REPÚBLICA DEL ECUADOR

DOCUMENTOS DE SELECCIÓN PARA COMPARACIÓN DE PRECIOS EN ADQUISICIÓN DE BIENES Y SERVICIOS DIFERENTES DE CONSULTORÍA Y/O CONEXOS

País: **Ecuador**

Contratante: **Ministerio de Salud Pública**

Nombre del proyecto: **PROGRAMA MULTIFASE DE MEJORA DE LA CALIDAD EN PRESTACIÓN DE LOS SERVICIOS SOCIALES**

Número del préstamo/crédito: **4364/OC-EC**

Título de la adquisición: **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL**

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023
CP No: CP-S-002-2023

Fecha de emisión: **junio de 2023**

Banco Interamericano de Desarrollo (BID)

INDICE GENERAL

SECCIÓN 01: CARTA DE INVITACIÓN A PRESENTAR OFERTAS

Comparación de Precios CP No.: CP-S-002-2023

Título de la adquisición: **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL**

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023

Quito, julio de 2023

Señores

Proveedores

Presente.-

De mi consideración:

1. El 07 septiembre de 2018, el Gobierno del Ecuador y el Banco Interamericano de Desarrollo (BID) suscribieron el Contrato de Préstamo número **4364**/OC-EC**,** cuyo objetivo es **PROGRAMA MULTIFASE DE MEJORA DE LA CALIDAD EN PRESTACIÓN DE LOS SERVICIOS SOCIALES**; su ejecución se encuentra a cargo Ministerio de Salud Pública (MSP)**,** y se propone utilizar parte de los fondos de este préstamo para efectuar los pagos bajo el Contrato "PROGRAMA MULTIFASE DE MEJORA DE LA CALIDAD EN LA PRESTACIÓN DE LOS SERVICIOS SOCIALES - FASE I" componente 3 **.**
2. El Ministerio de Salud Pública invita a presentar su oferta para la **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL** de acuerdo con los lineamientos y términos de referencia que se adjuntan.
3. El procedimiento para la selección de las ofertas corresponde al procedimiento de "Comparación de Precios", el cual se efectuará conforme a lo establecido en las *Políticas para la Adquisición de Bienes y Obras financiados por el Banco Interamericano de Desarrollo (BID)* GN *2349-15, y* en los Documentos de Selección que se anexan.
4. El presupuesto referencial de la adquisición es de USD $ 94.816,15 (Noventa y cuatro mil ochocientos dieciséis dólares de los Estados Unidos de América con 15/100 ctvs.), más IVA. La modalidad del contrato es precios unitarios en una lista de cantidades**.** El precio del contrato no está sujeto a ajuste de precios.
5. El plazo de ejecución de los servicios es de 60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.
6. Las ofertas, deben entregarse de forma física contenidas en un sobre cerrado, en la dirección que se consigna a continuación. Los Oferentes no podrán presentar Ofertas electrónicamente. Las ofertas que se reciban fuera del plazo serán rechazadas. La fecha límite de recepción de ofertas es **28/07/2023,** hasta las **14:00** horas (GMT-5).
    - Dirección: Av. Quitumbe Ñan y Av. Amaru Ñan

- Edificio: Plataforma Gubernamental de Desarrollo Social
- Departamento: Oficina 105
- Ciudad: Quito
- País: Ecuador
- Código postal: 170702
- Correo electrónico: proyecto.bid@mspsalud.gob.ec

7. La apertura de ofertas se realizará el día **28/07/2023** a las **15:00** horas (GMT-5) en la misma dirección donde se entregaron las ofertas. Las ofertas se abrirán en presencia de los representantes de los Oferentes que deseen asistir en persona.

8. El Contratante realizará las aclaraciones o enmiendas que correspondan por iniciativa propia o a solicitud de los invitados, por lo menos **5** días antes de la fecha límite para la presentación de las Ofertas[1]. Las aclaraciones o enmiendas serán entregadas a través de boletines de aclaraciones y/o boletines de enmiendas al Documento de Selección sin identificar el nombre del Oferente que planteó la aclaración o enmienda, y serán puestos a disposición de los potenciales oferentes en la página web del Contratante, y también se enviarán a todos los Oferentes que hayan remitido su solicitud de aclaraciones.

9. Anexo encontrará los Documentos del Procedimiento. Por favor informarnos por escrito de su intención de participar a la misma dirección consignada en el numeral anterior o a través del siguiente correo electrónico: **proyecto.bid@mspsalud.gob.ec.**

Atentamente,

_____

Mgs. Mercedes Liliana Lascano Gómez
Gerente del Proyecto de Apoyo a la Transformación Digital y Fortalecimiento de los Servicios Integrales de Salud - BID
DELEGADO DE LA MAXIMA AUTORIDAD
MINISTERIO DE SALUD PÚBLICA

[1] Pudiera ser necesario extender el plazo para la presentación de Ofertas si la respuesta del Contratante resulta en cambios sustanciales a los Documentos de Selección, o si la elaboración de los boletines de aclaraciones o boletines de enmiendas toman un tiempo que hace necesario extender el plazo para permitir a los Oferentes un tiempo razonable para valorar las aclaraciones o enmiendas en la preparación de las Ofertas.

SECCIÓN 02: DOCUMENTO DE SELECCIÓN: COMPARACION DE PRECIOS

1. OBJETO DE LA CONTRATACIÓN Y ALCANCE DE LOS TRABAJOS

El objeto de esta comparación de precios es la: **"ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL"**, de conformidad con las/los términos de referencia de la sección 05 del presente documento.

2. IDENTIFICACIÓN DEL PROYECTO

El nombre e identificación del contrato es **4364**/OC-EC**,** cuyo objetivo es **PROGRAMA MULTIFASE DE MEJORA DE LA CALIDAD EN PRESTACIÓN DE LOS SERVICIOS SOCIALES,** número de identificador SEPA**: MULTIFASE I-133-CP-S-002-2023**

3. PRACTICAS PROHIBIDAS

Para GN 2349-15:

1.1. El Banco exige a todos los Prestatarios (incluidos los beneficiarios de donaciones), organismos ejecutores y organismos contratantes, al igual que a todas las firmas, entidades o individuos oferentes por participar o participando en actividades financiadas por el Banco incluidos, entre otros, solicitantes, oferentes, proveedores de bienes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios y concesionarios (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) observar los más altos niveles éticos y denunciar al Banco12 todo acto sospechoso de constituir una Práctica Prohibida del cual tenga conocimiento o sea informado durante el proceso de selección y las negociaciones o la ejecución de un contrato. Las Prácticas Prohibidas comprenden (i) prácticas corruptas; (ii) prácticas fraudulentas; (iii) prácticas coercitivas; (iv) prácticas colusorias; (v) prácticas obstructivas; y (vi) apropiación indebida. El Banco ha establecido mecanismos para denunciar la supuesta comisión de Prácticas Prohibidas. Toda denuncia deberá ser remitida a la Oficina de Integridad Institucional (OII) del Banco para que se investigue debidamente. El Banco también ha adoptado procedimientos de sanción para la resolución de casos. Asimismo, el Banco ha celebrado acuerdos con otras instituciones financieras internacionales a fin de dar un reconocimiento recíproco a las sanciones impuestas por sus respectivos órganos sancionadores.

(a) A efectos del cumplimiento de esta Política, el Banco define las expresiones que se indican a continuación:

(i) Una práctica corrupta consiste en ofrecer, dar, recibir, o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar indebidamente las acciones de otra parte;

(ii) Una práctica fraudulenta es cualquier acto u omisión, incluida la tergiversación de hechos y circunstancias, que deliberada o

imprudentemente engañen, o intenten engañar, a alguna parte para obtener un beneficio financiero o de otra naturaleza o para evadir una obligación;

(iii) Una práctica coercitiva consiste en perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar indebidamente las acciones de una parte;

(iv) Una práctica colusoria es un acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, lo que incluye influenciar en forma inapropiada las acciones de otra parte;

(v) Una práctica obstructiva consiste en

i. destruir, falsificar, alterar u ocultar evidencia significativa para una investigación del Grupo BID, o realizar declaraciones falsas ante los investigadores con la intención de impedir una investigación del Grupo BID;

ii. amenazar, hostigar o intimidar a cualquier parte para impedir que divulgue su conocimiento de asuntos que son importantes para una investigación del Grupo BID o que prosiga con la investigación; o

iii) actos realizados con la intención de impedir el ejercicio de los derechos contractuales de auditoría e inspección del Grupo BID previstos en el párrafo 60.1 (f) de abajo, o sus derechos de acceso a la información; y

(vi) La apropiación indebida consiste en el uso de fondos o recursos del Grupo BID para un propósito indebido o para un propósito no autorizado, cometido de forma intencional o por negligencia grave.

(b) Si el Banco determina que cualquier firma, entidad o individuo actuando como oferente o participando en una actividad financiada por el Banco incluidos, entre otros, solicitantes, oferentes, proveedores, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios, Prestatarios (incluidos los Beneficiarios de donaciones), organismos ejecutores o contratantes (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) ha cometido una Práctica Prohibida en cualquier etapa de la adjudicación o ejecución de un contrato, el Banco podrá:

(i) No financiar ninguna propuesta de adjudicación de un contrato para la adquisición de bienes o la contratación de obras financiadas por el Banco;

(ii) Suspender los desembolsos de la operación, si se determina, en cualquier etapa, que un empleado, agencia o representante del Prestatario, el Organismo Ejecutor o el Organismo Contratante ha cometido una Práctica Prohibida;

(iii) Declarar una contratación no elegible para financiamiento del Banco y cancelar o acelerar el pago de una parte del préstamo o de la donación relacionada inequívocamente con un contrato, cuando exista evidencia de que el representante del Prestatario, o Beneficiario de una donación, no ha tomado las medidas correctivas adecuadas (lo que incluye, entre otras cosas, la notificación adecuada al Banco tras tener conocimiento de la comisión de la Práctica Prohibida) en un plazo que el Banco considere razonable;

(iv) Emitir una amonestación a la firma, entidad o individuo en el formato de una carta formal de censura por su conducta;

(v) Declarar a una firma, entidad o individuo inelegible, en forma permanente o por determinado período de tiempo, para que (i) se le adjudiquen o participe en actividades financiadas por el Banco, y (ii) sea designado13 subconsultor, subcontratista o proveedor de bienes o servicios por otra firma elegible a la que se adjudique un contrato para ejecutar actividades financiadas por el Banco;

(vi) Remitir el tema a las autoridades pertinentes encargadas de hacer cumplir las leyes; o

(vii) Imponer otras sanciones que considere apropiadas bajo las circunstancias del caso, incluida la imposición de multas que representen para el Banco un reembolso de los costos vinculados con las investigaciones y actuaciones. Dichas sanciones podrán ser impuestas en forma adicional o en sustitución de las sanciones arriba referidas.

(c) Lo dispuesto en los incisos (i) y (ii) del párrafo 1.1 (b) se aplicará también en casos en los que las partes hayan sido temporalmente declaradas inelegibles para la adjudicación de nuevos contratos en espera de que se adopte una decisión definitiva en un proceso de sanción, o cualquier otra resolución.

(d) La imposición de cualquier medida que sea tomada por el Banco de conformidad con las provisiones referidas anteriormente será de carácter público.

(e) Asimismo, cualquier firma, entidad o individuo actuando como oferente o participando en una actividad financiada por el Banco, incluidos, entre otros, solicitantes, oferentes, proveedores de bienes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios, Prestatarios (incluidos los beneficiarios de donaciones), organismos ejecutores o contratantes (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) podrá verse sujeto a sanción de conformidad con lo dispuesto en convenios suscritos por el Banco con otra institución financiera internacional concernientes al reconocimiento recíproco de decisiones de inhabilitación. A efectos de lo dispuesto en el presente párrafo, el término "sanción" incluye toda inhabilitación permanente, imposición de condiciones para la participación en futuros contratos o adopción pública de medidas en respuesta a una contravención del marco vigente de una institución financiera internacional aplicable a la resolución de denuncias de comisión de Prácticas Prohibidas.

(f) El Banco requiere que en los documentos de licitación y los contratos financiados con un préstamo o donación del Banco se incluya una disposición que exija que los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas subconsultores, proveedores de servicios y concesionarios permitan al Banco revisar cualesquiera cuentas, registros y otros documentos relacionados con la presentación de propuestas y con el cumplimiento del contrato y someterlos a una auditoría por auditores designados por el Banco. Bajo esta política, todo

solicitante, oferente, proveedor de bienes y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios y concesionario deberá prestar plena asistencia al Banco en su investigación. El Banco requerirá asimismo que se incluya en contratos financiados con un préstamo o donación del Banco una disposición que obligue a solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios y concesionarios a (i) conservar todos los documentos y registros relacionados con actividades financiadas por el Banco por un período de siete (7) años luego de terminado el trabajo contemplado en el respectivo contrato; (ii) entregar cualquier documento necesario para la investigación de denuncias de comisión de Prácticas Prohibidas y hacer que empleados o agentes de los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, subcontratistas, subconsultores, proveedores de servicios y concesionarios que tengan conocimiento de las actividades financiadas por el Banco estén disponibles para responder a las consultas relacionadas con la investigación provenientes de personal del Banco o de cualquier investigador, agente, auditor o consultor apropiadamente designado. Si el solicitante, oferente, proveedor de servicios y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios o concesionario se niega a cooperar o incumple el requerimiento del Banco, o de cualquier otra forma obstaculiza la investigación por parte del Banco, el Banco, bajo su sola discreción, podrá tomar medidas apropiadas contra el solicitante, oferente, proveedor de bienes y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios o concesionario.

(g) El Banco exigirá que, cuando un Prestatario adquiera bienes, obras o servicios diferentes a los de consultoría directamente de una agencia especializada, de conformidad con lo establecido en el párrafo 3.10, en el marco de un acuerdo entre el Prestatario y dicha agencia especializada, todas las disposiciones contempladas en el párrafo 1.1 (b) relativas a sanciones y Prácticas Prohibidas se apliquen íntegramente a los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas), o cualquier otra entidad que haya suscrito contratos con dicha agencia especializada para la provisión de bienes, obras o servicios diferentes a los de consultoría en conexión con actividades financiadas por el Banco. El Banco se reserva el derecho de obligar al Prestatario a que se acoja a recursos tales como la suspensión o la rescisión. Las agencias especializadas deberán consultar la lista de firmas e individuos declarados inelegibles de forma temporal o permanente por el Banco. En caso de que una agencia especializada suscriba un contrato o una orden de compra con una firma o individuo declarado inelegible de forma temporal o permanente por el Banco, el Banco no financiará los gastos conexos y se acogerá a otras medidas que considere convenientes.

1.2. Los oferentes al presentar sus ofertas declaran y garantizan:

(i) que han leído y entendido las definiciones de Prácticas Prohibidas del Banco y las sanciones aplicables a la comisión de las mismas que constan de este documento y se obligan a observar las normas pertinentes sobre las mismas;

(ii) que no han incurrido en ninguna Práctica Prohibida descrita en este documento;

(iii) que no han tergiversado ni ocultado ningún hecho sustancial durante los procesos de selección, negociación, adjudicación o ejecución de un contrato;

(iv) que reconocen que el incumplimiento de cualquiera de estas garantías constituye el fundamento para la imposición por el Banco de una o más de las medidas que se describen en la Cláusula 1.1 (b).

4. OFERENTES ELEGIBLES

4.1 Un Oferente, y todas las partes que constituyen el Oferente, deberán ser originarios de países miembros del Banco. Los Oferentes originarios de países no miembros del Banco serán descalificados de participar en contratos financiados en todo o en parte con fondos del Banco. En la Sección Anexos de este documento se indican los países miembros del Banco al igual que los criterios para determinar la nacionalidad de los Oferentes y el origen de los bienes y servicios. Los oferentes de un país miembro del Banco, al igual que los bienes suministrados, no serán elegibles si:

Para GN 2349-15:

(a) Las firmas de un país o los bienes producidos en un país pueden ser excluidos si, (i) las leyes o las reglamentaciones oficiales del país del Prestatario prohíben las relaciones comerciales con aquel país, a condición de que se demuestre satisfactoriamente al Banco que esa exclusión no impedirá la competencia efectiva respecto al suministro de los bienes o la construcción de las obras de que se trate, o (ii) en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada en virtud del Capítulo VII de la Carta de las Naciones Unidas del país Prestatario prohíbe la importación de bienes del país en cuestión o pagos de cualquier naturaleza a ese país, a una persona o una entidad. Cuando se trate de que el país del Prestatario, en cumplimiento de este mandato, prohíba pagos a una firma o compras de bienes en particular, esta firma puede ser excluida.

(b) Toda firma (incluidos sus accionistas, directores ejecutivos y personal clave) contratada por el Prestatario para proveer servicios de consultoría respecto de la preparación o ejecución de un proyecto, al igual que su matriz y todas sus filiales, quedará descalificada para suministrar bienes o construir obras o servicios que resulten directamente relacionados con los servicios de consultoría para la preparación o ejecución. Esta disposición no se aplica a las diversas firmas (consultores, contratistas o proveedores) que conjuntamente estén cumpliendo las obligaciones del contratista en virtud de un contrato llave en mano o de un contrato de diseño y construcción.

(c) Toda firma (incluidos sus accionistas, directores ejecutivos y personal clave) que tenga una relación de negocios, incluida una relación de empleo u otro arreglo financiero, antes o durante la ejecución del contrato, una relación familiar o personal con un miembro del personal, consultor, empresa de consultoría del Prestatario o personal del Banco que participe directa o indirectamente en (i) la preparación de las especificaciones técnicas o una actividad equivalente; (ii) el proceso de licitación del contrato; o (iii) la supervisión del contrato, puede quedar excluida de la adjudicación del contrato, a menos que el conflicto derivado de esa relación se haya divulgado y resuelto de manera aceptable para el Banco a lo largo del proceso de selección y de la ejecución del contrato.

(d) Las empresas estatales del país del Prestatario podrán participar solamente si pueden demostrar que (i) tienen autonomía legal y financiera; (ii) funcionan conforme a las leyes comerciales; y (iii) no dependen de entidades del Prestatario o Subprestatario[2].

(e) Toda firma, individuo, empresa matriz o filial, u organización anterior constituida o integrada por cualquiera de los individuos designados como partes contratantes que el Banco declare inelegible de conformidad con lo dispuesto en los incisos (b)(v) y (e) párrafo 1.16 de las Políticas de Adquisición de bienes y obras GN 2349-15, relativos a Prácticas Prohibidas, o que otra institución financiera internacional declare inelegible y con sujeción a lo dispuesto en acuerdos suscritos por el Banco concernientes al reconocimiento recíproco de sanciones será inelegible para la adjudicación o derivación de beneficio alguno, financiero o de cualquier otra índole, de un contrato financiado por el Banco durante el período que el Banco determine.

4.2 Un Oferente no deberá tener conflicto de interés. Los Oferentes que sean considerados que tienen conflicto de interés serán descalificados. Se considerará que los Oferentes tienen conflicto de interés con una o más partes en este proceso si ellos:

(a) están o han estado asociados, directa o indirectamente, con una firma o con cualquiera de sus afiliados, que ha sido contratada por el Contratante para la prestación de servicios de consultoría para la preparación del diseño, las especificaciones técnicas y otros documentos que se utilizarán en el proceso para la contratación de las obras y/o adquisición de bienes objeto de estos Documentos de Selección; o

(b) presentan más de una oferta en este proceso licitatorio. Sin embargo, esto no limita la participación de subcontratistas en más de una oferta

4.3 Los Oferentes deberán proporcionar al Contratante evidencia satisfactoria de su continua elegibilidad, cuando el Contratante razonablemente la solicite.

5. PRECIO REFERENCIAL

El precio referencial es de US$ 94.816,15 (Noventa y cuatro mil ochocientos dieciséis dólares de los Estados Unidos de América con 15/100 ctvs.), más IVA.

[2] Salvo las empresas de construcción públicas que se permiten en virtud del párrafo 3.9 de las Políticas de Adquisición de bienes y obras GN 2349-15.

El precio de la oferta incluye el valor de los servicios diferentes de consultoría, su entrega, así como todos los costos directos e indirectos, impuestos (incluido el IVA), tasas, contribuciones y servicios; es decir, absolutamente todo lo necesario para entregar los servicios a plena satisfacción del Programa/Proyecto.

6. PLAZO DE ENTREGA

El plazo de ejecución de los servicios es de 60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.

7. LUGAR DE ENTREGA DE LOS SERVICIOS DIFERENTES DE CONSULTORÍA Y/O SERVICIOS CONEXOS

Los servicios diferentes de consultoría serán entregados en la provincia de Pichincha, cantón Quito, Plataforma Gubernamental de Desarrollo Social, ubicado en la Av. Amaru Ñan y Av. Lira Ñan.

8. FORMA DE PAGO

El pago se realizará 100% CONTRAENTREGA.

El pago total se realizará en DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA. Del monto total del contrato se realizarán las retenciones de ley correspondientes.

9. COMUNICACIONES

Todos los trámites y presentaciones referidos a este proceso de selección por comparación de precios deberán realizarse por escrito al Contratante a la siguiente dirección:

- Dirección: Av. Quitumbe Ñan y Av. Amaru Ñan
- Edificio: Plataforma Gubernamental de Desarrollo Social
- Departamento: Oficina 105
- Ciudad: Quito
- País: Ecuador
- Correo electrónico: **proyecto.bid@mspsalud.gob.ec**
- Código postal: 170702

10. SOLICITUD DE ACLARACIONES Y ENMIENDAS

El Contratante realizará las aclaraciones o enmiendas que correspondan por iniciativa propia o a solicitud de los invitados, por lo menos **5** días antes de la fecha límite para la presentación de las Ofertas[3]. Las aclaraciones o enmiendas serán entregadas a través de

[3] Pudiera ser necesario extender el plazo para la presentación de Ofertas si la respuesta del Contratante resulta en cambios sustanciales a los Documentos de Selección, o si la elaboración de los boletines de aclaraciones o boletines de enmiendas toman un tiempo que hace necesario extender el plazo para permitir a los Oferentes un tiempo razonable para valorar las aclaraciones o enmiendas en la preparación de las Ofertas.

boletines de aclaraciones y/o boletines de enmiendas al Documento de Selección sin identificar el nombre del Oferente que planteó la aclaración o enmienda, y serán puestos a disposición de los potenciales oferentes en la página web del Contratante, y también se enviarán a todos los Oferentes invitados cuando se ha aplicado el mecanismo de invitación en el proceso.

11. MONEDA DE LA OFERTA

La oferta debe presentarse en Dólares de los Estados Unidos de América (US$).

12. PREPARACIÓN Y PRESENTACIÓN DE OFERTAS

La oferta deberá estar foliada correlativamente y firmada por el representante legal o apoderado debidamente acreditado por el oferente.

El oferente presentará su oferta en formato físico y adjuntará una copia en formato magnético (CD) o digital (memoria USB) no editable. El Oferente preparará un original de los documentos que comprenden la Oferta lo colocará en un sobre lo sellará y lo marcará claramente como "ORIGINAL". Además, presentará 1 (una) copia impresa también contenida en un sobre sellado y marcado como "COPIA". En caso de discrepancia entre el original y la copia, el texto del original prevalecerá sobre el de las copias.

Los dos sobres (original y copia) deben ser colocados en un único sobre exterior y cada uno de estos debe contener la siguiente carátula:

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023

Título de la adquisición: **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL**

Señores

[Indicar el nombre del Contratante]

Oferta presentada por **[Indicar el nombre del Oferente]**

Dirección **[describir dirección exacta del Oferente]**

No abrir antes de **[Colocar fecha], [Colocar hora de apertura] (GMT-5)**

El Contratante conferirá un comprobante de recepción por la entrega de oferta y anotará, tanto en el recibo como en el sobre de la oferta, la fecha y hora (GMT-5) de recepción (en caso de ofertas físicas).

13. PERÍODO DE VALIDEZ DE LA OFERTA

Las ofertas deberán permanecer válidas por un periodo de 90 (noventa) días a partir de la fecha de presentación de las ofertas.

14. CONTENIDO DE LAS OFERTAS

El sobre único de la oferta a presentar deberá contener la siguiente documentación:

a) **Índice del contenido de la Oferta.**

b) **Información Institucional**

- Designación de representante legal y/o apoderado con facultades suficientes para obligar a la firma.
- Copia del instrumento constitutivo de la firma y, de corresponder, el documento de la modificación del cual surja claramente que el objeto social es afín al objeto de la contratación.
- Declaración de Mantenimiento de Oferta **(Formulario N° 06).**
- Autorización del Fabricante **(Formulario N° 07) (no aplica)**.

c) **Información Técnica:**

- Formulario de Presentación de oferta debidamente suscrita **(Formulario N° 01).**
- Datos Generales del Oferente **(Formulario N° 02)**.
- Lista de Cantidades y precios **(Formulario N° 03)**.
- Documentación que acredite la conformidad de los Servicios, cumplen con los Términos de referencia y los estándares especificados.
- Descripción detallada de las características esenciales técnicas de los servicios a ejecutar demostrando conformidad sustancial con los términos de referencia solicitados **(Formulario N° 04)**.
- Cronograma de cumplimiento y Plan de Entregas **(Formulario N° 05)**.
- En el caso de un Oferente que no está establecido comercialmente en el país del Contratante, el Oferente está o estará (si se le adjudica el Contrato) representado por un Agente en el país del Contratante equipado y con capacidad para cumplir con las obligaciones de mantenimiento, reparaciones y almacenamiento de repuestos, estipuladas en las Condiciones del Contrato y/o las Especificaciones Técnicas.

d) **El formulario y los documentos de Información para la Calificación**: Evidencia documentada acreditando que el oferente cumple con los siguientes requisitos de admisibilidad:

- **FACTURACION (Formulario N° 08):** No aplica
- **EXPERIENCIA COMO CONTRATISTA PRINCIPAL (Formulario N° 09):**

Experiencia General Mínima

DESCRIPCIÓN	TEMPORALIDAD	MONTO MÍNIMO POR CONTRATO	CONTRATOS PERMITIDOS	FUENTE DE VERIFICACIÒN
VENTA O INSTALACIÓN/ACTIVACIÒN DE LICENCIAS DE SOFTWARE	DENTRO DE LOS ÚLTIMOS 5 AÑOS, PREVIOS A LA PUBLICACIÓN DE ESTE PROCESO	$ 16.000,00	3	Copia (s) simple(s) de contratos con sus respectivas actas entrega recepción definitiva (para entidades públicas) o facturas debidamente legalizadas (para empresas del sector privado), que demuestren la experiencia solicitada.

Tabla de experiencia general mínima

Nota: Valores no incluyen IVA

- El oferente podrá presentar hasta 3 (TRES) contratos, cuya suma sea igual o mayor a $ 48.000,00

Experiencia Específica Mínima

DESCRIPCIÓN	TEMPORALIDAD	MONTO MÍNIMO POR CONTRATO	CONTRATOS PERMITIDOS	FUENTES DE VERIFICACION
VENTA O INSTALACIÓN/ ACTIVACIÒN DE SOLUCIONES DE SEGURIDAD PARA EQUIPO DE USUARIO FINAL (EDR) O ANTIVIRUS	DENTRO DE LOS ÚLTIMOS 2 AÑOS, PREVIOS A LA PUBLICACIÓN DE ESTE PROCESO	$ 16.000,00	1	Copia (s) simple(s) de contratos con sus respectivas actas entrega recepción definitiva (para entidades públicas) o facturas debidamente legalizadas (para empresas del sector privado), que demuestren la experiencia solicitada.

Tabla de experiencia especifica mínima

Nota: Valores no incluyen IVA

- **DISPONIBILIDAD DE EQUIPO (Formulario N° 10):** No aplica

- **PERSONAL TÉCNICO CLAVE (Formulario N° 11):** El potencial oferente deberá acreditar que cuenta con el siguiente personal:

ÍTEM NRO.	FUNCIÓN	CANTIDAD	NIVEL DE ESTUDIO	TITULACIÓN ACADÉMICA	FUENTE O MEDIO DE VERIFICACIÓN
1	Técnico de soporte (conocimiento en la Herramienta EDR)	1	Tercer nivel	Ing. /Lic. /Tnlgo. Sistemas, o Ing. /Lic. /Tnlgo. en Telemática, o Ing. /Lic. /Tnlgo. Electrónico, o Ing. /Lic. /Tnlgo. En Redes, o Ing. /Lic. /Tnlgo. de Desarrollo, o Ing. /Lic. /Tnlgo. En Telecomunicaciones, o Ing. /Lic. /Tnlgo. En Sistemas Informáticos y Computación, o Ing. /Lic. /Tnlgo. en Sistemas Computacionales	Presentar hoja de vida y copia simple del título profesional

Tabla de personal técnico mínimo

Experiencia Mínima del personal técnico

ÍTEM NRO.	FUNCIÓN	DESCRIPCIÓN	FUENTE O MEDIO DE VERIFICACIÓN	CERTIFICACIÓN
1	Técnico de soporte (conocimiento en soluciones EDR)	Experiencia en soporte técnico, dentro de los últimos 2 años, previos a la publicación de este proceso, con un mínimo de 6 meses comprobable.	Copia de la hoja de vida, títulos o registros, actas, certificados de experiencia en diferentes instituciones, con el tiempo de experiencia requerida.	Certificaciones o Cursos en soluciones de EDR o ANTIVIRUS.

Tabla de Experiencia mínima del personal técnico

Para acreditar este requisito deberá adjuntar la siguiente información de respaldo:

- Los documentos a ser presentados deben ser en copias simple.
- El oferente deberá adjuntar a la oferta la hoja de vida, documento de ciudadanía, título obtenido del personal técnico y certificados solicitados.

Presentación en Copia Simple: La documentación puede ser presentada en copia simple, en tal caso la copia deberá ser legible.

15. EVALUACIÓN Y COMPARACIÓN DE LAS OFERTAS

Las ofertas serán evaluadas por una Comisión Técnica, observando los siguientes parámetros:

15.1. Examen preliminar:

(a) cumple con los requisitos de elegibilidad establecidos en este documento de selección;

(b) ha sido debidamente firmada;

(c) está acompañada de la Declaración de Mantenimiento de la Oferta, y

(d) cumple sustancialmente con los requisitos de los documentos de selección.

Una Oferta que cumple sustancialmente es la que satisface todos los términos, condiciones y especificaciones de los Documentos de Selección sin desviaciones, reservas u omisiones significativas. Una desviación, reserva u omisión significativa es aquella que:

i. afecta de una manera sustancial el alcance, la calidad o a la ejecución de los Servicios especificados en el Documento de Selección; o

ii. limita de una manera considerable, inconsistente con los Documentos de Selección, los derechos del CONTRATANTE o las obligaciones del Oferente en virtud del Contrato; o

iii. de rectificarse, afectaría injustamente la posición competitiva de los otros Oferentes cuyas Ofertas cumplen sustancialmente con los requisitos del Documento de selección

Si una Oferta no cumple sustancialmente con los requisitos de los Documentos de Selección, será rechazada por el Contratante.

15.2.Corrección de errores:

El Contratante verificará si las Ofertas que cumplen sustancialmente con los requisitos de los Documentos de Selección contienen errores aritméticos. Dichos errores serán corregidos por el Contratante de la siguiente manera:

i. Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido, a menos que, en opinión del Comprador, hay un error obvio en la colocación del punto decimal, entonces el precio total cotizado prevalecerá y se corregirá el precio unitario,

ii. Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total; y,

iii. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos de los incisos (i) y (ii) mencionados.

El CONTRATANTE ajustará el monto indicado en la Oferta de acuerdo con el procedimiento antes señalado para la corrección de errores y, con la anuencia del Oferente, el nuevo monto se considerará de obligatorio cumplimiento para el Oferente. Si el Oferente no estuviera de acuerdo con el monto corregido, la oferta será rechazada y podrá hacerse efectiva la Declaración de Mantenimiento de la Oferta.

15.3.Comparación de las Ofertas

El Contratante comparará solamente las Ofertas que determine que cumplen sustancialmente con los requisitos de este Documento de Selección y establecerá el orden de prelación en función de los precios ofertados. Para proceder con la comparación se debe contar por lo menos con 3 ofertas válidas.

15.4. Poscalificación del oferente

El CONTRATANTE determinará, a su entera satisfacción, si el Oferente seleccionado como el que ha presentado la oferta considerada como la más ventajosa[4] y ha cumplido sustancialmente con los Documentos de Selección está calificado para ejecutar el Contrato satisfactoriamente.

Dicha determinación se basará en el examen de la evidencia documentada de las calificaciones del Oferente. Una determinación afirmativa será un prerrequisito para la adjudicación del Contrato al Oferente.

Una determinación negativa resultará en la descalificación de la oferta del Oferente, en cuyo caso el Contratante procederá a determinar si el Oferente que presentó la

[4] Para GN 2349-15.

siguiente oferta considerada como la más ventajosa[5] está calificado para ejecutar el Contrato satisfactoriamente.

16. DERECHO DEL CONTRATANTE A ACEPTAR CUALQUIER OFERTA Y A RECHAZAR TODAS O CUALQUIERA DE LAS OFERTAS

El CONTRATANTE se reserva el derecho a aceptar o rechazar cualquier Oferta, de anular el proceso y de rechazar todas las Ofertas en cualquier momento antes de la adjudicación del Contrato, sin que por ello adquiera responsabilidad alguna ante los Oferentes o la obligación de informar a los mismos acerca de las razones para tomar tal decisión.

17. DERECHO DEL CONTRATANTE A VARIAR LAS CANTIDADES

El Contratante se reserva el derecho a aumentar o disminuir la cantidad de los Bienes y Servicios Conexos especificados originalmente siempre y cuando esta variación no exceda los porcentajes 0 % y no altere los precios unitarios u otros términos y condiciones de la oferta y de los Documentos de Selección.

18. ADJUDICACIÓN

El CONTRATANTE adjudicará el contrato al Oferente cuya Oferta se encuentre válida, cumpla sustancialmente con los requisitos de los Documentos de Selección y que representa el costo evaluado como más bajo, siempre y cuando el CONTRATANTE haya determinado que dicho Oferente (a) es elegible y (b) y cumple con los requisitos de calificación consignados en esta sección.

Tan pronto se adjudique, el Contratante notificará por escrito la decisión de adjudicación del contrato al Oferente cuya Oferta haya sido aceptada, quien deberá presentar la Garantía de Cumplimiento del Contrato en un plazo máximo de **3** días, adjuntando además la documentación que a continuación se consigna, como condición previa a la suscripción del contrato.

a) Registro Único de Contribuyentes (RUC).

b) Garantía de Cumplimiento aceptable al Contratante. Esta Garantía emitida en dólares de los Estados Unidos de América y deberá ser:

i. Garantía por un valor equivalente correspondiente al 5 (cinco) % del monto del contrato incondicional irrevocable y de cobro inmediato, otorgada por un banco o institución financiera, establecida en el país o por intermedio de ellos, o

ii. Fianza instrumentada en una póliza de seguros, por un valor equivalente al por al 5 (cinco) % del monto del contrato incondicional e irrevocable, de cobro inmediato, emitida por una compañía de seguro establecida en el país.

Estas garantías no admitirán cláusula alguna que establezca trámite administrativo previo, bastando para su ejecución el requerimiento por escrito del Contratante.

[5] Para GN 2349-15.

c) Garantía Técnica: Al momento de la suscripción del contrato y como parte integrante del mismo se entregará por parte del contratista una garantía técnica. Esta garantía se mantendrá vigente de acuerdo con las estipulaciones establecidas en el contrato y de acuerdo a las siguientes consideraciones:

- La vigencia de la garantía técnica de las licencias será por 365 días, contados a partir de la fecha de activación de las licencias en la consola.
- La garantía técnica debe ser entregada a través de un certificado emitido por el fabricante o distribuidor autorizado y debe estar registrada a nombre del Ministerio de Salud Pública del Ecuador.
- La garantía técnica incluirá el compromiso de realizar el soporte técnico por parte de Contratista durante la vigencia de las licencias.
- Las actualizaciones de software de la solución EDR deberán ser provistas sin costo durante la vigencia de las licencias.

La no presentación de la documentación requerida en tiempo y forma podrá determinar el rechazo de su oferta y ejecutar la Declaración de Mantenimiento de la Oferta.

Tan pronto como el Oferente seleccionado presente la Garantía de Cumplimiento y documentación arriba requerida se suscribirá el contrato y el Contratante comunicará el nombre del Oferente seleccionado a todos los Oferentes no seleccionados.

19. GARANTÍA DE LOS BIENES (no aplica)

El PROVEEDOR garantiza:

a) que todos los bienes suministrados en virtud del Contrato son nuevos, sin uso, del modelo más reciente o actual e incorporan todas las mejoras recientes en cuanto a diseño y materiales, a menos que el Contrato disponga otra cosa,

b) que todos los bienes suministrados estarán libres de defectos derivados de actos y omisiones que éste hubiese incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en el país de destino final.

La garantía permanecerá vigente durante el período cuya fecha de terminación sea la más temprana entre los períodos siguientes:

SECCIÓN 03: FORMULARIOS PARA PRESENTACIÓN DE OFERTAS

Formulario 01 - Formulario de Presentación de la Oferta

Comparación de Precios CP No: CP-S-002-2023

Título de la adquisición: ***[insertar el título]***

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023

[insertar la fecha]

Señores

[Nombre del Contratante]

Presente.-

De mi consideración:

El que suscribe, en atención a la invitación efectuada por el Ministerio de Salud Pública (MSP), luego de examinar los lineamientos recibidos, ofrece los **[servicios diferentes de consultoría y/o servicios conexos]** por un Precio del Contrato de **US$ [indique el monto en cifras y en letras]** dólares de los Estados Unidos de América, incluido el valor del IVA.

El precio incluye todos los tributos, impuesto y/o cargos, comisiones, etc. y cualquier gravamen que pueda recaer sobre el CONTRATISTA, incluido el IVA.

El plazo total propuesto de entrega es de **[XX]** días calendario, contados a partir de la suscripción del contrato.

Al presentar la oferta como Representante Legal de **[Nombre del Oferente]**, declaro bajo juramento, que:

1. Nos comprometemos a entregar los **[servicios diferentes de consultoría y/o servicios conexos]** con sujeción a los requisitos que se estipulan en los documentos de selección y sus secciones y por los precios fijos arriba indicados y consignados también en la Oferta.
2. Garantizo la veracidad y exactitud de la información y las declaraciones incluidas en los documentos de la oferta, formularios y otros anexos.
3. Nos comprometemos a denunciar cualquier acto relacionado con prácticas prohibidas que fuere de mi conocimiento durante el desarrollo del proceso.
4. Confirmamos por la presente que esta Oferta tiene un período de validez de **[XX]** días, y que está acompañada de una Declaración de Mantenimiento de Oferta.
5. Manifestamos con carácter de declaración jurada que: i) no tenemos conflicto de intereses, ii) nuestra empresa, sus afiliados o subsidiarias, incluyendo todos los subcontratistas o proveedores para ejecutar cualquier parte del Contrato, no han sido declarados inelegibles por el Banco, bajo las leyes del país del Contratante o normativas oficiales, y iii) no tenemos ninguna sanción del Banco o de alguna otra

Institución Financiera Internacional (IFI).

En caso de ser adjudicado, nos comprometemos a suscribir el contrato en los términos previstos en este documento de selección.

Entendemos que esta oferta, junto con su aceptación por escrito incluida en la notificación de adjudicación, constituirá una obligación hasta la suscripción del contrato, y que el Programa/Proyecto no está obligada a aceptar la oferta considerada como la más ventajosa[6] ni ninguna otra Oferta que reciban, sin que tal decisión permita reclamación por parte del oferente.

Conocemos y aceptamos que el Programa/Proyecto se reserva el derecho de adjudicar el contrato, cancelar el proceso, rechazar todas las ofertas o declarar desierto el proceso si conviniese a los intereses nacionales o institucionales, sin que ello le genere responsabilidad alguna.

Esta Oferta y su aceptación por escrito constituirán un Compromiso de obligatorio cumplimiento. Entendemos que ustedes no están obligados a aceptar la Oferta más baja ni ninguna otra Oferta que pudieran recibir.

Atentamente,

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

[6] Para GN 2349-15.

Formulario 02 – Datos generales del oferente

Comparación de Precios CP No: CP-S-002-2023

Título de la adquisición: [insertar el título]

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023

[insertar la fecha]

a) Información del oferente

1. Nombre del Oferente: **[indicar el nombre del Oferente]** Nacionalidad: **[indicar la nacionalidad]**
2. Naturaleza: **Persona natural: _____** **Persona jurídica: _____**
3. Año de registro del Oferente: **[indicar el año de registro del Oferente]**
4. Dirección del Oferente en el país donde está registrado: **[indicar la Dirección del Oferente en el país donde está registrado]**
5. Información del representante autorizado del Oferente: Nombre: **[indicar el nombre del representante autorizado]** Dirección: **[indicar la dirección del representante autorizado]** Números de teléfono: **[indicar los números de teléfono del representante autorizado]** Dirección de correo electrónico: **[indicar el correo electrónico del oferente]**
7. Se adjuntan copias de los documentos originales de: **[marcar la(s) casilla(s) de los documentos originales adjuntos]** ☐ Estatutos de la Sociedad o Registro de la empresa indicada en el párrafo1 anterior. ☐ Si se trata de una Asociación en Participación o Consorcio, Convenio de Asociación en Participación o del Consorcio.

Formulario 03 – Lista de cantidades y precios

ITEM	DESCRIPCIÓN	UNIDAD	CANTIDAD *(a)*	PRECIO UNITARIO *(b)*	PRECIO TOTAL *(c)*
1	*Detallar los servicios de no consultoría*				*c=a*b*
2					
n					
				SUBTOTAL *(d)*	***d = ∑(c) (todos los ítems)***
				IVA *(e)*	***(e) = (d) * 12%***
				TOTAL *(f)*	***(f) = (d) + (e)***

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

Formulario 04 – Lista de Servicios, ofertados.

ITEM	DESCRIPCIÓN	UNIDAD	PAÍS DE ORIGEN DE LOS SERVICIOS	ESPECIFICACIONES TÉCNICAS REQUERIDAS	ESPECIFICACIONES TÉCNICAS OFERTADAS
1	*Detallar lista de los servicios de No consultoría*				
2					
n					

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

Formulario 05 – Cronograma de cumplimiento y Plan de Entregas

N° de Artículo	Descripción de los Servicios	Cantidad	Unidad física	Lugar de destino convenido	Fecha de Entrega		
					Fecha más Temprana de Entrega	Fecha Límite de Entrega	Fecha de Entrega Ofrecida por el Oferente *[a ser proporcionada por el Oferente]*
[indicar el No.]	*[indicar la descripción de los Servicios]*	*[indicar la cantidad de los artículos a suministrar]*	*[indicar la unidad física de medida de la cantidad]*	*[indicar el lugar de entrega destino convenido]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*
1	*LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL*	979	*Unidad*	*Provincia de Pichincha, cantón Quito, Plataforma Gubernamental de Desarrollo Social, ubicado en la Av. Amaru Ñan, y Av. Lira Ñan.*	*60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.*	*60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.*	

SERVICIOS CONEXOS – NO APLICA

N° de Artículo	Descripción de los Servicios Conexos y/o Servicios de No Consultoría	Cantidad	Unidad	Lugar de prestación del servicio	Fecha de Entrega		
					Fecha de inicio	Fecha de finalización	Plazo de Ejecución
[indicar el No.]	*[indicar la descripción de los servicios conexos y/o servicios de no consultoría]*	*[indicar la cantidad]*	*[indicar la unidad de medida de la cantidad]*	*[indicar el lugar de prestación del servicio]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el plazo ofertado para prestar el servicio]*

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

Formulario 06 - Declaración de Mantenimiento de la Oferta

*[Si se solicita, **el Oferente** completará este Formulario de acuerdo con las instrucciones indicadas en corchetes.]*

Fecha: *[indique la fecha]*
Nombre del Contrato.: *[indique el nombre]*
No. de Identificación del Contrato: *[indique el número]*
Comparación de Precios CP No: CP-S-002-2023

A: _____

Nosotros, los suscritos, declaramos que:

1. Entendemos que, de acuerdo con sus condiciones, las Ofertas deberán estar respaldadas por una Declaración de Mantenimiento de la Oferta.

2. Aceptamos que automáticamente seremos declarados inelegibles para participar en cualquier licitación de contrato con el Contratante por un período de 3 años contado a partir de la presentación de la oferta si violamos nuestra(s) obligación(es) bajo las condiciones de la Oferta sea porque:

   (a) retiráramos nuestra Oferta durante el período de vigencia de la Oferta especificado por nosotros en el Formulario de Oferta; o

   (b) no aceptamos la corrección de los errores de conformidad con los Documentos de Selección; o

   (c) si después de haber sido notificados de la aceptación de nuestra Oferta durante el período de validez de la misma, (i) no firmamos o rehusamos firmar el Convenio, si así se nos solicita; o (ii) no suministramos o rehusamos suministrar la Garantía de Cumplimiento de conformidad con las IAO.

3. Entendemos que esta Declaración de Mantenimiento de la Oferta expirará, si no somos el Oferente Seleccionado, cuando ocurra el primero de los siguientes hechos: (i) hemos recibido una copia de su comunicación informando que no somos el Oferente seleccionado; o (ii) haber transcurrido veintiocho días después de la expiración de nuestra Oferta.

Firmada: *[firma del representante autorizado]*. En capacidad de *[indique el cargo]*

Nombre: *[indique el nombre en letra de molde o mecanografiado]*

Debidamente autorizado para firmar la Oferta por y en nombre de: *[indique el nombre la entidad que autoriza]*

Fechada el *[indique el día]* día de *[indique el mes]* de *[indique el año]*

Formulario 07: Autorización del Fabricante (no aplica)

[El Oferente solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membrete del Fabricante y deberá estar firmado por la persona debidamente autorizada para firmar documentos que comprometan el Fabricante. El Oferente lo deberá incluirá en su oferta, si así se establece en estos documentos.]

Fecha: *[indicar la fecha (día, mes y año) de presentación de la oferta]*

Comparación de Precios No.: *[indicar el número del proceso]*

A: *[indicar el nombre completo del Contratante]*

POR CUANTO

Nosotros *[indicar nombre completo del Fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]* mediante el presente instrumento autorizamos a *[indicar el nombre completo del Oferente]* a presentar una oferta con el solo propósito de suministrar los siguientes Bienes de fabricación nuestra *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y plena garantía, respecto a los bienes ofrecidos por la firma antes mencionada.

Nombre: *[indicar el nombre completo del representante autorizado del Fabricante]*

Cargo: *[indicar cargo]*

Debidamente autorizado para firmar esta Autorización en nombre de: *[nombre completo del Oferente]*

Fechado en el día _____ de _____de __ [fecha de la firma]

Formulario 08 - Facturación Promedio Anual (no aplica)

Mi representada tiene una facturación promedio anual por *[venta de los siguientes bienes* **,** servicios diferentes de consultoría y/o servicios conexos *como: (detallar)]* por el período del *_(indicar fecha)__ al _(indicar fecha)__, de _(indicar monto),* adjunto documentos de respaldo. *(Ejem: facturas, declaración del impuesto a la renta, etc)*

Atentamente,

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

Formulario 09: Experiencia General y Específica del Oferente[7]

EXPERIENCIA GENERAL DEL OFERENTE COMO CONTRATISTA								
No	**CONTRATANTE (*)**	**OBJETO DEL CONTRATO**	**UBICACIÓN**	**VALOR USD**		**FECHAS EJECUCIÓN**		**PARTICIPACIÓN % EN ASOCIACIÓN – NOMBRE DEL SOCIO (**)**
				ORIGINAL	**FINAL**	**ORIGINAL**	**FINAL**	
A) CONTRATOS EJECUTADOS DE [VENTA DE LOS SIGUIENTES BIENES: (DETALLAR)/PRESTACIÓN DE SERVICIOS COMO: (DETALLAR)]								
1								
2								
TOTAL FACTURADO (INDICAR LA SUMA TOTAL EN US $)								

EXPERIENCIA ESPECIFICA DEL OFERENTE COMO CONTRATISTA								
No	**CONTRATANTE (*)**	**OBJETO DEL CONTRATO**	**UBICACIÓN**	**VALOR USD**		**FECHAS EJECUCIÓN**		**PARTICIPACIÓN % EN ASOCIACIÓN – NOMBRE DEL SOCIO (**)**
				ORIGINAL	**FINAL**	**ORIGINAL**	**FINAL**	
A) CONTRATOS EJECUTADOS DE [VENTA DE LOS SIGUIENTES BIENES: (DETALLAR)/PRESTACIÓN DE SERVICIOS COMO: (DETALLAR)]								
1								
2								
TOTAL FACTURADO (INDICAR LA SUMA TOTAL EN US $)								

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

[7] Para cada contratante, indicar el nombre, dirección, teléfono, fax, e-mail, persona de contacto y cargo. Si el contrato lo ejecutó asociado, indicar en esta casilla el nombre del o de los socios.

Formulario 10: Disponibilidad del Equipo (No aplica)

DESCRIPCIÓN DEL EQUIPO	*CARACTERÍSTICAS MÍNIMAS*	*ANTIGUEDAD*	*CONDICIÓN*	*CANTIDAD*	*PROPIETARIO*	*DISPONIBILIDAD*

Atentamente,

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

Dirección: _____

Formulario 11 - Personal Principal Propuesto – Curriculum Vitae

CARGO A EJERCER	*NACIONALIDAD*	*TÍTULO PROFESIONAL*[8]	*FECHA DE GRADO*	*PARTICIPACIÓN EN EL PROYECTO*

MODELO DE CURRICULUM VITAE DEL PERSONAL PRINCIPAL[9]

Nombre Completo: ……..

Edad: ……..

Nacionalidad: ……..

Ciudad de residencia: ……..

Títulos profesionales: Fecha obtención (d/m/a):

_____ _____

Cursos de especialización con duración mayor a 100 horas (Indicar el nombre del curso, lugar/institución que dio el curso, duración, fecha de realización).

Nombre curso Institución Duración Fechas (d/m/a)

Actividad actual y lugar de trabajo: ……**.**

Experiencia profesional: *(Indicar experiencia en proyectos similares)* ……

Asociaciones a las que pertenece: ……

Licencia o Registro Profesional *(profesionales nacionales):* ……

Artículos técnicos y publicaciones: ……

Declaro que la información proporcionada es verídica.

[insertar la fecha]

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Oferente: _____

[9] El oferente debe presentar un "Modelo de Currículum Vitae" por cada profesional que formará parte del personal técnico.

SECCIÓN 04: MODELO DE CONTRATO

Comparación de Precios CP No: CP-S-002-2023

Título de la adquisición: **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL**

Identificador SEPA: MULTIFASE I-133-CP-S-002-2023

Comparecen a la celebración del presente contrato, por una parte el Ministerio de Salud Pública (MSP), ubicado en la Plataforma Gubernamental de Desarrollo Social, en la Av. Amaru Ñan y Av. Lira Ñan de la ciudad de Quito, provincia de Pichincha, República del Ecuador representada por la Mgs. Mercedes Liliana Lascano Gómez, en su calidad de Gerente del Proyecto de Apoyo a la Transformación Digital y Fortalecimiento de los Servicios Integrales de Salud – BID, conforme la delegación conferida mediante Acuerdos Ministeriales No. 0324-2019 de 08 de marzo de 2019; No. 00055-2020 de 28 de agosto de 2020; y, No. 00077-2020 de 23 de octubre de 2020, a quien en adelante se le denominará CONTRATANTE o MSP; y, por otra **[Indicar el nombre del Contratista]**, representado por **[Indicar el nombre del Representante]** a quien en adelante se le denominará CONTRATISTA. Las partes se obligan en virtud del presente contrato, al tenor de las siguientes cláusulas:

Cláusula Primera.- ANTECEDENTES

La República del Ecuador y El Banco Interamericano de Desarrollo (BID) denominado "El Banco" o "El BID" denominado "El Contratante, han suscrito el contrato de préstamo No. 4364/OC-EC, para implementar el PROGRAMA MULTIFASE DE MEJORA DE LA CALIDAD EN PRESTACIÓN DE LOS SERVICIOS SOCIALES y el Componente No. 3 tiene entre sus objetivos financiar compras y contrataciones para la "ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL"

En el contrato de préstamo suscrito entre el Banco Interamericano de Desarrollo (BID) y el Ministerio de Salud Pública (MSP) se estableció que la contratación se efectuará atendiendo las Políticas para la Selección y Contratación de Consultores financiados por el BID GN 2349-15.

El Banco Interamericano de Desarrollo (BID) denominado "El Banco" o "El BID" y la República del Ecuador denominado "El Prestatario", suscribieron el 13 de abril de 2020, además el contrato modificatorio No. 1 al contrato de préstamo No. 4364/OC-EC, para la ejecución del Proyecto "PROGRAMA MULTIFASE DE LA CALIDAD EN LA PRESTACIÓN DE LOS SERVICIOS SOCIALES – FASE I",

Dentro del Plan de Adquisiciones aprobado a través del Sistema de Ejecución de Planes de Adquisiciones -SEPA, con fecha **[día/mes/año]** se incluyó el proceso de adquisición

para la "**ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL".**

[insertar antecedentes adicionales pertinentes].

Cláusula Segunda.- DOCUMENTOS DEL CONTRATO

Los documentos que constituyen el Contrato son:

Los documentos que acreditan la calidad de los comparecientes y su capacidad para celebrar este tipo de contratos. Los Términos de Referencia/especificaciones técnicas/lista de los servicios y plan de entregas y demás secciones del Documento de Selección en los cuales se detallan el objeto y alcance de la contratación. La oferta presentada por el oferente adjudicado. Las Garantías presentadas por el oferente adjudicado La Certificación de Disponibilidad Presupuestaria No. XXX La Notificación de adjudicación al oferente adjudicado

Demás documentación que se considere pertinente

Anexos: Prácticas Prohibidas y Elegibilidad

Cláusula Tercera.- OBJETO DEL CONTRATO

El objeto del Contrato es la adquisición de **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL** para El CONTRATANTE, de conformidad con las disposiciones del presente Contrato y según se define en los lineamientos del proceso de Comparación de Precios No. CP-S-002-2023.

Cláusula Cuarta.- PRECIO DEL CONTRATO

El precio del presente contrato, que el CONTRATANTE pagará al CONTRATISTA, es el de **US$ [indique el monto en cifras y en letras]** dólares de los Estados Unidos de América, más IVA, de conformidad con la oferta presentada por el CONTRATISTA.

El precio de la oferta incluye el valor de los **servicios diferentes de consultoría**, así como todos los costos directos e indirectos, impuestos (incluido el IVA), tasas, contribuciones y servicios; es decir, absolutamente todo lo necesario para entregar los servicios a plena satisfacción del Programa/Proyecto.

Cláusula Quinta. - FORMA DE PAGO

Conforme lo establecen las *Políticas para la Adquisición de Bienes y Obras financiados por el Banco Interamericano de Desarrollo (BID), numeral 2.41 GN 2349-15, los servicios se pagarán en su totalidad a la entrega y, si así se requiriere, inspección de los servicios contratados.*

El pago se realizará 100% CONTRAENTREGA, previa entrega de la siguiente documentación:

- Certificado de Activación del total de licencias.
- Certificado de Soporte y Garantía Técnica.
- Manual de Usuario de Administración de la Consola de la solución EDR.
- Certificados de asistencia de la Transferencia de Conocimiento.
- Informe técnico de la DTIC del MSP.
- Informe de conformidad del Administrador de Contrato.
- Acta de Entrega Recepción Definitiva
- Factura emitida por el Contratista.

El pago total se realizará en DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA. Del monto total del contrato se realizarán las retenciones de ley correspondientes.

Cláusula Sexta.- GARANTÍAS

Para la suscripción del contrato se rindieron las siguientes garantías:

6.1 Garantía de Cumplimiento aceptable al Contratante. Esta Garantía emitida en dólares de los Estados Unidos de América y deberá ser:

i. Garantía por un valor correspondiente al 5 (cinco) % del monto del contrato incondicional irrevocable y de cobro inmediato, otorgada por un banco o institución financiera, establecida en el país o por intermedio de ellos, o

ii. Fianza instrumentada en una póliza de seguros, por un valor equivalente al cinco por ciento (5 %) del monto del contrato incondicional e irrevocable, de cobro inmediato, emitida por una compañía de seguro establecida en el país.

Estas garantías no admitirán cláusula alguna que establezca trámite administrativo previo, bastando para su ejecución el requerimiento por escrito del Contratante.

6.2 Garantía Técnica: De acuerdo a lo indicado en el numeral 13.2 de la Sección 5 del Documento de Selección para Comparación de Precios.

6.3 Ejecución de las garantías: Las garantías contractuales podrán ser ejecutadas por el CONTRATANTE en los siguientes casos:

La de Cumplimiento del contrato:

a) Cuando el CONTRATANTE declare anticipada y unilateralmente terminado el contrato por causas imputables al CONTRATISTA.

b) Si el CONTRATISTA no la renovare cinco días antes de su vencimiento.

La Garantía técnica:

a) Cuando se incumpla con el objeto de esta garantía.

Cláusula Séptima.- PLAZO

El plazo de ejecución de los servicios es de 60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.

Cláusula Octava.- PRÓRROGAS DE PLAZO

El CONTRATANTE prorrogará el plazo total o los plazos parciales en los siguientes casos, y siempre que el CONTRATISTA así lo solicitare, por escrito, justificando los fundamentos de la solicitud, dentro del plazo de quince días siguientes a la fecha de producido el hecho que motiva la solicitud.

a) Por fuerza mayor o caso fortuito aceptado como tal por el CONTRATANTE, previo informe del administrador del contrato, en base al informe debidamente fundamentado de la administración. Tan pronto desaparezca la causa de fuerza mayor o caso fortuito, el CONTRATISTA está obligado a continuar con la ejecución del contrato, sin necesidad de que medie notificación por parte del administrador del contrato.

b) Cuando el CONTRATANTE ordenare la ejecución de trabajos adicionales, o cuando se produzcan aumentos de las cantidades dentro de los límites establecidos en el presente contrato.

c) Por suspensiones en los trabajos o cambios de las actividades previstas en el cronograma, motivadas por el CONTRATANTE por él ordenadas por ella, a través de la administración, y que no se deban a causas imputables al CONTRATISTA.

d) Si el CONTRATANTE no hubiera solucionado los problemas administrativos-contractuales o constructivos en forma oportuna, cuando tales circunstancias incidan en la ejecución de los trabajos.

En casos de prórroga de plazo, las partes elaborarán un nuevo cronograma, que sustituirá al original o precedente y tendrá el mismo valor contractual del sustituido.

El hecho de permitir al CONTRATISTA que continúe y finalice el contrato o cualquier parte de la misma después del vencimiento del plazo concedido, cuando éste haya incurrido en mora, no implica prórroga automática de plazo por parte del CONTRATANTE y tal terminación se ejecutará no obstante la aplicación de las multas estipuladas en el presente contrato.

Cláusula Novena.- DAÑOS Y PERJUICIOS

El contratista deberá indemnizar al contratante por demora en la ejecución de los servicios diferentes de consultoría el valor del (1/1000) diario del porcentaje de las obligaciones que se encuentren pendientes de ejecutarse conforme lo establecido en el contrato. Excepto en el evento de caso fortuito o fuerza mayor conforme lo dispuesto en el artículo 30 del Código Civil.

Cláusula Décimo- DEL AJUSTE DE PRECIOS

El precio del contrato no está sujeto a ajuste de precios.

Cláusula Décima Primera.- SUBCONTRATACIÓN

El CONTRATISTA se obliga a subcontratar los trabajos que han sido comprometidos en su oferta y por el monto en ella establecido.

(En caso de que el CONTRATISTA no haya ofertado subcontratación, la cláusula dirá: "El CONTRATISTA podrá subcontratar determinados trabajos previa autorización del CONTRATANTE siempre que el monto de la totalidad de lo subcontratado no exceda del 30% del valor total del contrato principal o % que se especifique).

Nota: (El CONTRATANTE escogerá una de las dos opciones, dependiendo de si el CONTRATISTA ofertó o no la subcontratación)

Nada de lo expresado en los documentos del contrato, creará relaciones contractuales entre un Subcontratista y El CONTRATANTE. La autorización para subcontratar una o más partes de los trabajos o la aprobación de un Subcontratista no relevará al CONTRATISTA de ninguna de las obligaciones que ha adquirido en virtud de este contrato, ni podrá interpretarse como suspensión de alguna de las disposiciones del contrato.

Cláusula Décimo Segunda.- DE LA ADMINISTRACIÓN DEL CONTRATO:

En todas las relaciones con el CONTRATISTA, el CONTRATANTE designa a **[Nombre del funcionario],** en calidad de Administrador de Contrato, quien deberá atenerse a las condiciones de los documentos de selección que forman parte del presente contrato.

EL CONTRATANTE podrá cambiar de administrador del contrato, para lo cual bastará cursar al CONTRATISTA la respectiva comunicación; sin que sea necesaria la modificación del texto contractual.

El Administrador velará por el cabal y oportuno cumplimiento de todas y cada una de las obligaciones derivadas del contrato, y adoptará las acciones que sean necesarias para evitar retrasos injustificados e impondrá las multas y sanciones a las que hubiere lugar.

Cláusula Décimo Tercera: RECEPCIÓN DEFINITIVA

Una vez finalizada la **ejecución de los servicios diferentes de consultoría**, el CONTRATISTA solicitará la recepción definitiva del contrato, debiéndose iniciar ésta en el plazo de diez [10] días contados desde la solicitud presentada por el CONTRATISTA.

Cláusula Décimo Cuarta: ACTAS DE RECEPCIÓN:

Las actas de entrega recepción contendrán los antecedentes, condiciones generales de ejecución, condiciones operativas, liquidación económica, liquidación de plazos, constancia de la recepción, cumplimiento de las obligaciones contractuales, y cualquier otra circunstancia que la entidad contratante estime necesaria.

Clausula Décimo Quinta: MODIFICACIONES

Para efectos de modificaciones a contratos firmados se actuará conforme a lo establecido en las *Políticas para la Adquisición de Bienes y Obras financiados por el Banco Interamericano de Desarrollo (BID)* GN 2349-15.

Cláusula Décimo Sexta- TERMINACIÓN DEL CONTRATO

El contrato terminará:

1. Por cumplimiento de las obligaciones contractuales;
2. Por mutuo acuerdo de las partes;
3. Por declaración unilateral del CONTRATANTE, en caso de incumplimiento del CONTRATISTA; y,
4. Por muerte del CONTRATISTA o por disolución de la persona jurídica CONTRATISTA que no se origine en decisión interna voluntaria de los órganos competentes de tal persona jurídica.
5. Si el CONTRATISTA no observa lo prescripto respecto de Prácticas Prohibidas y/o Elegibilidad de este Contrato.

Cláusula Décimo Séptima.- SOLUCIÓN DE CONTROVERSIAS

Contratista extranjero:

Los procedimientos de arbitraje serán: "Comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI)" *(UNCITRAL, por sus siglas en inglés)*

Reglamento de Arbitraje:
" Subcláusula 25.3 – Cualquiera disputa, controversia o reclamo generado por o en relación con este Contrato, o por incumplimiento, rescisión, o anulación del mismo, deberán ser resueltos mediante arbitraje de conformidad con el Reglamento de Arbitraje vigente de la UNCITRAL."

El lugar de arbitraje será: [indique la ciudad y el país]

Contratista nacional (local):

1. Si se suscitaren divergencias o controversias en la interpretación o ejecución del presente contrato, cuando las partes no llegaren a un acuerdo amigable directo, podrán utilizar los métodos alternativos para la solución de controversias en el Centro de Mediación de la Procuraduría General del Estado en la ciudad de Quito

2. Si respecto de la divergencia o divergencias suscitadas no existiere acuerdo, y las partes deciden someterlas al procedimiento establecido en el Código Orgánico General de Procesos, será competente para conocer la controversia el Tribunal Distrital de lo Contencioso Administrativo que ejerce jurisdicción en la ciudad de Quito.

Contratista local es la persona jurídica o natural con domicilio o sede principal de sus negocios dentro del territorio de la República del Ecuador.

En caso de que la entidad contratante sea de derecho privado: "Solución de Controversias dirá: Si respecto de la divergencia o controversia existentes no se lograre un acuerdo directo entre las partes, éstas recurrirán ante la justicia ordinaria del domicilio de la Entidad Contratante".

Cláusula Décimo Octava: COMUNICACIONES ENTRE LAS PARTES

Todas las comunicaciones, sin excepción, entre las partes, relativas a los trabajos, serán formuladas por escrito y en idioma castellano.

Las comunicaciones también podrán efectuarse a través de medios electrónicos.

Cláusula Décimo Novena: LEY APLICABLE

Este contrato, su significado e interpretación y la relación que crea entre las partes se regirán por las leyes de la República del Ecuador y las disposiciones establecidas en este contrato.

Cláusula Vigésima: DOMICILIO

Para todos los efectos de este contrato, las partes convienen en señalar su domicilio en la ciudad de Quito D.M.

Para efectos de comunicación o notificaciones, las partes señalan como su dirección, las siguientes:

El CONTRATANTE:

- Nombre: Ministerio de Salud Pública (MSP)
- Dirección: Av. Quitumbe Ñan y Av. Amaru Ñan
- Edificio: Plataforma Gubernamental de Desarrollo Social
- Departamento: Oficina 105
- Ciudad: Quito
- País: Ecuador

El CONTRATISTA*: (dirección y teléfonos, correo electrónico).*

- Nombre: XXXXXXXXXXXXXXXXX
- Dirección: XXXXXXXXXXXX
- Edificio: XXXXXXXXXXXX
- Departamento: XXXXXXXXXXXXX
- Ciudad: Quito
- País: Ecuador

Libre y voluntariamente, las partes expresamente declaran su aceptación a todo lo convenido en el presente contrato y se someten a sus estipulaciones.

Para constancia de la conformidad con todas y cada una de las cláusulas y estipulaciones constantes en este instrumento, firman las partes en XX (x) ejemplares.

Dado, en la ciudad de _____, a los……de……de…….

Por el CONTRATANTE

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

CONTRATISTA

Firma Autorizada: _____

Nombre y Cargo del Firmante: _____

Nombre del Contratista:

_____

Anexo 1: Prácticas Prohibidas y Elegibilidad

1. Prácticas Prohibidas

Para GN 2349-15:

1.1. El Banco exige a todos los Prestatarios (incluidos los beneficiarios de donaciones), organismos ejecutores y organismos contratantes, al igual que a todas las firmas, entidades o individuos oferentes por participar o participando en actividades financiadas por el Banco incluidos, entre otros, solicitantes, oferentes, proveedores de bienes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios y concesionarios (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) observar los más altos niveles éticos y denunciar al Banco12 todo acto sospechoso de constituir una Práctica Prohibida del cual tenga conocimiento o sea informado durante el proceso de selección y las negociaciones o la ejecución de un contrato. Las Prácticas Prohibidas comprenden (i) prácticas corruptas; (ii) prácticas fraudulentas; (iii) prácticas coercitivas; (iv) prácticas colusorias; (v) prácticas obstructivas; y (vi) apropiación indebida. El Banco ha establecido mecanismos para denunciar la supuesta comisión de Prácticas Prohibidas. Toda denuncia deberá ser remitida a la Oficina de Integridad Institucional (OII) del Banco para que se investigue debidamente. El Banco también ha adoptado procedimientos de sanción para la resolución de casos. Asimismo, el Banco ha celebrado acuerdos con otras instituciones financieras internacionales a fin de dar un reconocimiento recíproco a las sanciones impuestas por sus respectivos órganos sancionadores.

(a) A efectos del cumplimiento de esta Política, el Banco define las expresiones que se indican a continuación:

(i) Una práctica corrupta consiste en ofrecer, dar, recibir, o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar indebidamente las acciones de otra parte;

(ii) Una práctica fraudulenta es cualquier acto u omisión, incluida la tergiversación de hechos y circunstancias, que deliberada o imprudentemente engañen, o intenten engañar, a alguna parte para obtener un beneficio financiero o de otra naturaleza o para evadir una obligación;

(iii) Una práctica coercitiva consiste en perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar indebidamente las acciones de una parte;

(iv) Una práctica colusoria es un acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, lo que incluye influenciar en forma inapropiada las acciones de otra parte;

(v) Una práctica obstructiva consiste en

i. destruir, falsificar, alterar u ocultar evidencia significativa para una investigación del Grupo BID, o realizar declaraciones falsas ante los

investigadores con la intención de impedir una investigación del Grupo BID;

ii. amenazar, hostigar o intimidar a cualquier parte para impedir que divulgue su conocimiento de asuntos que son importantes para una investigación del Grupo BID o que prosiga con la investigación; o

iii) actos realizados con la intención de impedir el ejercicio de los derechos contractuales de auditoría e inspección del Grupo BID previstos en el párrafo 60.1 (f) de abajo, o sus derechos de acceso a la información; y

(iv) La apropiación indebida consiste en el uso de fondos o recursos del Grupo BID para un propósito indebido o para un propósito no autorizado, cometido de forma intencional o por negligencia grave.

(b) Si el Banco determina que cualquier firma, entidad o individuo actuando como oferente o participando en una actividad financiada por el Banco incluidos, entre otros, solicitantes, oferentes, proveedores, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios, Prestatarios (incluidos los Beneficiarios de donaciones), organismos ejecutores o contratantes (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) ha cometido una Práctica Prohibida en cualquier etapa de la adjudicación o ejecución de un contrato, el Banco podrá:

(i) No financiar ninguna propuesta de adjudicación de un contrato para la adquisición de bienes o la contratación de obras financiadas por el Banco;

(ii) Suspender los desembolsos de la operación, si se determina, en cualquier etapa, que un empleado, agencia o representante del Prestatario, el Organismo Ejecutor o el Organismo Contratante ha cometido una Práctica Prohibida;

(iii) Declarar una contratación no elegible para financiamiento del Banco y cancelar o acelerar el pago de una parte del préstamo o de la donación relacionada inequívocamente con un contrato, cuando exista evidencia de que el representante del Prestatario, o Beneficiario de una donación, no ha tomado las medidas correctivas adecuadas (lo que incluye, entre otras cosas, la notificación adecuada al Banco tras tener conocimiento de la comisión de la Práctica Prohibida) en un plazo que el Banco considere razonable;

(iv) Emitir una amonestación a la firma, entidad o individuo en el formato de una carta formal de censura por su conducta;

(v) Declarar a una firma, entidad o individuo inelegible, en forma permanente o por determinado período de tiempo, para que (i) se le adjudiquen o participe en actividades financiadas por el Banco, y (ii) sea designado subconsultor, subcontratista o proveedor de bienes o servicios por otra firma elegible a la que se adjudique un contrato para ejecutar actividades financiadas por el Banco;

(vi) Remitir el tema a las autoridades pertinentes encargadas de hacer cumplir las leyes; o

(vii) Imponer otras sanciones que considere apropiadas bajo las circunstancias del caso, incluida la imposición de multas que representen para el Banco un reembolso de los costos vinculados con las investigaciones y actuaciones. Dichas sanciones podrán ser impuestas en forma adicional o en sustitución de las sanciones arriba referidas.

(c) Lo dispuesto en los incisos (i) y (ii) del párrafo 1.1 (b) se aplicará también en casos en los que las partes hayan sido temporalmente declaradas inelegibles para la adjudicación de nuevos contratos en espera de que se adopte una decisión definitiva en un proceso de sanción, o cualquier otra resolución.

(d) La imposición de cualquier medida que sea tomada por el Banco de conformidad con las provisiones referidas anteriormente será de carácter público.

(e) Asimismo, cualquier firma, entidad o individuo actuando como oferente o participando en una actividad financiada por el Banco, incluidos, entre otros, solicitantes, oferentes, proveedores de bienes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios, Prestatarios (incluidos los beneficiarios de donaciones), organismos ejecutores o contratantes (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas) podrá verse sujeto a sanción de conformidad con lo dispuesto en convenios suscritos por el Banco con otra institución financiera internacional concernientes al reconocimiento recíproco de decisiones de inhabilitación. A efectos de lo dispuesto en el presente párrafo, el término "sanción" incluye toda inhabilitación permanente, imposición de condiciones para la participación en futuros contratos o adopción pública de medidas en respuesta a una contravención del marco vigente de una institución financiera internacional aplicable a la resolución de denuncias de comisión de Prácticas Prohibidas.

(f) El Banco requiere que en los documentos de licitación y los contratos financiados con un préstamo o donación del Banco se incluya una disposición que exija que los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas subconsultores, proveedores de servicios y concesionarios permitan al Banco revisar cualesquiera cuentas, registros y otros documentos relacionados con la presentación de propuestas y con el cumplimiento del contrato y someterlos a una auditoría por auditores designados por el Banco. Bajo esta política, todo solicitante, oferente, proveedor de bienes y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios y concesionario deberá prestar plena asistencia al Banco en su investigación. El Banco requerirá asimismo que se incluya en contratos financiados con un préstamo o donación del Banco una disposición que obligue a solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios y concesionarios a (i) conservar todos los documentos y registros relacionados con actividades financiadas por el Banco por un período de siete (7)

años luego de terminado el trabajo contemplado en el respectivo contrato; (ii) entregar cualquier documento necesario para la investigación de denuncias de comisión de Prácticas Prohibidas y hacer que empleados o agentes de los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, subcontratistas, subconsultores, proveedores de servicios y concesionarios que tengan conocimiento de las actividades financiadas por el Banco estén disponibles para responder a las consultas relacionadas con la investigación provenientes de personal del Banco o de cualquier investigador, agente, auditor o consultor apropiadamente designado. Si el solicitante, oferente, proveedor de servicios y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios o concesionario se niega a cooperar o incumple el requerimiento del Banco, o de cualquier otra forma obstaculiza la investigación por parte del Banco, el Banco, bajo su sola discreción, podrá tomar medidas apropiadas contra el solicitante, oferente, proveedor de bienes y su representante, contratista, consultor, miembro del personal, subcontratista, subconsultor, proveedor de servicios o concesionario.

(g) El Banco exigirá que, cuando un Prestatario adquiera bienes, obras o servicios diferentes a los de consultoría directamente de una agencia especializada, de conformidad con lo establecido en el párrafo 3.10, en el marco de un acuerdo entre el Prestatario y dicha agencia especializada, todas las disposiciones contempladas en el párrafo 1.1 (b) relativas a sanciones y Prácticas Prohibidas se apliquen íntegramente a los solicitantes, oferentes, proveedores de bienes y sus representantes, contratistas, consultores, miembros del personal, subcontratistas, subconsultores, proveedores de servicios, concesionarios (incluidos sus respectivos funcionarios, empleados y representantes, ya sean sus atribuciones expresas o implícitas), o cualquier otra entidad que haya suscrito contratos con dicha agencia especializada para la provisión de bienes, obras o servicios diferentes a los de consultoría en conexión con actividades financiadas por el Banco. El Banco se reserva el derecho de obligar al Prestatario a que se acoja a recursos tales como la suspensión o la rescisión. Las agencias especializadas deberán consultar la lista de firmas e individuos declarados inelegibles de forma temporal o permanente por el Banco. En caso de que una agencia especializada suscriba un contrato o una orden de compra con una firma o individuo declarado inelegible de forma temporal o permanente por el Banco, el Banco no financiará los gastos conexos y se acogerá a otras medidas que considere convenientes.

Anexo 2: Elegibilidad

Países Miembros cuando el financiamiento provenga del Banco Interamericano de Desarrollo.

Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Territorios elegibles

a) Guadalupe, Guyana Francesa, Martinica, Reunión – por ser Departamentos de Francia.
b) Islas Vírgenes Estadounidenses, Puerto Rico, Guam – por ser Territorios de los Estados Unidos de América.
c) Aruba – Por ser País Constituyente del Reino de los Países Bajos; y Bonaire, Curazao, Sint Maarten, Sint Eustatius – por ser Departamentos de Reino de los Países Bajos.
d) Hong Kong – por ser Región Especial Administrativa de la República Popular de China

2) Criterios para determinar Nacionalidad y el país de origen de los bienes y servicios

Para efectuar la determinación sobre: a) la nacionalidad de las firmas e individuos elegibles para participar en contratos financiados por el Banco y b) el país de origen de los bienes y servicios, se utilizarán los siguientes criterios:

A) Nacionalidad

a) **Un individuo** tiene la nacionalidad de un país miembro del Banco si él o ella satisface uno de los siguientes requisitos:

(i) es ciudadano de un país miembro; o

(ii) ha establecido su domicilio en un país miembro como residente "bona fide" y está legalmente autorizado para trabajar en dicho país.

b) **Una firma** tiene la nacionalidad de un país miembro si satisface los dos siguientes requisitos:

(i) esta legalmente constituida o incorporada conforme a las leyes de un país miembro del Banco; y

(ii) más del cincuenta por ciento (50%) del capital de la firma es de propiedad de individuos o firmas de países miembros del Banco.

Todos los socios de una asociación en participación, consorcio o asociación (APCA) con responsabilidad mancomunada y solidaria y todos los subcontratistas deben cumplir con los requisitos arriba establecidos.

B) Origen de los Bienes

Los bienes se originan en un país miembro del Banco si han sido extraídos, cultivados, cosechados o producidos en un país miembro del Banco. Un bien es producido cuando mediante manufactura, procesamiento o ensamblaje el resultado es un artículo comercialmente reconocido cuyas características básicas, su función o propósito de uso son substancialmente diferentes de sus partes o componentes.

En el caso de un bien que consiste de varios componentes individuales que requieren interconectarse (lo que puede ser ejecutado por el suministrador, el comprador o un tercero) para lograr que el bien pueda operar, y sin importar la complejidad de la interconexión, el Banco considera que dicho bien es elegible para su financiación si el ensamblaje de los componentes individuales se hizo en un país miembro. Cuando el bien es una combinación de varios bienes individuales que normalmente se empacan y venden comercialmente como una sola unidad, el bien se considera que proviene del país en donde este fue empacado y embarcado con destino al comprador.

Para efectos de determinación del origen de los bienes identificados como "hecho en la Unión Europea", estos serán elegibles sin necesidad de identificar el correspondiente país específico de la Unión Europea.

El origen de los materiales, partes o componentes de los bienes o la nacionalidad de la firma productora, ensambladora, distribuidora o vendedora de los bienes no determina el origen de los mismos

C) Origen de los Servicios

El país de origen de los servicios es el mismo del individuo o firma que presta los servicios conforme a los criterios de nacionalidad arriba establecidos. Este criterio se aplica a los servicios conexos al suministro de bienes (tales como transporte, aseguramiento, montaje, ensamblaje, etc.), a los servicios de construcción y a los servicios de consultoría.

Sección 05. Lista de Servicios, Cantidades, Términos de Referencia y Plan de entrega

El oferente "debe" presentar los análisis de Precios Unitarios en el presente proceso.

En caso de requerirse, esta información servirá únicamente como referencia para el contratante.

ITEM[10]	DESCRIPCIÓN	UNIDAD	CANTIDAD *(a)*	PRECIO UNITARIO *(b)*	PRECIO TOTAL *(c)*
1	LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL	Unid.	979		*c=a*b*
				SUBTOTAL *(d)*	***d = ∑ (c) (todos los ítems)***
				IVA *(e)*	***(e) = (d) * 12%***
				TOTAL *(f)*	***(f) = (d) + (e)***

REQUERIMIENTOS TÉCNICOS/TERMINOS DE REFERENCIA

[10] Este es un cuadro modelo para la descripción de la Lista de Cantidades.

No. De Artículo	*Nombre del Servicio*	*Cantidad de licencias requeridas*
1	LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL	979

1. ANTECEDENTES

El Ministerio de Salud Pública fue creado el 16 de junio del 1967, y de acuerdo al estatuto vigente la misión es: "*Garantizar el derecho a la salud de la población en el territorio ecuatoriano, a través de la gobernanza, promoción de la salud, prevención de enfermedades, vigilancia, calidad, investigación y provisión de servicios de atención integrada e integral*."

El Ministerio de Salud Pública tiene como visión: "*Ser la institución referente de todo el Sistema Nacional de Salud que garantizará una atención sanitaria de calidad, inclusiva y equitativa, con énfasis en la promoción de la salud y la prevención de enfermedades para el pleno desarrollo de oportunidades de la población*."

Los objetivos estratégicos del Ministerio de Salud Pública son:

- Incrementar la efectividad de la Gobernanza en el Sistema Nacional de Salud.
- Incrementar la investigación en salud.
- Incrementar la calidad de la vigilancia, prevención y control sanitario en el Sistema Nacional de Salud.
- Incrementar la calidad en la prestación de los servicios de salud.
- Incrementar la cobertura de las prestaciones de servicios de salud.
- Incrementar la promoción de la salud en la población.
- Incrementar la eficiencia institucional en el Ministerio de Salud Pública.

El Acuerdo Ministerial Nro. 00023-2022 de 30 de septiembre de 2022 donde se expide la reforma Integral al Estatuto Orgánico Sustitutivo de Gestión Organizacional por Procesos del Ministerio de Salud Pública señala que:

"*1.3.1.5. DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES*

Misión: *Asesorar y coordinar la gestión de los servicios de tecnologías de la información de la entidad, alineados al plan estratégico institucional, al cumplimiento del Plan Nacional de Gobierno Electrónico y las políticas y objetivos gubernamentales, mediante la formulación, implementación y administración de políticas, normas, y procedimientos que optimicen la gestión y administración de las tecnologías de la información y comunicaciones*".

Responsable: Director/a de Tecnologías de la Información y Comunicaciones
Atribuciones y Responsabilidades:

d. Aprobar los términos de referencia y especificaciones técnicas requeridas relacionadas con el área de TICs.

e. Monitorear y disponer las acciones necesarias para la aplicación de criterios de seguridad informática asociados al esquema gubernamental de seguridad de la información tecnológica institucional, así como el ciclo de vida de las aplicaciones y sistemas informáticos de la entidad tanto internos como externos.

i. Disponer los estándares, políticas y procedimientos para fortalecer la gestión de regulación en el nivel central y desconcentrado operativo de la gestión de tecnologías de la información y comunicaciones.

"***Entregables:*** *(…) Gestión Interna de Seguridad Informática y Calidad de Software"*

1.- Políticas y estándares actualizados para administración de seguridad informática y prevención contra software malicioso, redes y conectividad, equipamiento de usuario final, identidad y acceso lógico a las aplicaciones y servicios de TI, el acceso físico a las áreas TIC.

2.- Procedimientos operativos y estándares definidos para la entrega de servicios de TI relacionados con seguridad y calidad.

7.- Especificaciones técnicas para adquisición de equipamiento tecnológico de seguridad y servicios relacionados con la seguridad de la información.

(…)"

Adicionalmente, las atribuciones y responsabilidades de la Gestión Interna de Seguridad de la Información y Calidades de Software (GISIC) son las siguientes:

"1. Políticas y estándares actualizados para administración de seguridad informática y prevención contra software malicioso, redes y conectividad, equipamiento de usuario final, identidad y acceso lógico a las aplicaciones y servicios de TI, el acceso físico a las áreas TIC.
2. Procedimientos operativos y estándares definidos para la entrega de servicios de TI relacionados con seguridad y calidad.
3. Informe de evaluación de implementación de estándares, políticas, metodologías, procesos y procedimientos establecidos por todas las gestiones internas de la DNTIC.
4. Reportes de administración y configuración de los equipos de seguridad informática de Planta Central
5. Insumos para el Plan de Contingencia de servicios de TI y de respuestas ante incidentes críticos.
6. Informes de evaluación de seguridad de los sistemas informáticos del MSP a nivel nacional
7. Especificaciones técnicas para adquisición de equipamiento tecnológico de seguridad y servicios relacionados con la seguridad de la información.
8. Informe de cumplimiento del proceso de Gestión de Riesgos de TI
9. Informes periódicos de pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir las vulnerabilidades.
10. Políticas y estándares de calidad para productos y servicios de TI basados en buenas prácticas y marcos de referencia vigentes.
11. Políticas, procesos y procedimientos de gestión del cambio en infraestructura tecnológica, aplicaciones informáticas y servicios de TI.
12. Metodología de aseguramiento de la calidad para la DNTIC.
13. Metodología para gestión de la configuración y base de configuraciones gestionada.
14. Informes de pruebas funcionales y no funcionales.
15. Pasos a producción revisados e informes de pasos a producción."

El Acuerdo de la Contraloría General del Estado Nro. 004-CG-2023, publicado en el Registro Oficial No. 257 de 27 de febrero de 2023, denominado: "Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos" en el grupo 410 "Tecnología de la Información" indica:

410-09 Adquisiciones de infraestructura tecnológica señala que: *"**La unidad de tecnologías de la información y comunicaciones definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización (…)**"* numeral 1 "*Las adquisiciones tecnológicas deben basarse en los estándares vigentes para el sector público, y estarán alineadas a los objetivos de la organización, a los principios de calidad de servicio, y constarán en el plan estratégico de tecnologías de la información y comunicación y en el plan anual de contrataciones aprobado de la institución. Las excepciones serán autorizadas por la máxima autoridad previa justificación técnica documentada (…)".* Numeral 4 "*Los contratos con proveedores de servicios incluirán las especificaciones formales sobre acuerdos de nivel de servicio y puntualizarán explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información. Deberán incluir cláusulas de garantías y multas, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante. La dirección de la organización debe monitorear el servicio contratado para asegurar el cumplimiento de las obligaciones comprometidas.". (…)*

410-13 Administración de soporte de tecnología de información señala que: "***La unidad de tecnologías de la información y comunicaciones definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, así como la oportunidad de los servicios tecnológicos que se ofrecen. (…)***". Numeral 5 "*Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos."*

410-13 Monitoreo y evaluación de los procesos y servicios señala que: "***Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad. (…)***", indica que:

"*La unidad de tecnologías de la información y comunicaciones definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.*

La unidad de tecnologías de la información y comunicaciones definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnologías de la información y comunicaciones presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.".

Mediante Acuerdo Ministerial Nro. 025-2019 de 10 de enero de 2020 el MINTEL emitió el EGSI versión 2.0, de cumplimiento obligatorio de las entidades públicas; mismo que establece los siguientes controles:

> *"5.1.1.1 Gestionar los accesos de los usuarios a los sistemas de información asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.*

5.1.2.3 Implementar los controles necesarios para el ingreso a la red y los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red.

5.1.2.6 Monitorear continuamente el uso de los servicios de la red, con alertas sobre aquellos recursos que se considere críticos.

5.4.1.6 Implementar controles de acceso tanto físico o lógico para aislar las aplicaciones sensibles, los datos de aplicación o los sistemas (DMZ).

5.4.2.6 Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema, generando la alerta respectiva.

8.4.1.5 Registro de intentos de acceso a los sistemas exitosos y fallidos.

8.4.1.6 Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos.

8.4.1.7 Registrar cambios en la configuración de sistema.

8.6.1.9.3 Aumentar el monitoreo para detectar o prevenir los ataques reales.

8.7.1.8 Monitorear y registrar todo acceso para crear un rastreo para referencia. El uso de rastreo de referencia de tiempo se debe considerar datos o sistemas críticos.

9.1.1.4 Registro y monitoreo de eventos que permita registrar y detectar acciones que podrían afectar, o ser relevantes para la seguridad de la información.

9.1.2.2 Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc.

12.1.1.1.2 Establecer procedimientos para monitorear, detectar, analizar y comunicar eventos e incidente de seguridad de la información"

El Ministerio de Salud Pública actualmente cuenta con un centro de datos ubicado en la Av. Juan de Dios Morales y Manuel Almeida, sector La Armenia - Centro de Datos CNT E.P; contratado en calidad de "SERVICIO HOUSING EN UN CENTRO DE DATOS CATEGORÍA TIER III PARA LA INFRAESTRUCTURA TECNOLÓGICA DEL MSP PLANTA CENTRAL", mediante contrato 00003-2023 con fecha 31 enero del 2023.

Ley Orgánica de Protección de Datos Personales, con fecha 21 de mayo de 2021 describe en su Artículo 30.- Datos relativos a la salud.- *"(…) Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas.(…)"*

Mediante memorando Nro. MINTEL-MINTEL-2021-0312-O, con fecha 23 de julio del 2021, que indica lo siguiente: "*El constante crecimiento de ciberataques, demanda de una mayor concienciación sobre la necesidad de proteger los activos de información y así minimizar o evitar el daño económico e imagen institucional de la Administración Pública. La información que custodian las instituciones*

públicas constituye uno de los activos más valiosos y exige ser protegida, así como clasificada y valorada según su criticidad".

"Bajo el contexto del ataque cibernético, de público conocimiento, en contra de la Corporación Nacional de Telecomunicaciones CNT EP., y a efectos de evitar eventuales afectaciones o posibles ataques similares en otras entidades gubernamentales, de lo cual no hay evidencia hasta el momento, se recomienda tomar al menos las siguientes medidas como necesarias:

1. Medidas Preventivas

- *Revisión de la seguridad perimetral como: políticas de firewall, antispam, IPS, SandBox, IDS, filtrado de contenidos, WAF, etc. (…)"*

- *Monitoreo continuo de las amenazas concurrentes que presenta la infraestructura tecnológica del ministerio de salud pública.*

La rápida evolución y alta demanda de tecnología para gestionar los procesos de negocio en las organizaciones han traído como consecuencia que las instituciones, independientemente de su tamaño, refuercen sus medidas de seguridad para protegerse de intrusiones indeseables, internas o externas, causantes en muchos casos, de perdida, hurto, daño o fuga de información, y por consiguiente grandes pérdidas económicas y de imagen para la institución.

La evolución natural de los antivirus tradicionales, son los sistemas de ciberseguridad Endpoint Detection and Response (EDR). Estos sistemas avanzados no dependen de una base de datos como las soluciones de antivirus tradicionales, sino que usan motores de Inteligencia Artificial que estudian tanto el comportamiento del equipo como la forma de trabajar diaria del usuario. Esto, unido con el Big Dada y Machine Learning, hacen que el sistema vaya mejorando de forma autónoma a la hora de detectar amenazas complejas sin falsos positivos.

Contar con la suscripción de una herramienta licenciada Endpoint Detection and Response (EDR), permitirá unificar los eventos y las respuestas a los incidentes informáticos de la organización, que de forma proactiva y centralizada será la encargada de brindar protección a los equipos de usuario final y servidores de manera automática y permitirá detectar, advertir y eliminar posibles virus o ataques cibernéticos que intenten acceder o dañar a los equipos y causar daño en la información. La licencia de EDR además será actualizada en los equipos de usuario final y servidores de manera automática, debe realizar escaneos de los equipos periódicamente y ayudar a la detección y eliminación de archivos y comportamientos maliciosos que puedan poner en riesgo los datos que contiene el equipo.

El riesgo fundamental de mantener la infraestructura tecnológica del Ministerio de Salud Pública Planta Central sin EDR puede resultar invaluable, ya que además de los posibles daños ocasionados a la información almacenada y a los equipos y dispositivos de red, debemos tener en cuenta otros importantes perjuicios como:

- Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos.
- Robo de información confidencial y su posible revelación a terceros no autorizados.
- Filtración de datos personales de usuarios registrados en el sistema.
- Consecuencia del incumplimiento de la legislación en materia de protección de datos personales vigente.
- Posible impacto en la reputación de la institución ante terceros.

- Retrasos en los procesos de producción, impacto en la calidad del servicio, pérdidas de oportunidades de negocio.

Mediante los tickets Nro. 2023033181000901 y Nro. 2023033181000938 con fecha 31 de marzo del 2023 generados a través del sistema de gestión de tickets (OTRS), se solicitó se escale la consulta al administrador del sistema QUIPUX solicitando el número de usuarios activos en el sistema a nivel de Planta Central y a la Gestión Interna de Infraestructura solicitando el número de servidores físicos y virtuales en los cuales se requerirá la instalación de las licencias EDR.

Tomando en cuenta las respuestas emitidas en contestación a la consulta realizada se tiene que: el número usuarios activos en el sistema QUIPUX es igual a: 838; número de servidores es igual a: 250; que actualmente tiene el MSP en Planta Central.

Cantidad de usuarios computadoras	Cantidad de Servidores	Total
838	250	1088

Tabla de usuario activos en el sistema de gestión documental y Servidores

Realizando una proyección de crecimiento para un año, considerando como referencia el memorando Nro. MSP-DNTH-2022-2219-M, mediante el cual se indica que se debe considerar un crecimiento del 1% del personal del MSP Planta Central, tenemos la proyección de computadoras para 12 meses:

Mes	Incremento 1% mensual usuarios computadoras
marzo 2023	838
abril 2023	846
mayo 2023	854
junio 2023	862
julio 2023	870
agosto 2023	878
septiembre 2023	886
octubre 2023	894
noviembre 2023	902
diciembre 2023	911
enero 2024	920
febrero 2024	929

Tabla de posible crecimiento de usuarios

El informe Nro. MSP-DNTIC-GISIC-INF-038-2022, la Gestión Interna de Seguridad de la Información y Comunicaciones, concluye "(…) Existe una brecha del 17% que no ha podido ser utilizado en función de la obsolescencia tecnología que presentan los equipos del Ministerio de Salud - Planta Central, que se reserva para contingencia. (…)".

Cantidad de usuarios computadoras proyectado	Cantidad de Servidores	Total Licencias	Brecha tecnológica 17% (disminuye)	Total Licencias Requeridas
929	250	1179	200	979

Tabla de Licencias proyectadas

El total de licencias proyectadas a 12 meses requeridas para usuarios que utilizan computadoras es (929) especificado en la "Tabla de posible crecimiento de usuarios", más la cantidad de servidores (250) especificado en la "Tabla de usuario activos en el sistema de gestión documental y

Servidores", da un total de (1179) licencias, pero se puede inferir que existe un total de (200) licencias que representan el 17% de brecha por obsolescencia que no serían utilizadas, por lo cual se concluye que el total de licencias que se requieren para cubrir la necesidad serían de 979.

2. GLOSARIO DE TÉRMINOS CLAVE

Término/Sigla	Definición
Exploit	Un exploit es un programa o código malicioso que aprovecha una vulnerabilidad en un software o sistema para obtener acceso no autorizado o ejecutar comandos no deseados. Los EDRs pueden detectar y responder a intentos de explotación.
Out of the box	Este término se refiere a un producto o solución que está listo para usar sin necesidad de realizar configuraciones adicionales. En el contexto de las licencias de EDR, podría referirse a una licencia que incluye todas las funciones y características necesarias desde el momento de su instalación.
Webshells	Las webshells son scripts o programas maliciosos que se instalan en un servidor web comprometido para permitir el acceso remoto y controlar el servidor de manera no autorizada. Los EDRs pueden detectar y bloquear el uso de webshells en un sistema.
Return Oriented Programming (ROP)	ROP es una técnica utilizada en ataques informáticos para ejecutar código malicioso utilizando fragmentos de código existentes en una aplicación. Los EDRs pueden detectar y bloquear intentos de ROP en un sistema.
Stack Pivoting	Stack pivoting es una técnica utilizada en ataques de desbordamiento de pila para redirigir la ejecución del programa hacia una porción de memoria controlada por un atacante. Los EDRs pueden detectar y bloquear intentos de stack pivoting.
VB Script God Mode	El término "VB Script God Mode" no es muy común en el contexto de EDR o ciberseguridad. Sin embargo, el "modo Dios" o "God Mode" a menudo se refiere a una característica oculta o una configuración avanzada que brinda un acceso más completo y amplio a un sistema. En este caso, podría referirse a la capacidad de un EDR para acceder y controlar de manera más profunda y extensa los sistemas de VB Script.
Malware	El malware es un software malicioso diseñado para dañar, infectar o comprometer un sistema informático. Los EDRs son herramientas utilizadas para detectar y responder a la presencia de malware en los endpoints o dispositivos finales.
Ransomware	El ransomware es un tipo de malware que cifra los archivos o bloquea el acceso a un sistema y luego exige un rescate a cambio de restaurar el acceso. Los EDRs pueden ayudar a detectar y responder a los ataques de ransomware y mitigar sus efectos.
Endpoint	En el contexto de la ciberseguridad, un endpoint se refiere a un dispositivo final (como una computadora, portátil, teléfono móvil, tableta) que se conecta a una red y es potencialmente vulnerable a ataques. Los EDRs están diseñados específicamente para proteger y monitorear estos endpoints.
Footprint	El término "footprint" (rastro o huella) en ciberseguridad se refiere a la presencia o actividad digital dejada por un sistema o usuario. En el contexto de los EDRs, podría referirse a la capacidad de rastrear y monitorear las actividades de un endpoint para detectar
DTIC	Dirección de Tecnologías de la Información y Comunicaciones

Tabla de términos clave

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Adquirir 979 licencias de protección y respuesta de amenazas informáticas para equipos de usuario final y servidores del tipo - Endpoint Detection and Response (EDR) para el MSP-Planta Central, con la finalidad de brindar protección de seguridad informática contra malware (software malicioso).

3.2 OBJETIVOS ESPECÍFICOS

- Realizar monitoreo continuo de: eventos de seguridad, archivos, procesos, registros, memoria y red en equipamiento de usuario final y servidores del Ministerio de Salud Pública-Planta Central a través de una herramienta de nueva generación de tipo - Endpoint Detection and Response (EDR).

- Visualizar de manera continua: eventos de seguridad, archivos, procesos, registros, memoria y red en equipamiento de usuario final y servidores del Ministerio de Salud Pública-Planta Central a través de una herramienta de nueva generación de tipo - Endpoint Detection and Response (EDR).

- Detectar, identificar, analizar, contener, investigar, eliminar y prevenir amenazas informáticas avanzadas (conocidas y no conocidas como virus, troyanos, gusanos, keyloggers, rasomware, malware, archivos infecciosos, ataques de ciberseguridad) en tiempo real, de manera activa y pasiva en equipamiento de usuario final y servidores del Ministerio de Salud Pública-Planta Central a través de una herramienta de nueva generación de tipo - Endpoint Detection and Response (EDR).

- Dar cumplimiento al Acuerdo Ministerial Nro. 025-2019 *"Esquema Gubernamental de Seguridad de la Información -EGSI-", que refiera la obligatoriedad de las instituciones para establecer mecanismos que protejan y salvaguarden contra pérdidas de información".*

4. ENTREGABLES DEL SERVICIO

A continuación, se detallan los entregables del servicio:

Ítem	Entregable	Descripción
1	Certificado de Activación del total de licencias	Certificado emitido por el fabricante o distribuidor autorizado, del total de licencias activas 979 a nombre del Ministerio de Salud Pública
2	Manual de Usuario de administración de Consola de la solución EDR	Debe contener al menos los siguientes temas: • Administración de la consola. • Instalación de la solución a nivel de consola y estaciones, a nivel del equipo y de forma remota. • Configuración de políticas de seguridad, firewall de forma personalizada. • Configuración de actualizaciones. • Generación de reportes.
3	Transferencia de Conocimiento (Certificado de Asistencia)	La transferencia de conocimientos se realizará acorde al objeto del contrato, conforme a los siguientes temas: • El manejo de la herramienta EDR • Configuraciones.

		• Interpretación de reportes. • Criterios sobre amenazas. • Estrategias de mitigación. El contratista entregará un certificado de asistencia.
4	Certificado de Soporte y Garantía Técnica	Certificado y/o Carta de Compromiso entregado por el Contratista sobre la Garantía Técnica y Soporte por el periodo de vigencia de las licencias (365 días calendario contados a partir de la activación de las licencias a nivel de la consola).

Tabla de entregables esperados

5. Especificaciones Técnicas

El Ministerio de Salud Pública requiere adquirir las **LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL**, a instalarse en un total de 979 equipos, de acuerdo a las características que se indican a continuación:

CARACTERÍSTICAS TÉCNICAS	
CARACTERÍSTICA	**DESCRIPCIÓN**
Prevención contra exploits.	Detección y prevención del mecanismo de identificación de propiedades de un sistema por parte de un exploit kit (técnicas conocidas como exploit kit fingerprinting) o amenazas avanzadas sin necesidad de utilizar firmas, patrones o heurísticas. Detección de técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits para los sistemas operativos Windows y Linux. Mitigación de vulnerabilidades o amenazas avanzadas conocidas, desconocidas y día cero. Protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box". Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación o proceso, incluyendo aquellas desarrolladas internamente. Configurar perfiles de protección en modo de prevención o monitoreo. Prevención de técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux. Protección contra webshells de PHP para servidores Linux. Deberá contar con políticas de prevención de técnicas de explotación, así como de compatibilidad de manera predeterminada, con la finalidad de mejorar la experiencia del usuario final y reducir la creación de falsos positivos. Deberá contar con protección contra la explotación de vulnerabilidades o amenazas sin necesidad de tener una conexión a la consola.

	Deberá contar con protección contra ataques basados en exploits que comprometen aplicaciones legítimas asegurando que esas vulnerabilidades no puedan ser utilizadas. Deberá contar con protección contra vulnerabilidades de manipulaciones de memoria en tiempo de ejecución. Deberá proteger aplicaciones ampliamente usadas como Microsoft Office, Adobe PDF Reader, navegadores y Adobe Flash y proteger contra exploits existentes y nuevos al menos para Return Oriented Programming (ROP), Stack Pivoting, VB Script God Mode y Import/Export Address Table Parsing. La consola proporcionará información detallada bajo demanda de eventos identificados como exploits.
Identificación de ataques post-explotación.	Identificación y prevención de intentos de escalar privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux. Detectar y determinar los comportamientos considerados como maliciosos mediante el análisis continuo de la cadena de eventos que sucedan en un endpoint. Esta detección debe considerar varios eventos y no sólo un evento para poder proporcionar un veredicto de la actividad maliciosa. La detección debe utilizar varias reglas pre-configuradas, las cuales, deben de tener la capacidad de analizar varios eventos y no sólo un evento. En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos.
Prevención contra malware conocido.	Generación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas. Capacidad escanear la computadora comparando los hashes de los archivos ejecutables que estén almacenados en la computadora y consultar su veredicto en una nube de inteligencia de amenazas. Capacidad de enviar los archivos clasificados como maliciosos a cuarentena, ya sea que, hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo. Deberá contar con un módulo de prevención de ransomware, el cual debe evitar un proceso de encriptación identificando intentos de modificación de archivos. La solución deberá contar con motores de Inteligencia Artificial (IA) y Aprendizaje de Máquina (ML) que realizan análisis estáticos y dinámicos de archivos y ejecutables, análisis de comportamiento, clasificación de malware para prevenir los ataques de tipo ransomware o criptominers. La solución EDR deberá supervisar constantemente el comportamiento específico del ransomware e identificar el cifrado de archivos de manera ilegítima. La solución EDR deberá realizar prevención y restauración de ataques de Ransomware deberá funcionar en todos los entornos en tiempo real y sin depender de la conexión a Internet. La solución EDR deberá detectar y poner en cuarentena todos los elementos de

	un ataque de ransomware. En caso de ataque de ramsomware o cualquier amenaza que se llegue a materializar en los equipos modificando las configuraciones, eliminación o encriptación de cualquier archivo del equipo; la solución EDR deberá permitir la recuperación y/o restauración rápida automática o manual para deshacer todos los cambios realizados por el ramsomware o amenaza con el objetivo de reanudar su operación de forma inmediata, minimizando el tiempo de inactividad y reduciendo el impacto del ataque, garantizando que todos los datos afectados no se pierdan ni comprometan, manteniendo la integridad y confidencialidad de la información sensible. Está funcionalidad deberá estar en la solución EDR sin la necesidad de agentes o productos adicionales para garantizar la integridad de la defensa ante el ataque.
Prevención de malware desconocido.	Capacidad de identificar si la macro contenida en un documento de Word, Excel maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa. Capacidad de proporcionar protección contra malware desconocido sin necesidad de tener una conexión a la consola ni a Internet. Capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas. Deberá permitir poner los archivos detectados como maliciosos en una cuarentena, ya sea de manera automática o bajo demanda. Deberá utilizar un modelo matemático generado a partir de aprendizaje de máquina para comparar una gran cantidad de características de un archivo ejecutable, de manera estática para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows, Linux y Mac Bloquee el malware proveniente de la navegación web. Cada archivo descargado por un usuario a través de un navegador web debe ser inspeccionado para determinar si hay malware. La solución EDR deberá prevenir amenazas ocultas en comunicaciones cifradas SSL y TLS. Todos los registros escritos en el sistema de archivos serán monitoreados y analizados estáticamente. Si se encuentran como potencialmente maliciosos se pondrán en cuarentena. La solución EDR deberá mostrar el proceso afectado, las claves de registro afectadas y los archivos afectados en el entorno del sistema operativo. La solución EDR deberá incluir inteligencia artificial y machine learning con el fin de detectar/prevenir malware de día cero.
Escaneo de archivos ejecutables.	Permitirá realizar el escaneo de archivos ejecutables sin la necesidad de firmas. Permitirá realizar el escaneo de archivos de manera manual. El consumo de recursos al momento de realizar el escaneo no debe de impactar

	en las funciones cotidianas del usuario. Permitirá habilitar el escaneo de dispositivos de almacenamiento removible. Deberá poder analizar los archivos desconocidos de forma estática para determinar si son maliciosos, así como enviar estos archivos desconocidos al servicio de protección en la nube para que sean analizados. La solución EDR deberá supervisar constantemente los archivos y la actividad de la red en busca de comportamientos sospechosos.
Protección contra el robo de contraseñas.	Deberá proporcionar una protección en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz o similares.
Restricciones de ejecución.	Restricciones de ejecución de archivos a partir de cierta carpeta. Restricciones de ejecución de archivos a partir de recursos compartidos. Contará con políticas de restricción de creación de procesos hijo configuradas de manera predeterminada. Capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles. Configurar perfiles en modo de prevención o monitoreo.
Restricción de uso de puertos USB.	Deberá permitir generar perfiles que gestionen las siguientes características de bloqueo de puertos USB cuando se conecten los siguientes tipos de dispositivos: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB, adaptadores de red en formato USB. Deberá permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo (discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB), tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una predeterminada) y número de serie. Los parámetros tipo de dispositivo, tipo de permiso y fabricante deben de ser mandatorios. Deberá permitir la creación de políticas que utilicen los perfiles de bloqueo y de excepciones generados y sin ser excluyentes. Las políticas generadas deberán poder asignarse a una computadora en particular o a un grupo de computadoras definido previamente. Deberá permitir la creación de excepciones temporales a partir de una violación registrada. Deberá mostrar las violaciones a las políticas que se hayan registrado mostrando lo siguiente: horario, computadora, usuario, dirección IP, tipo de dispositivo, producto, fabricante y número de serie del dispositivo que intentó conectarse. Se prefiere esta funcionalidad, deberá de estar soportada para sistemas

	operativos Windows, Mac Linux (opcional) La solución EDR permitirá notificaciones de mensajes de usuario personalizados al conectar un dispositivo según el escenario. La solución EDR deberá controlar la entrada y salida en todos los puertos de conexión, específicamente: • Medios de almacenamiento USB, unidades DVD/CD-ROM; Modems, Impresoras, Controladores USB. • Dispositivos de captura de imágenes (Ej: Cámaras digitales, Web Cams, scanners, etc.), Dispositivos Infrarrojos, Smart Card Readers, Memorias PCMCIA. • Adaptadores de red tanto cableados como inalámbricos, adaptador Bluetooth, Bluetooth USB, entre otros. Deberá ser compatible con listas blancas y listas negras para control de medios extraíbles y/o dispositivos de E/S en cualquier puerto (USB, Bluetooth). Deberá poder controlar medios extraíbles por su número de serie, lo que permite la creación de políticas para dispositivos únicos, específicos.
Firewall de host.	Esta funcionalidad deberá de estar disponible para los sistemas operativos Windows, Mac y Linux. **Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Windows/Linux:** - Controlar todas las comunicaciones entrantes y salientes utilizando direcciones IP. - Permitir que las reglas sean aplicadas de acuerdo con la ubicación del dispositivo, por ejemplo, que sólo apliquen si están en la red interna. - La solución EDR debe de poder determinar, mediante la configuración, si el dispositivo se encuentra dentro o fuera de la organización. - La regla podrá especificar direcciones locales o remotas, así como puertos locales o remotos. También se podrá especificar el protocolo dentro de estas cuatro opciones: ICMP, TCP, UDP, ICMPv6. **Las siguientes funcionalidades deberán de estar disponibles para sistemas operativos Mac:** - Permitir o bloquear las comunicaciones de red entrantes. - La solución para reducir la superficie de ataque debe permitir reglas de Firewall para bloquear el tráfico de red a los equipos terminales en función de la información de conexión, como direcciones IP, puertos y protocolos. - La solución se utilizará para determinar si los usuarios pueden conectarse a redes inalámbricas mientras se encuentran en la LAN de su organización para proteger la red de las amenazas asociadas con las redes inalámbricas. - La solución definirá si los usuarios pueden conectarse a la red de la organización desde puntos de acceso en lugares públicos, como hoteles o aeropuertos. - La solución se utilizará para restringir o permitir el tráfico de red IPV6.
Captura de datos en el endpoint.	**La solución EDR deberá poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Windows:**

	- Proceso ejecutado, incluyendo el tiempo de inicio, el hash del archivo asociado. - Actividades de creación, escritura, renombre, eliminación, modificación y creación de enlaces simbólicos de un archivo. - Las siguientes acciones de red: accept, connect, create, listen, close, bind, con los siguientes parámetros: IP y puerto destino, IP y puerto fuente, conexiones fallidas, protocolo (TCP/UDP), resolver los nombres de computadoras dentro de la red local. - Protocolos de red: peticiones DNS y respuestas UDP, HTTP connect, HTTP disconnect, HTTP proxy parsing. - Estadísticas de red. - Registro, configuración o eliminación de valores del registro - Creación, modificación, eliminación, adición, restauración y guardar llaves del registro. - Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión y si la sesión es local o remota. - Estado de la computadora: inicio, suspendida, reinicio. Con los siguientes atributos: nombre de la computadora, versión del sistema operativo, dominio, estado anterior y actual. - Logs de eventos de Windows. **La solución EDR deberá poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Mac:** - Creación, escritura, eliminación, renombre, cambio de ruta y apertura de archivos. Con los siguientes atributos: ruta completa del archivo modificado antes y después de su modificación. - Generación de hashes con los algoritmos SHA256 y MD5 para el archivo después de su modificación. - Inicio y detención de procesos con los siguientes parámetros: ID de proceso para el proceso padre, id del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo. - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics, con los siguientes parámetros: IP y puerto destino, conexiones fallidas, protocolo (TCP/UDP), estadísticas agregadas de envío/recepción para la conexión. **La solución EDR deberá poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Linux:** - Para los archivos, las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Copiar o renombrar los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos. - Las siguientes acciones de red: listen, accept, connect, connect failure y disconnect; con los siguientes atributos: dirección IP y puertos fuente para binds explícitos, dirección IP y puerto destino, conexiones TCP fallidas, protocolo UDP/TCP. - Procesos. Creación de procesos, con los siguientes atributos: ID del

	proceso hijo, id del proceso padre, ruta completa del a imagen del proceso, línea de comando del proceso, valores hash calculados con los algoritmos SHA256 y MD5, terminación de procesos, incluyendo el ID del proceso.
Inventario de aplicaciones y vulnerabilidades.	La solución EDR podrá generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, Mac, Linux(opcional) Permitirá obtener de forma automática los siguientes detalles de las computadoras: usuarios, grupos de usuarios, servicios instalados, drivers, autoruns, unidades de almacenamiento compartidas configuradas y drivers instalados. Deberá ofrecer visibilidad en tiempo real de las vulnerabilidades o amenazas existentes, que afectan tanto al sistema operativo como a las aplicaciones instaladas. Deberá ofrecer detalles de los CVEs, incluyendo el nivel de severidad y métricas según la base de datos de vulnerabilidades de NIST.
Recolección de datos forenses.	Deberá tener la capacidad de recopilar evidencia histórica como ejecución de programas, acceso a archivos, actividad de navegación, registros de eventos, sesiones de red y otros artefactos forenses de una computadora comprometida. La información forense deberá estar integrada dentro de la consola administrativa de la solución EDR**.** La solución EDR deberá incluir una funcionalidad para realizar análisis forense que pueda monitorear y registrar automáticamente los eventos de endpoint incluidos los archivos afectados, los procesos iniciados, los cambios en el registro del sistema y la actividad de la red y crear un reporte forense detallado. El proceso de análisis forense deberá iniciar automáticamente cuando se produce un evento de malware. El reporte forense deberá identificar el punto de entrada de la actividad maliciosa y destacará el daño potencial, las actividades maliciosas, las acciones de remediación y toda la cadena de ataque. La solución EDR deberá mostrar gráficamente (árboles de proceso u otro tipo de interfaz de mapeo) el ataque en el sistema para ayudar en las investigaciones. El reporte forense registrará, presentará y desenmascarará los scripts de PowerShell utilizados durante un ataque. El reporte forense enumerará el análisis de reputación de los archivos y URL utilizados durante un ataque. La solución EDR deberá proporcionar acceso a todos los datos forenses desde la consola de administración. Los resultados del análisis forense deberán enviarse continuamente a la consola central y si un endpoint no puede enviar de inmediato los hallazgos, los resultados deben almacenarse localmente hasta que se puedan cargar en el sistema de administración central de la solución.
Análisis de alertas e investigación de actividad sospechosa.	Deberá contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.

	Deberá correlacionar alertas, sin importar si estas vengan de datos de endpoint, red o nube y agruparlas dentro de incidentes. Deberá mostrar el número total de alertas e incidentes, y debe incluir la capacidad de filtrar la información de forma flexible. La solución EDR deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque. La solución EDR deberá mostrar información específica de cada proceso involucrado en la secuencia gráfica. En la pantalla emergente, en caso de estar disponible, deberá de mostrarse los datos relacionado con el perfil de comportamiento y la ejecución del archivo. La solución EDR deberá mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso, valor SHA256 y línea de comandos de la ejecución. La solución EDR deberá proporcionar la capacidad de decodificar cadenas de caracteres codificadas en base-64 para mostrarlo en texto plano. La solución EDR deberá mostrar si existió una inyección de código o si el protocolo RPC es utilizado en otro proceso desde una computadora local o remota. La solución EDR deberá proporcionar la interacción que existe con las direcciones IP que se quieran investigar. Deberá de poder mostrar diferentes opciones de vistas los archivos ejecutables que generaron esa comunicación. La solución EDR deberá proporcionar de manera gráfica la interacción que existe entre uno o varios procesos que sean investigados. La gráfica deberá demostrar la interacción entre los procesos y si existe una relación entre las computadoras que ejecutan dichos procesos, entre otros aspectos.
Configuración y elementos de identificación.	La solución EDR deberá contar con mecanismos de generación de alertas considerando el comportamiento mostrado por los procesos de las computadoras. Las alertas generadas por el comportamiento de los procesos no deberán de utilizar firmas o heurísticas. Cada alerta generada por el comportamiento de los procesos deberá tener una descripción y contar con una clasificación de acuerdo a su severidad. La solución EDR deberá permitir la generación de excepciones a los comportamientos de los procesos que hayan sido identificados como maliciosos o sospechosos. La solución EDR deberá permitir deshabilitar, modificar, exportar o eliminar los comportamientos que generen las alertas por el comportamiento de los procesos. La solución EDR deberá soportar el uso de indicadores de compromiso tradicionales, incluyendo rutas de archivos, nombres de archivos, dominios, direcciones IP y hashes.

	La solución EDR deberá soportar (IoC) Indicadores de Compromiso donde el usuario puede iniciar un bloqueo sobre IP, URL, HASH (MD5, SHA). La solución EDR deberá permitir la gestión de los indicadores de compromiso por comportamiento de procesos e indicadores de compromiso tradicionales mediante la consola de administración.
Acciones de respuesta.	Permitirá aislar una computadora desde la propia consola de administración para que sólo exista comunicación entre el agente y la consola, ofrecer la capacidad para poder agregar comentarios los cuales explican la razón por la cual fue aislada una computadora. La solución EDR deberá mostrar los detalles de los archivos que han sido puestos en cuarentena, permitir filtrar los archivos que han sido puestos en cuarentena por nombre de la computadora, dominio, ruta del archivo, fuente de la cuarentena y fecha de la cuarentena. La solución EDR deberá de permitir la restauración de uno o más archivos que hayan sido puestos en cuarentena de manera simultánea. La solución EDR deberá permitir una conexión inversa al dispositivo afectado, en versiones superiores a Windows 7 SP1, a través de una conexión remota para permitir las siguientes acciones: • Terminar el proceso de ejecución. • Suspender o reanudar el proceso de ejecución. • Agregar un proceso a un indicador de compromiso (IOC). • Copiar binario en ejecución para futuras investigaciones. La solución EDR deberá permitir una conexión inversa al dispositivo afectado a través de una conexión remota para permitir ejecutar secuencias de comandos o comandos en Powershell. La solución EDR deberá permitir explorar las unidades de almacenamiento de manera remota, incluyendo no sólo discos duros sino también dispositivos de almacenamiento removibles. Deberá permitir mover, renombrar, eliminar, descargar y calcular el hash de cualquier archivo como mínimo. La solución EDR deberá de permitir la creación de listas blancas o negras. La solución EDR deberá permitir aislar un sistema y garantizar que los controles preventivos se mantengan aun al reiniciar el equipo. El aislamiento deberá permitir que el Endpoint aislado pueda conectarse a los sistemas de investigación/reparación. La solución EDR deberá tener capacidad de remediación integrada en las capacidades de Threat Hunting (como la cuarentena de archivos y el proceso de eliminación). Una vez que cualquiera de los motores de seguridad de la solución EDR detecta actividad maliciosa, las actividades de protección y remediación deberá poder activarse automáticamente (por ejemplo, poner en cuarentena el archivo ofensivo, terminar los procesos y revertir la actividad de ataque). La solución EDR deberá poder aplicar inmediatamente controles preventivos (bloquear actividad específica o maliciosa conocida).

	La solución EDR deberá tener una capacidad de respuesta en vivo que permita la capacidad de interactuar de forma remota con el sistema. La solución EDR deberá permitir a los analistas la capacidad de pivotar rápidamente entre las diferentes actividades observadas en un punto final y proporcionar información contextual si está disponible. La solución EDR deberá tener la capacidad de buscar en todos los puntos finales para IOC u otros atributos del sistema que no se capturan en los datos de telemetría en tiempo real.
Administración y revisión de eventos.	Administración de políticas centralizado, vía una consola basada en la nube. La consola podrá clasificar los eventos en tres niveles de acuerdo a su severidad: bajo, medio y alto. Clasificar el estado de los incidentes en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional. Capacidad para clasificar el estado de las alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional. Capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto del mismo. Capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente. Permitirá la actualización y desinstalación del agente a partir de la consola. Permitirá utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente. Contará con integración con Active Directory para la gestión de computadoras y configuración de políticas. Contará con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory. Contará con la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica. La alimentación dinámica de los grupos virtuales podrá ser de forma estática y dinámica, siendo posible configurar para la forma dinámica el nombre de la computadora y dirección IP como mínimo. La consola deberá de ser proporcionada bajo un esquema *software as a service.* La solución EDR deberá tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes de endpoint. La solución EDR deberá incluir una Gestión Basada en nube en modalidad SaaS provista como servicio del fabricante. La solución EDR deberá contar con un dashboard interactivo donde se muestran los incidentes de seguridad que no han sido atendidos, un resumen sobre los

	incidentes de seguridad, la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente. La solución EDR deberá contar con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente. Deberá permitir gestionar las excepciones en una pantalla específica. Deberá permitir crear excepciones a reglas, mecanismos de detección y/o mecanismos de protección desde la consola. Estas excepciones deben de poder aplicarse a una computadora en específico, o a un grupo de computadoras. La solución EDR deberá permitir alertas en tiempo real o registro de eventos.
Características del agente.	Agente con un footprint mínimo que no impacte la experiencia de usuario. Poco almacenamiento en disco debido a que no utiliza firmas, patrones y/o heurísticas. Compatibilidad con todos los sistemas operativos servidores y/o estaciones de trabajo en sistemas operativos Windows, Linux y Mac. **La solución deberá soportar al menos los siguientes sistemas operativos Windows:** - Windows 7 SP1 - Windows 8.1 U1 - Windows 10 32/64bit (versiones 1607,1709,1803,8909,1903,1909,2004,2009,2103, 21H2) - Windows 11 - Windows 2008 R2 32/64bit - Windows 2012 R2 64bit - Windows 2016 64bit - Windows 2019 64bit - Windows 2022 64bit **La solución deberá soportar al menos los siguientes sistemas operativos Linux:** - Ubuntu 16.04//18.04//20.04 - Debian 9.12 - 10.10 - RHEL 7.8 - 8.4 - CentOS 7.8 - 8.4 - Oracle Linux 7.9 - 8.4 - Amazon Linux 2 **La solución deberá soportar al menos los siguientes sistemas operativos Mac:** - macOS Monterey (12) - macOS Big Sur (11) - macOS Catalina (10.15) La solución de Endpoint deberá soportar ambientes con Windows Virtual Desktop Infrastructure (VDI) al menos Vmware Horizon y Citrix XenDesktops. Capacidad para configurar la captura de metadata que será enviada a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y

	respuesta a incidentes. Retención de datos hasta por 14 días. Retención de información de datos de alertas e incidentes hasta por 365 días.
Servicio de Cacería de amenazas.	Buscar, programar y guardar consultas para identificar amenazas difíciles de encontrar. Deberá ofrecer capacidades de hunting flexibles que permitan descubrir amenazas utilizando un generador de consultas intuitivo, así como construir consultas avanzadas y visualizar resultados de forma ordenada. El servicio deberá automáticamente contextualizar amenazas utilizando inteligencia de amenazas. El servicio deberá producir reportes de amenazas detallados que revelen las herramientas y pasos de los ataques que permitan erradicar a los adversarios rápidamente.
Gestión de usuarios.	La consola permitirá la gestión de usuarios mediante roles. **Se prefiere que los roles preconfigurados tengan las siguientes características:** • Viewer: Cuenta con permisos para revisar toda la consola, pero no puede tomar acciones. • IT Admin: Cuenta con permisos para ver alertas, la gestión e instalación de agentes, las acciones realizadas en la consola, los perfiles, las políticas, el control de dispositivos y las excepciones globales. Puede instalar y gestionar agentes. • IT Admin con privilegios: Cuenta con los mismos permisos que une IT Admin pero adicionalmente puede realizar sesiones remotas y extracción de archivos de manera remota. • Administrador de seguridad: Puede ver las políticas, perfiles, acciones tomadas en la consola, incidentes, alertas, reglas, gestión de agentes, excepciones globales y el control de dispositivos. Puede realizar ciertas acciones de configuración. • Administrador de seguridad con privilegios: Cuenta con los mismos permisos que el administrador de seguridad, adicionalmente puede interactuar con APIs públicas, la auditoría y la integración de plataformas de inteligencia de amenazas. Puede realizar sesiones remotas y extracción de archivos de manera remota. La consola de gestión deberá permitir crear usuarios, grupos para una gestión de acceso a la consola basado en roles.
Reportes.	Permitirá la generación de reportes bajo demanda o programados. El formato de los reportes generados es PDF o HTML. La consola mantiene un historial de los reportes que han sido generados para su posterior consulta. La frecuencia para la generación de los reportes programados podrá ser diaria, semanal o mensual, de acuerdo a la necesidad institucional. El rango de tiempo para la generación de los reportes es expresado en días. Se pueden especificar varias direcciones de correo electrónico para que los reportes sean enviados.

<table>
<tr><td></td><td>Para los reportes bajo demanda se podrá especificar el rango de tiempo a considerar.

Los reportes pueden ser generados a partir de plantillas predeterminadas, o se puede generar un reporte personalizado utilizando los “widgets” disponibles.

La solución EDR deberá generar reportes periódicos sobre tipos de malware, tipos de vulnerabilidades explotadas, etc.

La solución EDR deberá tener la capacidad de generar reportes visuales.

La solución EDR deberá proporcionar un reporte relacionadas con el estado general del endpoint, cumplimiento, salud, el estado de implementación, seguridad.</td></tr>
<tr><td>Transferencia de conocimiento</td><td>El contratista deberá realizar la transferencia de conocimiento sin costo para el Ministerio de Salud Pública de mínimo 12 horas para al menos 8 analistas designados por la Dirección de Tecnologías de la Información y Comunicaciones. La transferencia de conocimiento se realizará dentro del plazo contractual y se puede llevar a cabo de manera presencial o virtual.

El contenido de la transferencia de conocimiento deberá enfocarse en el manejo de la herramienta EDR, configuraciones, interpretación de reportes y criterios sobre amenazas, estrategias de mitigación.

El Contratista entregará un certificado de asistencia a la capacitación.</td></tr>
<tr><td>Soporte Técnico</td><td>Los incidentes reportados durante la vigencia de las licencias deben ser solventados de acuerdo a la modalidad 8 horas x 5 días (laborales), durante el período de vigencia de las licencias EDR (365 días) y bajo el siguiente esquema de aplicación:

<table>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo de Respuesta para iniciar trabajos de diagnóstico y solución de incidentes</th><th>Forma de contacto</th></tr>
<tr><td rowspan="2">Alta</td><td rowspan="2">El contratista solventará requerimientos determinados por la DTIC como urgentes o de alto impacto</td><td>Inmediata</td><td>Remoto, Telefónico</td></tr>
<tr><td>1 - 6 horas</td><td>En sitio</td></tr>
<tr><td>Moderada</td><td>El contratista solventará requerimientos determinados por la DTIC como moderados o de impacto bajo</td><td>3 – 9 horas</td><td>Telefónico o Correo Electrónico o Remoto y en Sitio solo si la DTIC lo requiere.</td></tr>
<tr><td>Baja</td><td>El contratista solventará requerimientos determinados por la DTIC como programados o controlados</td><td>24 horas</td><td>De acuerdo a lo determinado por la DTIC puede ser en sitio, telefónico o Correo Electrónico</td></tr>
</table>

El Ministerio de Salud Pública a través de la Dirección de Tecnologías de la Información definirá la prioridad de los incidentes a reportar.

El Contratista proporcionará los respectivos niveles de escalamiento de soporte técnico con la respectiva información de contacto (número telefónico, celular, correo electrónico).

El Contratista entregará un reporte de la atención al incidente o soporte, bajo</td></tr>
</table>

	solicitud a la Dirección de Tecnologías de la Información y Comunicaciones, que contenga todas las actividades realizadas.
Instalación de la solución Endpoint Detection and Response (EDR)	El Contratista realizará el despliegue de las licencias con base al listado de equipos de usuario final y servidores que será entregado por el Administrador del Contrato. El Contratista realizará la desinstalación de la solución de seguridad que se encuentre previamente instalada en los equipos informáticos de usuario final y servidores, procederá a realizar la instalación de las licencias del EDR en los equipos informáticos de usuario final y servidores del Ministerio de Salud Pública de forma coordinada con el personal técnico del contratista, personal técnico de la DTIC y el Administrador del Contrato. El Contratista instalará la licencia para la administración centralizada (consola en la nube), acorde las mejores prácticas y recomendaciones del fabricante de la solución de EDR. La totalidad de licencias activas deberá ser visible en la consola de administración de la solución EDR.
Acuerdo de confidencialidad	El Contratista deberá Firmar un acuerdo de confidencialidad de manera que se garantice que la información y detalles propios de la institución guarden los criterios de reserva, confidencialidad y propiedad, como exclusiva del Ministerio de Salud Pública.

6. ALCANCE

El Endpoint Detection and Response (EDR) monitorizará, evaluará y analizará continuamente eventos de los usuarios, archivos, procesos, registros, memoria y red que presentan los equipos de usuario final y servidores del Ministerio de Salud Pública -Planta Central, el cual tiene como finalidad identificar, detectar, contener, investigar, analizar, eliminar y prevenir amenazas informáticas avanzadas (conocidas y no conocidas como virus, troyanos, gusanos, keyloggers, rasomware, malware, archivos infecciosos) en tiempo real de manera activa y pasiva en los diferentes equipos tecnológicos, pudiendo así obtener reportes en tiempo real del estado de los eventos, incidentes, datos sobre procesos, registros, cambios de configuración, conexiones de red, descargas o transferencias de archivos y datos, comportamientos de usuarios finales o dispositivos a fin de mitigar los riesgos derivados de los activos de información y dar cumplimiento al Acuerdo Ministerial Nro. 025-2019 "Esquema Gubernamental de Seguridad de la Información -EGSI-", que refiera la obligatoriedad de las instituciones para establecer mecanismos que protejan y salvaguarden contra pérdidas de información.

Para el funcionamiento del Endpoint Detection and Response (EDR), es necesario la administración centralizada mediante una consola basada en la nube, con la activación de las 979 licencias y las características técnicas adquiridas en el licenciamiento.

7. METODOLOGIA DE TRABAJO

Al inicio, se mantendrá una reunión de trabajo entre el Contratista y el MSP, a fin de coordinar el despliegue de las licencias EDR, con base a un listado de los equipos de usuario final y servidores, entregado por el Administrador de Contrato. El contratista a su costo, realizará la instalación de las licencias. Esta actividad será realizada en los equipos que indique el Administrador del contrato en coordinación con la DTIC, hasta que finalice el plazo contractual.

El Contratista procederá con la entrega y activación de la consola de administración y de las licencias de la solución Endpoint Detection and Response (EDR). La totalidad de licencias deberá

tener una vigencia de 365 días calendario contados a partir de la activación de las mismas a nivel de la consola, para lo cual el Contratista entregará el Certificado de Activación del total de licencias emitido por el fabricante o distribuidor autorizado a nombre del Ministerio de Salud Pública con la fecha de vigencia de las mismas.

El Contratista, realizará la desinstalación de la solución de seguridad que se encuentre previamente instalada en los equipos informáticos de usuario final y servidores del Ministerio de Salud Pública Planta Central, procederá a realizar la instalación de las licencias de la solución EDR de forma coordinada con el personal técnico del Contratista, el personal técnico de la DTIC y el Administrador del Contrato.

El Contratista deberá entregar dentro del plazo de 60 días calendario a partir del día siguiente de la firma del contrato, un reporte con el detalle de las licencias instaladas y novedades presentadas.

El Contratista deberá realizar la transferencia de conocimiento sin costo para el Ministerio de Salud Pública de mínimo 12 horas para al menos 8 analistas designados por la Dirección de Tecnologías de la Información y Comunicaciones, se pueda llevar a cabo de manera presencial o virtual. Se deberá entregar el Certificado de asistencia.

8. DETALLE DE CANTIDADES Y PRECIO

El presupuesto referencial para la **ADQUISICIÓN DE LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES -ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL** es de USD 94.816,15 (NOVENTA Y CUATRO MIL OCHOCIENTOS DIECISÉIS CON 15/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA), más IVA.

No.	Rubro / Descripción del Servicio	Cantidad de licencias requeridas
1	LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL	979

9. REQUISITOS MINIMOS

Los criterios que deben considerarse como requisitos mínimos son:

9.1 EXPERIENCIA Y CAPACIDAD TÉCNICA

9.1.1. Experiencia general mínima

DESCRIPCIÓN	TEMPORALIDAD	MONTO MÍNIMO POR CONTRATO	CONTRATOS PERMITIDOS	FUENTE DE VERIFICACIÒN

VENTA O INSTALACIÓN/ACTIVACIÒN DE LICENCIAS DE SOFTWARE	DENTRO DE LOS ÚLTIMOS 5 AÑOS, PREVIOS A LA PUBLICACIÓN DE ESTE PROCESO	$ 16.000,00	3	Copia (s) simple(s) de contratos con sus respectivas actas entrega recepción definitiva (para entidades públicas) o facturas debidamente legalizadas (para empresas del sector privado), que demuestren la experiencia solicitada.

Tabla de experiencia general mínima

Nota: Valores no incluyen IVA

- El oferente podrá presentar hasta 3 (TRES) contratos, cuya suma sea igual o mayor a $ 48.000,00

9.1.2. Experiencia específica mínima

DESCRIPCIÓN	TEMPORALIDAD	MONTOMÍNIMO POR CONTRATO	CONTRATOS PERMITIDOS	FUENTES DE VERIFICACION
VENTA O INSTALACIÓN/ ACTIVACIÒN DE SOLUCIONES DE SEGURIDAD PARA EQUIPO DE USUARIO FINAL (EDR) O ANTIVIRUS	DENTRO DE LOS ÚLTIMOS 2 AÑOS, PREVIOS A LA PUBLICACIÓN DE ESTE PROCESO	$ 16.000,00	1	Copia (s) simple(s) de contratos con sus respectivas actas entrega recepción definitiva (para entidades públicas) o facturas debidamente legalizadas (para empresas del sector privado), que demuestren la experiencia solicitada.

Tabla de experiencia especifica mínima

Nota: Valores no incluyen IVA

9.2 PERSONAL TÉCNICO MÍNIMO

ÍTEM NRO.	FUNCIÓN	CANTIDAD	NIVEL DE ESTUDIO	TITULACIÓN ACADÉMICA	FUENTE O MEDIO DE VERIFICACIÓN
1	Técnico de soporte (conocimiento en la Herramienta EDR)	1	Tercer nivel	Ing. /Lic. /Tnlgo. Sistemas, o Ing. /Lic. /Tnlgo. en Telemática, o Ing. /Lic. /Tnlgo. Electrónico, o Ing. /Lic. /Tnlgo. En Redes, o Ing. /Lic. /Tnlgo. de Desarrollo, o Ing. /Lic. /Tnlgo. En Telecomunicaciones, o Ing. /Lic. /Tnlgo. En Sistemas Informáticos y Computación, o Ing. /Lic. /Tnlgo. en Sistemas Computacionales	Presentar hoja de vida y copia simple del título profesional

Tabla de personal técnico mínimo

9.2.1. Experiencia mínima del personal técnico

ÍTEM NRO.	FUNCIÓN	DESCRIPCIÓN	FUENTE O MEDIO DE VERIFICACIÓN	CERTIFICACIÓN
1	Técnico de soporte (conocimiento en soluciones EDR)	Experiencia en soporte técnico, dentro de los últimos 2 años, previos a la publicación de este proceso, con un mínimo de 6 meses comprobable.	Copia de la hoja de vida, títulos o registros, actas, certificados de experiencia en diferentes instituciones, con el tiempo de experiencia requerida.	Certificaciones o Cursos en soluciones de EDR o ANTIVIRUS.

Tabla de Experiencia mínima del personal técnico

Nota Importante:

- Los documentos a ser presentados deben ser en copias simple.
- El oferente deberá adjuntar a la oferta la hoja de vida, documento de ciudadanía, título obtenido del personal técnico y certificados solicitados.

9.3 CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Se verificará el cumplimiento expreso y puntual de las especificaciones técnicas descritas en la **"SECCIÓN 5 DE ESTE DOCUMENTO"**

9.4 CUADRO DE REQUERIMIENTOS MINIMOS

PARAMETRO	CUMPLE	NO CUMPLE
Experiencia general mínima		
Experiencia específica mínima		
Personal técnico mínimo		
Experiencia mínima del personal técnico		
Cumplimiento de los Términos de Referencia y especificaciones técnicas.		

Tabla de requerimiento mínimos.

10. PLAZO DE EJECUCIÓN

El plazo de ejecución es de 60 días calendario contados a partir del día siguiente de la firma del contrato.

11. FORMA Y CONDICIONES DE PAGO

El pago se realizará 100% CONTRAENTREGA, previa entrega de la siguiente documentación:

- Certificado de Activación del total de licencias.
- Certificado de Soporte y Garantía Técnica.
- Manual de Usuario de Administración de la Consola de la Solución EDR.
- Certificados de asistencia de la Transferencia de Conocimiento.
- Informe técnico de la DTIC del MSP.
- Informe de conformidad del Administrador de Contrato.
- Acta de Entrega Recepción Definitiva
- Factura emitida por el Contratista.

El pago total se realizará en DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA. Del monto total del contrato se realizarán las retenciones de ley correspondientes.

11.1 PRESENTACIÒN DE LOS ENTREGABLES ESPERADOS

A continuación, se detalla los formatos, cantidad total y copias que se requiere presentar durante la ejecución del contrato:

- ✓ Los entregables definitivos deberán ser presentados al ADMINISTRADOR DE CONTRATO para revisión y aprobación.
- ✓ Los entregables solicitados serán generados de acuerdo al ítem de **"PRODUCTOS Y/O SERVICIOS ESPERADOS".**

- ✓ La entrega de los productos y/o servicios se realizará en **forma física 2 ejemplares y 1 digital** CD/DVD ROM

12. LUGAR Y FORMA DE ENTREGA

Las licencias de la solución EDR serán entregadas en:

Provincia	Cantón	Lugar	Dirección	
			Calle Principal	Calle Secundaria
Pichincha	Quito	Plataforma Gubernamental de Desarrollo Social	Av. Amaru Ñan, Plaza Quitumbe	Av. Lira Ñan

De ser necesario el MSP podrá modificar el lugar de entrega, mismo que estará en la ciudad de Quito, y el cuál no tendrá costo adicional para el MSP, previa validación por parte del administrador del contrato.

13. GARANTÍAS

13.1 GARANTÍA CUMPLIMIENTO

Garantía de Cumplimiento: Equivalente a un rango del 5% del valor del contrato.

13.2 GARANTIA TÉCNICA

- La vigencia de la garantía técnica de las licencias por 365 días, contados a partir de la fecha de activación de las licencias en la consola.
- La garantía técnica debe ser entregada a través de un certificado emitido por el fabricante o distribuidor autorizado y debe estar registrada a nombre del Ministerio de Salud Pública del Ecuador.
- La garantía técnica incluirá el compromiso de realizar el soporte técnico por parte de Contratista durante la vigencia de las licencias.
- Las actualizaciones de software de la solución EDR deberán ser provistas sin costo durante la vigencia de las licencias.

14. MULTAS

Por cada día de retardo en la ejecución de las obligaciones contractuales por parte del contratista, se aplicará la multa del 1 por 1.000 diaria del porcentaje de las obligaciones que se encuentren pendientes de ejecutarse conforme lo establecido en el contrato. Excepto en el evento de caso fortuito o fuerza mayor conforme lo dispuesto en el artículo 30 del Código Civil.

15. OBLIGACIONES DEL CONTRATISTA

- El Contratista debe firmar un acuerdo de confidencialidad de manera que se garantice que la información y detalles propios de la institución guarden los criterios de reserva, confidencialidad y propiedad, como exclusiva del Ministerio de Salud Pública.
- Dar cumplimiento cabal a lo establecido en las especificaciones técnicas.
- Realizar la activación de las licencias las cuales tendrán una vigencia de 365 días.
- Realizar el despliegue de las licencias conforme el detalle del listado de equipos de usuario final y servidores, entregado por el Administrador del Contrato.

- Suscribir el Acta Entrega Recepción conforme lo establecido en el artículo 325 del RGLOSNCP.
- El Contratista deberá garantizar el soporte técnico y el cumplimiento de la vigencia de las licencias de la solución EDR, que corresponde a 365 días calendario y que serán contados a partir de la activación de las licencias en la consola.

16. OBLIGACIONES DEL CONTRATANTE

- Designar al administrador del contrato.
- Elaborar y firmar el acuerdo de confidencialidad que debe firmar el contratista.
- La DTIC entregará el listado de equipos de usuario final y servidores en los cuales será instaladas las licencias.
- Dar solución a las peticiones y problemas que se presentaren en la ejecución del contrato, en un plazo 15 días contados a partir de la petición escrita formulada por el contratista.
- Suscribir el Acta Entrega Recepción conforme lo establecido en el artículo 325 del RGLOSNCP.
- Verificar de conformidad con los intereses institucionales la documentación que el contratista debe presentar.
- Realizar el pago correspondiente de acuerdo a la forma y condiciones de pago establecida para el contrato.
- Otorgar al contratista las facilidades necesarias para la recepción y despliegue de las licencias.
- La instalación será de forma controlada y supervisada por el administrador del contrato y la DTIC, de forma que se asegure la integridad y disponibilidad de la información.

LISTA DE BIENES Y PLAN DE ENTREGA (NO APLICA)

N° de Artículo	Descripción de los Bienes	Cantidad	Unidad física	Lugar de destino convenido	Fecha de Entrega		
					Fecha más Temprana de Entrega	Fecha Límite de Entrega	Fecha de Entrega [11]Ofrecida por el Oferente *[a ser proporcionada por el Oferente]*
*[indicar **el** No.]*	*[indicar la descripción de los Bienes]*	*[indicar la cantidad de los artículos a suministrar]*	*[indicar la unidad física de medida de la cantidad]*	*[indicar el lugar de entrega destino convenido]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*

[11] El Contratante completará este cuadro, excepto por la columna "Fecha de entrega ofrecida por el Oferente", la cual será completada por el Oferente.

LISTA DE SERVICIOS Y PLAN DE ENTREGA

N° de Ítem	Descripción de los Servicios de No Consultoría	Cantidad	Unidad	Lugar de prestación del servicio	Fecha de Entrega		
					Fecha de inicio	Fecha de finalización	Plazo de Ejecución
[indicar el No.]	*[indicar la descripción de los servicios conexos y/o servicios de no consultoría]*	*[indicar la cantidad]*	*[indicar la unidad de medida de la cantidad]*	*[indicar el lugar de prestación del servicio]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el número de días después de la fecha de efectividad del Contrato]*	*[indicar el plazo ofertado para prestar el servicio]*
1	LICENCIAS DE PROTECCIÓN Y RESPUESTA DE AMENAZAS INFORMÁTICAS PARA EQUIPOS DE USUARIO FINAL Y SERVIDORES - ENDPOINT DETECTION AND RESPONSE (EDR) PARA EL MINISTERIO DE SALUD PÚBLICA EN PLANTA CENTRAL	979	Unidad	Provincia de Pichincha, cantón Quito, Plataforma Gubernamental de Desarrollo Social, ubicado en la Av. Amaru Ñan, y Av. Lira Ñan.	*60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.*	*60 (sesenta) días calendario, contados a partir del día siguiente de la suscripción del contrato.*	