	28 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

ser miembro como mínimo de 5 años como país de origen México (el incumplimiento del punto es motivo de desechamiento).

Es indispensable que todos LOS LICITANTES participantes cuenten con la acreditación como ISTQB PARTNER para demostrar que cuenta con la especialidad en la realización de pruebas de caja blanca o estructurales para examinar el código, la infraestructura y la interacción con sistemas externos, verificar el código fuente, identificar errores y vulnerabilidades y obtener información sobre la calidad y seguridad del código de software.

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.

SERV#	Descripción
SERVICIO 1 - Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad	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 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 en la infraestructura tecnológica de manera trimestral con personal que cuente con

[Handwritten signature]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	29 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

	capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia, 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 8.1 "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 el titular de 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.
--	---

[Handwritten signature and date 20/11/25]

- 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.

[Handwritten signature and date 24/10]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	32 de 86
			Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

- 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 o a petición de BANOBRAS

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

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.
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 8.1 "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 8.1 "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.
7. EL LICITANTE GANADOR deberá elaborar un reporte de resultados conforme lo establecido en el componente S1, del numeral 8.1 "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 enlistan las siguientes actividades de manera enunciativa más no limitativa:

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

SERVICIO 2 **-** **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 BANOBAS 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 "7.1.3 Entregables y 8.1 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

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	36 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

	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 “7.1.3 Entregables y 8.1 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 8.1 “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),
--	---

[Handwritten signature]

- 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 8.1 "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 "7.1.3 Entregables y 8.1 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 8.1 "Niveles de Servicio".
SERVICIO 3 - 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 ✓ 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 8.1 "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

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	40 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

	• 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
SERVICIO 4 - 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

[Handwritten signature]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	41 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

	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 híbrida conforme a lo establecido en el componente S4, del numeral 8.1 "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.

[Handwritten signature]
Cafro

- ✓ 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 reuso 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, ETD.
- 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.

[Handwritten signature]
20/10

- 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.

[Handwritten signature]

[Handwritten signature]

SERVICIO 5
- Modelado
de
adversario
Blue-Team
Red-Team.

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.

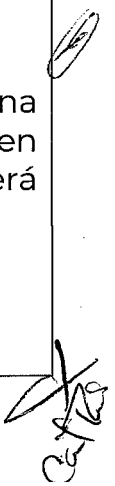
Los servicios deberán ser realizados durante la vigencia del contrato y con estricto apego a las políticas y procedimientos actuales y sus respectivas actualizaciones de BANOBRAS, las cuales serán dadas a conocer al licitante ganador, en la oficina de la DSI, ubicada en Av. Javier Barros Sierra 515, 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 8.1 "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.
- Identificar los activos bajo prueba.
- Identificar la existencia de algunos controles detectivos de la actividad probada por parte del equipo AZUL.
- 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

Handwritten signature and initials:
C/RE

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 8.1 "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

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	50 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

	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 interceptación de llamadas ✓ No se puede comprometer a subsidiarias ni afiliadas sin un permiso explícito ✓ 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.

5.3. Aplicaciones y/o procesos de Negocio involucrados en el Servicio

Se enlistan las aplicaciones de manera enunciativa más no limitativa:

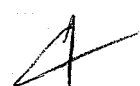
- Roles y Facultades
- Portal FONADIN
- Portal Intranet Banobras
- Sistema de Contabilidad Financiera
- Módulo de Contingencia en SPEI

4

20/12

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	51 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

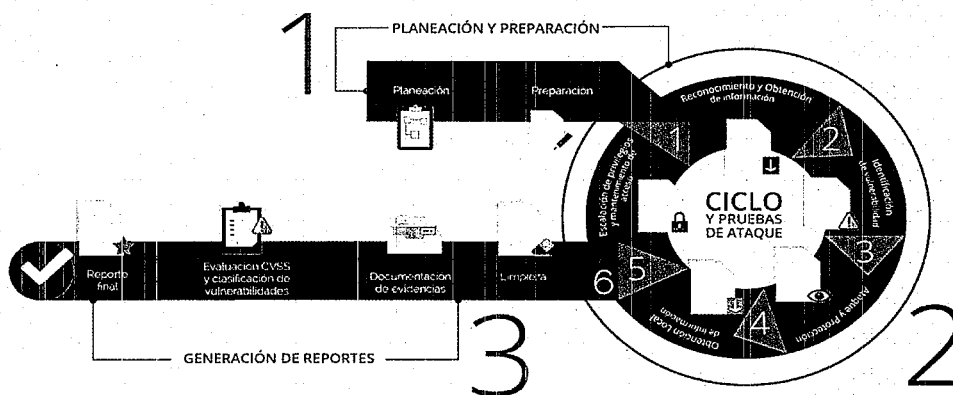
- Sistema de Reportes TRANSFINT
- Sistema de Información Crediticia a Buró de Crédito
- Sistema de Planeación y Control
- Sistema de Control de Gestión Documental
- Fideicomiso 1936 FONADIN
- Sistema de Seguimiento, Supervisión y Alertamientos de los Reportes Regulatorios de Banobras
- Sistema de Administración y Actualización del Inventario de Procesos de Banobras
- Herramienta de Reportes para Módulo de Rentabilidad en SICOFIN
- Sistema de Control de Viáticos
- Módulo de Análisis de Crédito
- Sistema Var Mercados
- Sistema de Administración de Riesgos de Crédito
- Sistema Fiduciario Yatla
- Sistema Integral de Cartera
- Consulta a la Base de Datos de Transferencias
- Sistema de Consulta de Comprobante Electronico de Pagos
- Portal de Consulta de Comprobantes Fiscales Digitales
- Portal de Transparencia
- Enlace Financiero Indéval
- Enlace Financiero SPEI
- Registro Nacional de Población
- Sistema de Requerimientos de Capital
- Portal Proyectos México
- Banobras Hoy
- Sistema para Seguimiento y Clasificación del Crédito
- Sistema de Consulta y Descarga de Expediente Electronico de Crédito
- Sistema de Administración de Clientes
- Sistema de Administración de Originación de Crédito
- Sistema de Prevención de Lavado de Dinero y Financiamiento al Terrorismo de Banobras
- Almacén de datos Operativos
- Sistema de Recursos Humanos LOBO-RH/Intra LOBO
- Sistema de Recursos Humanos LOBO-RH (Activos)
- Sistema de Recursos Humanos LOBO-RH (Jubilados)
- Sistema de Recursos Humanos LOBO-RH (Citrix)
- Capacitación de Recursos Humanos
- Registro de Eventos de Riesgos Operativos
- Gestión Integral de Riesgo Operacional
- Sistema de Control de Gestión del Área de Presupuesto
- "Sistema de Mercados Financieros
- IKOSNET"
- "Sistema de Mercados Financieros
- CASHNET"
- Interfaz P&L-SIMEFIN
- ESB Enterprise Service BUS
- Calificadoras
- Portales de Colaboración 2022
- Portales de Colaboración 2016


	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	Hoja	52 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

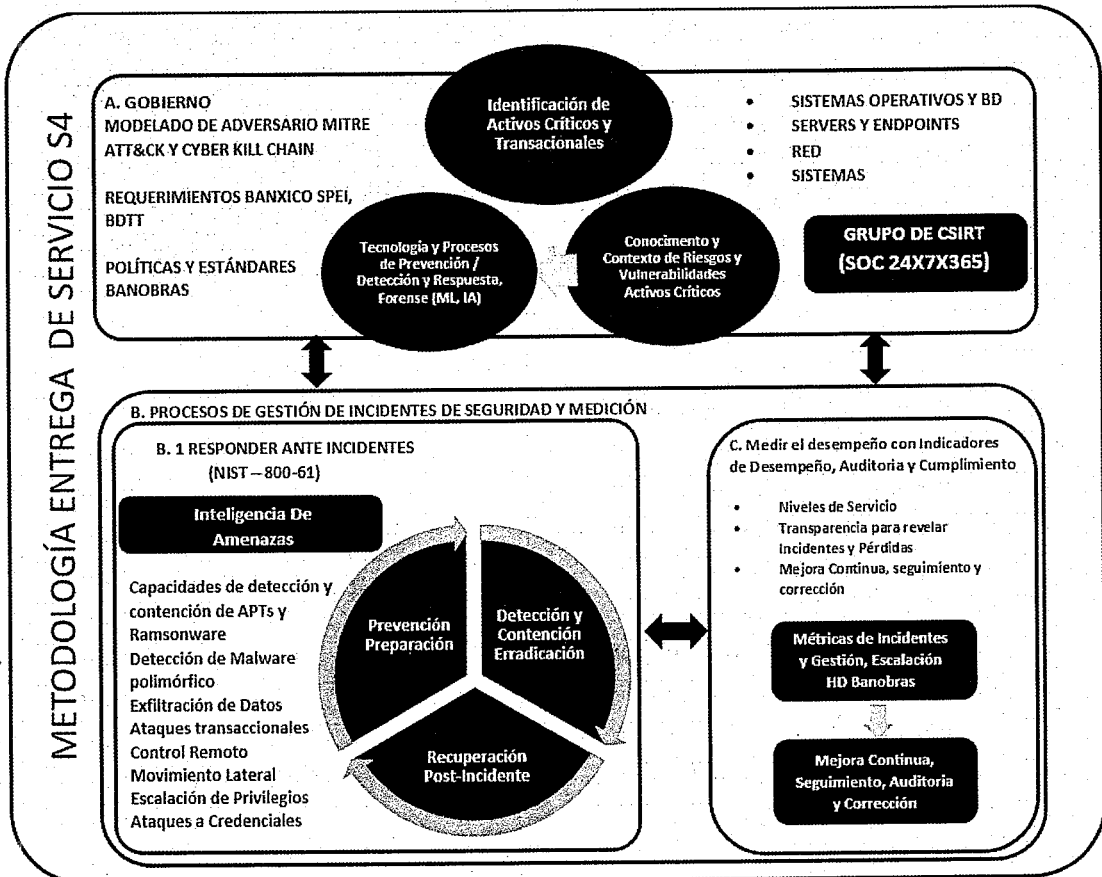
- Portal de Contabilidad (WEBCONTA)
- XVAS Derivados
- Tableros de Información de la DTIC (QLIK)
- Portal de Operación de la DTIC
- Portal Institucional
- "Sistema de Pérdida Crediticia Esperada para Cuentas por Cobrar
- PCE CXC"
- Sistema de Pérdida Crediticia Esperada para Instrumentos Financieros PCE IF
- PCC Plataforma Integral de Calificación de Cartera
- Conciliación de Corros
- REPOFIDU Sistema Contenedor Documental de Instrucciones de Pago de Fideicomisos
- Seguimiento de Reportes Regulatorios
- PCE IF Módulo de Cálculo de Perdida Crediticia para Instrumentos Financieros
- PCE CXC Módulo de Cálculo de Perdida Crediticia para Cuentas por Cobrar

5.4. Arquitectura Propuesta



[Handwritten signature]

[Handwritten signature]



6. Alcance

Alcance	Número aproximado
Infraestructura virtual	648
Infraestructura física	523
Aplicaciones o sistemas	63
Estaciones de trabajo	1516

6.1. Vigencia

Fecha de inicio: Al siguiente día hábil de la notificación del fallo.
 Fecha de término: 31 de diciembre de 2026.

6.2. Roles y responsabilidades

0

4
06/12/2025

Tabla Roles y Responsabilidades Generales

Núm.	Actividad	Licitante Adjudicado	Responsable de Ciberseguridad Institucional (RIC)
1	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.	X	
2	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.	X	
3	EL LICITANTE GANADOR deberá ejecutar los servicios en ambientes controlados y en horarios previamente acordados con la DSI responsable del servicio	X	X
4	EL LICITANTE GANADOR deberá firmar un acuerdo de confidencialidad al día siguiente de la notificación del fallo, el cual debe ser elaborado por BANOBRAS	X	X
5	El personal del LICITANTE GANADOR deberá firmar un acuerdo de confidencialidad personal al día siguiente de la notificación del fallo, el cual	X	X

0

A
25/12

Tabla Roles y Responsabilidades Generales

	debe ser elaborado por BANOBRAS		
6	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.	X	
7	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	X	
8	EL LICITANTE GANADOR deberá incluir los recursos informáticos y herramientas asociadas, hardware y/o software que sea requerido para brindar los servicios solicitados	X	
9	EL LICITANTE GANADOR deberá considerar una etapa de transición de servicio de al menos 1 mes a partir de la finalización del contrato	X	
10	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	X	

[Handwritten signature]

21/12/25

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	56 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

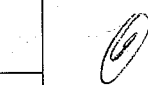
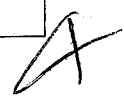
Tabla Roles y Responsabilidades Generales			
	parte de BANXICO, CNBV, u otra Comisión Regulatoria, sin que genere costo alguno para BANOBRAS		
11	EL LICITANTE GANADOR deberá garantizar que el personal certificado que brindará los servicios del presente Requerimiento Técnico, sea personal interno contratado dentro de la organización.	X	
12	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	X	
13	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.	X	
14	EL LICITANTE GANADOR asignará personal para la atención de cualquier garantía de los servicios del presente anexo y será válida dentro de los 6 meses después de haber	X	





 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	Hoja	57 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

Tabla Roles y Responsabilidades Generales			
	entregado los servicios y entregables.		
15	Validar previo a la ejecución de cada servicio el protocolo de pruebas con el Director de Seguridad de la Información	X	X
16	Entregar el detalle de la infraestructura, ambientes, bases de datos y sistemas, durante los 5 primeros días hábiles después de la notificación del fallo, y en caso de actualización se deberá de entregar solamente los activos actualizados.		X
17	Proporcionar los accesos por VPN site to site o para equipo personal en caso de requerirse		X
18	Proporcionar durante los 5 primeros días hábiles después de la notificación del fallo las políticas y procedimientos de seguridad de BANOBRAS.		X
19	Proporcionar el espacio físico, acceso a internet, facilidades para el acceso a la red, conectividad a los sistemas, así como usuarios válidos y alimentación eléctrica.		X
20	Mantener actualizado el inventario de activos tecnológicos		X
21	Proporcionar el acceso a los activos sujetos a análisis en el periodo correspondiente		X


 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANOBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	58 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

6.3. Calidad

- Contar con una lista de verificación de entregables, mismos que deberán estar requisitados al 100% y debidamente firmados por los responsables del servicio dentro del período establecido en la sección de 7.1.3 Entregables
- Los entregables deben proporcionarse en formato editable y físico.
- Cumplimiento en la resolución de eventos en los tiempos definidos, mismos que serán dados a conocer al LICITANTE GANADOR por parte del responsable del contrato.
- Las herramientas deben mantenerse actualizadas y funcionando de manera adecuada durante la vigencia de contrato de los servicios de ciberseguridad.
- Proporcionar servicios de prevención, detección, cibervigilancia, protección y respuesta ante cualquier tipo de amenaza identificadas por BANOBRAS o por el LICITANTE GANADOR.
- Definir acciones encaminadas a proteger a BANOBRAS del hackeo de datos, y aplicar estrictas medidas que ayuden a la detección de vulnerabilidades, así como la gestión de posibles amenazas que afecten la seguridad de la red.
- Los servicios proporcionados en este anexo técnico, deben ayudar a identificar y controlar los riesgos y amenazas de BANOBRAS a corto, mediano y largo plazo.
- Atención personalizada e inmediata con recursos especializados.
- Gestión de la entrega del Servicio controlando que todos los recursos asignados están operativos en la fecha planificada.
- Cumplimiento de los niveles de servicio establecidos en el numeral 8.1 Niveles de Servicio.
- Entender y cubrir las expectativas de la Dirección de Seguridad de la Información.
- Analizar los indicadores y dar propuestas de mejora continua de los servicios.
- Durante la vigencia del contrato, el LICITANTE GANADOR debe apegarse a las políticas de seguridad de la información de BANOBRAS.

6.4. Lugar para la Prestación de Servicios

20/11/25

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	59 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03, Anexo Técnico	

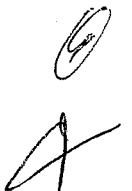
Avenida Javier Barros Sierra 515, Lomas de Santa Fe, Ciudad de México, 01219, en piso 9

6.5. Forma y términos en que se realizará la verificación y aceptación del servicio

Conforme a lo establecido en la planeación del proyecto, los entregables de los servicios de ciberseguridad deben ser verificados, validados y autorizados conforme a lo requerido en el anexo técnico por el titular de la Dirección de Seguridad de la Información.

6.6. Cronograma

Se presenta el cronograma de trabajo con las diferentes etapas de los servicios de ciberseguridad, cuyo detalle será acordado por el LICITANTE GANADOR y el responsable del contrato.




			2026							
	Responsable	Recursos	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
Etapas 1 - Planificación y Arranque										
Presentación de KickOff	Proveedor	AP	X							
Elaboración de Plan de trabajo	Proveedor	AP	X							
Elaboración de Metodologías	Proveedor	AP, EC, LTC, AC	X							
Etapas 2 - Implementación										
Mesas de trabajo para definiciones técnicas, permisos de accesos físicos a infraestructura para los servicios S1, S3 y S4	Proveedor	AP, LTC, LTSS, SADA, LO	X	X						
Instalación de Plataformas en Infraestructuras de Banobras	Proveedor	AP, LTC, LTSS, SADA, LO	X	X						
Etapas 3 - Operación del Servicio										
Servicio S1.- Análisis de vulnerabilidades, pruebas de penetración y verificación de suficiencia de controles de seguridad.	Proveedor	AP, LTSS, EC, LTC, AC	X	X	X	X	X	X	X	
Elaboración y Entrega de reportes del Servicio S1	Proveedor	AP, LTSS, EC, LTC, AC	X	X	X	X	X	X	X	
Servicio S2.- Realización periódica de análisis de seguridad de sistemas	Proveedor	LTSS, EPE, EPD	X	X	X	X	X	X	X	
Elaboración y Entrega de reportes del Servicio S2	Proveedor	LTSS, EPE, EPD	X	X	X	X	X	X	X	
Servicio S3.- Reducción de la superficie de ataque del ecosistema de los sistemas	Proveedor	SADA, ARS	X	X	X	X	X	X	X	
Elaboración y Entrega de reportes del Servicio S3	Proveedor	SADA, ARS	X	X	X	X	X	X	X	
Servicio S4.- Sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad en esquema de 24x7x365	Proveedor	AS, LO	X	X	X	X	X	X	X	
Elaboración y Entrega de reportes del Servicio S4	Proveedor	AS, LO	X	X	X	X	X	X	X	
Servicio S5 - Modelado de adversario Blue-Team Red-Team	Proveedor	AP, LTRT, ERT	X	X	X	X	X	X	X	
Elaboración y Entrega de reportes del Servicio S5	Proveedor	AP, LTRT, ERT	X	X	X	X	X	X	X	

AP	Administrador del proyecto
EC	Especialista en cumplimiento
LTC	Líder técnico de ciberseguridad
AC	Auditor de ciberseguridad
LTSS	Líder técnico de seguridad en sistemas
EPE	Especialista en pruebas estáticas
EPD	Especialista en pruebas dinámicas
SADA	Arquitecto de seguridad en arquitecturas de directorio activo
ARS	Auditor de riesgos de seguridad
AS	Analistas de seguridad
LO	Líder de operación
LTRT	Líder técnico de Red Team
ERT	Especialista de Red Team

7. Requerimientos y/o servicios específicos

7.1.1. Operación del Servicio

7.1.1.1. Puesta a punto del servicio

Durante el primer mes todos los servicios y herramientas deben estar en operación, por lo que, el LICITANTE GANADOR debe informar durante los primeros 5 días hábiles los requerimientos técnicos que se requieren con la finalidad de que se realicen las gestiones necesarias con la Dirección de Tecnologías de Información y Comunicaciones para la puesta a punto de los servicios de ciberseguridad.

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	61 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

7.1.2. Entregables

7.1.2.1. Entregables de Única Vez

Los criterios de aceptación de entregables de única vez se definen en la siguiente tabla:

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito – FCE – s)	Fecha de entrega
E1.PA1	KickOff	Reunión de inicio del proyecto, el cual es una oportunidad para reunirte con tu equipo de trabajo y los participantes antes de que comience el proyecto para que puedan alinearse en cuanto a los detalles clave y así conseguir la aceptación de los hitos críticos	• Presentación • Antecedentes del proyecto • Misión del proyecto • Alcance • Planificación • Roles • Colaboración • Sesión de preguntas y respuestas	Durante los 10 días hábiles posteriores de inicio del servicio
E1.PA2	Plan de trabajo	Definición de actividades para los 5 servicios del presente anexo técnico S1, S2, S3, S4 Y S5	• Establece el objetivo. • Reconoce las limitaciones y facilidades. • Fija las metas y objetivos particulares. • Define responsabilidades en el equipo. • Crea una estrategia.	A los 10 días hábiles posteriores de inicio del servicio

[Handwritten signature and date 24/12]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito – FCE – s)	Fecha de entrega
			• Establece los plazos. • Determina los recursos necesarios. • Mide los resultados	
E1.PA3	Documento de definición de metodologías de los servicios dentro del alcance	Definición de Metodologías para los 5 servicios del presente anexo técnico S1, S2, S3, S4 Y S5	Una metodología de auditoría de seguridad que integre los procesos de los principales estándares de Hacking Ético, Pruebas de Penetración, Análisis de Vulnerabilidades, Escaneos Automatizados y buenas prácticas recomendadas para la seguridad de la información.	A los 10 días hábiles posteriores de inicio del servicio
E2.II	S3 - Memoria técnica de implementación de solución de cuentas de administración local para servidores críticos de la Institución.	Herramienta que permita administrar automáticamente las contraseñas de administración local, en las computadoras miembros del dominio de BANOBRAS, para tener un mayor control de acceso local a los equipos críticos.	• Objetivo • Marco normativo • Propósito • Funcionalidad • Arquitectura • Características principales • Requisitos	Durante el primer mes del servicio

[Handwritten signature]

[Handwritten signature]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito - FCE's)	Fecha de entrega
E2.I3	S4 - Memoria técnica de instalación de soluciones tecnológicas	Presentar de manera descriptiva la "Arquitectura de Soluciones de Ciberseguridad" que permitan a BANOBRAS prevenir, detectar y contener las distintas amenazas y responder de manera oportuna para su erradicación mediante procesos, personas y tecnología.	• Objetivo • Marco normativo • Arquitectura • Instalación • Proceso de comunicación entre servidores • Solución para la prevención, detección, contención y respuesta a amenazas	A los 5 días hábiles posteriores al finalizar la implementación
E2.I4	S4 - Memoria técnica de modelado de indicadores de ataque	Modelado de los indicadores de ataque que serán utilizados para clasificar los eventos de seguridad relacionados con amenazas o agentes de amenaza, tácticas o técnicas de ataque	• Objetivo • Marco normativo • Propósito • Definición de indicadores de ataque	A los 5 días hábiles posteriores al finalizar la implementación

7.1.2.2. Entregables Periódicos

24/12

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito - FCE's)	Fecha de entrega
		infraestructura tecnológica	- Severidad de vulnerabilidades - Activos con mayor número de vulnerabilidades - Vulnerabilidades más frecuentes	ejecución de cada evento
E3.OP4.S1	Reporte de riesgo tecnológico	Información de riesgos asociados a las vulnerabilidades identificadas, así como su nivel de criticidad, que abarcó servidores específicos y estaciones de trabajo de la institución.	- Objetivo - Alcance de la evaluación - Riesgos Operacionales - Riesgos de seguridad - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP5.S2	Reporte de análisis de código estático	Pruebas estáticas con diferentes perspectivas de análisis de código, en conjunto con prácticas internacionales reconocidas por la industria de seguridad de la información, en apego al modelo OWASP Top Ten	- Objetivo - Alcance de la evaluación - Análisis estático - Vulnerabilidades identificadas - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP6.S2	Reporte de análisis dinámico	Ejecución de Pruebas dinámicas, en conjunto con prácticas internacionales	- Objetivo - Alcance de la evaluación - Análisis dinámico	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento

[Handwritten signature]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito - FCE's)	Fecha de entrega
		reconocidas por la industria de seguridad de la información, en apego al modelo OWASP Top Ten	- Vulnerabilidades identificadas - Recomendaciones	
E3.OP7.S2	Reporte de indicadores de vulnerabilidades de sistemas	Indicadores gráficos de las vulnerabilidades identificadas de las aplicaciones	- Severidad de vulnerabilidades en aplicativos - Vulnerabilidades por aplicativos - Riesgos por aplicativos - Causas de vulnerabilidad por su tipo de solución	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP8.S3	Memoria técnica de implementación de la herramienta con las características detalladas en la sección "Herramienta de Monitoreo y validación de cambios del directorio activo".	Auditar los cambios del Directorio Activo en tiempo real, a través del diagnóstico del estado de riesgo del Directorio Activo, permitiendo la capacidad de proponer una estrategia de mejora	- Objetivo - Requisitos del sistema - Configuraciones - Arquitectura y funcionamiento - Controladores de dominio - Instalación de agentes - Cambios en configuraciones - Monitoreo	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP9.S3	Informe de Riesgos de ciberseguridad, recomendaciones y validaciones de implementación de hardening en el directorio Activo	Validar a través de este informe la implementación de las recomendaciones de "hardening", para el incremento de la	- Objetivo - Seguridad de los controladores de dominio - Seguridad física	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento

[Handwritten signature and date 05/10]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito – FCE's)	Fecha de entrega
		seguridad de los controladores de dominio	- Validación de resultados - Medidas correctivas - Recomendaciones	
E3.OP10.S3	Reporte de recomendaciones y validaciones en la implementación de las estrategias de aislamiento o actualización en sistemas obsoletos definidos por la Institución.	Activos que integran el directorio activo que presentan un posible riesgo al no contar con un soporte, se encuentran desactualizados o sistemas que no cuentan con los parches de seguridad necesarios	- Objetivo - Estrategias de aislamiento o migración de sistemas obsoletos - Uso de servicios de soporte extendido - Sistemas operativos sin soporte - Monitoreo - Validación de resultados - Medidas correctivas - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP11.S3	Reporte de recomendaciones y validaciones en la implementación de las estrategias de depuración con criterios de ciberseguridad del Grupo de Domain Admins y cuentas de altos privilegios.	Revisar y proponer recomendaciones de seguridad para realizar la correcta depuración de cuentas del grupo "Domain Admins" y cuentas de altos privilegios, con la finalidad de disminuir los riesgos dentro de las configuraciones ante intentos de suplantación,	- Objetivo - Entorno Actual - Enterprise Admin - Domain Admin - Local Admin - Schema Admin - Configuración de cuentas - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento

[Handwritten signature and initials]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito - FCE's)	Fecha de entrega
		robo y/o daño de activos existentes		
E3.OP12.S3	Reporte de recomendaciones y validaciones de la implementación de las estrategias de depuración de cuentas de Directorio Activo, incluyendo permisos, privilegios y ACLs.	Brindar las recomendaciones necesarias para la ejecución de tareas de depuración sobre cuentas que forman parte del directorio activo, asegurando que las cuentas, permisos y privilegios mantienen su integridad, revisadas mediante un proceso de certificación periódico y depuradas conforme a la normatividad interna	- Objetivo - Comprobación de cuentas de usuario - Verificación de Unidades Organizacionales - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP13.S3	Memoria técnica de implementación del sistema de accesos privilegiados de administración del directorio activo (PAW).	El propósito es poder aplicar los controles de seguridad para generar conexiones de confianza hacia equipos que son de alto riesgo, mayormente el enfoque es para sistemas críticos	- Objetivo - Requisitos - Controles de seguridad - Proceso de integración al Directorio Activo	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento
E3.OP17.S4	Reporte mensual de actividades sospechosas	"ACTIVIDADES SOSPECHOSAS" identificadas en el proceso de monitoreo y	- Objetivo - Actividades sospechosas identificadas	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario

[Handwritten signature]

[Handwritten signature]

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito – FCE's)	Fecha de entrega
		respuesta a incidentes de seguridad y cacería de amenazas de ciberseguridad que pudieran comprometer la seguridad de la Institución.	• Estatus de seguridad e inteligencia • Monitoreo de actividades sospechosas a través de una herramienta • Reporte de amenazas • Recomendaciones	
E3.OP18.S4	Reporte mensual de eventos de seguridad	Informe de sistemas de prevención, cacería de amenazas avanzadas de ciberseguridad tiene un esquema de entrega 24 x 7 x 365; con un equipo de consultores certificados en un esquema de SOC en sitio, con capacidades de identificación de amenazas avanzadas, forenses y de respuesta a incidentes	• Objetivo • Gráficas de actividades • Top de alertas MITRE ATT&CK • Técnicas MITRE y ataques por técnica • Top 5 agentes • Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
E3.OP19.S4	Reporte mensual de indicadores de seguridad	Indicadores que permiten medir la seguridad en BANOBRAS	• Severidad de alertas • Vulnerabilidades críticas • Agentes detectados y afectados • Top paquetes afectados por CVE's	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito - FCE's)	Fecha de entrega
			- Vulnerabilidades publicadas en la industria (zero-day) - Recomendaciones	
E3.OP20.S4	Reporte mensual de indicadores de ataque	Indicadores basados en técnicas y tácticas MITRE ATT&CK	- Técnicas y tácticas de ATT&CK - Eventos de ataque - Técnicas acumuladas - Evolución de alertas - Alertas relevantes de seguridad - Recomendaciones	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
E3.OP21.S4	Reporte mensual de disponibilidad del servicio	Plataforma para el monitoreo, detección y respuesta	- Objetivo - Alcance - Disponibilidad de la herramienta de monitoreo	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
E3.OP22.S4	Reporte mensual de Investigación de Ciberdelitos	Actividades mensuales de monitoreo e investigaciones de Ciberdelitos	- Objetivo - Alcance - Investigación de fraudes financieros. - Espionaje - Acceso no autorizado - Robo o pérdida de información	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
E3.OP23.S5	Reporte mensual de misión de equipos Blue Team y Red Team	Describe la misión de los equipos Blue Team y Red Team	- Objetivo - Reglas de la misión	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario

6

Arturo

ID del Entregable de acuerdo a la Fase o servicio	Nombre	Descripción	Criterios de Aceptación (Factores críticos de éxito – FCE´s)	Fecha de entrega
			• Límites • Activos de prueba • Plan de trabajo • Ejecución de pruebas • Actividades del Blue Team y Read Team • Mapeo de resultados del adversario MITRE ATT&CK • Recomendaciones	

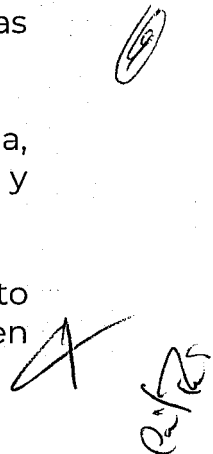
7.1.3. Cumplimiento Normativo

7.1.3.1. Cumplimiento Normativo

El licitante adjudicado, durante la vigencia del servicio y sin costo adicional, deberá dar cumplimiento a lo especificado en el Manual de Seguridad de la Información de BANOBRAS vigente o en su caso los que los sustituyan, así como a la normatividad de las entidades fiscalizadoras y regulatorias que rigen al Banco, a las cuales debe dar cumplimiento en materia de Telecomunicaciones y seguridad de la información como son, de manera enunciativa más no limitativa, la CUB de CNVB, Manual de Operación del SPEI de Banco de México, Manual de Operación de la BDT, INDEVAL, las vigentes o en su caso los que los sustituyan.

En este sentido, el licitante adjudicado deberá realizar, sin excepción alguna, las acciones necesarias para atender los requerimientos normativos y aplicables a BANOBRAS.

Asimismo, el licitante adjudicado deberá cumplir y vigilar que se dé estricto cumplimiento a las disposiciones legales y reglamentarias que resulten



	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	72 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

aplicables a la prestación del servicio; por lo que, en caso de presentarse incumplimientos a dichas disposiciones, que deriven en la imposición de alguna multa o sanción a BANOBRAS, el licitante adjudicado, estará obligado a cubrir, por su cuenta, el importe de éstas y a realizar de inmediato los trámites correspondientes, a fin de regularizar la situación creada.

Por último, el licitante adjudicado deberá presentar un reporte con la descripción y evidencia del cumplimiento de lo descrito en los documentos mencionados, el cual será entregado dentro de los 10 días hábiles posteriores al inicio de la operación.

7.2.Requerimientos Operativos

7.2.1. Derecho de uso y soporte

EL LICITANTE GANADOR será responsable del uso y soporte de cualquier software, herramienta o licenciamiento que se requiere para la prestación de los servicios de ciberseguridad.

7.2.2. Tiempos de respuesta de soporte y servicio

Incidentes		
Tipo (Crítico/ Medio/Bajo)	Tiempo de Atención	Tiempo de Solución
Crítico	1 horas	Depende del impacto del incidente
Medio	2 horas	
Bajo	3 horas	

8. Acuerdos de Niveles de Servicios y operacionales

8.1.Acuerdos de Nivel de Servicios (SLA´s)

En esta sección se definen el conjunto mínimo de características que EL LICITANTE GANADOR deberá cumplir con todos los entregables para determinar la entera satisfacción por parte de la DSI en el ámbito que corresponda BANOBRAS de la recepción 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

[Handwritten signature and initials]

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	73 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

correspondiente según los términos y el procedimiento definido en la sección Penalizaciones.

ID	Nombre	Nivel de Servicio
NS1	Plan de trabajo	A los 10 días hábiles posteriores de inicio del servicio
NS2	Documento de definición de metodologías de los servicios dentro del alcance	A los 10 días hábiles posteriores de inicio del servicio
NS3	S3 - Memoria técnica de implementación de solución de cuentas de administración local para servidores críticos de la Institución.	Durante el primer mes del servicio
NS4	S4 - Memoria técnica de instalación de soluciones tecnológicas	A los 5 días hábiles posteriores al finalizar la implementación
NS5	S4 - Memoria técnica de modelado de indicadores de ataque	A los 5 días hábiles posteriores al finalizar la implementación

ID	Nombre	Nivel de Servicio
NS6	Reporte de ejecución de pruebas	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS7	Reporte de vulnerabilidades	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS8	Indicadores de vulnerabilidades	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS9	Reporte de riesgo tecnológico	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS10	Reporte de análisis de código estático	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento

[Handwritten signature and date 21/12]

ID	Nombre	Nivel de Servicio
NS11	Reporte de análisis dinámico	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS12	Reporte de indicadores de vulnerabilidades de sistemas	Una vez al mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS13	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
NS14	Informe de Riesgos de ciberseguridad, recomendaciones y validaciones de implementación de hardening en el directorio Activo	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento
NS15	Reporte de recomendaciones y validaciones en la 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
NS16	Reporte de recomendaciones y validaciones en la 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
NS17	Reporte de recomendaciones y validaciones de la implementación de las estrategias 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
NS18	Memoria técnica de implementación del sistema de accesos privilegiados de administración del directorio activo (PAW).	Una vez cada tercer mes, a los 5 días hábiles posteriores a la ejecución de cada evento

[Handwritten signature]

[Handwritten signature]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	75 de 86
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		Fecha de elaboración	06/11/2025
			ACTDTIC-FI03.Anexo Técnico	

ID	Nombre	Nivel de Servicio
NS19	Reporte mensual de actividades sospechosas	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
NS20	Reporte mensual de eventos de seguridad	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
NS21	Reporte mensual de indicadores de seguridad	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
NS22	Reporte mensual de indicadores de ataque	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
NS23	Reporte mensual de disponibilidad del servicio	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
NS24	Reporte mensual de Investigación de Ciberdelitos	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario
NS25	Reporte mensual de misión de equipos Blue Team y Red Team	Una vez al mes, a los 5 días hábiles posteriores al finalizar el mes calendario

8.2. Acuerdos de niveles de operación entre contratos (OLA´s)

Los acuerdos de operación serán definidos durante la vigencia del contrato, conforme a las necesidades del Banco y a petición del Director de Seguridad de la Información.

9. Penas convencionales y deducciones al pago.

9.1. Penas convencionales

Con fundamento en los artículos 66 fracción XIX, 75, 77 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 141 y 142 de su Reglamento, se aplicará al licitante adjudicado una pena convencional, por cada día natural de atraso en la prestación de los servicios, en el entendido que el monto de las penas convencionales por atraso no excederá del monto de la garantía de cumplimiento del Contrato.

6

A

2/12

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	76 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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.

Las penas convencionales serán determinadas, calculadas y notificadas por escrito al licitante adjudicado por la Dirección de Seguridad de la Información a través del administrador Operativo del Contrato.

El pago del servicio quedará condicionado proporcionalmente al pago que el licitante adjudicado deba efectuar por concepto de penas convencionales por atraso en el cumplimiento de las obligaciones, en el entendido de que en el supuesto de que sea rescindido el Contrato, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento.

En ningún caso las penas convencionales podrán negociarse en especie.

Independientemente de la aplicación de las penas mencionadas, BANOBRAS, a través de la Dirección de Seguridad de la Información podrá en cualquier momento optar por la rescisión del Contrato, por incumplimiento.

9.2.Deducciones al pago

Con fundamento en el artículo 76 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 143 de su Reglamento, en caso de que se presenten fallas en la prestación del servicio, derivadas de la prestación parcial o deficiente del mismo, la Dirección de Seguridad de la Información a través del administrador Operativo del Contrato, aplicará las siguientes deducciones:

[Handwritten signature and date 20/10]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	77 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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.

En ningún caso las deducciones al pago podrán negociarse en especie.

Independientemente de la aplicación de las deducciones mencionadas, BANOBRAS, a través de la Dirección de Seguridad de la Información podrá en cualquier momento optar por la rescisión del Contrato, por incumplimiento.

10. Confidencialidad

El licitante adjudicado, se obliga a que no divulgará ni utilizará la información documentada o electrónica identificada como "confidencial o reservada", que conozca durante la ejecución y cumplimiento del servicio, así como también cuidará en su caso, los documentos a que tuviera acceso.

El licitante adjudicado deberá incluir en su propuesta técnica, un escrito en el que refiera su compromiso para garantizar la confidencialidad de la información que reciba, resguarde, registre o genere derivado de la prestación de los servicios requeridos, indicando que solamente serán difundidos aquellos que así le indique BANOBRAS, a través de la Dirección de Seguridad de la Información o el Administrador Operativo del Contrato.

11. Licencias, autorizaciones y permisos.

El licitante adjudicado será responsable por el uso de patentes, licencias y derechos que pudieran corresponder a terceros, sobre los sistemas técnicos, procedimientos, dispositivos, partes, equipos, accesorios y herramientas que utilice y/o proporcione para cumplir con los servicios requeridos, y dado el caso de presentarse alguna violación, el licitante adjudicado asumirá toda la responsabilidad por dichas violaciones que se causen en materia, respondiendo ante las reclamaciones que pudiera tener o que le hicieran a BANOBRAS por dichos conceptos, relevándola de cualquier responsabilidad, quedando obligado a resarcirlo de cualquier gasto o costo comprobable que se erogue por dicha situación y que sea determinado por autoridad judicial correspondiente.

21/12

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	78 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

12.Auditoría.

En términos de lo establecido en el artículo 87 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 152 de su Reglamento; con motivo de las auditorías, visitas o inspecciones que se practiquen en relación al Contrato por parte de la Secretaría Anticorrupción y Buen Gobierno ó por el Órgano Interno de Control en BANOBRAS, el licitante adjudicado se compromete a proporcionar la información que en su momento se le requiera.

Complementario a lo anterior, BANOBRAS se reserva el derecho de contratar un tercero que pueda auditar las prácticas, procedimientos de medición de los Niveles de Servicio del licitante adjudicado, y/o sus procedimientos para cálculo de importes en facturas; para lo cual el licitante adjudicado proporcionará todas las facilidades, autorizaciones y accesos a información que le sean requerida. El número de auditorías no está limitado y será responsabilidad de BANOBRAS su ejecución y en todo caso su contratación.

La auditoría observará las mejores prácticas internacionales aplicables de la Industria y en caso de discrepancia se podrá verificar con un tercero reconocido por la industria y aceptado para tal efecto por BANOBRAS y el licitante adjudicado.

El licitante adjudicado estará obligado a mantener registros contables, algoritmos y elementos de cálculo para SLA's y Facturación.

13.Modelo de Propuesta económica y forma de pago

13.1. Modelo de Propuesta Económica

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

(Handwritten signatures and initials)

 HACIENDA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO  BANBRAS BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Hoja	79 de 86
			Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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

[Handwritten signature]

[Handwritten signature]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	80 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

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.
- *Todos los precios deberán estar expresados en pesos mexicanos.
- *Los servicios prestados deben ser de procedencia nacional.

13.2. Forma de pago

Con fundamento en los artículos 66, 72 y 73 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 134 de su Reglamento, BANOBRAS cubrirá el costo del servicio, en un plazo que no podrá exceder los 17 (diecisiete) días hábiles posteriores a la aceptación de las facturas y entrega de las mismas en la Dirección de Seguridad de la Información.

A fin de dar cumplimiento a lo anterior, es necesario que la factura que presente el licitante adjudicado, reúna los requisitos fiscales que establece la legislación vigente en la materia.

De conformidad con lo establecido en el artículo 135 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de que la factura entregada por el licitante adjudicado para su pago presente errores o deficiencias, BANOBRAS, a través del administrador del Contrato o administrador Operativo del mismo, dentro de los 3 (tres) días hábiles siguientes al de su recepción, indicará por escrito al licitante adjudicado las deficiencias que deberá corregir. El periodo que transcurre a partir de la entrega del citado escrito y hasta que el licitante adjudicado presente las correcciones no se computará para efectos del artículo 73 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; hasta que presente las correcciones se computará nuevamente el plazo para los efectos de la fecha de pago.

Los pagos se realizarán en Moneda Nacional, de conformidad con el artículo 66 fracción XIII de la Ley de Adquisiciones, Arrendamientos y Servicios.

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	81 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

14. Propuesta técnica

Los licitantes deberán presentar los elementos y requisitos que BANOBRAS solicita en el presente Anexo Técnico, para realizar la evaluación técnica.

La propuesta técnica deberá presentarse en el formato requerido por BANOBRAS.

14.1. Presentación de la Propuesta Técnica

El licitante deberá integrar en su propuesta técnica los elementos indispensables y con carácter de obligatorio, los cuales serán considerados por el Equipo Técnico designado por BANOBRAS durante la evaluación del procedimiento de contratación. Se requiere que esta información complemente los servicios solicitados en este documento, independientemente del formato de presentación de la Propuesta Técnica. Sin embargo, la propuesta deberá estar debidamente foliada incluyendo un índice que indique claramente dónde inicia y dónde termina cada uno de los apartados. La propuesta técnica puede no limitarse en alcance y extensión a los elementos solicitados; sin embargo, éstos son obligatorios.

La entrega de proposiciones se hará en sobre digital generado por la Plataforma, que contendrá la oferta técnica y económica, dichos sobres serán generados mediante el uso de tecnologías que resguarden la confidencialidad de la información de tal forma que sean inviolables.

14.1.1. Lenguaje

El licitante deberá entregar su propuesta técnica en lenguaje español. Sin embargo, dada la naturaleza del proyecto y los servicios que se administrarán, se permitirá el uso de anglicismos para aquellos términos que sean de origen extranjero; o bien, que representen nombres de tecnologías, marcas y términos comúnmente aceptados en la Industria.

En los casos donde así se indique o que el licitante adjudicado juzgue necesario, se deberá entregar documentación completa y detallada de los puntos en cuestión. En los casos en los que esta documentación sólo esté

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.		Hoja	82 de 86
	UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad		ACTDTIC-FI03.Anexo Técnico	

disponible en el idioma inglés, se permitirá que el licitante traduzca únicamente aquel párrafo(s) que sea de interés para el punto que se esté documentando, siempre y cuando el licitante haga entrega del resto de la documentación en su formato e idioma original. No se aceptarán propuestas que incluyan secciones de la documentación en ningún otro idioma que no sea inglés o español.

14.1.2. Diagramas

Todos los diagramas que formen parte de la propuesta técnica deberán estar diseñados en Microsoft Visio y cada página deberá estar debidamente rotulada, incluyendo el nombre del proyecto, el título del gráfico y el número de diagrama o figura.

Estos diagramas, junto con el resto de la presentación deberán entregarse en formato electrónico además del original en papel

14.2. Documentación Requerida para la entrega de la Propuesta Técnica

Los siguientes elementos son prioritarios e indispensables para la evaluación técnica, por lo que se sugiere al licitante indicar correctamente en sus carpetas la ubicación de cada uno de los siguientes rubros para su fácil identificación y revisión, indicando el número identificador (ID) que aparece en la siguiente figura:

ID	Entregable
1	Propuesta Técnica
2	Dominio de Herramientas conforme a lo requerido en el Anexo Técnico para la ejecución de los servicios
3	Toda la documentación solicitada en el apartado 4.3. Personal
4	Acreditación como ISTQB PARTNER
5	Certificaciones ISO vigentes
6	Membresía FIRST con una antigüedad de al menos 5 años de ser miembro

[Handwritten signature and initials]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	83 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

7	Metodología especializada y detallada conforme a lo requerido en el Anexo Técnico para la ejecución de los servicios
8	Contar con experiencia de al menos 5 años en servicios similares
9	Contar con al menos 5 contratos en servicios similares

15. Criterio 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.

16. Garantía de Anticipo / Garantía de Cumplimiento / Excepción de la presentación de la Garantía de cumplimiento.

La garantía que deberá proporcionar EL LICITANTE GANADOR, de conformidad con lo dispuesto en los artículos 69 fracción II, 70 fracción II de la LAASSP, se deberá realizar mediante la entrega de una póliza de fianza indivisible 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**

[Handwritten signature]
[Handwritten signature]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	84 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

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**, con relación a las especificaciones contenidas en el Documento del Anexo Técnico y de los entregables definidos en el mismo.

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 definidas en el presente anexo técnico y sus entregables.

17. Normas de Calidad (ISO), Normas Oficiales, Normas Mexicanas, Normas Internacionales.

- ISO/IEC 27001:2022 o superior
- ISO 9001:2015 o superior
- ISO/IEC 20000-1: 2018 o superior
- ISO 37001:2016 o superior
- ISO/IEC 22301:2019 o superior

18. Tipo de Contrato.

El contrato a celebrar será en modalidad de cerrado de conformidad con lo establecido en el artículo 66 fracciones VI y VII de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 126 de su Reglamento.

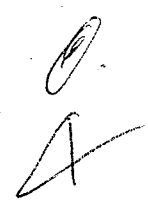
19. Denominación del área administradora y técnica del Contrato.

Con fundamento en el artículo 129, 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

[Handwritten signature and date 24/12/25]

	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	85 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

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.




	BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C. UNIDAD DE ADMINISTRACIÓN DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	Hoja	86 de 86
		Fecha de elaboración	06/11/2025
	Propuesta de Anexo Técnico Servicios de Ciberseguridad	ACTDTIC-FI03.Anexo Técnico	

20. Firmas de elaboración, revisión y aprobación

Elaboró



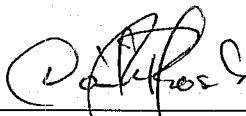
Omar Manuel Mata Rubio
Gerente de Seguridad de la Información 2

Revisó



Claudio Rueda Wong
Gerente de Seguridad de la Información 1

Aprobó



Humberto David Rosales Herrera
Director de Seguridad de la Información



ANEXO "B"

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 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 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. **"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.

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 este contrato.
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 este contrato.

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 conexas 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 (antispymware) 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 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.



ACTA DE JUNTA DE ACLARACIONES (CIERRE)

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

En la Ciudad de México, siendo las 11:00 horas del día 01 de julio del 2026, en la oficina de la Gerencia Ejecutiva 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 las personas servidoras públicas cuyos nombres aparecen al final de la presente acta y firman electrónicamente de conformidad con el artículo 50 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), con el objeto de concluir la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, lo anterior, de acuerdo a lo previsto en los artículos 43, párrafo cuarto y 44 de la LAASSP, 90 y 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en el apartado 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.

El acto fue presidido por la servidora pública Karla De Tuya García, persona Titular de la Gerencia Ejecutiva de Adquisiciones, facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el inciso B) de la Sección I Visión General, del apartado I.4. "Responsabilidades" de las POBALINES.

Se informa que se cuenta con la asistencia del servidor público Moisés Isaac Herrera Ordóñez, persona Titular de la Subgerencia de Contrataciones, como representante del área contratante, del servidor público Humberto David Rosales Herrera, persona Titular de la Dirección de Seguridad de la Información, como representante del área requirente y técnica; del servidor público Héctor Javier González Galicia, persona Titular de la Gerencia Jurídica de lo Contencioso, en su calidad de representante de la Dirección Jurídica de lo Contencioso y Servicios Institucionales, y del servidor público Carlos Enrique Ramírez Pérez, representante del Órgano Interno de Control en BANOBRAS (en adelante OIC).

Se hace mención que el 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 constar que de conformidad con lo dispuesto por los artículos 35, párrafo décimo de la LAASSP y 90, párrafo sexto 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 que preside el acto, informa a los interesados en el procedimiento de contratación que de conformidad con lo dispuesto por el artículo 91, fracción I del RLAASSP, a las **11:11 horas** del día **29 de junio del 2026**, mediante el **SEGUNDO 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 a partir de su publicación en la plataforma Compras MX, para realizar las solicitudes de aclaración que consideren necesarias únicamente en relación con las respuestas emitidas por la





convocante mediante el citado **SEGUNDO AVISO**, el cual, se adjunta a la presente Acta como **ANEXO 1** para efectos de referencia, precisando que, éste fue publicado en la Plataforma a las **17:51 horas** del 29 de junio del 2026. De igual manera se adjunta a la presente acta el **PRIMER AVISO**.

En virtud del plazo otorgado de 6 (seis) horas a partir de la publicación del **SEGUNDO AVISO** en la Plataforma Compras MX, hasta las **23:58 horas** del 29 de junio del 2026, fue la fecha y hora límite para enviar solicitudes de aclaración en relación a las respuestas emitidas por la convocante a través de la Plataforma Compras MX, por lo cual, después de haber realizado una verificación al citado sistema, se desprende que **NO** se recibieron repreguntas en la Plataforma Compras MX.

En cumplimiento a lo dispuesto por el artículo 44, penúltimo párrafo 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 **12:00 horas del día 8 de julio del 2026**, a través de la Plataforma Compras MX.

En términos de lo dispuesto por el artículo 43, penúltimo párrafo 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.

Asimismo, en términos de lo dispuesto por los artículos 50 de la LAASSP y 94, párrafo segundo del RLAASSP, la presente Acta será difundida a través de la Plataforma Compras MX, en la dirección electrónica <https://comprasmx.buengobierno.gob.mx/>, 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 11:10 horas del día 01 de julio del 2026, firmando electrónicamente los que en ella intervinieron para dejar constancia, así como los efectos legales a que haya lugar.

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

NOMBRE	CARGO
Karla De Tuya García	Gerente Ejecutiva de Adquisiciones
Moisés Isaac Herrera Ordóñez	Subgerente de Contrataciones
Humberto David Rosales Herrera	Director de Seguridad de la Información
Héctor Javier González Galicia	Gerente Jurídico de lo Contencioso

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

NOMBRE
Carlos Enrique Ramírez Pérez

Anexo 1



ACTA DE JUNTA DE ACLARACIONES (PRIMER AVISO)

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

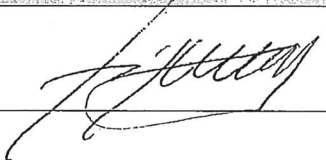
En la Ciudad de México, siendo las 11:00 horas del día 24 de junio del 2026, en la oficina de la Gerencia Ejecutiva de Adquisiciones del Banco Nacional de Obras y Servicios Públicos, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo (en adelante BANOBRAS), ubicada en el primer piso del 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 las personas servidoras públicas designadas 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 44 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 90 y 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en el apartado 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.

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

La que preside el acto materia del presente Aviso hace constar lo siguiente:

Derivado del número de solicitudes de aclaración recibidas en tiempo y forma por parte de los licitantes (**111 preguntas**), así como del tiempo que se requiere emplear para darles contestación debido a la complejidad de las mismas, se informa que siendo las 11:06 horas del día 24 de junio del 2026, se suspende la junta de aclaraciones a la convocatoria antes citada, para reanudarse a las **11:00 horas del 29 de junio del 2026**, de conformidad con lo dispuesto por el artículo 91, fracción I del RLAASSP.

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

NOMBRE	CARGO	FIRMA
Karla De Tuya García	Gerencia Ejecutiva de Adquisiciones	

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

ELABORÓ: TANIA PAULINA ROMERO JIMÉNEZ



ACTA DE JUNTA DE ACLARACIONES (SEGUNDO AVISO)

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

En la Ciudad de México, siendo las 11:00 horas del día 29 de junio del 2026, en la oficina de la Gerencia Ejecutiva 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 las personas servidoras públicas designadas para intervenir en el presente acto, con el objeto de continuar la junta de aclaraciones a la convocatoria del procedimiento de contratación señalado al rubro, de acuerdo a lo previsto en los artículos 43, párrafo cuarto, 44 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante LAASSP), 90 y 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (en adelante RLAASSP), así como de conformidad con lo señalado en el apartado 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.

El acto fue presidido por la servidora pública Karla De Tuya García, Titular de la Gerencia Ejecutiva de Adquisiciones, facultada para presidir los actos del procedimiento de contratación, de conformidad con lo señalado en el inciso B) de la Sección I Visión General, del apartado I.4. "Responsabilidades" de las POBALINES.

Se informa que se cuenta con la asistencia del servidor público Moisés Isaac Herrera Ordóñez, Titular de la Subgerencia de Contrataciones, como representante del área contratante, del servidor público Omar Manuel Mata Rubio, Titular de la Gerencia de Seguridad de la Información 2, como representante del área requirente y técnica; del servidor público Héctor Javier González Galicia, Titular de la Gerencia Jurídica de lo Contencioso, en su calidad de representante de la Dirección Jurídica de lo Contencioso y Servicios Institucionales, y del servidor público Daniel Mendiola Fonseca, representante del Órgano Interno de Control en BANOBRAS (en adelante OIC).

Se hace mención que el 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 constar que de conformidad con lo dispuesto por los artículos 35, párrafo décimo de la LAASSP y 90, párrafo sexto del RLAASSP, al acto no asistió ningún representante o persona que manifestara su interés de estar presente en el mismo con calidad de observador.

Dando inicio al evento, la servidora pública que preside el acto comunicó a las personas servidoras públicas asistentes que de conformidad con lo dispuesto por los artículos 44, párrafos cuarto y quinto de la LAASSP, 90 y 91, del RLAASSP, así como en términos de lo señalado en el numeral 3.2. "Junta de aclaraciones de la licitación pública" de la convocatoria, solamente se atenderán las solicitudes de aclaración de las personas que hayan presentado a través de la plataforma Compras MX, 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 establecida para la celebración de la junta de aclaraciones, es decir, a más tardar a las **11:00 horas del día 23 de junio del 2026**, que cumplan en tiempo y forma con lo señalado en el numeral de la convocatoria antes mencionado.



Acto seguido, habiendo verificado en la plataforma Compras MX la recepción de escritos de interés en participar en el procedimiento de contratación y/o solicitudes de aclaración, se desprende que **SÍ** se recibieron escritos de interés y solicitudes de aclaración por parte de los siguientes licitantes:

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL LICITANTE	NÚMERO DE SOLICITUDES DE ACLARACIÓN
TIC DEFENSE, S.A. DE C.V.	5
SCITUM, S.A. DE C.V.	36
SILENT4BUSINESS, S.A. DE C.V.	16
CYBOLT MANAGED SERVICES, S.A. DE C.V.	41
ID SEC GROUP, S.A. DE C.V.	13

Por lo que respecta a los licitantes **SOLUCIONES TECNOLOGICAS Y DE NEGOCIO CITIC, S.A. DE C.V.**; **HAYKUN SISTEMAS, S.A. DE C.V.**; y **INNOVATI CONSULTING GROUP, S.A. DE C.V.**, únicamente presentaron escritos de interés en participar sin solicitudes de aclaración.

Las respuestas a las solicitudes de aclaración enviadas por los licitantes antes mencionados, fueron atendidas por el área requirente y la convocante, por lo que forman parte integral del presente **SEGUNDO AVISO** como **ANEXO A**.

Se hace constar que la Dirección de Seguridad de la Información, al ser el área técnica y requirente de los servicios objeto del presente procedimiento, se considera bajo su total y absoluta responsabilidad las respuestas de las preguntas que se pudieran recibir de carácter técnico, en términos de lo dispuesto en el artículo 2 fracciones II y III del RLAASSP.

La que preside el acto, señala que las preguntas han sido solventadas por la convocante en su totalidad, informando que en cumplimiento a lo dispuesto por el artículo 91, fracción I, del RLAASSP, las respuestas son publicadas y puestas a disposición de los interesados a través de la plataforma Compras MX, 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 la plataforma Compras MX, 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 el requisito antes señalado 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 mencionada, con la finalidad de no generar desigualdad entre los participantes y motivar la libre participación.

En cumplimiento a lo dispuesto por el artículo 94, párrafo segundo del RLAASSP, se incorpora a la plataforma Compras MX el presente **SEGUNDO AVISO**.

Se adjunta precisiones por parte de la Convocante a solicitud del área técnica y requirente de los servicios, como **ANEXO B**.

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 11:11 horas del día 29 de junio del 2026, para reanudarse a las **11:00 horas** del día **1° de julio del 2026**.

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

NOMBRE	CARGO
Karla De Tuya García	Gerente Ejecutiva de Adquisiciones

ANEXO A



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

ID	Licitante	Tipo de aclaración	Sección de la convocatoria	Aclaración	Respuesta
1142767	TIC DEFENSE SA DE CV	TÉCNICO	INCISO: 4.3. PERSONAL	DICE: ANEXO INCISO: 4.3. LÍDER TÉCNICO DE RED CERTIFICACIÓN OBLIGATORIA: • GIAC PENETRATION TESTER (GPEN) PAGINA: 20 ACLARACIÓN: SE SOLICITA A LA CONVOCANTE DE LA MANERA MÁS ATENTA PERMITA EL CUMPLIMIENTO DE LA CITADA CERTIFICACIÓN TANTO EN EL ANEXO TÉCNICO COMO EN LOS CRITERIOS DE EVALUACIÓN A TRAVÉS DEL CUMPLIMIENTO DE CERTIFICACIONES CON LA ESPECIALIDAD EN PRUEBAS DE PENETRACIÓN, ESTO PRIVILEGIARA EL CRITERIO DEL CUMPLIMIENTO DE LA ESPECIALIDAD QUE SE BUSCA EN EL PERFIL Y NO SOLO ASOCIARLO A UNA MARCA O ENTIDAD CERTIFICADORA. ¿ACEPTA LA CONVOCANTE?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 DEL ANEXO TÉCNICO
1142769	TIC DEFENSE SA DE CV	TÉCNICO	INCISO: 5.2. REQUERIMIENTOS Y/O SERVICIOS GENERALES	DICE: ANEXO INCISO: 5.2. REQUERIMIENTOS Y/O SERVICIOS GENERALES ES INDISPENSABLE QUE TODOS LOS LICITANTES PARTICIPANTES CUENTEN CON LAS CERTIFICACIONES EN LAS SIGUIENTES NORMAS: ISO/IEC 27001:2022 O SUPERIOR, ISO 9001:2015 O SUPERIOR, ISO/IEC 22301:2019 O SUPERIOR, ISO/IEC 20000-1: 2018 O SUPERIOR E ISO 37001:2016 O SUPERIOR (EL INCUMPLIMIENTO DEL PUNTO ES MOTIVO DE DESECHAMIENTO). PAGINA: 27 ACLARACIÓN: SE PIDE DE LA MANERA MÁS ATENTA A LA CONVOCANTE PUEDA ACLARAR SI LOS PROCESOS CITADOS EN EL APARTADO MENCIONADO SON DE CARÁCTER OBLIGATORIO PARA LA SOLVENCIA DE LA	ES CORRECTA SU APRECIACIÓN, LOS PROCESOS REQUERIDOS SON DE CARÁCTER OBLIGATORIO EN TODAS LAS NORMAS ISOs SOLICITADAS



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				PROPUESTA FAVOR DE PRONUNCIARSE AL RESPECTO DICE:	TÉCNICA.
				ANEXO INCISO: 4.3. LÍDER TÉCNICO DE CIBERSEGURIDAD CERTIFICACIÓN • CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL) OBLIGATORIA: PÁGINA: 20	
1142792	TIC DEFENSE SA DE CV	TÉCNICO	INCISO: 4.3. PERSONAL	ACLABACIÓN: SE SOLICITA A LA CONVOCANTE DE LA MANERA MÁS ATENTA PERMITA EL CUMPLIMIENTO DE LA CITADA CERTIFICACIÓN TANTO EN EL ANEXO TÉCNICO COMO EN LOS CRITERIOS DE EVALUACIÓN A TRAVÉS DE CERTIFICACIONES RELACIONADAS A SEGURIDAD DE LA INFORMACIÓN COMO LA ISO 27001, ESTO PRIVILEGIARÁ EL CRITERIO DEL CUMPLIMIENTO DE LA ESPECIALIDAD QUE SE BUSCA EN EL PERFIL Y NO SOLO ASOCIARLO A UNA MARCA O ENTIDAD CERTIFICADORA. ¿ACEPTA LA CONVOCANTE? DICE: CONVOCATORIA INCISO: 1.6 IDIOMA EN QUE SE DEBERÁN PRESENTAR LAS PROPOSICIONES TODA LA DOCUMENTACIÓN SOLICITADA EN LA LICITACIÓN, ASÍ COMO LAS PROPOSICIONES QUE PRESENTEN LOS LICITANTES Y LOS DEMÁS DOCUMENTOS RELATIVOS, DEBERÁN SER REDACTADOS EN IDIOMA ESPAÑOL. PÁGINA: 7	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 DEL ANEXO TÉCNICO
1142793	TIC DEFENSE SA DE CV	TÉCNICO	INCISO: 1.6 IDIOMA EN QUE SE DEBERÁN PRESENTAR LAS PROPOSICIONES		SE ACEPTA



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1142796	TIC DEFENSE SA DE CV	TÉCNICO	INICIO: 5.2. REQUERIMIENTOS Y/O SERVICIOS GENERALES	ACLARACIÓN: SE PIDE A LA CONVOCANTE DE LA MANERA MÁS ATENTA PERMITA ACEPTAR EN EL IDIOMA INGLÉS AQUELLOS TECNISMOS, FOLLETOS, DIPLOMAS Y/O CERTIFICACIONES EN SU IDIOMA NATIVO SIEMPRE Y CUANDO SEA EL INGLÉS. ¿ACEPTA LA CONVOCANTE? DICE: ANEXO TÉCNICO INICIO: 5.2. REQUERIMIENTOS Y/O SERVICIOS GENERALES ES INDISPENSABLE QUE TODOS LOS LICITANTES PARTICIPANTES CUENTEN CON LA ACREDITACIÓN COMO ISTQB PARTNER PARA DEMOSTRAR QUE CUENTA CON LA ESPECIALIDAD EN LA REALIZACIÓN DE PRUEBAS DE CAJA BLANCA O ESTRUCTURALES PARA EXAMINAR EL CÓDIGO, LA INFRAESTRUCTURA Y LA INTERACCIÓN CON SISTEMAS EXTERNOS, VERIFICAR EL CÓDIGO FUENTE, IDENTIFICAR ERRORES Y VULNERABILIDADES Y OBTENER INFORMACIÓN SOBRE LA CALIDAD Y SEGURIDAD DEL CÓDIGO DE SOFTWARE. PÁGINA: 28 SOLICITUD DE ACLARACIÓN: SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR QUE, PARA ACREDITAR EL CUMPLIMIENTO DEL REQUISITO ANTES CITADO Y DE IGUAL MANERA DEL INCISO: 14.2. DOCUMENTACIÓN REQUERIDA PARA LA ENTREGA DE LA PROPUESTA TÉCNICA Y DE LOS CRITERIOS DE EVALUACIÓN, TAMBIÉN SERÁN ACEPTADOS PROCESOS CERTIFICADOS O ACREDITACIONES EQUIVALENTES QUE DEMUESTREN CAPACIDADES ESPECIALIZADAS EN ANÁLISIS DE SEGURIDAD DE CÓDIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES (SAST) Y/O REVISIÓN DE CÓDIGO SEGURO, SIEMPRE QUE DICHAS CAPACIDADES SE ENCUENTREN RESPALDADAS MEDIANTE CERTIFICACIONES DE PROCESOS ALINEADOS A LAS NORMAS ESTABLECIDAS EN EL INCISO 17 DEL ANEXO TÉCNICO. LO ANTERIOR, CONSIDERANDO QUE LA FINALIDAD DEL REQUISITO CONSISTE EN ACREDITAR LA EXPERIENCIA, CAPACIDAD TÉCNICA Y ESPECIALIZACIÓN DEL LICITANTE PARA REALIZAR PRUEBAS DE CAJA BLANCA O ESTRUCTURALES, EXAMINAR EL CÓDIGO FUENTE, IDENTIFICAR VULNERABILIDADES, EVALUAR LA INTERACCIÓN CON COMPONENTES EXTERNOS Y DETERMINAR LA CALIDAD Y SEGURIDAD DEL SOFTWARE. CAPACIDADES QUE PUEDEN SER DEMOSTRADAS MEDIANTE CERTIFICACIONES DE PROCESOS ESPECIALIZADOS Y NO EXCLUSIVAMENTE MEDIANTE LA ACREDITACIÓN ISTQB PARTNER. LO SOLICITADO FAVORECERÍA LA LIBRE PARTICIPACIÓN DE LICITANTES SE ACEPTA SIEMPRE Y CUANDO SEA AL MENOS UNO DE LOS SIGUIENTES PROCESOS ESPECÍFICOS DE ANÁLISIS DE SEGURIDAD DE CÓDIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES (SAST) Y/O REVISIÓN DE CÓDIGO SEGURO, CERTIFICADO EN TODAS LAS NORMAS ISOs SOLICITADAS POR LA CONVOCANTE
---------	----------------------	---------	---	---



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			QUE CUENTAN CON PROCESOS CERTIFICADOS Y EXPERIENCIA COMPROBABLE EN SEGURIDAD DE APLICACIONES, SIN MENOSCABO DE LOS OBJETIVOS TÉCNICOS PERSEGUIDOS POR LA CONVOCANTE. ¿ACEPTA LA CONVOCANTE?	
1144256	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 1 YA QUE DE LO CONTRARIO SI EL LICITANTE NO TIENE UNA DE ELAS SE ENTENDERIA QUE LA CONVOCANTE PODRIA DESCALIFICARNOS, ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	SE ACLARA QUE LAS CERTIFICACIONES DE CARÁCTER OBLIGATORIO DEBERAN CUMPLIRSE PARA QUE LA PROPUESTA TECNICA SEA SOLVENTE, Y LAS CERTIFICACIONES V/O REQUISITOS NO OBLIGATORIOS SOLO SON SUSCEPTIBLES PARA SU RESPECTIVA EVALUACIÓN.
1144257	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 2 YA QUE DE LO CONTRARIO SI EL LICITANTE NO TIENE UNO DE ESTOS DOCUMENTOS EN UN PERFIL SE ENTENDERIA QUE LA CONVOCANTE PODRIA DESCALIFICARN A CUALQUIER LICITANTE QUE NO ENTREGUE O CUMPLA TAL CUAL EL REQUERIMIENTO, ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	ES CORRECTA SU APRECIACIÓN
1144258	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 3 2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL ESPECIALISTA EN CUMPLIMIENTO CON LA FINALIDAD DE FOMENTAR LA LIBRE PARTICIPACIÓN, TRANSPARENCIA Y CONCURRENCIA DE LICITANTES, Y CONSIDERANDO QUE LAS FUNCIONES DE UN ESPECIALISTA EN CUMPLIMIENTO ABARCAN LA EVALUACIÓN DE CONTROLES INTERNOS, MITIGACIÓN DE RIESGOS Y EL APEGO A NORMATIVAS INSTITUCIONALES: SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTAR COMO EQUIVALENTE A LA CERTIFICACIÓN CFE (CERTIFIED FRAUD EXAMINER), LA CERTIFICACIÓN CISA (CERTIFIED INFORMATION SYSTEMS AUDITOR) EMITIDA POR ISACA, LO ANTERIOR, EN VIRTUD DE QUE LA CERTIFICACIÓN CISA GARANTIZA INTERNACIONALMENTE QUE EL ESPECIALISTA CUENTA CON LAS COMPETENCIAS NECESARIAS PARA AUDITAR, CONTROLAR, ASEGURAR Y EVALUAR LOS SISTEMAS DE INFORMACIÓN Y LOS MARCOS DE CONTROL INTERNO DE LA ORGANIZACIÓN, ELEMENTOS INDISPENSABLES PARA EL	NO SE ACEPTA, LA CERTIFICACIÓN REQUERIDA OFRECE UNA ESPECIALIDAD FINANCIERA EN CIBERSEGURIDAD REQUERIDA ACTUALMENTE POR LA CONVOCANTE



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144379	SCITTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 4	ASEGURAMIENTO DEL CUMPLIMIENTO REGULATORIO MODERNO. ¿SE ACEPTA NUESTRA SOLICITUD? 2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL ESPECIALISTA EN PRUEBAS ESTÁTICAS. TOMANDO EN CONSIDERACIÓN QUE EL NÚCLEO DE CONOCIMIENTOS, EL TEMARIO DEL EXAMEN Y LAS COMPETENCIAS TÉCNICAS VALIDADAS POR LA ORGANIZACIÓN GLOBAL COMPTIA SON IDENTÍFICOS PARA AMBOS ESQUEMAS, Y CON EL FIN DE PROMOVER LA LIBRE CONCURRENCIA Y NO LIMITAR LA PARTICIPACIÓN DE PROFESIONALES CON AMPLIA Y PROBADA EXPERIENCIA EN EL RAMO; SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTAR COMO VÁLIDA LA CERTIFICACIÓN COMPTIA SECURITY+ (EN SU MODALIDAD VITALICIA / GFL) COMO EQUIVALENTE A LA VERSIÓN COMPTIA SECURITY+ CE. CABE DESTACAR QUE AMBAS MODALIDADES AVALAN FORMALMENTE LAS MISMAS HABILIDADES CRÍTICAS EN SEGURIDAD INFORMÁTICA, GESTIÓN DE RIESGOS Y MITIGACIÓN DE AMENAZAS REQUERIDAS PARA ESTE PERFIL. ¿SE ACEPTA NUESTRA SOLICITUD? EN ALCANCE A NUESTRA SOLICITUD ANTERIOR, Y ÚNICAMENTE EN CASO DE QUE LA RESPUESTA A LA MISMA SEA NEGATIVA, SOLICITAMOS AMABLEMENTE A LA CONVOCANTE QUE, CON EL OBJETIVO DE GARANTIZAR LA MÁXIMA CALIDAD EN LOS SERVICIOS, LA LIBRE CONCURRENCIA Y NO LIMITAR LA PARTICIPACIÓN DE EXPERTOS CON UN PERFIL DE SEGURIDAD AVANZADO, SE ACEPTEN COMO EQUIVALENTES O SUPERIORES LAS CERTIFICACIONES ISO 27001 LEAD AUDITOR O ISO 27001 LEAD IMPLEMENTER, EMITIDAS POR ORGANISMOS DE CERTIFICACIÓN RECONOCIDOS INTERNACIONALMENTE (COMO PECB, IRCA, BSI, ENTRE OTROS).LO ANTERIOR SE FUNDAMENTA EN QUE LAS CERTIFICACIONES INTERNACIONALES ISO 27001 AVALAN METODOLOGÍAS ESTRUCTURADAS PARA EL DISEÑO, IMPLEMENTACIÓN, AUDITORÍA Y MEJORA CONTINUA DE LA SEGURIDAD DE LA INFORMACIÓN, CUBRIENDO DE MANERA INTEGRAL Y A NIVEL DIRECTIVO LOS OBJETIVOS DE PROTECCIÓN QUE BUSCA LA CONVOCANTE PARA ESTE PERFIL. ¿SE ACEPTA NUESTRA SOLICITUD?	NO SE ACEPTA. FAVOR DE APEGARSE AL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES.
1144380	SCITTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 5	SOLICITUD RESPONDIDA EN EL CUESTIONAMIENTO ANTERIOR	
1144381	SCITTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 6	2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL ESPECIALISTA EN PRUEBAS DINÁMICAS CON EL OBJETIVO DE GARANTIZAR LA MÁXIMA CALIDAD TÉCNICA EN LA EJECUCIÓN DE LOS SERVICIOS. SALVAGUARDAR LA LIBRE CONCURRENCIA Y PERMITIR LA PARTICIPACIÓN DE EXPERTOS CON CREDENCIALES DE ALTO RECONOCIMIENTO INTERNACIONAL. SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTAR COMO EQUIVALENTE O SUPERIOR A LA CERTIFICACIÓN OPSA, LA CREDENCIAL EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH) MASTER.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				LO ANTERIOR SE FUNDAMENTA EN QUE LA DESIGNACIÓN CEH MASTER NO SOLO VALIDA LOS CONOCIMIENTOS METODOLÓGICOS TEÓRICOS, SINO QUE EXIGE OBLIGATORIAMENTE LA APROBACIÓN DE UN EXAMEN RIGUROSO DE CARÁCTER 100% PRÁCTICO EN LABORATORIOS EN VIVO (CEH PRACTICAL). ESTA CREDENCIAL CUENTA CON EL MÁXIMO RECONOCIMIENTO GLOBAL, ESTÁ RESPALDADA POR ESTÁNDARES INTERNACIONALES COMO ANSI Y EL DEPARTAMENTO DE DEFENSA DE EE.UU. (DOD 8140), Y AVALA CAPACIDADES AVANZADAS PARA LA EJECUCIÓN DE PRUEBAS DINÁMICAS DE SEGURIDAD, ANÁLISIS DE VULNERABILIDADES Y HACKING ÉTICO. ¿SE ACEPTA NUESTRA SOLICITUD?	
1144382	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 7	2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL ANALISTA DE SEGURIDAD, CON LA FINALIDAD DE GARANTIZAR LA LIBRE COMPETENCIA, TRANSPARENCIA Y LA MÁXIMA CONCURRENCIA DE LICITANTES EN EL PRESENTE PROCESO, Y CONSIDERANDO QUE EL TEMARIO, EL ESTÁNDAR TÉCNICO Y LAS HABILIDADES OPERATIVAS VALIDADAS POR EL ORGANISMO GLOBAL COMPTIA SON PLENAMENTE EQUIVALENTES EN AMBAS MODALIDADES. SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTAR COMO VÁLIDA LA CERTIFICACIÓN COMPTIA SECURITY+ (EN SU MODALIDAD VITALICA / GFH) COMO ALTERNATIVA A LA VERSIÓN COMPTIA SECURITY+ CE PARA EL PERFIL DE ANALISTA DE SEGURIDAD. ESTA APERTURA PERMITIRÁ LA PARTICIPACIÓN DE ANALISTAS CON AMPLIA TRAYECTORIA Y EXPERIENCIA COMPROBABLE EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS, CUYOS CONOCIMIENTOS TÉCNICOS CENTRALES CUMPLEN CABALMENTE CON LOS OBJETIVOS DE SEGURIDAD QUE LA CONVOCANTE REQUIERE. ¿SE ACEPTA NUESTRA SOLICITUD?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
1144383	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 8	EN ALCANCE A NUESTRA SOLICITUD ANTERIOR, Y ÚNICAMENTE EN CASO DE QUE LA RESPUESTA A LA MISMA SEA NEGATIVA, SOLICITAMOS AMABLEMENTE A LA CONVOCANTE QUE, CON EL OBJETIVO DE GARANTIZAR LA MÁXIMA CALIDAD EN LOS SERVICIOS, LA LIBRE CONCURRENCIA Y NO LIMITAR LA PARTICIPACIÓN DE EXPERTOS CON UN PERFIL DE ANALISTA DE SEGURIDAD, SE ACEPTEN COMO EQUIVALENTES O SUPERIORES LAS CERTIFICACIONES ISO 27001 LEAD AUDITOR O ISO 27001 LEAD IMPLEMENTER, EMITIDAS POR ORGANISMOS DE CERTIFICACIÓN RECONOCIDOS INTERNACIONALMENTE (COMO PECB, IRCA, BSI, ENTRE OTROS). LO ANTERIOR SE FUNDAMENTA EN QUE LAS CERTIFICACIONES INTERNACIONALES ISO 27001 AVALAN METODOLOGÍAS ESTRUCTURADAS PARA EL DISEÑO, IMPLEMENTACIÓN, AUDITORÍA Y MEJORA CONTINUA DE LA SEGURIDAD DE LA INFORMACIÓN, CUBRIENDO DE MANERA	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144384	SCITUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 9	INTEGRAL Y A NIVEL DIRECTIVO LOS OBJETIVOS DE PROTECCIÓN QUE BUSCA LA CONVOCANTE PARA ESTE PERFIL. ¿SE ACEPTA NUESTRA SOLICITUD? 2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL LÍDER DE OPERACIÓN. TOMANDO EN CONSIDERACIÓN QUE LAS FUNCIONES PRIMORDIALES DE UN LÍDER DE OPERACIÓN SE CENTRAN EN LA GESTIÓN ESTRATÉGICA, SUPERVISIÓN DE PROCESOS, MITIGACIÓN DE RIESGOS Y EL ASEGURAMIENTO DE LA CONTINUIDAD DEL SERVICIO, MÁS QUE EN LA CONFIGURACIÓN TÉCNICA OPERATIVA DE INFRAESTRUCTURA DE RED; SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTE COMO EQUIVALENTE O SUPERIOR A LA CERTIFICACIÓN CNSS, LA CREDENCIAL INTERNACIONAL ISO 27001:2013 INTERNAL AUDITOR. LO ANTERIOR SE FUNDAMENTA EN QUE LA CERTIFICACIÓN ISO 27001 FACULTA FORMALMENTE AL ESPECIALISTA PARA SUPERVISAR, AUDITAR Y GARANTIZAR QUE LOS PROCESOS OPERATIVOS SE EJECUTEN BAJO LOS MÁS ALTOS ESTÁNDARES GLOBALES DE SEGURIDAD Y CONTROL INTERNO. ESTA APERTURA PROMUEVE LA LIBRE CONCURRENCIA Y ASEGURA UN PERFIL CON CAPACIDADES DE LIDERAZGO Y GOBIERNO OPERATIVO ALINEADO A LAS MEJORES PRÁCTICAS INTERNACIONALES. ¿SE ACEPTA NUESTRA SOLICITUD? 2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS CON LA FINALIDAD DE GARANTIZAR LA LIBRE CONCURRENCIA, PROMOVER LA COMPETENCIA JUSTA Y NO LIMITAR LA PARTICIPACIÓN DE PROFESIONALES CON CREDENCIALES DE ALTO PRESTIGIO Y RECONOCIMIENTO INTERNACIONAL; SOLICITAMOS AMABLEMENTE A LA CONVOCANTE ACEPTE COMO EQUIVALENTES PARA EL PERFIL DE LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS LAS CERTIFICACIONES EWPT (ELEARNSECURITY WEB PENETRATION TESTER), CWSP (CERTIFIED WIRELESS SECURITY PROFESSIONAL) O CEH PRACTICAL (CERTIFIED ETHICAL HACKER PRACTICAL). LO ANTERIOR SE FUNDAMENTA TÉCNICAMENTE EN LOS SIGUIENTES CRITERIOS DE EQUIVALENCIA: CWSP (DE CWNP): ES EL ESTÁNDAR COMERCIAL GLOBAL DE MAYOR AUTORIDAD EN LA INDUSTRIA ENFOCADO DE MANERA EXCLUSIVA EN LA ARQUITECTURA, AUDITORÍA, ANÁLISIS DE VULNERABILIDADES Y ASEGURAMIENTO DE REDES INALÁMBRICAS (WIRELESS). CEH PRACTICAL (DE EC-COUNCIL) Y EWPT: SON CERTIFICACIONES DE CORTE 100% PRÁCTICO EJECUTADAS EN ENTORNOS DE LABORATORIO EN VIVO BAJO TIEMPO LÍMITE. AMBAS METODOLOGÍAS DE EVALUACIÓN VALIDAN RIGUROSAMENTE LAS HABILIDADES TÉCNICAS E	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
1144385	SCITUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 10	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO





RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			INDISPENSABLES DEL ESPECIALISTA PARA IDENTIFICAR VECTORES DE ATAQUE, INTERCEPTAR TRÁFICO Y VULNERAR PERÍMETROS DE RED, CUMPLIENDO PLENAMENTE CON LOS OBJETIVOS DE SEGURIDAD QUE LA CONVOCANTE BUSCA MITIGAR.	
		¿SE ACEPTA NUESTRA SOLICITUD?	2. COMPETENCIA O HABILIDADES, TABLA A Y TABLA B. PERFIL ARQUITECTO DE SEGURIDAD EN ARQUITECTURA DE DIRECTORIO ACTIVO	
1144386	SCTTUM SA DE CV	TÉCNICO	ANEXO A. TABLA DE PUNTOS Y PORCENTAJES PREGUNTA 11	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
			¿SE ACEPTA NUESTRA SOLICITUD?	
			ES CORRECTO ENTENDER QUE LOS PERFILES REQUERIDOS EN EL ANEXO TÉCNICO SON PERFILES QUE DEBERÁN PROPORCIONAR SERVICIOS EN LAS OFICINAS DE BANOBRAS DE CONFORMIDAD AL NUMERAL 4.4. UBICACIÓN Y 5.2. REQUERIMIENTOS V/O SERVICIOS GENERALES PÁRRAFO 4TO O LOS PERFILES QUE CORRESPONDEN EN SITIO SON SOLO LOS SEÑALADOS EN LOS SERVICIOS 51 Y 54, FAVOR DE ACLARAR.	ES CORRECTO SU ENTENDER
1144387	SCTTUM SA DE CV	TÉCNICO	ANEXO TÉCNICO N. 4.3 PERSONAL PREGUNTA 12	
			SOLICITAMOS A LA CONVOCANTE ACLARE QUE EL PERIODO DE TRANSICIÓN DEL SERVICIO SOLO SERÁ POR UN MES, YA QUE LA CONVOCANTE AL SEÑALAR "AL MENOS" PODRÍA DEJAR A INTERPRETACIÓN QUE EL PROVEEDOR QUE RESULTE ADJUDICADO DEBA DE PROPORCIONAR MÁS DE UN MES DE SERVICIO. ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	ES CORRECTO SU ENTENDER
1144388	SCTTUM SA DE CV	TÉCNICO	ANEXO TÉCNICO N. 5.2. REQUERIMIENTOS PREGUNTA 13	
			SOLICITAMOS A LA CONVOCANTE PERMITA QUE LAS CERTIFICACIONES DE EMPRESA REQUERIDAS EN LA LICITACIÓN COMO ISO/IEC 27001:2022, ISO 9001:2015, ETC., A FIN DE PODER ACREDITAR QUE DENTRO DE ESAS ISO SE CUENTE CERTIFICADOS CUANDO MENOS 5 PROCESOS, PERMITA	NO SE ACEPTA. LA CANTIDAD Y ALCANCE DE LOS PROCESOS CERTIFICADOS DE CARÁCTER OBLIGATORIO A EVIDENCIAR EN LOS CERTIFICADOS EN LAS NORMAS ISO SE ESTABLECEN EN EL APARTADO: 5.2. REQUERIMIENTOS V/ O SERVICIOS
1144389	SCTTUM SA DE CV	TÉCNICO	ANEXO TÉCNICO N. 5.2. REQUERIMIENTOS	



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144390	SCITUM SA DE CV	TÉCNICO	PREGUNTA 14 ANEXO TECNICO N. 5.2. REQUERIMIENTOS PREGUNTA 15	Y ACEPTO ESCRITO LIBRE POR PARTE DEL ORGANISMO CERTIFICADOR COMO PARTE DE LA PROPUESTA, EN EL QUE CITADO ESCRITO SEÑALE QUE LA EMPRESA EVALUADA DOCUMENTA Y CERTIFICA LOS PROCESOS SEÑALADOS. ¿ES ACEPTABLE NUESTRA SOLICITUD? SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE ACLARAR SI LA ACREDITACION ISTQB PARTNER COMO REQUISITO OBLIGATORIO PARA LA REALIZACION DE PRUEBAS DE CAJA BLANCA O ESTRUCTURALES, PUEDE SER UN REQUISITO OPCIONAL YA QUE DICHO ESQUEMA DE CERTIFICACION ESTA PRINCIPALMENTE ENFOCADO EN PRUEBAS FUNCIONALES DE SOFTWARE Y TESTING DE CALIDAD, MAS QUE EN EL ANALISIS TECNICO PROFUNDO DE CODIGO, INFRAESTRUCTURA E INTERACCION CON SUBSISTEMAS QUE REQUIERE EL SERVICIO SOLICITADO. FUNDAMENTAMOS LO ANTERIOR EN VIRTUD DE QUE SI LA ISTQB ESTABLECE ESTANDARES VALIOSOS PARA PRUEBAS DE SOFTWARE, SU ACREDITACION PARTNER TIENE COMO OBJETIVO PRINCIPAL, VALIDAD CAPACIDADES PARA CERTIFICAR PERSONAS EN SUS ESQUEMAS DE FORMACION, NO NECESARIAMENTE DEMUESTRA COMPETENCIAS TECNICAS DIRECTAS EN PRUEBAS ESTRUCTURALES O DE SEGURIDAD A NIVEL DE CODIGO. LAS CAPACIDADES INDIVIDUALES DEL EQUIPO ESTAN DEBIDAMENTE ACREDITADAS A TRAVES DE CERTIFICACIONES ESPECIALIZADAS, ¿SE ACEPTA LA PROPUESTA DE QUE ESTE REQUISITO SEA OPCIONAL MAS NO OBLIGATORIO? DICE: 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. PREGUNTA: ¿ES CORRECTO INFERIR QUE LOS PERFILES REQUERIDOS PARA BRINDAR LOS SERVICIOS DE CIBERSEGURIDAD, DEBERÁN ESTAR EN LAS INSTALACIONES DEL LICITANTE ADJUDICADO Y DESEMPEÑARÁN SUS ACTIVIDADES DE FORMA REMOTA? ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO?	GENERALES, LOS CUALES DEBEN ESTAR LEGIBLES Y ENUNCIADOS DIRECTAMENTE EN EL ALCANCE CERTIFICADO DE SU NORMA RESPECTIVA. SE ACLARA QUE SE PODRA CUMPLIR ESTE REQUISITO DE IGUAL MANERA AL PRESENTAR AL MENOS UNO DE LOS SIGUIENTES PROCESOS: ANÁLISIS DE SEGURIDAD DE CÓDIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES (SAST) Y/O REVISIÓN DE CÓDIGO SEGURO, CERTIFICADO EN TODAS LAS NORMAS ISO SOLICITADAS POR LA CONVOCANTE. ES CORRECTO SU ENTENDER, DE IGUAL MANERA A SOLICITUD DE LA CONVOCANTE PODRÁN PRESENTARSE DE MANERA FÍSICA
1144391	SCITUM SA DE CV	TÉCNICO	4.3. PERSONAL PREGUNTA 16	DICE: SE ENLISTAN LAS HERRAMIENTAS DE MANERA ENUNCIATIVA MÁS NO LIMITATIVA QUE PODRÁN EMPLEARSE:	ES CORRECTO SU ENTENDER





RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			PREGUNTA: ES CORRECTO INFERIR QUE AL SER ENUNCIATIVAS MÁS NO LIMITATIVAS LAS HERRAMIENTAS LISTADAS EN EL PARTADO "HERRAMIENTAS TECNOLÓGICAS", EL LICITANTE ADJUDICADO PODRÁ EMPLEAR DICHAS HERRAMIENTAS O DISTINTAS A LAS LISTADAS, SIEMPRE Y CUANDO GARANTICE EL CUMPLIMIENTO DE LAS ACTIVIDADES LISTADAS DENTRO DEL ANEXO. ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO? DICE: 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 PREGUNTA: ¿ES CORRECTO INFERIR QUE EL LICITANTE EN CASO DE PROPONER HERRAMIENTAS DE SOFTWARE LIBRE, ACEPTA LA CONVOCANTE QUE DICHAS HERRAMIENTAS CUENTEN CON SOPORTE DEL PROPIO LICITANTE? ¿ES CORRECTA NUESTRA APRECIACIÓN?	
1144393	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 18	ES CORRECTO SU ENTENDER
1144394	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 19 PREGUNTA: SE SOLICITA A LA CONVOCANTE PRECISAR EN CASO DE QUE EL LICITANTE REQUIERA HABILITAR HARDWARE EN LAS INSTALACIONES DE LA CONVOCANTE, SERÁ RESPONSABILIDAD DE LA CONVOCANTE PROVEER DE NODOS DE RED, ESPACIO EN RACK Y ENERGÍA PARA LA HABILITACIÓN DE DICHO HARDWARE. ¿ES CORRECTA NUESTRA APRECIACIÓN? DICE: EL LICITANTE GANADOR DEBERÁ REALIZAR PRUEBAS DE PENETRACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA DE MANERA TRIMESTRAL CON PERSONAL QUE CUENTE CON CAPACIDAD TÉCNICA COMPROBABLE MEDIANTE CERTIFICACIONES ESPECIALIZADAS DE LA INDUSTRIA EN LA MATERIA, CON LA FINALIDAD DE DETECTAR ERRORES, VULNERABILIDADES, FUNCIONALIDAD NO AUTORIZADA O CUALQUIER CÓDIGO QUE PUEDA PONER EN RIESGO LA INFORMACIÓN Y	ES CORRECTO SU ENTENDER
1144395	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 20	EL ALCANCE Y VOLUMETRÍA SERÁ ACORDADO EN CADA SOLICITUD POR EVENTO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144396	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 21	PATRIMONIO DE LOS CLIENTES Y DE LA PROPIA INSTITUCIÓN. PREGUNTA: ¿SE LE SOLICITA A LA CONVOCANTE PRECISAR SI LAS PRUEBAS TRIMESTRALES CONTEMPLAN OBJETIVOS ESPECÍFICOS A MANERA DE MUESTREO DE LA TOTALIDAD DE INFRAESTRUCTURA? DICE: EL LICITANTE GANADOR DEBERÁ REALIZAR PRUEBAS DE PENETRACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA DE MANERA TRIMESTRAL CON PERSONAL QUE CUENTE CON CAPACIDAD TÉCNICA COMPROBABLE MEDIANTE CERTIFICACIONES ESPECIALIZADAS DE LA INDUSTRIA EN LA MATERIA, 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. PREGUNTA: EN CASO DE QUE LA RESPUESTA ANTERIOR SEA AFIRMATIVA, ¿PODRÍA LA CONVOCANTE PRECISAR LA CANTIDAD DE OBJETIVOS QUE SE DEBERÁN CONTEMPLAR EN CADA EVENTO?	LA CANTIDAD DE OBJETIVOS ESTÁ DEFINIDO EN EL NUMERAL 6. ALCANCE DEL ANEXO TÉCNICO
1144397	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 22	DICE: 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. PREGUNTA: ¿PODRÍA LA CONVOCANTE PRECISAR LA CANTIDAD DE PRUEBAS ESTÁTICAS QUE SE REQUIEREN DE FORMA MENSUAL? DICE: 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. PREGUNTA: ¿SE SOLICITA A LA CONVOCANTE PRECISAR EL LENGUAJE O LENGUAJES DE PROGRAMACIÓN QUE MANEJA EN DICHS CODIGOS? ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO?	LA CANTIDAD DE PRUEBAS ESTÁTICAS SERÁ ACORDADO EN CADA SOLICITUD POR EVENTO
1144398	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 23	DICE: 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. PREGUNTA: ¿SE SOLICITA A LA CONVOCANTE PRECISAR EL LENGUAJE O LENGUAJES DE PROGRAMACIÓN QUE MANEJA EN DICHS CODIGOS? ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO?	SE LISTAN LOS LENGUAJES DE PROGRAMACIÓN: JAVA, PHP, PYTHON, ANGULAR, .NET, C#, PL/SQL, JASPER, VISUAL BASIC, ORACLE FORMS, ORACLE DEVELOPER, JAVASCRIPT, COBOL, C++, QLIK, PERL, ABAP.
1144399	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES	DICE: 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	SE PRECISA QUE PARA EL DIMENSIONAMIENTO DEL SERVICIO DE PRUEBAS ESTÁTICAS, EL LICITANTE NO DEBERÁ CONSIDERAR EL NÚMERO DE LÍNEAS DE CÓDIGO, SINO EL NÚMERO TOTAL DE COMPONENTES/REPOSITARIOS INDEPENDIENTES A ANALIZAR, EL CUAL ASCIENDE A UN TOTAL DE 63 APLICATIVOS



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

		PREGUNTA 24	BANOBAS POR MES DURANTE LA VIGENCIA DEL CONTRATO: PREGUNTA: SE SOLICITA A LA CONVOCANTE PRECISAR ¿CUAL ES LA CANTIDAD DE LINEAS DE CODIGO EN PROMEDIO POR APLICACIÓN? DICE: 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 52, DEL NUMERAL 8.1 "NIVELES DE SERVICIO", DE MANERA ENUNCIATIVA MÁS NO LIMITATIVA COMO SON: PREGUNTA: ¿ES CORRECTO INTERPRETAR QUE LAS PRUEBAS DINAMICAS TAMBIEN SE REALIZARAN DE MANERA MENSUAL? EN CASO CONTRARIO FAVOR DE ACLARAR. DICE: 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 52, DEL NUMERAL 8.1 "NIVELES DE SERVICIO", DE MANERA ENUNCIATIVA MÁS NO LIMITATIVA COMO SON: PREGUNTA: ¿ES CORRECTO INTERPRETAR QUE EL SERVICIO DE PRUEBAS DINAMICAS SE APLICARÁ A LA MISMA CANTIDAD DE APLICACIONES SUJETAS AL SERVICIO DE REVISIÓN DE CODIGO? DICE: APOYO PARA SO.LVENTAR 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 52, DEL NUMERAL "7.1.3 ENTREGA BLES Y 8.1 NIVELES DE SERVICIO". SE DEBEN REALIZAR LOS INDICADORES DE SEGURIDAD INCLUYENDO DE	
1144400	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS V/O SERVICIOS GENERALES PREGUNTA 25	ES CORRECTO SU ENTENDER
1144401	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS V/O SERVICIOS GENERALES PREGUNTA 26	ES CORRECTO, EL SERVICIO DE PRUEBAS DINAMICAS SE APLICARÁ A LA MISMA CANTIDAD DE APLICACIONES SUJETAS AL SERVICIO DE REVISIÓN DE CODIGO.
1144402	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS V/O SERVICIOS GENERALES PREGUNTA 27	ES CORRECTO SU ENTENDER



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				FORMA ENUNCIATIVA MÁS NO LIMITATIVA LOS SIGUIENTES: • VULNERABILIDADES POR TIPO • VULNERABILIDADES POR CRITICIDAD	
1144403	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 28	PREGUNTA: ¿ES CORRECTO INTERPRETAR QUE EL LICITANTE DEBERÁ EMITIR UN REPORTE DE RECOMENDACIONES PARA MITIGAR LA VULNERABILIDAD, SIN EMBARGO SERÁ RESPONSABILIDAD DEL ADMINISTRADOR DEL SISTEMA EJECUTAR DICHAS RECOMENDACIONES PARA MITIGAR LA VULNERABILIDAD, SIENDO PARTICIPE EL LICITANTE ÚNICAMENTE EN DICHO SEGUIMIENTO Y EN SU DEFECTO EN DOCUMENTAR LAS ACCIONES? ¿ES CORRECTA NUESTRA APRECIACIÓN? DICE: REINGENIERÍA Y GESTIÓN DEL RIESGO DE CIBERSEGURIDAD DEL DIRECTORIO ¿ IMPLEMENTACIÓN DE UNA HERRAMIENTA DE MONITOREO Y VALIDACIÓN DE CAMBIOS DEL DIRECTORIO ACTIVO PREGUNTA: ES CORRECTO INFERIR, EN CASO DE QUE EL LICITANTE CONTEMPLA UNA HERRAMIENTA EN FORMA DE AGENTE PARA EL MONITOREO DEL AD, ¿ESTA SE PUEDA INSTALAR DENTRO DEL SERVIDOR DE DIRECTORIO ACTIVO DE LA CONVOCANTE? ¿PODRÍA LA COANVOCANTE PRONUNCIARSE AL RESPECTO? DICE: REINGENIERÍA Y GESTIÓN DEL RIESGO DE CIBERSEGURIDAD DEL DIRECTORIO ¿ IMPLEMENTACIÓN DE UNA HERRAMIENTA DE MONITOREO Y VALIDACIÓN DE CAMBIOS DEL DIRECTORIO ACTIVO PREGUNTA: SE LE SOLICITA A LA CONVOCANTE PRECISAR, ¿CUÁL ES EL NÚMERO DE USUARIOS DECLARADOS DENTRO DE SU DIRECTORIO ACTIVO? DICE: 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. PREGUNTA: SE LE SOLICITA A LA CONVOCANTE CON EL FIN DE CONTAR CON UNA	NO ES CORRECTO, NO SE PODRÁ INSTALAR NINGÚN AGENTE EN EL DIRECTORIO ACTIVO, SE DEBE IMPLEMENTAR UN MONITOREO SIN AGENTE
1144404	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 29	PREGUNTA: SE LE SOLICITA A LA CONVOCANTE PRECISAR, ¿CUÁL ES EL NÚMERO DE USUARIOS DECLARADOS DENTRO DE SU DIRECTORIO ACTIVO? DICE: 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. PREGUNTA: SE LE SOLICITA A LA CONVOCANTE CON EL FIN DE CONTAR CON UNA	1,620 CUENTAS EN LA OU DE USUARIOS 246 CUENTAS DE SERVICIO ACTIVAS
1144405	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 30	PREGUNTA: SE LE SOLICITA A LA CONVOCANTE CON EL FIN DE CONTAR CON UNA	ESTA INFORMACIÓN SERÁ PROPORCIONADA AL LICITANTE ADJUDICADO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			INTEGRACIÓN TOTAL DE FUENTES DE SEGURIDAD QUE APORTEN ALERTAS Y EVENTOS RELEVANTES MENCIONE, CON QUE HERRAMIENTAS DE SEGURIDAD CUENTA LA CONVOCANTE Y SI ESTAS PODRÁN INTEGRARSE AL SIEM PROPORCIONADO POR EL LICITANTE ADJUDICADO? ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO?	
1144406	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 31 DICE: LA CAZA DEI 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. PREGUNTA: SE SOLICITA A LA CONVOCANTE PRECISAR LA CANTIDAD DE EVENTOS POR SEGUNDO QUE GENERAN SUS FUENTES EXISTENTES A FIN DE INTEGRARLAS AL SIEM PROPUESTO. ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO? DICE: 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) PREGUNTA: ¿ES CORRECTO INFERIR QUE LA REMEDIACIÓN DEBERÁ REALIZARLA EL PERSONAL DEL LICITANTE ADJUDICADO MEDIANTE UNA SOLICITUD HACIA LAS TORRES DE ADMINISTRACIÓN DE LAS HERRAMIENTAS DE SEGURIDAD CON LAS QUE HOY CUENTA LA CONVOCANTE?. ¿EN CASO CONTRARIO FAVOR DE PRECISAR? DICE: 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) PREGUNTA: ¿ES CORRECTO INTERPRETAR QUE SERÁ RESPONSABILIDAD DEL LICITANTE Y DEL ADMINISTRADOR DE LAS HERRAMIENTAS DE SEGURIDAD QUE HOY BRINDAN SERVICIO A LA CONVOCANTE HABILITAR LA INTEGRACIÓN ENTRE HERRAMIENTAS PARA AUTOMATIZAR PLAYBOOKS DE RESPUESTA? ¿ES CORRECTA NUESTRA APRECIACIÓN?	EVENTOS POR SEGUNDO PROMEDIO: 1,200 - 3,500 EPS
1144407	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 32	ES CORRECTO SU ENTENDER
1144408	SCTTUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/O SERVICIOS GENERALES PREGUNTA 33	REFERIRSE A LA RESPUESTA ANTERIOR



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144409	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/ O SERVICIOS GENERALES PREGUNTA 34	DICE: 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. PREGUNTA: ¿ES CORRECTO INTERPRETAR QUE EL EQUIPO AZUL SOLO PODRÁ APLICAR POLÍTICAS DE SEGURIDAD EN LAS HERRAMIENTAS PROPUESTAS DENTRO DE ESTE CONTRATO O EN SU DEFECTO, SE LE SOLICITA A LA CONVOCANTE PRECISAR SI EL LICITANTE PARA EFECTOS DE APLICAR LAS POLÍTICAS DE SEGURIDAD PODRÁ HACER USO DE HERRAMIENTAS DE SEGURIDAD AJENAS AL PRESENTE CONTRATO? ¿PODRÍA LA CONVOCANTE PRONUNCIARSE AL RESPECTO? DICE: 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 MISION 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. PREGUNTA: SE SOLICITA A LA CONVOCANTE PRECISAR, ¿CUAL ES LA DURACIÓN ESTIMADA DEL SERVICIO? DICE: 6.1. FECHA DE INICIO: AL SIGUIENTE DÍA HÁBIL DE LA NOTIFICACIÓN DEL FALLO. PREGUNTA: SE SOLICITA A LA CONVOCANTE, EN CASO DE QUE MI REPRESENTADA CONSIDERE HARDWARE DENTRO DE SU PROPUESTA, SE HACE NOTAR A LA CONVOCANTE QUE DICHO HARDARE TIENE TIEMPOS DE FABRICACIÓN Y LLEGADA, PUDIENDO TENER UN TIEMPO DE ENTREGA DE 6 SEMANAS A PARTIR DEL FALLO. ¿ACEPTA LA CONVOCANTE QUE AL INICIO DEL CONTRATO SE PUEDA BRINDAR EL SERVICIO CON EQUIPO HARDWARE TEMPORAL SEMINUEVO?	LAS REGLAS ESPECIFICAS SERAN ACORDADAS CON EL LICITANTE ADJUDICADO
1144410	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/ O SERVICIOS GENERALES PREGUNTA 35	EL SERVICIO SERÁ EJECUTADO DE MANERA MENSUAL	
1144411	SCITUM SA DE CV	TÉCNICO	5.2.REQUERIMIENTOS Y/ O SERVICIOS GENERALES PREGUNTA 36	SE ACEPTA SU PROPUESTA	



Hacienda
Secretaría de Hacienda y Crédito Público

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



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144608	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL - ESPECIALISTA EN CUMPLIMIENTO	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "ESPECIALISTA EN CUMPLIMIENTO" ACEPTE LA CERTIFICACIÓN DE CISA EN LUGAR DE CERTIFIED FRAUD EXAMINER (ACFE). ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, LA CERTIFICACIÓN REQUERIDA OFRECE UNA ESPECIALIDAD FINANCIERA EN CIBERSEGURIDAD REQUERIDA POR LA CONVOCANTE, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 DEL ANEXO TÉCNICO
1144609	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL - ESPECIALISTA EN PRUEBAS ESTÁTICAS	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "ESPECIALISTA EN PRUEBAS ESTÁTICAS" ACEPTE LA CERTIFICACIÓN DE ISO 27001 EN LUGAR DE COMPTIA SECURITY + CE. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 ANEXO TÉCNICO
1144610	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL - ESPECIALISTA EN PRUEBAS DINÁMICAS	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "ESPECIALISTA EN PRUEBAS DINÁMICAS" ACEPTE LA CERTIFICACIÓN DE CEH EN LUGAR DE CERTIFIED OOSTMM 3.0 PROFESSIONAL SECURITY ANALYST (OPSA). ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 ANEXO TÉCNICO
1144611	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL - ARQUITECTO DE SEGURIDAD EN ARQUITECTURAS DE DIRECTORIO ACTIVO	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "ARQUITECTO DE SEGURIDAD EN ARQUITECTURAS DE DIRECTORIO ACTIVO" ACEPTE LA CERTIFICACIÓN DE MICROSOFT MS-900 Y AZ-500. ¿SE ACEPTA LA PROPUESTA?	SE ACEPTA SU PROPUESTA TODA VEZ QUE NO SE PIDE COMO REQUISITO UNA CERTIFICACIÓN ESPECÍFICA
1144612	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL AUDITOR DE RIESGOS	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "AUDITOR DE RIESGOS DE SEGURIDAD" ACEPTE LA CERTIFICACIÓN ISO 31000 EN LUGAR DE CCISO - CHIEF INFORMATION SECURITY OFFICER. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 ANEXO TÉCNICO
1144613	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL ANALISTAS	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "ANALISTA DE SEGURIDAD" ACEPTE LA CERTIFICACIÓN ISO 27032 IMPLEMENTADOR EN LUGAR DE COMPTIA SECURITY+ CE O CERTIFIED INCIDENT HANDLER (CIH). ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 ANEXO TÉCNICO
1144614	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL LÍDER DE OPERACIÓN	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERIL "LÍDER DE OPERACIÓN" ACEPTE LAS CERTIFICACIONES CISA, CISM, ITIL, INTERMEDIATE CERTIFICATE IN IT OPERATIONAL SUPPORT AND ANALYSIS. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL NUMERAL 4.3 ANEXO TÉCNICO
1144615	SILENT4BUSINESS SA DE CV	TÉCNICO	4.3 PERSONAL	SE SOLICITA A LA CONVOCANTE DEJAR COMO OPCIONAL LA PRESENTACIÓN DE LAS CARTAS DE RECOMENDACIÓN DE LOS EMPLEOS ANTERIORES PARA LOS RECURSOS SOLICITADOS.	SE ACLARA QUE NO ES DE CARÁCTER OBLIGATORIO, SOLO ES CONSIDERADO PARA LA EVALUACIÓN DE PUNTOS
1144616	SILENT4BUSINESS SA DE CV	TÉCNICO	52 REQUERIMIENTOS V/O SERVICIO	SE SOLICITA A LA CONVOCANTE PERMITIR LA PRESENTACIÓN DE LOS CERTIFICADOS VIGENTES PARA LAS NORMAS ISO 9001, 20000-1, 22301, 27001 Y 37001 ENFOCADAS A LOS PROCESOS QUE SOPORTAN LOS SERVICIOS ADMINISTRADOS V/O GESTIÓN OPERATIVA V/O PROCESOS SIMILARES. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA, FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A, TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
1144617	SILENT4BUSINESS SA DE CV	TÉCNICO	52 REQUERIMIENTOS V/O SERVICIOS	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PERMITIR LA LIBRE PARTICIPACIÓN Y PERMITIR LA ACREDITACIÓN DEL FIRST CON AL MENOS 4 AÑOS A LA FECHA DE PRESENTACIÓN DE LA PROPUESTA. ¿SE ACEPTA LA PROPUESTA?	SE ACEPTA SU PROPUESTA



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144618	SILENT4BUSINESS SA DE CV	TÉCNICO	52 REQUERIMIENTOS Y/O SERVICIOS	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PERMITIR LA LIBRE PARTICIPACIÓN Y DEJAR COMO OPCIONAL EL REQUISITO DE ISTQB PARTNER, EN EL ENTENDIDO QUE LA CONVOCANTE SOLICITA RECURSOS ESPECIALIZADOS PARA LA EJECUCIÓN DE LOS SERVICIOS LOS CUALES SE ACREDITAN CON LA PRESENTACIÓN DEL CV Y CERTIFICADOS SOLICITADOS DENTRO DE LA PRESENTE CONVOCATORIA. ¿SE ACEPTA LA PROPUESTA?	SE ACLARA QUE SE PODRÁ CUMPLIR ESTE REQUISITO DE IGUAL MANERA AL PRESENTAR AL MENOS UNO DE LOS SIGUIENTES PROCESOS: ANÁLISIS DE SEGURIDAD DE CÓDIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES (SAST) Y/O REVISIÓN DE CÓDIGO SEGURO, CERTIFICADO EN TODAS LAS NORMAS ISO SOLICITADAS POR LA CONVOCANTE.
1144639	SILENT4BUSINESS SA DE CV	TÉCNICO	ANEXO A CRITERIOS COMPETENCIAS	SE SOLICITA A LA CONVOCANTE CONSIDERAR PARA LA MATRIZ DE PUNTOS LAS CERTIFICACIONES OBLIGATORIAS MENCIONADAS EN LA TABLA A Y DEJANDO COMO OPCIONAL LA TABLA B PERMITIENDO LA LIBRE PARTICIPACIÓN. ¿SE ACEPTA LA PROPUESTA?	SE ACLARA QUE LAS CERTIFICACIONES DE CARÁCTER OBLIGATORIO SON LAS ESTABLECIDAS EN LA TABLA A) Y DEBERÁN CUMPLIRSE PARA QUE LA PROPUESTA TÉCNICA SEA SOLVENTE, Y LAS CERTIFICACIONES Y/O REQUISITOS NO OBLIGATORIOS COMO LA TABLA B) SOLO SON SUSCEPTIBLES PARA SU RESPECTIVA EVALUACIÓN.
1144640	SILENT4BUSINESS SA DE CV	TÉCNICO	ANEXO A CRITERIOS EQUIPAMIENTO	SE SOLICITA A LA CONVOCANTE PERMITIR LA ACREDITACIÓN DE LOS PUNTOS MEDIANTE LA PRESENTACIÓN DE UNA CARTA FIRMADA POR EL REPRESENTANTE LEGAL DE MI REPRESENTADA EN DONDE SE COMPROMETA A LA PRESENTACIÓN DEL TOTAL DEL EQUIPAMIENTO SOLICITADO EN CASO DE RESULTAR ADJUDICADA MI REPRESENTADA. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
1144641	SILENT4BUSINESS SA DE CV	TÉCNICO	ANEXO A CRITERIOS EQUIPAMIENTO	SE SOLICITA A LA CONVOCANTE PERMITIR LA PRESENTACIÓN DE LOS CERTIFICADOS VIGENTES PARA LAS NORMAS ISO 9001, 20000-1, 22301, 27001 Y 37001 ENFOCADAS A LOS PROCESOS QUE SOPORTAN LOS SERVICIOS ADMINISTRADOS Y/O GESTIÓN OPERATIVA Y/O PROCESOS SIMILARES. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO A. TABLA DE PUNTOS Y PORCENTAJES Y ANEXO TÉCNICO
1144642	SILENT4BUSINESS SA DE CV	TÉCNICO	ANEXO A CRITERIOS EQUIPAMIENTO	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PERMITIR LA LIBRE PARTICIPACIÓN Y PERMITIR LA ACREDITACIÓN DEL FIRST CON AL MENOS 4 AÑOS A LA FECHA DE PRESENTACIÓN DE LA PROPUESTA. ¿SE ACEPTA LA PROPUESTA?	SE ACEPTA SU PROPUESTA
1144643	SILENT4BUSINESS SA DE CV	TÉCNICO	43 PERSONAL LIDER TÉCNICO	SE SOLICITA A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERÍFIL "LIDER TÉCNICO DE CIBERSEGURIDAD" ACEPTAR LA CERTIFICACIÓN ISO 27032 IMPLEMENTADOR COMO CERTIFICACIÓN DESEABLE EN LUGAR DE ISO 27032 LEAD CYBERSECURITY MANAGER. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144727	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	PÁGINA 27 DE 85. NUMERAL 5.2 REQUERIMIENTOS Y/O SERVICIOS GENERALES DEL ANEXO 1.	CON LA FINALIDAD DE ASEGURAR EL CUMPLIMIENTO DEL ARTÍCULO 134 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS Y DE LOS PRINCIPIOS DE LIBRE CONCURRENCIA Y COMPETENCIA ECONÓMICA, CONSAGRADOS EN EL ARTÍCULO 26 FRACCIÓN IV Y ARTÍCULO 29 DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO (LAASSP), SE SOLICITA ATENTAMENTE A LA CONVOCANTE RECONSIDERAR EL REQUISITO DE ANTIGÜEDAD MÍNIMA DE 5 AÑOS COMO MIEMBRO ACREDITADO ANTE FIRST. ES NUESTRO ENTENDER QUE EL VALOR SUSTANTIVO DEL REQUERIMIENTO RADICA EN CONTAR CON UN EQUIPO CERT DEBIDAMENTE ACREDITADO BAJO LOS ESTÁNDARES INTERNACIONALES DE FIRST, Y QUE LA SOLA	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			ACREDITACIÓN VIGENTE—OBTENIDA TRAS UN RIGUROSO PROCESO DE EVALUACIÓN— RESULTA SUFICIENTE PARA GARANTIZAR LA MADUREZ OPERATIVA, TÉCNICA Y PROCEDIMENTAL REQUERIDA POR BANOBRA. ¿SE ACEPTA ELIMINAR LA ANTIGÜEDAD MÍNIMA DE 5 AÑOS Y ACEPTAR COMO SUFICIENTE LA ACREDITACIÓN FIRST VIGENTE AL MOMENTO DE LA PRESENTACIÓN DE PROPUESTAS? FAVOR DE PRONUNCIARSE AL RESPUESTO.		
1144728	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL "ESPECIALISTA EN CUMPLIMIENTO"	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL "ESPECIALISTA EN CUMPLIMIENTO" (NUMERAL 4.3), ACEPTE LA CERTIFICACIÓN DE CISA EN LUGAR DE CERTIFIED FRAUD EXAMINER (CFE), ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144729	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL "LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS - SERVICIO 2"	SE SOLICITA AMABLEMENTE A LA CONVOCANTE RECONSIDERAR EL REQUISITO OBLIGATORIO DE LA CERTIFICACIÓN OFFENSIVE SECURITY WIRELESS PROFESSIONAL (OSWP) PARA EL PERFIL DE LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS, CONSIDERANDO OTRAS CERTIFICACIONES EQUIVALENTES TALES COMO LA CERTIFICACIÓN CEH MASTER (CERTIFIED ETHICAL HACKER MASTER) DE EC-COUNCIL QUE DEMUESTRAN HABILIDADES AVANZADAS EN SEGURIDAD OFENSIVA Y ÉTICA, CON MAYOR ADOPCIÓN EN EL SECTOR PÚBLICO Y FINANCIERO EN MÉXICO, LAS CUALES VALIDAN COMPETENCIAS TÉCNICAS EN AUDITORÍA DE SEGURIDAD Y PRUEBAS DE PENETRACIÓN CON METODOLOGÍAS RECONOCIDAS INTERNACIONALMENTE ABARCANDO NO SOLO REDES INALÁMBRICAS, SINO TAMBIÉN SISTEMAS, APLICACIONES Y CONTROLES FÍSICOS, ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144730	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL ESPECIALISTA EN PRUEBAS ESTÁTICAS - CERT COMPTIA SECURITY+ CE	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL ESPECIALISTA EN PRUEBAS ESTÁTICAS (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LA CERTIFICACIÓN OBLIGATORIA COMPTIA SECURITY PLUS CE, CUALQUIERA DE LAS SIGUIENTES CERTIFICACIONES: 1. ISO/IEC 27001 LEAD AUDITOR. 2. ISO/IEC 27001 LEAD IMPLEMENTER. 3. CERTIFIED ETHICAL HACKER (CEH). LO ANTERIOR CONSIDERANDO QUE LAS CERTIFICACIONES PROPUESTAS VALIDAN COMPETENCIAS EN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, EVALUACIÓN DE RIESGOS Y AUDITORÍA DE CONTROLES DIRECTAMENTE APLICABLES AL ANÁLISIS ESTÁTICO DE CÓDIGO Y DETECCIÓN DE VULNERABILIDADES, Y QUE ISO/IEC 27001 ES UNA NORMA INTERNACIONAL DE MAYOR JERARQUÍA Y RECONOCIMIENTO QUE COMPTIA SECURITY PLUS EN EL ÁMBITO DE INSTITUCIONES	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144731	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL ESPECIALISTA EN PRUEBAS DINAMICAS - CERT OSSTMM OPSA	FINANCIERAS REGULADAS POR CNBV Y BANXICO. ¿SE ACEPTA NUESTRA PROPUESTA?, FAVOR DE PRONUNCIARSE AL RESPECTO. SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL ESPECIALISTA EN PRUEBAS DINAMICAS (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTE A LA CERTIFICACION OBLIGATORIA OSSTMM 3.0 PROFESSIONAL SECURITY ANALYST (OPSA), CUALQUIERA DE LA CERTIFICACIONES INTERNACIONAL CERTIFIED ETHICAL HACKER MASTER (CEH MASTER) DE EC-COUNCIL. LO ANTERIOR CONSIDERANDO QUE LA PROPUESTA REPRESENTAN UN NIVEL AVANZADO DE COMPETENCIAS EN PRUEBAS DE PENETRACION, HACKEO ETICO Y ANALISIS DINAMICO DE APLICACIONES, CON MAYOR ADOPCION EN EL SECTOR FINANCIERO MEXICANO Y RECONOCIMIENTO INTERNACIONAL. ASIMISMO, CEH MASTER YA SE ENCUENTRA LISTADA COMO CERTIFICACION OPCIONAL EN EL PROPIO PERFIL DENTRO DEL ANEXO TECNICO. SE ACEPTA NUESTRA PROPUESTA. FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TECNICO
1144732	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL ARQUITECTO DE SEGURIDAD EN ARQUITECTURAS DE DIRECTORIO ACTIVO	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL ARQUITECTO DE SEGURIDAD EN ARQUITECTURAS DE DIRECTORIO ACTIVO (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LOS CURSOS OBLIGATORIOS DE ENTERPRISE SECURITY FUNDAMENTALS Y DIRECTORIO ACTIVO, LAS SIGUIENTES CERTIFICACIONES Y CURSOS OFICIALES DEL FABRICANTE MICROSOFT: 1. MICROSOFT MS-900 (MICROSOFT SECURITY, COMPLIANCE AND IDENTITY FUNDAMENTALS) 2. AZ-900 (AZURE FUNDAMENTALS) 3. SC-900 (MICROSOFT 365 FUNDAMENTALS) LO ANTERIOR CONSIDERANDO QUE DICHAS CERTIFICACIONES MICROSOFT VALIDAN COMPETENCIAS EN ARQUITECTURA Y SEGURIDAD DE DIRECTORIO ACTIVO CON MAYOR PROFUNDIDAD TECNICA, ACTUALIZACION CONTINUA Y RECONOCIMIENTO DEL FABRICANTE QUE LOS CURSOS GENERICOS LISTADOS. ¿SE ACEPTA NUESTRA PROPUESTA? SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL AUDITOR DE RIESGOS DE SEGURIDAD (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LA CERTIFICACION OBLIGATORIA CCISO (CHIEF INFORMATION SECURITY OFFICER) DE EC-COUNCIL, CUALQUIERA DE LAS SIGUIENTES CERTIFICACIONES INTERNACIONALES: 1. ISO 31000 LEAD RISK MANAGER. 2. CISM (CERTIFIED INFORMATION SECURITY MANAGER) DE ISACA. 3. CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL) DE ISC2.	SE ACEPTA SU PROPUESTA TODA VEZ QUE NO SE PIDE COMO REQUISITO UNA CERTIFICACIÓN ESPECÍFICA
1144733	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1. PERFIL AUDITOR DE RIESGOS DE SEGURIDAD - CERT OBLIGATORIA CCISO	SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL AUDITOR DE RIESGOS DE SEGURIDAD (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LA CERTIFICACION OBLIGATORIA CCISO (CHIEF INFORMATION SECURITY OFFICER) DE EC-COUNCIL, CUALQUIERA DE LAS SIGUIENTES CERTIFICACIONES INTERNACIONALES: 1. ISO 31000 LEAD RISK MANAGER. 2. CISM (CERTIFIED INFORMATION SECURITY MANAGER) DE ISACA. 3. CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL) DE ISC2.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TECNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			4. ISO/IEC 27001 LEAD AUDITOR. 5. ISO 22301 LEAD AUDITOR. LO ANTERIOR CONSIDERANDO QUE DICHAS CERTIFICACIONES VALIDAN COMPETENCIAS DIRECTIVAS EN GOBIERNO, GESTION DE RIESGOS Y AUDITORIA DE SEGURIDAD DE LA INFORMACION CON MAYOR RECONOCIMIENTO INTERNACIONAL Y ADOPCION EN EL SECTOR FINANCIERO MEXICANO QUE CCISO. ASIMISMO, ISO/IEC 27001 LEAD AUDITOR E ISO 22301 LEAD AUDITOR YA SE ENCUENTRAN LISTADA COMO CERTIFICACION OPCIONAL EN EL PROPIO PERFIL. SE ACEPTA NUESTRA PROPUESTA, FAVOR DE PRONUNCIARSE AL RESPECTO.	
1144734	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1, PERFIL ANALISTAS DE SEGURIDAD SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL ANALISTAS DE SEGURIDAD (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LA CERTIFICACION OBLIGATORIA COMPTIA SECURITY+ CE, LA CERTIFICACION ISO IEC/27001 LIDER IMPLEMENTADOR COMO PARTE DE LOS RECURSOS PROPUESTOS. ¿SE ACEPTA NUESTRA PROPUESTA? FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TECNICO
1144735	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1, PERFIL LIDER DE OPERACIÓN SE SOLICITA AMABLEMENTE A LA CONVOCANTE PARA EL CUMPLIMIENTO DEL PERFIL LIDER DE OPERACION (NUMERAL 4.3), ACEPTAR COMO EQUIVALENTES A LA CERTIFICACION OBLIGATORIA CNSS (CERTIFIED NETWORK SECURITY SPECIALIST), CUALQUIERA DE LAS SIGUIENTES CERTIFICACIONES INTERNACIONALES: ISO/IEC 27001 LEAD IMPLEMENTER O LEAD AUDITOR. LO ANTERIOR CONSIDERANDO QUE EL ROL DE LIDER DE OPERACION DE UN SOC EN ESQUEMA 24X7X365 DEMANDA COMPETENCIAS EN GESTION DE SERVICIOS DE TI, AUDITORIA Y GESTION DE SEGURIDAD DE LA INFORMACION, COMPETENCIAS QUE SON VALIDADAS DE MANERA MAS COMPLETA POR LAS CERTIFICACIONES PROPUESTAS QUE POR CNSS. LA CUAL TIENE UN ENFOQUE TECNICO EXCLUSIVAMENTE EN REDES. ¿SE ACEPTA NUESTRA PROPUESTA? FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TECNICO
1144736	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1, 4.3 PERSONAL SE SOLICITA A LA CONVOCANTE DEJAR COMO OPCIONAL LA PRESENTACION DE LAS CARTAS DE RECOMENDACION DE LOS EMPLEADOS ANTERIORES PARA LOS RECURSOS SOLICITADOS.	SE ACLARA QUE LAS CARTAS NO SON DE CARÁCTER OBLIGATORIO, SIN EMBARGO, SON TOMADAS EN CUENTA PARA LA ASIGNACIÓN DE PUNTOS.
1144737	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A CRITERIOS DE EVALUACIÓN 3- DOMINIO DE LAS SE SOLICITA A LA CONVOCANTE PERMITIR LA ACREDITACIÓN DE LOS PUNTOS MEDIANTE LA PRESENTACIÓN DE UNA CARTA FIRMADA POR EL REPRESENTANTE LEGAL DE MI REPRESENTADA EN DONDE SE COMPROMETA A LA PRESENTACIÓN DEL TOTAL DEL EQUIPAMIENTO SOLICITADO EN CASO DE RESULTAR ADJUDICADA MI REPRESENTADA. ¿SE ACEPTA LA PROPUESTA?	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TECNICO
1144738	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO 1, 5.2 REQUERIMIENTOS UN EN ENTENDIDO QUE LA ACREDITACION ISTQB PARTNER REPRESENTA UN PROGRAMA COMERCIAL ESPECIFICO DEL INTERNACIONAL SOFTWARE TESTING QUALIFICATIONS BOARD ORIENTADO	SE ACLARA QUE SE PODRA CUMPLIR ESTE REQUISITO DE IGUAL MANERA AL PRESENTAR AL MENOS UNO DE LOS SIGUIENTES PROCESOS: ANALISIS DE SEGURIDAD DE CODIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			Y/O SERVICIOS GENERALES	PRINCIPALMENTE A EMPRESAS DE TESTING DE SOFTWARE Y NO CONSTITUYE UN ESTANDAR INTERNACIONAL DE GESTION DE SEGURIDAD DE LA INFORMACION, NORMA OFICIAL MEXICANA, NI REQUISITO REGULATORIO PARA INSTITUCIONES DE CREDITO ESTABLECIDO POR CNBV, BANXICO O LA UNIDAD DE GOBIERNO DIGITAL. SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE PERMITIR LA LIBRE PARTICIPACION Y DEJAR COMO OPCIONAL EL REQUISITO DE ISTOB PARTNER, EN LE ENTENDIDO QUE LA CONVOCANTE SOLICITA RECURSOS ESPECIALIZADOS PARA LA EJECUCIÓN DE LOS SERVICIOS LOS CUALES SE ACREDITAN CON LA PRESENTACIÓN DEL CURRÍCULUM Y CERTIFICACIONES SOLICITADOS DENTRO DE LA PRESENTE CONVOCATORIA. ¿SE ACEPTA NUESTRA PROPUESTA?	(SAST) Y/O REVISIÓN DE CÓDIGO SEGURO, CERTIFICADO EN TODAS LAS NORMAS ISOs SOLICITADAS POR LA CONVOCANTE.
1144779	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A CRITERIOS DE EVALUACIÓN, SUBRUBRO EXPERIENCIA	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE ACLARAR SI SE CONSIDERARÁ VÁLIDO QUE LOS LICITANTES ACREDITEN LA ESPECIALIDAD A TRAVÉS DE LA PRESENTACIÓN DE DIVERSOS CONTRATOS QUE, DE MANERA CONJUNTA, COMPRENDAN SERVICIOS EQUIVALENTES O SUSTANCIALMENTE SIMILARES A LOS REQUERIDOS EN LA PRESENTE CONVOCATORIA.	ES CORRECTO SU ENTENDER
1144780	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S1 ANÁLISIS DE VULNERABILIDADES, PRUEBAS ...	SE SOLICITA A LA CONVOCANTE CONFIRMAR QUE LA EXPERIENCIA REQUERIDA PARA S1 PODRÁ ACREDITARSE MEDIANTE LA PRESENTACIÓN DE CONTRATOS QUE, DE MANERA CONJUNTA, CUBRAN SERVICIOS DE ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN DE APLICACIONES, INFRAESTRUCTURA Y VERIFICACIÓN DE CONTROLES DE SEGURIDAD, AUN CUANDO DICHO SERVICIO NO SE HAYAN CONTRATADO BAJO UN ÚNICO PROYECTO INTEGRAL. LO ANTERIOR, CONSIDERANDO QUE EN EL MERCADO ES HABITUAL QUE ESTOS SERVICIOS SE CONTRATEN DE FORMA SEPARADA O POR FASES. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144781	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S2 REALIZACIÓN PERIÓDICA DE ANÁLISIS DE ...	SE SOLICITA A LA CONVOCANTE CONFIRMAR QUE PARA ACREDITAR LA EXPERIENCIA EN SERVICIOS DE S2 SERÁ VÁLIDO PRESENTAR CONTRATOS QUE INCLUYAN SERVICIOS RECURRENTE DE ESCANEO DE VULNERABILIDADES, ANÁLISIS DE CONFIGURACIÓN SEGURA, HARDENING Y REVISIÓN PERIÓDICA DE CUMPLIMIENTO NORMATIVO (POR EJEMPLO, ISO 27001, CNBV, BANXICO), AUN CUANDO LA DENOMINACIÓN CONTRACTUAL NO COINCIDA LITERALMENTE CON EL NOMBRE DEL SERVICIO S2. ¿ES CORRECTA NUESTRA APRECIACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144789	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A - CRITERIOS DE EVALUACIÓN, COMPETENCIAS	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR QUE LAS CERTIFICACIONES ADICIONALES A LAS MÍNIMAS OBLIGATORIAS PARA CADA PERFIL (POR EJEMPLO, OSCP, CEH MASTER, ISO/IEC 27001 LEAD IMPLEMENTER, ISO 22301 LEAD AUDITOR, ETC.) PODRÁN PRESENTARSE COMO PARTE DEL CURRÍCULO DEL PERSONAL	SE ACLARA QUE SE DEBERÁN PRESENTAR LAS CERTIFICACIONES CONFORME A LO SOLICITADO EN EL ANEXO TÉCNICO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				PROPUESTO Y QUE DICHAS CERTIFICACIONES SERÁN CONSIDERADAS DENTRO DEL RUBRO DE 'CERTIFICACIONES DESEABLES' PARA EFECTOS DE PUNTAJE, AUN CUANDO NO ESTÉN LISTADAS DE FORMA EXPLÍCITA EN LA TABLA B. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	
1144790	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A - CRITERIOS DE EVALUACIÓN, EXPERIENCIA	SE SOLICITA A LA CONVOCANTE ACLARAR EL PERIODO DE TIEMPO QUE SE CONSIDERARÁ VÁLIDO PARA LOS CONTRATOS PRESENTADOS COMO EVIDENCIA DE EXPERIENCIA (POR EJEMPLO, ÚLTIMOS 3 O 5 AÑOS), ASÍ COMO SI SE ACEPTARÁN CONTRATOS CUYO PERIODO DE EJECUCIÓN HAYA INICIADO ANTES PERO CONTINUEN VIGENTES A LA FECHA DE LA CONVOCATORIA. LO ANTERIOR CON EL OBJETO DE PRESENTAR LA EVIDENCIA DE EXPERIENCIA DE MANERA ALINEADA A SUS EXPECTATIVAS. FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144791	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A - EXPERIENCIA DEL LICITANTE	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR SI SERÁ POSIBLE ACREDITAR LA EXPERIENCIA MEDIANTE CONTRATOS CELEBRADOS POR EMPRESAS FILIALES O MATRICES DEL MISMO GRUPO CORPORATIVO DEL LICITANTE. SIEMPRE QUE SE PRESENTE CARTA DEL REPRESENTANTE LEGAL QUE ACREDITE LA RELACIÓN CORPORATIVA Y LA TRANSFERENCIA DE CAPACIDADES, PROCESOS Y PERSONAL ENTRE DICHAS ENTIDADES. ¿SE ACEPTARÁ ESTA FORMA DE ACREDITACIÓN DE EXPERIENCIA? FAVOR DE PRONUNCIARSE AL RESPECTO.	SE ACLARA QUE PARA EL CUMPLIMIENTO ENTRE VARIAS EMPRESAS SE DEBERA ESTABLECER LA PARTICIPACIÓN EN CONJUNTO A TRAVÉS DE UN CONSORCIO QUE PERMITA DEJAR CLARO LAS RESPONSABILIDADES DE CADA PARTICIPANTE EN DICHO CONSORCIO
1144792	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S1	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR QUE, PARA ACREDITAR LA EXPERIENCIA REQUERIDA EN EL SERVICIO S1 (ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN Y VERIFICACIÓN DE SUFICIENCIA DE CONTROLES DE SEGURIDAD), SERÁ VÁLIDO PRESENTAR CONTRATOS QUE, DE MANERA CONJUNTA, INCLUYAN SERVICIOS DE PRUEBAS DE PENETRACIÓN DE APLICACIONES, INFRAESTRUCTURA, DISPOSITIVOS PERIMÉTRICOS, ASÍ COMO REVISIONES DE CONFIGURACIÓN SEGURA Y HARDENING, AUNQUE DICHS SERVICIOS NO SE HAYAN CONTRATADO BAJO UNA ÚNICA DENOMINACIÓN O PROYECTO INTEGRAL. LO ANTERIOR EN VIRTUD DE QUE, EN EL MERCADO, ESTOS SERVICIOS SUELEN CONTRATARSE DE FORMA MODULAR O POR FASES. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144793	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S2	SE SOLICITA A LA CONVOCANTE CONFIRMAR QUE LA EXPERIENCIA PARA EL SERVICIO S2 (REALIZACIÓN PERIÓDICA DE ANÁLISIS DE SEGURIDAD DE SISTEMAS) PODRÁ ACREDITARSE MEDIANTE CONTRATOS DE SERVICIOS RECURRENTES DE ESCANEO DE VULNERABILIDADES, ANÁLISIS DE CONFIGURACIÓN SEGURA, EVALUACIÓN DE CUMPLIMIENTO NORMATIVO Y SEGUIMIENTO DE PLANES DE REMEDIACIÓN, AUN CUANDO LA DENOMINACIÓN CONTRACTUAL NO COINCIDA LITERALMENTE CON EL NOMBRE DEL SERVICIO S2. ¿ES	ES CORRECTO SU ENTENDER



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				CORRECTA NUESTRA APRECIACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	
1144794	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S3	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR QUE, PARA EFECTOS DE S3, SE CONSIDERARÁN COMO EXPERIENCIA VÁLIDA LOS PROYECTOS DE HARDENING DE SISTEMAS OPERATIVOS, SEGMENTACIÓN Y MICROSEGMENTACIÓN DE REDES, IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN ENDPOINTS Y DESACTIVACIÓN DE SERVICIOS INNECESARIOS, AUNQUE LOS CONTRATOS NO UTILICEN DE FORMA EXPRESA EL TÉRMINO "REDUCCIÓN DE LA SUPERFICIE DE ATAQUE". ¿SE ACEPTARÁN DICHO PROYECTOS COMO EXPERIENCIA EQUIVALENTE? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144795	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S4	SE SOLICITA ATENTAMENTE A LA CONVOCANTE ACLARAR SI EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC) DESDE EL CUAL SE PRESTARÁN LOS SERVICIOS DEL SERVICIO S4 DEBERÁ UBICARSE NECESARIAMENTE DENTRO DE TERRITORIO NACIONAL, O SI SE PERMITE UN MODELO HÍBRIDO EN EL QUE PARTE DE LAS FUNCIONES DE MONITOREO Y ANÁLISIS SE REALICEN DESDE UN SOC REGIONAL FUERA DE MÉXICO, SIEMPRE QUE EL LICITANTE CUENTE CON PERSONAL DE ENLACE EN MÉXICO, CUMPLA CON LOS TIEMPOS DE RESPUESTA Y GARANTICE LA RESIDENCIA DE LA INFORMACIÓN SENSIBLE EN TERRITORIO NACIONAL. FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144796	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S4 / 4.3 PERSONAL	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE CONFIRMAR QUE EL NÚMERO DE RECURSOS INDICADO POR PERFIL CORRESPONDE AL DIMENSIONAMIENTO MÍNIMO REQUERIDO Y QUE EL LICITANTE PODRÁ PROPONER ESQUEMAS DE TURNOS DISTINTOS (POR EJEMPLO, 12X12, 4X3, MODELOS HÍBRIDOS PRESENCIAL/REMOTO) SIEMPRE QUE SE GARANTICE LA COBERTURA CONTINUA 24X7X365, LOS TIEMPOS DE RESPUESTA Y LOS NIVELES DE SERVICIO ESTABLECIDOS EN LA CONVOCATORIA. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144797	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S4	SE SOLICITA A LA CONVOCANTE ACLARAR SI, PARA LA PRESTACIÓN DEL SERVICIO S4, ES OBLIGATORIO UTILIZAR ÚNICAMENTE LAS HERRAMIENTAS DE MONITOREO, CORRELACIÓN, EDR Y THREAT-HUNTING EXPRESAMENTE MENCIONADAS EN EL ANEXO TÉCNICO, O SI EL LICITANTE PODRÁ PROPONER HERRAMIENTAS TECNOLÓGICAS PROPIAS O DE TERCEROS CON CAPACIDADES EQUIVALENTES O SUPERIORES, SIEMPRE QUE SE CUMPLAN LOS REQUERIMIENTOS FUNCIONALES, DE INTEGRACIÓN Y DE REPORTE ESTABLECIDOS. ¿SE ACEPTA ESTA FLEXIBILIDAD TECNOLÓGICA? FAVOR DE PRONUNCIARSE AL RESPECTO.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144798	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S5	SE SOLICITA A LA CONVOCANTE ACLARAR SI, PARA ACREDITAR LA EXPERIENCIA REQUERIDA PARA EL SERVICIO S5 (MODELADO DE	SE ACEPTA SU PROPUESTA



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			ADVERSARIO BLUE-TEAM / RED-TEAM), SE CONSIDERARÁN VALIDOS PROYECTOS DE EJERCICIOS DE RED-TEAMING, PURPLE-TEAMING, SIMULACIONES DE ADVERSARIO BASADAS EN EL MARCO MITRE ATT&CK Y EJERCICIOS DE MESA (TABLE-TOP) DE RESPUESTA A INCIDENTES, AUN CUANDO LA DENOMINACIÓN CONTRACTUAL NO COINCIDA CON LA EXPRESIÓN "MODELO DE ADVERSARIO BLUE-TEAM RED-TEAM". ¿SE ACEPTARÁN DICHOS PROYECTOS COMO EXPERIENCIA EQUIVALENTE? FAVOR DE PRONUNCIARSE AL RESPECTO.		
1144799	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S5	SE SOLICITA A LA CONVOCANTE DETALLAR LA FRECUENCIA MÍNIMA ESPERADA DE LOS EJERCICIOS DE MODELO DE ADVERSARIO DEL SERVICIO S5 (POR EJEMPLO, NÚMERO DE EJERCICIOS RED-TEAM / BLUE-TEAM POR AÑO), ASÍ COMO SI SE CONTEMPLA LA INCLUSIÓN DE ESCENARIOS DE INGENIERÍA SOCIAL, PRUEBAS FÍSICAS Y SIMULACIONES SOBRE PROCESOS DE NEGOCIO. ADEMÁS DE LAS PRUEBAS ESTRUCTURALMENTE TÉCNICAS, FAVOR DE PRONUNCIARSE AL RESPECTO.	SE REALIZARÁ UNA MISIÓN MENSUAL DE BLUE TEAM - RED TEAM. LAS MISIONES SERÁN DEFINIDAS AL LICITANTE GANADOR Y SE CONTEMPLAN ESCENARIOS DE INGENIERÍA SOCIAL, PRUEBAS FÍSICAS Y SIMULACIONES.
1144800	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S5	SE SOLICITA RESPETUOSAMENTE A LA CONVOCANTE ACLARAR CUALES SERÁN LOS CRITERIOS DE ACEPTACIÓN DEL SERVICIO S5, EN PARTICULAR SI EL ÉXITO DEL EJERCICIO SE VALORARÁ EN FUNCIÓN DE LA CALIDAD DE LOS ESCENARIOS, LA EVIDENCIA TÉCNICA Y LAS RECOMENDACIONES DE MEJORA ENTREGADAS, INDEPENDIENTEMENTE DE QUE SE LOGRE COMPROMETER ACTIVOS CRÍTICOS, CON EL FIN DE EVITAR QUE LA IDENTIFICACIÓN DE BRECHAS DE SEGURIDAD PUEDA INTERPRETARSE COMO INCUMPLIMIENTO DEL PROVEEDOR. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTA LA INTERPRETACIÓN.
1144801	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIOS S4 Y S5	SE SOLICITA A LA CONVOCANTE CONFIRMAR SI EL SERVICIO S5 DEBERÁ EJECUTARSE EN ESTRECHA COORDINACIÓN CON EL SERVICIO S4 (SOC / CACERÍA DE AMENAZAS), DE FORMA QUE LOS CASOS DE PRUEBA Y LAS TÁCTICAS SIMULADAS SE UTILICEN PARA AJUSTAR REGLAS DE DETECCIÓN, UMBRALES DE ALERTAS Y PLAYBOOKS DE RESPUESTA, BAJO UN ENFOQUE DE PURPLE-TEAM. EN CASO AFIRMATIVO, SE SOLICITA PRECISAR LOS ENTREGABLES ESPERADOS EN TÉRMINOS DE ACTUALIZACIÓN DE CASOS DE USO DE MONITOREO Y PROCEDIMIENTOS DE RESPUESTA A INCIDENTES, FAVOR DE PRONUNCIARSE AL RESPECTO.	LOS HALLAZGOS OBTENIDOS EN CADA SERVICIO PUEDEN COMPLEMENTAR O INTERACTUAR CON LOS OTROS SERVICIOS. LOS ENTREGABLES Y SUS CRITERIOS DE ACEPTACIÓN ESTÁN DEFINIDOS EN EL ANEXO TÉCNICO PARA CADA UNO DE LOS SERVICIOS.
1144802	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S5	EN RELACIÓN CON LAS HERRAMIENTAS LISTADAS PARA EL SERVICIO S5 (MITRE CALDERA, ATOMIC RED TEAM, PICUS, BURSUITE, ETC.), SE SOLICITA CONFIRMAR QUE EL LICITANTE PODRÁ UTILIZAR FRAMEWORKS Y HERRAMIENTAS PROPIAS O DE TERCEROS (POR EJEMPLO, PLATAFORMAS COMERCIALES DE EMULACIÓN DE ADVERSARIO O DESARROLLOS INTERNOS), SIEMPRE QUE SE BASE EN TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS ALINEADOS A MITRE ATT&CK Y SE ENTREGUEN LOS EVIDENCIALES REQUERIDOS EN EL ANEXO	ES CORRECTO SU ENTENDER



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

				TÉCNICO. ¿ES CORRECTA NUESTRA INTERPRETACIÓN? FAVOR DE PRONUNCIARSE AL RESPECTO.	
1144803	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S5	SE SOLICITA A LA CONVOCANTE PRECISAR SI, DENTRO DE LOS ENTREGABLES DEL SERVICIO S5, SE ESPERA QUE EL LICITANTE ENTREGUE UNA MATRIZ DE COBERTURA MITRE ATT&CK ESPECÍFICA PARA BANOBRAS (TÁCTICAS, TÉCNICAS, CONTROLES DE DETECCIÓN Y RESPUESTA ASOCIADOS), ASÍ COMO RECOMENDACIONES PRIORIZADAS DE CIERRE DE BRECHAS Y ACTUALIZACIÓN DE CONTROLES, A FIN DE ASEGURAR LA TRAZABILIDAD DE LOS EJERCICIOS DE MODELADO DE ADVERSARIO HACIA MEJORAS CONCRETAS EN LA POSTURA DE SEGURIDAD. FAVOR DE PRONUNCIARSE AL RESPECTO.	ES CORRECTO SU ENTENDER
1144804	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S3 SECCIÓN 4.2 LÍNEA BASE	EN RELACIÓN CON EL SERVICIO S3 "REDUCCIÓN DE LA SUPERFICIE DE ATAQUE DEL ECOSISTEMA DE LOS SISTEMAS", EL ANEXO TÉCNICO ESTABLECE COMO REQUERIMIENTO LA IMPLEMENTACIÓN DE UNA HERRAMIENTA DE MONITOREO Y VALIDACIÓN DE CAMBIOS DEL DIRECTORIO ACTIVO CON CAPACIDADES DE AUDITORÍA SOBRE DOMAIN CONTROLLERS, SERVIDORES MIEMBRO, SERVIDORES DE ARCHIVOS Y ESTACIONES DE TRABAJO. ASIMISMO, LA SECCIÓN 4.2 PRESENTA UNA LÍNEA BASE DE INFRAESTRUCTURA TECNOLÓGICA EN TÉRMINOS DE CÓMPUTO, SIN DETALLAR LA ARQUITECTURA DEL DIRECTORIO ACTIVO. A FIN DE GARANTIZAR UN DIMENSIONAMIENTO TÉCNICO CORRECTO DE LA HERRAMIENTA DE MONITOREO REQUERIDA, Y CON EL PROPÓSITO DE PRESENTAR UNA PROPUESTA TÉCNICA Y ECONÓMICA QUE CUBRA EN SU TOTALIDAD EL ALCANCE SOLICITADO, SE SOLICITA AL ÁREA TÉCNICA PROPORCIONAR LA SIGUIENTE INFORMACIÓN: NÚMERO DE BOSQUES (FORESTS) Y DOMINIOS (DOMAINS) DE ACTIVE DIRECTORY QUE CONFORMAN EL ECOSISTEMA INSTITUCIONAL DE BANOBRAS. NÚMERO DE DOMAIN CONTROLLERS ACTIVOS EN PRODUCCIÓN. NÚMERO APROXIMADO DE CUENTAS DE USUARIO ACTIVAS EN EL DIRECTORIO NÚMERO DE SERVIDORES MIEMBRO (MEMBER SERVERS) INTEGRADOS AL DOMINIO. ¿EXISTEN DOMINIOS O BOSQUES ADICIONALES EN AMBIENTES DE DESARROLLO, PRUEBAS O PRE-PRODUCCIÓN QUE DEBAN SER INCLUIDOS DENTRO DEL ALCANCE DEL SERVICIO S3? LO ANTERIOR CON FUNDAMENTO EN EL NUMERAL 5.2 DEL PRESENTE ANEXO TÉCNICO, QUE ESTABLECE QUE EL LICITANTE GANADOR DEBERÁ CONSIDERAR LA TOTALIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA INCLUYENDO SITIOS PRIMARIOS, ALTERNOS Y AMBIENTES NO	1 BOSQUE CON 4 CONTROLADORES DE DOMINIO 2 CONTROLADORES DE DOMINIO EN PRODUCCIÓN Y 2 DE DESARROLLO 1,620 CUENTAS EN LA OU DE USUARIOS 246 CUENTAS DE SERVICIO ACTIVAS 1,271 SERVIDORES INCORPORADOS AL DIRECTORIO ACTIVO



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			PRODUCTIVOS DETERMINADOS POR BANOBRAS ANTES DE EJECUTAR EL SERVICIO.	
			EL ANEXO TÉCNICO ESTABLECE QUE LA HERRAMIENTA DE MONITOREO DEL DIRECTORIO ACTIVO DEBERÁ "UTILIZAR UN MOTOR DE PERSISTENCIA EMBEBIDO, TRANSACCIONAL, QUE ALMACENE DATOS ESTRUCTURADOS EN GRAFOS EN LUGAR DE EN TABLAS CON FINES DE EFICIENCIA", ASÍ COMO PERMITIR LA VISUALIZACIÓN DE TRAYECTORIAS DE ATAQUE, RUTAS MÁS CORTAS A DOMAIN ADMIN, USUARIOS SUJETOS A KERBEROAST, Y RELACIONES DE RIESGO ENTRE ENTIDADES (ACL EDGES, DELEGACIÓN, ETC.), AL RESPECTO SE SOLICITA AL ÁREA TÉCNICA CONFIRMAR: ¿EL REQUISITO DE MOTOR DE PERSISTENCIA EN GRAFOS ES UN REQUERIMIENTO TÉCNICO MANDATORIO QUE SERÁ EVALUADO COMO CRITERIO DE ACEPTACIÓN O DESECHAMIENTO, O CONSTITUYE UNA CARACTERÍSTICA DESEABLE QUE PUEDE SER CUBIERTA MEDIANTE FUNCIONALIDAD EQUIVALENTE? EN CASO DE QUE EL LICITANTE PROPONGA UNA HERRAMIENTA QUE CUBRA EL 100% DE LAS CAPACIDADES FUNCIONALES DE VISUALIZACIÓN Y ANÁLISIS DE RUTAS DE ATAQUE DESCRITAS EN EL ANEXO TÉCNICO, PERO MEDIANTE UNA ARQUITECTURA DE BASE DE DATOS DISTINTA A GRAFOS, ¿DICHIA PROPUESTA SERÁ CONSIDERADA TÉCNICAMENTE ACEPTABLE?	ES CORRECTA LA INTERPRETACIÓN.
1144805	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO TÉCNICO - SERVICIO S3 SECCIÓN 5.2 REQUERIMIENTOS GENERALES	
1144806	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SECCIÓN 5.2 SERVICIO S4 REQUERIMIENTOS GENERALES	SE REQUIERE PRESENCIA FÍSICA DEL PERSONAL EN UN ESQUEMA DE 24X7X365.



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".					
				NOCTURNOS Y FINES DE SEMANA SEAN ATENDIDOS DE FORMA REMOTA DESDE EL SOC DEL LICITANTE? ¿CUÁNTAS POSICIONES FÍSICAS (ESTACIONES DE TRABAJO) HABILITARÁ BANOBRAS EN EL ÁREA DESIGNADA PARA EL PERSONAL DEL LICITANTE? ¿EL EQUIPAMIENTO (CÓMPUTO, MONITORES, CONECTIVIDAD) DEL ÁREA DE TRABAJO EN SITIO SERÁ PROPORCIONADO POR BANOBRAS O DEBERÁ SER PROVISTO POR EL LICITANTE GANADOR?	
1144807	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SECCIÓN 5.2 SERVICIO 54 REQUERIMIENTOS GENERALES	EL ANEXO TÉCNICO INDICA QUE EL LICITANTE GANADOR DEBERÁ INSTALAR UN CONJUNTO DE HERRAMIENTAS ON-SITE, CLOUD O HÍBRIDAS PARA LAS LABORES DE MONITOREO Y CACERÍA DE AMENAZAS, Y QUE LA HERRAMIENTA DEBERÁ INTEGRARSE CON FUENTES DE BITÁCORA SIEM DISPONIBLES EN EL ENTORNO DE BANOBRAS. AL RESPECTO SE SOLICITA CONFIRMAR: ¿BANOBRAS CUENTA ACTUALMENTE CON UNA PLATAFORMA SIEM EN OPERACIÓN? EN CASO AFIRMATIVO, ¿CUÁL ES LA PLATAFORMA, VERSIÓN Y MODELO DE LICENCIAMIENTO VIGENTE? ¿EL LICITANTE GANADOR DEBERÁ INTEGRAR SUS HERRAMIENTAS DE MONITOREO AL SIEM EXISTENTE DE BANOBRAS, O DEBERÁ PROPVEER E INSTALAR UNA PLATAFORMA SIEM NUEVA COMO PARTE DEL ALCANCE DEL SERVICIO 54? EN CASO DE QUE EL LICITANTE DEBA PROPVEER LA PLATAFORMA SIEM, ¿LA PROPIEDAD DE LAS LICENCIAS Y LA INFRAESTRUCTURA QUEDARÁ EN POSESIÓN DE BANOBRAS AL TÉRMINO DEL CONTRATO, O CORRESPONDERÁ AL LICITANTE COMO PARTE DEL MODELO DE SERVICIO ADMINISTRADO?	ESTA INFORMACIÓN SERÁ PROPORCIONADA AL LICITANTE ADJUDICADO
1144808	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SECCIÓN 4.2 SERVICIO 54 LÍNEA BASE	CON BASE EN LA LÍNEA BASE DECLARADA EN EL ANEXO TÉCNICO (648 ACTIVOS VIRTUALES, 523 ACTIVOS FÍSICOS, 1,516 ESTACIONES DE TRABAJO Y 63 APLICACIONES), Y CONSIDERANDO QUE EL SERVICIO 54 REQUIERE LA INGESTA DE FUENTES COMO DNS, IPS, VPN, FIREWALL, DIRECTORIO ACTIVO, LOGS DE CORREO ELECTRÓNICO Y DEMÁS FUENTES DE RED, SE SOLICITA AL ÁREA TÉCNICA PROPORCIONAR: VOLUMEN APROXIMADO DE EVENTOS POR SEGUNDO (EPS) O GIGABYTES POR DÍA (GB/DÍA) GENERADOS ACTUALMENTE POR LA INFRAESTRUCTURA DE BANOBRAS. LISTADO ENUNCIATIVO DE LAS FUENTES DE LOG QUE DEBERÁN INTEGRARSE AL SERVICIO DE MONITOREO (FIREWALLS, ENDPOINTS, APLICACIONES CRÍTICAS, SPEI/BDT/INDEVAL, ETC.). ¿EXISTE ALGUNA RESTRICCIÓN NORMATIVA O DE SEGURIDAD RESPECTO A LA SALIDA DE LOGS FUERA DE LAS INSTALACIONES DE BANOBRAS HACIA INFRAESTRUCTURA CLOUD O EXTERNA DEL LICITANTE?	EVENTOS POR SEGUNDO PROMEDIO: 1,200 - 3,500 EPS LA FUENTE DE LOGS QUE SE INTEGRARÁN SON: LOGS DE RED, SERVIDORES INCLUYENDO SPEI, BDT E INDEVAL, LOGS DE INTEGRIDAD DE ARCHIVOS, EVENTOS DE SISTEMA OPERATIVO (WINDOWS/LINUX), LOGS DE ANTIMALWARE/EDR, LOGS DE APLICACIONES Y LOGS DE BASE DE DATOS. LA INFRAESTRUCTURA SERÁ ON PREMISE, MISMA QUE DEBE SER PROPORCIONADA POR EL LICITANTE GANADOR Y SE INSTALARÁ EN EL CENTRO DE DATOS DE BANOBRAS.



Hacienda
Secretaría de Hacienda y Crédito Público

**BAN
BRAS**
BANCO NACIONAL DE OBRAS Y SERVICIOS PÚBLICOS S.N.C.



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

			LO ANTERIOR CON EL PROPOSITO DE QUE LOS LICITANTES PUEDAN DIMENSIONAR CORRECTAMENTE LA CAPACIDAD DE INGESTA, ALMACENAMIENTO Y PROCESAMIENTO REQUERIDA PARA CUMPLIR CON EL SLA DE DISPONIBILIDAD DEL 99.8% ESTABLECIDO EN EL NUMERAL NS23 DE LOS NIVELES DE SERVICIO.	
1144809	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SERVICIO 2- REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD ¿PUEDE INDICAR LA CONVOCANTE SI LAS HERRAMIENTAS/PLATAFORMAS/SOLUCIONES QUE UTILICE EL PROVEEDOR TENDRÁN SALIDA A INTERNET O SI ¿ES POSIBLE UTILIZAR SOLUCIONES BASADAS EN LA NUBE PARA EJECUTAR LAS PRUEBAS ESTÁTICAS DE SEGURIDAD EN EL CÓDIGO?	NO SE PERMITE EL USO DE SOLUCIONES BASADAS EN LA NUBE NI LA SALIDA A INTERNET PARA EL PROCESAMIENTO DEL CÓDIGO. TODAS LAS HERRAMIENTAS, PLATAFORMAS Y COMPONENTES UTILIZADOS PARA LAS PRUEBAS ESTÁTICAS DE SEGURIDAD DEBERÁN EJECUTARSE E INSTALARSE DE MANERA LOCAL (ON-PREMISE) DENTRO DE LA INFRAESTRUCTURA Y RED PRIVADA DE LA CONVOCANTE
1144810	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SERVICIO 2- REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD SE SOLICITA A LA CONVOCANTE INDIQUE SI ¿LOS SERVICIOS MENSUALES DE ANÁLISIS DE SEGURIDAD DE SISTEMAS, PRUEBAS ESTÁTICAS DE SEGURIDAD DEL CÓDIGO SE REALIZARÁN EN SITIO O PUEDEN EJECUTARSE DE FORMA REMOTA?	LAS PRUEBAS ESTÁTICAS DEBEN REALIZARSE EN SITIO
1144811	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SERVICIO 2- REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD SE SOLICITA A LA CONVOCANTE INDIQUE SI ¿LOS SERVICIOS MENSUALES DE ANÁLISIS DE PRUEBAS DINÁMICAS DE SISTEMAS SE REALIZARÁN EN SITIO O PUEDEN EJECUTARSE DE FORMA REMOTA?	LAS PRUEBAS DINÁMICAS DEBEN REALIZARSE EN SITIO
1144812	CYBOLT MANAGED SERVICES SA DE CV	LEGAL- ADMINISTRATIVA	SERVICIO 2- REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD ¿PUEDE INDICAR LA CONVOCANTE SI LAS HERRAMIENTAS/PLATAFORMAS/SOLUCIONES QUE UTILICE EL PROVEEDOR TENDRÁN SALIDA A INTERNET O SI ¿ES POSIBLE UTILIZAR SOLUCIONES BASADAS EN LA NUBE PARA EJECUTAR LAS PRUEBAS DINÁMICAS DE SISTEMAS?	LAS PRUEBAS DINÁMICAS DEBEN REALIZARSE EN SITIO
1144813	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	SERVICIO 2- REALIZACIÓN PERIÓDICA DE ANÁLISIS SEGURIDAD ES CORRECTO ENTENDER QUE EL APOYO PARA SOLVENTAR VULNERABILIDADES, NO INCLUYE LA MODIFICACIÓN AL CÓDIGO DE BANOBRAS Y SE PUEDE EJECUTAR DE FORMA REMOTA, PREVIA SOLICITUD, ¿ES CORRECTO NUESTRO ENTENDIMIENTO?	ES CORRECTO QUE EL APOYO PARA SOLVENTAR VULNERABILIDADES, NO INCLUYE LA MODIFICACIÓN AL CÓDIGO DE BANOBRAS, LAS PRUEBAS DE VULNERABILIDADES NO SE PUEDEN EJECUTAR DE FORMA REMOTA
1144814	CYBOLT MANAGED SERVICES SA DE CV	TÉCNICO	ANEXO A CRITERIOS DE EVALUACIÓN DENTRO DEL ANEXO A, CRITERIOS DE EVALUACIÓN, SE MENCIONA QUE EN CASO DE NO PRESENTAR EL CERTIFICADO DE MEMBERSHIP FIRST CON LOS REQUISITOS SEÑALADOS, NO SE OTORGARÁN PUNTOS. ¿PODRÍA CONFIRMAR LA CONVOCANTE SI EL NO PRESENTAR DICHA MEMBERSHIP ES MOTIVO DE DESACHAMIENTO DE LA PROPUESTA Y ÚNICAMENTE NO SE OTORGARÁN LOS PUNTOS?	SE ACLARA QUE LA ACREDITACIÓN Y ANTIGÜEDAD REQUERIDA EN EL ANEXO TÉCNICO ES DE CARÁCTER OBLIGATORIO Y SU FALTA DE CUMPLIMIENTO SERÁ MOTIVO DE DESACHAMIENTO.
1144815	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1, PDF 4.3. PERSONAL SE LE SOLICITA A LA CONVOCANTE ESPECIFICAR SI LAS 3 CARTAS DE RECOMENDACIÓN DE SUS ÚLTIMOS EMPLEOS CON ORGANIZACIONES DISTINTAS APLICAN CUANDO EL RECURSO TIENE MÁS DE 3 AÑOS LABORANDO EN LA ORGANIZACIÓN.	SE ACLARA QUE EL REQUISITO NO ES DE CARÁCTER OBLIGATORIO, Y AQUELLOS PERFILES QUE POR ANTIGÜEDAD SOLO HAYAN ESTADO EN UNA ORGANIZACIÓN PODRÁN SER ACREDITADO CON UNA CARTA DE SU ORGANIZACIÓN EXPONIENDO LO SOLICITADO POR LA CONVOCANTE.





RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

1144816	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "ESPECIALISTA EN CUMPLIMIENTO" EN LA CERTIFICACIÓN OBLIGATORIA CERTIFIED FRAUD EXAMINER - ACFE, PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA CFCs (CERTIFIED FINANCIAL CRIME SPECIALIST) CON LA QUE SE ABARCA UN ESPECTRO AMPLIO DE DELITOS FINANCIEROS.	SE ACEPTA SU PROPUESTA, TODA VEZ QUE ES UNA CERTIFICACIÓN SIMILAR PARA DEMOSTRAR LA ESPECIALIDAD FINANCIERA REQUERIDA POR LA CONVOCANTE
1144817	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "LÍDER TÉCNICO DE SEGURIDAD EN SISTEMAS" EN LA CERTIFICACIÓN OBLIGATORIA OSCP (OFFENSIVE SECURITY WIRELESS PROFESSIONAL), PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA GIAC ASSESSING AND AUDITING WIRELESS NETWORKS (GAWN).	SE ACEPTA SU PROPUESTA SIEMPRE Y CUANDO SEA LA CITADA
1144818	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "ESPECIALISTA EN PRUEBAS ESTÁTICAS" EN LA CERTIFICACIÓN OBLIGATORIA COMPTIA SECURITY+ CE, PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA (ISC)² SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP).	SE ACEPTA SU PROPUESTA SIEMPRE Y CUANDO SEA LA CITADA
1144819	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "ESPECIALISTA EN PRUEBAS DINÁMICAS" EN LA CERTIFICACIÓN OBLIGATORIA CERTIFIED OSMIM : 3.0 PROFESSIONAL SECURITY ANALYST (OPSA), PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA CEH (CERTIFIED ETHICAL HACKER) O COMPTIA PENTEST+.	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144820	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE ESPECIFICAR SI PARA EL PERFIL DE "ARQUITECTO DE SEGURIDAD EN ARQUITECTURAS DE DIRECTORIO ACTIVO" LOS CURSOS "ENTERPRISE SECURITY FUNDAMENTALS" Y "DIRECTORIO ACTIVO" DEBEN SER ESPECÍFICOS CON UN PROVEEDOR DE CURSO POR EJEMPLO MICROSOFT; O PUEDE SOLO PUEDE SER UN CURSO CON VALOR CURRICULAR	SE ACLARA QUE PUEDE CUMPLIRSE EL REQUISITO CON UN CURSO
1144821	ID SEC GROUP SA DE CV	LEGAL - ADMINISTRATIVA	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "AUDITOR DE RIESGO DE SEGURIDAD" EN LA CERTIFICACIÓN OBLIGATORIA CCISO - CHIEF INFORMATION SECURITY OFFICER, PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL).	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144822	ID SEC GROUP SA DE CV	LEGAL - ADMINISTRATIVA	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "LÍDER DE OPERACIÓN" EN LA CERTIFICACIÓN OBLIGATORIA CNSS (CERTIFIED SECURITY SPECIALIST), PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA ISC2 CERTIFIED IN CYBER SECURITY (CC) O SYSTEMS SECURITY CERTIFIED PRACTITIONER (SSCP).	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO
1144823	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 4.3. PERSONAL	SE LE SOLICITA A LA CONVOCANTE SI PARA EL PERFIL DE "LÍDER TÉCNICO DE RED TEAM" EN LA CERTIFICACIÓN OBLIGATORIA GIAC PENETRATION TESTER (GPEN), PUEDE CUMPLIRSE CON UNA CERTIFICACIÓN SIMILAR O SUPERIOR COMO LA GIAC RED TEAM PROFESSIONAL (GRTF).	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO



Hacienda
Secretaría de Hacienda y Crédito Público

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



RESPUESTAS A LAS SOLICITUDES DE ACLARACIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS “SERVICIOS DE CIBERSEGURIDAD”.

1144824	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 5.2 REQUERIMIENTOS V/O SERVICIOS GENERALES	SE LE SOLICITA A LA CONVOCANTE QUE SI PARA EL FIRST (GLOBAL FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS) SE PUEDA CUMPLIR LOS 5 AÑOS DURANTE EL TRANSCURSO DEL 2026.	SE ACEPTA SU PROPUESTA
1144825	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF 5.2 REQUERIMIENTOS V/O SERVICIOS GENERALES	SE LE SOLICITA A LA CONVOCANTE QUE SI PARA LA ACREDITACIÓN COMO ISTQB PARTNER SE PUEDE CUMPLIR CON UNA ACREDITACIÓN SIMILAR O SUPERIOR COMO LA CERTIFIED SOFTWARE TEST ENGINEER (CSTE) POR QUALITY ASSURANCE INSTITUTE)	SE ACEPTA SIEMPRE Y CUANDO SEA AL MENOS UNO DE LOS SIGUIENTES PROCESOS ESPECÍFICOS DE ANÁLISIS DE SEGURIDAD DE CÓDIGO FUENTE, PRUEBAS DE SEGURIDAD DE APLICACIONES (SAST) V/O REVISIÓN DE CÓDIGO SEGURO, CERTIFICADO EN TODAS LAS NORMAS ISOs SOLICITADAS POR LA CONVOCANTE
1144826	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF SERVICIO 5.- MODELADO DE ADVERSARIO BLUE- TEAM RED -TEAM.	SE LE SOLICITA A LA CONVOCANTE ESPECIFICAR COMO DEBERÁ DEMOSTRARSE QUE EL PERSONAL ASIGNADO AL SERVICIO CUMPLE CON CERTIFICADO PARA BLUE TEAM V/O RED TEAM. YA QUE LA CERTIFICACIÓN BURPSUTE SOLICITADO, NO CUENTA CON UN ALCANCE ESPECÍFICO PARA TEMAS DE RED TEAM, YA QUE ES UNA HERRAMIENTA OPERACIONAL.	SE ACLARA QUE LAS ESPECIFICACIONES REQUERIDAS SE ESTABLECEN EN EL ANEXO TÉCNICO
1144827	ID SEC GROUP SA DE CV	TÉCNICO	ANEXO 1.PDF SERVICIO 5.- MODELADO DE ADVERSARIO BLUE- TEAM RED -TEAM.	SE LE SOLICITA A LA CONVOCANTE SI EL CERTIFICADO PARA EL PERSONAL ASIGNADO DE BLUE TEAM Y RED TEAM, PUEDE SER EL DEL SANS SEC450 - BLUE TEAM FUNDAMENTALS V/O SEC670: RED TEAMING TOOLS	NO SE ACEPTA. FAVOR DE APEGARSE A LO ESTABLECIDO EN EL ANEXO TÉCNICO



ANEXO B



PRECISIÓN

LICITACIÓN PÚBLICA NACIONAL NÚMERO LA-06-G1C-006G1C001-N-68-2026, CUYO OBJETO ES LA CONTRATACIÓN DE LOS "SERVICIOS DE CIBERSEGURIDAD".

ANEXO TÉCNICO

De conformidad con el numeral 5.2 REQUERIMIENTOS Y/O SERVICIOS GENERALES, del ANEXO TÉCNICO, y toda vez que se solicitó personal bajo el esquema 24x7x365, deberá presentarse dentro de su propuesta técnica el siguiente requisito:

"De conformidad con lo establecido en los artículos Octavo y Decimo del ACUERDO POR EL QUE SE DAN A CONOCER LAS DISPOSICIONES DE CARÁCTER GENERAL PARA EL REGISTRO DE PERSONAS FÍSICAS O MORALES QUE PRESTEN SERVICIOS ESPECIALIZADOS O EJECUTEN OBRAS ESPECIALIZADAS A QUE SE REFIERE EL ARTÍCULO 15 DE LA LEY FEDERAL DEL TRABAJO, publicado en el Diario Oficial de la Federación el 24 de mayo del 2021, con última modificación el 21 de febrero de 2024, el Licitante debe de presentar el Aviso de registro en donde se demuestre que se encuentra inscrito en el Registro de Prestadoras de Servicios Especializadas u obras especializadas (REPSE), emitido por la Secretaría del Trabajo y Previsión Social".

Este requisito será obligatorio para cada empresa que preste los servicios, incluso en caso de participación conjunta, y el registro deberá identificar expresamente los servicios relacionados con el objeto de este procedimiento. La **NO** presentación será causa de desechamiento.

