



INSTITUTO DE PREVISION MILITAR

Régimen de Riesgos Especiales

INDICE

[IPM-LPR-GC-2024-010](#).....02

[IPM-LPR-GC-2024-008](#).....09

[IPM-LPN-GC-2024-002](#)25

"CONTRATO DE RESTAURACIÓN Y MEJORAS DEL CENTRO DE DATOS DEL IPM DE SAN PEDRO SULA E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO INTEGRADO A LOS CENTROS DE DATOS DEL IPM EN LAS CIUDADES DE TEGUCIGALPA Y SAN PEDRO SULA, SEGÚN LICITACIÓN PRIVADA NO. IPM-LPR-GC-2024-010".

Nosotros, **OTTO FABRICIO MEJÍA HÉRCULES**, Coronel de Defensa Aérea D.E.M.A, Actuario y MBA en Finanzas, mayor de edad, casado, hondureño, con Documento Nacional de Identificación número 0501-1971-02586, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR (I.P.M.)** Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guion Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis (2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Ordinaria Número Quinientos Diecinueve (519) mediante Resolución Número Seis Mil Noventa y Siete (6097) de fecha Trece (13) de Diciembre del año Dos Mil Veintitrés (2023), y el Poder General de Representación y Administración otorgado mediante Instrumento Público Número dieciocho (18) autorizado en esta ciudad, ante los oficios del Notario David Alfonso Velásquez, el catorce (14) de Marzo del año dos mil veinticuatro (2024), e inscrito bajo el Número Treinta y Nueve (39) del Tomo Cuatrocientos Dieciséis (416) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO Y RICARDO FRANCISCO TABORA MEARS**, mayor de edad, hondureño, casado, Técnico en electrónica, de este domicilio, con Documento Nacional de Identificación No. **0801-1963-06161**, RTN número **08011963061618** actuando en mi condición de Representante Legal de la Sociedad **INVERSIONES GENERALES EN MÁQUINAS Y EQUIPOS DE CONTROL S. DE R.L. DE C.V., (INGELMEC)**, Sociedad con RTN No. **08019003249590** y constituida en escritura pública No. 45 de fecha diecisiete (17) de mayo de mil novecientos noventa y tres (1993) autorizada por el Notario Israel Rodríguez Orellana, inscrita en folio 92, Tomo 296 del Registro de Comerciantes Sociales el 29 de octubre de 1993, con facultades suficientes para la suscripción del presente contrato según Poder de Administración autorizado en instrumento público No. 116 de fecha 06 de noviembre de 2007, por el Notario César Dolores Vaquedano, inscrito número 17 y Tomo 686, del Registro Mercantil de Francisco Morazán, Centro Asociado al IP, y para efectos de este contrato me denominaré como **EL PROVEEDOR**, hemos convenido en celebrar el presente **CONTRATO DE RESTAURACIÓN Y MEJORAS DEL CENTRO DE DATOS DEL IPM DE SAN PEDRO SULA E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO INTEGRADO A LOS CENTROS DE DATOS DEL IPM EN LAS CIUDADES DE TEGUCIGALPA Y SAN PEDRO SULA, SEGÚN LICITACIÓN PRIVADA NO. IPM-LPR-GC-2024-010**, Aprobado en Comité de Compras y Licitaciones No. 24-2024 del 21 de junio de 2024 y Resolución de fecha 24 de junio de 2024, el cual se registrará por las cláusulas y condiciones siguientes: **PRIMERA: OBJETO DEL CONTRATO:** La restauración y mejoras del centro de datos del IPM de San Pedro Sula e implementación de un sistema de monitoreo integrado a los centros de Datos del IPM en las ciudades de Tegucigalpa y San Pedro Sula de acuerdo con los ítems siguientes:

1. Requerimientos técnicos remodelación y reparación de centro de datos de San Pedro Sula

OBRA CIVIL Y ELECTRICA

Ítem	Descripción	Cantidad
1	Obra civil primaria	1
2	Obra civil secundaria	1
3	Piso elevado para implementar en área del Centro de Datos	11.75 m2
4	Cielo falso tipo Clean Room	11.75 m2

1.1 Obra Civil Primaria

Trabajo	Descripción
Desinstalación de cielo falso existente	Desinstalación de doble cielo de falso existente en área de data center
Instalación de cielo falso PVC	Suministro e instalación de 11.75m2 de cielo falso PVC entre techo y cielo visto de fibra mineral
Instalación de cielo falso fibra mineral	Suministro e instalación de 11.75m2 de cielo falso de fibra mineral 2x4 "

1.2 Obra Civil Secundaria

Trabajo	Descripción
Pintura fastyl en área data center	Pintura fastyl elastomérica para área de data center
Iluminación área data center	Colocación de iluminación sobre cada equipo de data center

1.3 Piso Elevado

Trabajo	Descripción
Cambio de estructura de madera y fascia en piso elevado	Cambio de estructura de madera en piso elevado, con sellador y anticorrosivo
Colocación anticorrosiva en estructura de soporte	Colocación de anticorrosivo en estructura de soporte de piso elevado data center

1.4 Cielo Falso

Trabajo	Descripción
Cielo Falso tipo Clean Room	Suministro e instalación de Cielo Falso tipo Clean Room Clase 100 y Clase 10M-100M con una cara laminada de vinilo en relieve con bordes y bordes sellados para uso en salas blancas Clase 100 o 10M-100M. - Cantidad 11.75 mts. cuadrados - Tamaño de paneles de 2' x 4' x 5/8" perforado - Color blanco - 52% de composición de material reciclado - Producto biológico certificado por USDA - Producto FiReCoDe diseñado para cumplir con los códigos de vida
Doble cielo falso	Suministro e instalación de doble cielo falso, este de PVC para sellar la sala sobre el cielo falso tipo Clean Room.

2. Implementación de un sistema de monitoreo para centros de datos de Tegucigalpa y San Pedro Sula.

Equipo / software

Ítem	Descripción	Cantidad
1	Licencia de Monitoreo totalmente compatible 100% con equipos Vertiv	1
2	Monitor Ambiental compatible 100 % con equipos Vertiv	1

1.1 Licencia Software de Monitoreo

Equipo	Descripción
Licencia Software	Suministro y configuración de una (1) licencia de monitoreo con las siguientes características técnicas: - Cobertura para 50 Dispositivos - Organización de datos - Monitoreo - Alertas - Idioma Español - Intuitivo
Configuración	Instalación de sistema en CPU con requerimientos específico

12

Requerimientos para instalación	Sistema operativo mínimo: -Windows 10 (64bit) -Windows Server 2016 -Windows Server 2019 CPU: (Intel o AMD) 4 CPU 2.0 GHz o superior RAM: 8 GB Espacio en disco: 100 GB Lectura/Escritura en disco: 15 MBps Redes: 10/100 MBps	Sistema operativo recomendado: - Windows Server 2019 CPU: (Intel o AMD) ≥ 6 CPU ≥ 2.2 GHz o superior RAM: ≥ 16 GB Espacio en disco: ≥ 300 GB Lectura/Escritura en disco: ≥ 200 MBps de velocidad de lectura/escritura Redes: ≥ 1 Gps
---------------------------------	---	--

1.2 Equipo de monitoreo ambiental

Equipo	Descripción
Equipo de monitoreo	Suministro e instalación de un (1) monitor ambiental con las siguientes características técnicas: -Montaje en rack -Sensor de temperatura -Sensor de humedad y punto de condensación -Capacidad para añadir 8 sensores externos adicionales -Fuente de alimentación universal incluida -Contacto de relé
Instalación	Montaje correspondiente en Rack

3. Requerimientos que debe cumplir el proveedor en ambos proyectos.

- 1 Contar con experiencia demostrable en el suministro de productos o servicios relacionados con la infraestructura de centros de datos, sistemas de energía crítica, gestión térmica, protección contra incendios, entre otros aspectos relevantes para equipos Vertiv Liebert.
- 2 Contar con certificación del personal por el fabricante Vertiv Liebert para las configuraciones del sistema de monitoreo a implementar.
- 3 Los productos o servicios ofrecidos deben ser compatibles con las soluciones y estándares técnicos de Vertiv Liebert, asegurando la integración efectiva en los sistemas y equipos existentes.
- 4 Ofrecer un sólido soporte técnico, con personal capacitado para resolver problemas técnicos, realizar mantenimiento preventivo y ofrecer asesoramiento especializado.

28

5 Presentar un historial de cumplimiento confiable, con referencias de clientes satisfechos y casos de éxito en proyectos similares con equipos Vertiv Liebert.

Todo lo anterior especificado en las bases de licitación. **SEGUNDA: MONTO DEL CONTRATO:** El monto del contrato es por SETECIENTOS OCHENTA Y CUATRO MIL TRESCIENTOS SESENTA Y DOS LEMPIRAS CON 47/100 (L. 784,362.47). Oferta que incluye el Impuesto sobre ventas y el cual será retenido por el Instituto. **TERCERA: FORMA DE PAGO:** EL INSTITUTO realizará un pago único contra el informe de aceptación y satisfacción emitido por la División de Tecnología y Procesos del IPM. **CUARTA: SUPERVISIÓN POR PARTE DEL INSTITUTO:** La División de Tecnología y Procesos del IPM asignará una persona que se encargará de verificar la calidad de los servicios solicitados.- **QUINTA: GARANTÍAS DEL PROVEEDOR:** UNA GARANTÍA DE CUMPLIMIENTO DE CONTRATO por la cantidad de CIENTO DIECISIETE MIL SEISCIENTOS CINCUENTA Y CUATRO LEMPIRAS CON 37/100 (L. 117,654.37) correspondiente al quince por ciento (15%) del monto total del Contrato, la cual tendrá una vigencia de seis (6) meses, contados a partir de la fecha en que se inicie el presente contrato. UNA GARANTÍA DE CALIDAD por la cantidad de TREINTA Y NUEVE MIL DOSCIENTOS DIECIOCHO LEMPIRAS CON 12/100 (L. 39,218.12) correspondiente al cinco por ciento (5%) del monto total del Contrato, la cual tendrá una vigencia de doce (12) meses, contados a partir de la fecha en que se recepcionen los trabajos y bienes solicitados en el presente contrato. Ambas garantías deberán ser emitidas por una Institución Bancaria o Entidad Aseguradora establecida legalmente en el País, de reconocida experiencia y capacidad, y ser aceptada por EL INSTITUTO. - **SEXTA: INCUMPLIMIENTO DEL CONTRATO:** En caso de incumplimiento comprobado por parte del PROVEEDOR en las cláusulas convenidas y en el objeto del presente contrato, EL INSTITUTO hará efectiva la garantía de cumplimiento de contrato, con previa notificación a EL PROVEEDOR. De igual forma el Proveedor pagará la indemnización que conforme a Ley corresponda. - **SÉPTIMA: MULTAS:** EL INSTITUTO cobrará al PROVEEDOR una multa correspondiente al 0.036% del monto restante del contrato incumplido. **OCTAVA: CAUSAS DE RESOLUCIÓN DEL CONTRATO:** Las partes contratantes podrán invocar cualesquiera de las causales de disolución del contrato tales como: 1) El grave o reiterado incumplimiento de las cláusulas convenidas, 2) La falta de constitución de las garantías a cargo del PROVEEDOR dentro de los plazos correspondientes; 3) En caso de muerte de EL PROVEEDOR y sus sucesores no pudieren concluir el Contrato; 4) La declaración de quiebra o suspensión de pagos del PROVEEDOR, o su comprobada insolvencia financiera; 5) Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor que surjan a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; 6) El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; 7) El mutuo acuerdo de las partes; 8) Las demás que establezca expresamente este contrato, las especificaciones técnicas y las Leyes vigentes en la República; y, 9) En caso de existir alguna orden de cambio y/o modificación no aprobada por la División de

Tecnología y Procesos del IPM o alguna modificación no contemplada por el INSTITUTO.-

NOVENA: CESIÓN, SUB CONTRATACIÓN, TRASPASO DEL CONTRATO: EL PROVEEDOR no podrá ceder, subcontratar o traspasar lo estipulado en el presente contrato sin previo consentimiento por escrito del INSTITUTO. La aprobación de cualquier subcontratación no eximirá a EL PROVEEDOR de ninguna responsabilidad u obligación bajo los términos de este contrato. EL PROVEEDOR no podrá ceder su derecho a recibir pago conforme a lo estipulado en el presente contrato, sin previo consentimiento por escrito del INSTITUTO. - **DÉCIMA:** **SOLUCIÓN DE CONFLICTOS:** Si existiera alguna desavenencia en la interpretación y ejecución de este contrato y la misma no fuera solucionada por el buen entendimiento extrajudicial o la conciliación, ambas partes nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil del Departamento de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicarán las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. **DÉCIMA PRIMERA: CLÁUSULA DE INTEGRIDAD Y CONFIDENCIALIDAD:** Las partes en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y acceso a la información pública (LTAIP) y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a: 1. Mantener el más alto nivel de conducta, ética, moral y de respeto a las Leyes de la República así como los valores de: INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS. 2. Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia. 3. Que durante la ejecución del contrato ninguna persona que actué debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado autorizado o no, realizará a) **Prácticas Corruptivas:** entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) **Prácticas Colusorias:** entendiendo estas como aquellas en las que denoten, surgieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado incluyendo influenciar en forma inapropiada las acciones de la otra parte. 4. Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte, para efectos del contrato y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente, imprecisa o

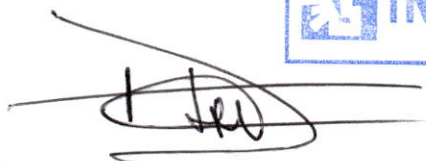
que no corresponda a la realidad para efectos de este contrato. 5. Mantener la debida confidencialidad sobre toda la información a la que se tenga acceso por razón del Contrato, y no proporcionarla, ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos. 6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta cláusula por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra. 7. Denunciar en forma oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al sub-contratista, con los cuales el contratista o consultor contrate así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar a: De parte del contratista o consultor: i. A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudiesen deducirse a. La aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b. De parte del contratante a la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o que pudiendo hacerlo no denunciaron la irregularidad de su Registro de proveedores y contratistas que al efecto llevaré para no ser sujeto de elegibilidad futura en procesos de contratación. ii. A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. **DÉCIMA SEGUNDA:** EL **PROVEEDOR** se compromete a facilitar cualquier tipo de información a los Auditores Externos contratados por el **INSTITUTO**, referente a los montos y ejecución del presente contrato. **DÉCIMA TERCERA: VIGENCIA DEL CONTRATO:** La vigencia del presente contrato es de tres (3) meses a partir de la orden de inicio. En fé de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los cinco (5) días del mes de julio del año Dos Mil veinticuatro (2024).

CORONEL DE DEFENSA AÉREA DEMA,

TÉCNICO EN ELECTRÓNICA

ACTUARIO Y MBA EN FINANZAS


OTTO FABRICIO MEJIA HÉRCULES
EL INSTITUTO


RICARDO FRANCISCO TABORA MEARS
EL PROVEEDOR



"CONTRATO DE LOS SERVICIOS DE MANTENIMIENTO CORRECTIVO, PREVENTIVO Y DIAGNOSTICO DE UNIDADES DE AIRE ACONDICIONADO EN PROPIEDAD DEL INSTITUTO DE PREVISIÓN MILITAR, SEGÚN LICITACIÓN PRIVADA NO. IPM-LPR-GC-2024-008".

Nosotros, **OTTO FABRICIO MEJIA HERCULES**, mayor de edad, casado, Coronel de Defensa Aérea D.E.M.A, Actuario y MBA en Finanzas, hondureño, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR (I.P.M.)** Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guion Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis (2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Ordinaria Número quinientos diecinueve (519) mediante Resolución Número Seis mil Noventa y Siete (6097) de fecha Trece (13) de diciembre del año dos mil veintitrés (2023), y el Poder General de Representación y Administración otorgado mediante Instrumento Publico Numero dieciocho (18) autorizado en esta ciudad, ante los oficios del Notario David Alfonso Velásquez, el catorce (14) de Marzo del año dos mil veinticuatro (2024), e inscrito bajo el Número treinta y nueve (39) del Tomo cuatrocientos dieciséis (416) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO** y **JOSE ALEJANDRO JIMENEZ ROMERO**, mayor de edad, Licenciado, hondureño, soltero, con Documento Nacional de Identificación Numero 0801-1990-20353, con RTN número 08011990203535, actuando en mi condición de Representante legal de la Sociedad **REFRICLIMA S. DE R.L** con RTN 08019021294799 constituida mediante contrato societario Ref-18ZJ191 con Matricula 2587950, del Registro Mercantil de Francisco Morazán, Centro Asociado IP, con facultades suficientes para la suscripción del presente contrato y que para efectos de este contrato me denominaré como **EL PROVEEDOR**, hemos convenido en celebrar el presente **CONTRATO DE LOS SERVICIOS DE MANTENIMIENTO CORRECTIVO, PREVENTIVO Y DIAGNOSTICO DE UNIDADES DE AIRE ACONDICIONADO EN PROPIEDAD DEL INSTITUTO DE PREVISIÓN MILITAR, SEGÚN LICITACIÓN PRIVADA NO. IPM-LPR-GC-2024-008**, Aprobado en Comité de Compras y Licitaciones No. 23-2024 del 12 de junio de 2024 y Resolución de fecha 12 de junio de 2024, el cual se regirá por las cláusulas y condiciones siguientes: **PRIMERA:** **OBJETO DEL CONTRATO:** El presente contrato tiene como objeto realizar mantenimiento correctivo, preventivo y diagnostico de las unidades de aire

acondicionado propiedad del Instituto de Previsión Militar, las actividades se detallan a continuación: 1) Mantenimiento **Preventivo**:

El proveedor deberá realizar durante la vigencia del contrato, mantenimiento preventivo mensual, para el cual deberá asignar personal técnico calificado y con las herramientas y equipo necesario así mismo deberá ser acompañado por el técnico de refrigeración del Departamento de Mantenimiento de IPM, de igual manera deberá presentar mensualmente adjunto a la solicitud de pago, un informe digital y físico con imágenes y descripción desglosando las actividades realizadas con el número de inventario de las unidades a las cuales se les dio el mantenimiento, de acuerdo a las que se indican en la tabla de descripción de equipos adjunto en este documento en ANEXO 1 el cual formara parte íntegra del presente contrato.

Previo a que el personal técnico de la empresa a quien se le adjudique el mantenimiento de inicio a los mismos, deberá realizar un diagnóstico de las unidades e informar la situación actual para priorizar el mantenimiento a realizar así mismo en el reporte de diagnóstico deberá describir el estado de cada máquina y recomendaciones del mantenimiento correctivo a realizar si así lo requieren, en el caso de que el equipo presente una falla, deberá revisarse en conjunto con el personal del Departamento de Mantenimiento asignado a supervisar dichos trabajos, mismo que deberá dar fe de la falla del equipo, el cual solo podrá realizarse con el visto bueno del Jefe del Departamento de Mantenimiento.

En la ejecución de este servicio, el proveedor deberá realizar como mínimo las siguientes actividades:

- Verificar y retorquear todas las conexiones eléctricas en periodos de una vez mensualmente.
- Verificar la operación de los motores de los ventiladores del evaporador, aspas, bandas y el debido engrase de balineras, motores y ventiladoras.
- Limpiar la bandeja de drenado y corroborar que tenga un drenado apropiado.
- Limpieza de la superficie del serpentín del evaporador.
- Limpieza de filtros de aluminio o sustitución por filtros ecológicos.
- Limpieza del serpentín del condensador, debe ser limpiado y lavado.
- Corroborar la operación de los ventiladores del condensador.
- Verificar todos los componentes eléctricos y aplicar limpiador de componentes eléctricos.

- Verificar la operación del sistema de control.
- Verificación y corrección del nivel de aceite del compresor.
- Verificar las condiciones del aislamiento de la línea del refrigerante.
- Verificación del nivel de refrigerante.
- Verificar el sobrecalentamiento del sistema.
- Verificar todos los capilares y las líneas con mangueras especiales.
- Reemplazar todos los tapones perdidos de las válvulas y las cubiertas de la unidad.
- Reposición de partes misceláneas menores como: tornillos, tuercas, remaches, fajillas para la sujeción de cables, terminales de presión, etc.
- Chequeo de voltajes y amperajes.
- Determinación de temperatura a la entrada y salida del serpentín del evaporador.
- Chequeo de presiones de succión y descarga.
- Limpieza y lavado general de la unidad.
- Revisión y ajuste de eliminadores de vibración.
- Revisión de válvulas de servicio.
- Verificación de hermeticidad del sistema.
- Comprobación de ausencia de humedad.
- Revisión y/o cambio del filtro secador (sí se requiere).
- Chequeo de operación de válvula de expansión.
- Chequeo de operación de contactores y limpieza de los mismos con limpia contactos.
- Verificación y ajuste de termostatos.
- Calibración válvula de expansión (si se requiere).
- Limpieza de difusores y rejillas de retorno.
- Limpieza de los Ductos en periodos semestrales.
- Lavado del serpentín del evaporador y condensador una vez al año con químico abrasivo según los requerimientos técnicos de las unidades.
- Lubricación de partes móviles.
- Cambio de bandas para las unidades que aplica.
- Atención de llamadas para revisión.
- Desmontaje, montaje y limpieza de condensador y evaporador.
- Limpieza de placas electrónicas con limpiador de contactos.
- Aplicar desengrasante a unidades condensadoras y evaporadoras.
- Desmontaje y montaje de Blower para su respectiva revisión y mantenimiento.
- Desmontaje y montaje de motores, ventiladora de condensadores y

evaporadores para engrase de balineras,

- Cambio de componentes eléctricos recalentados.

Al finalizar el mantenimiento preventivo, el proveedor deberá entregar el reporte en físico y digital al jefe del Departamento de Mantenimiento, las hojas de inspección y mantenimiento realizadas en campo deberán de estar firmadas por el técnico de IPM, que superviso los trabajos.

2. Mantenimiento Correctivo: Este servicio se solicitará cuando una unidad de aire acondicionado o equipo presente alguna falla en la operación de cualquiera de sus módulos, componentes, accesorios o sistema completo, conforme a lo establecido en este documento, siendo responsabilidad del proveedor realizar las acciones que sean necesarias para el restablecimiento a las condiciones normales de operación del equipo, de acuerdo a lo establecido en los manuales técnicos, apegándose siempre a las normativas internacionales vigentes. Los repuestos utilizados para la ejecución del servicio deberán ser nuevos y originales y podrán ser suministrados por el Instituto cuando este lo requiera, así mismo en el mantenimiento cuando el técnico observe un mal funcionamiento deberá hacer la revisión de la falla con el técnico del Departamento de Mantenimiento asignado, con el objetivo de que el técnico por parte del Instituto, de visto bueno para generar en conjunto el reporte correspondiente al Jefe del Departamento de Mantenimiento con el objetivo de gestionar la reparación de la unidad de aire acondicionado.

Los mantenimientos correctivos serán clasificados en MAYOR y MENOR dependiendo de la severidad de la falla y el tiempo de ejecución del servicio.

Para la ejecución de este servicio, el proveedor deberá considerar todos los materiales y gastos indirectos necesarios para el restablecimiento a la operación normal del equipo, realizando como mínimo las siguientes actividades: trabajos mecánicos, eléctricos montajes, desmontaje, sustitución o reparación de las partes, módulos, accesorios o

componentes dañados conforme a lo establecido en los manuales técnicos del fabricante y a las normas correspondientes.

El proveedor deberá cobrar únicamente el valor de los repuestos y materiales a utilizar ya que los trabajos deberán ejecutarse por el

personal técnico durante el mes de mantenimiento y estos deberán estar conforme al precio del mercado, sin cobro alguno en concepto de mano de obra, la cual será absorbida por el contrato de mantenimiento siempre y cuando esté en vigencia. Este cobro, podrá modificarse en todas aquellas reparaciones en las que se demuestre la complejidad de la misma y que implique un gasto extraordinario para el proveedor; lo que implica que podría haber un recargo de mano de obra siempre y cuando sea de común acuerdo entre el I.P.M. y el proveedor.

Al término del servicio el proveedor deberá entregar un reporte detallando las acciones efectuadas y partes reemplazadas, el cual deberá estar firmado por quien realizó el servicio y por el supervisor del I.P.M., en el sitio.

3. Diagnóstico: Este servicio será solicitado inicialmente, antes del primer servicio de mantenimiento preventivo a cada unidad de aire acondicionado; por lo que el proveedor deberá entregar un informe en físico y digital donde detallará con toda precisión el estado operacional de cada unidad de aire acondicionado que este bajo el contrato de mantenimiento vigente.

Además, cuando el I.P.M., por las particularidades de la falla o alteración de la operación de los equipos o unidades de aire acondicionado, no le sea posible determinar con toda precisión las acciones a ejecutar y los repuestos o partes a sustituir, y requiere de la revisión de un especialista para que las determine, para lo cual en estos casos, el I.P.M., emitirá una orden de servicio para realizar el diagnóstico, en la que describirá con toda claridad la falla detectada por el usuario, por lo que el proveedor deberá trasladarse al sitio donde se ubica el equipo para su revisión y análisis, después de lo cual deberá entregar al I.P.M., el diagnóstico correspondiente firmado por el supervisor responsable del contrato por parte del proveedor, en el que detallará con toda precisión las causas que originan la falla, las acciones a ejecutar y los repuestos o partes a sustituir para su corrección o reparación; el cual servirá para que el I.P.M., a través del administrador del contrato elabore y entregue al mismo, una orden complementaria de servicio en la que señalará los servicios requeridos.

4. Relación de Equipos y Ubicación:

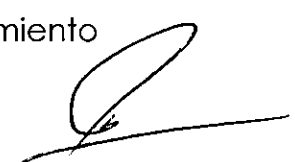
Los servicios solicitados se deberán proporcionar en el sitio donde se encuentre instalado el equipo motivo de la generación de la orden de servicio, conforme a la siguiente relación de equipos y ubicaciones.

5. Aspectos que el proveedor deberá de considerar para el análisis de su propuesta.

- Entregar al supervisor en sitio los repuestos que hayan sido sustituidos como resultado de alguna reparación.
- En caso de que el I.P.M., requiera un diagnóstico, el resultado lo entregará en papel membretado y de forma digital, debidamente firmado por el supervisor responsable del contrato; el dictamen deberá contener como mínimo la siguiente información: causa de la falla concepto de reparación, costo de reparación y tiempo de reparación.
- Las actividades objeto de este contrato deberán de efectuarse sin interrumpir las actividades normales de los empleados y clientes del I.P.M.
- El proveedor otorgará las facilidades necesarias para que el I.P.M., verifique la calidad de las reparaciones que se hagan a los equipos ya sea en el sitio donde están ubicados o dentro de las instalaciones del proveedor.
- Todos los repuestos, accesorios, módulos, consumibles, etc., utilizados para la atención de alguna falla o reparación deberán ser nuevos y originales.
- El proveedor deberá atender cualquier llamado de solicitud de urgencia servicio fuera de los mantenimientos preventivos sin costo adicional siempre y cuando el contrato de mantenimiento este vigente.
- El proveedor no podrá realizar ninguna sustitución de partes o componentes, sin previo aviso al supervisor designado del I.P.M., quién autorizará y verificará que la nueva parte o componente corresponda en calidad y marca, igual o superior a la existente.
- El proveedor deberá entregar su cronograma mensual de mantenimientos con el objetivo de poder coordinar de manera eficiente la prestación de sus servicios, con el cual el I.P.M., podrá asignar de la mejor manera al supervisor encargado para la supervisión de dichos mantenimientos.
- El proveedor deberá contar con todo el personal necesario y especializado para la prestación de los servicios solicitados.
- El proveedor es absoluto responsable del pago por concepto de bonos,

salarios e indemnizaciones por accidentes de trabajo de todo el personal que tenga bajo su cargo, eximiendo de cualquier responsabilidad al I.P.M.

- El I.P.M., prestará toda la colaboración que sea necesaria para que las operaciones del mantenimiento se desarrollen lo más efectivamente posible, así como acatar las disposiciones y recomendaciones de aspecto técnico que sean sugeridas por parte del proveedor.
- El proveedor deberá proporcionar a su personal técnico el equipo de seguridad personal y bioseguridad necesario para la protección de su seguridad física y los implementos de seguridad de acordonamiento del área de trabajo.
- El contrato de mantenimiento no incluye costo de equipos, repuestos y materiales, costo de reparaciones y trabajos adicionales, costo en trabajos realizados en equipo tipo Chiller ni la completación de carga de refrigerante si fuese necesario.
- La empresa adjudicada no deberá realizar cobro por mano de obra en el caso de que el IPM, proporcione el equipo para el mantenimiento correctivo de la unidad de aire acondicionado.



6. ACTIVIDADES MÍNIMAS EN LAS DIFERENTES UNIDADES DE AIRE ACONDICIONADO.

A. Actividades mínimas de mantenimiento en Unidades centralizadas de aire Acondicionado:

➤ Correctivo MAYOR:

- Suministro e instalación de motor eléctrico.
- Suministro e instalación de unidad condensadora.
- Suministro e instalación de unidad evaporadora.
- Suministro e instalación de compresor, incluye recarga de refrigerante hasta su valor nominal
- Suministro e instalación de serpentín evaporador de aluminio.
- Reparación de serpentín evaporador de aluminio.
- Suministro e instalación de serpentín condensador.
- Reparación de serpentín condensador.
- Suministro e instalación de ventilador.
- Suministro e instalación de tarjetas electrónicas de control.
- Reparación de tarjetas electrónicas de control.

- Suministro e instalación de tarjeta o módulo electrónico variador de velocidad de motor ventilador de condensador.
- Suministro e instalación de tarjeta o módulo electrónico de fuente de poder suministradora de voltaje para los circuitos electrónicos de control y fuerza.
- Suministro e instalación de válvula de control soldable.
- Suministro e instalación de válvula de expansión termostática.
- Suministro e instalación de válvula de descarga para compresor.
- Suministro e instalación de válvula de succión para compresor.

➤ Correctivo MENOR:

- Detección y corrección de fugas de refrigerante incluye limpieza con nitrógeno, vacío y soldadura de plata; recarga de refrigerante hasta su capacidad nominal.
- Suministro e instalación de filtro deshidratador soldable relleno de silica incluye válvula de control.
- Suministro e instalación de perilla para control de temperatura.
- Suministro e instalación de protector térmico para compresor.
- Suministro e instalación de rejilla de aluminio con marco biselado para inyección o retorno.
- Suministro e instalación de difusor fijo de aluminio extruido con marco biselado.
- Suministro e instalación de rodamientos a motor eléctrico.
- Suministro e instalación de transformador de control.
- Suministro e instalación de aspas metálicas para ventilador-condensador.
- Suministro e instalación de relevador.
- Suministro e instalación de vibro aisladores para base de compresor.
- Suministro e instalación de termostato.
- Suministro e instalación de interruptor multi posiciones para aplicación de selección de velocidad.
- Suministro e instalación de bulbo sensor de temperatura

de la salida del serpentín del evaporador.

- Suministro e instalación de válvula solenoide.
 - Suministro e instalación de interruptor de alta y baja presión.
 - Suministro e instalación de mirilla para visualizar presencia de refrigerante.
 - Suministro e instalación de contactor.
 - Suministro e instalación de contactor auxiliar.
 - Suministro e instalación de protector de fase.
 - Suministro e instalación de relevador de tiempo (timer) para retraso de arranque de compresor.
 - Suministro e instalación de protección anticorrosiva.
 - Suministro e instalación de capacitor de arranque.
 - Suministro e instalación de filtro de aire (si la unidad no cuenta con el mismo).
 - Suministro y competición de carga de refrigerante.
- 

B. Actividades mínimas de mantenimiento correctivo en una unidad tipo Mini Split y Split Ducto de aire acondicionado

➤ Correctivo MAYOR:

- Suministro e instalación de motor eléctrico de unidad condensadora.
- Suministro e instalación de unidad condensadora.
- Suministro e instalación de unidad evaporadora.
- Suministro e instalación de compresor incluye recarga de refrigerante hasta su valor nominal.
- Suministro e instalación de serpentín de aluminio para unidad evaporadora.
- Reparación de serpentín de aluminio para unidad evaporadora.
- Suministro e instalación de serpentín de aluminio para unidad condensadora.
- Reparación de serpentín de aluminio para unidad condensadora.
- Suministro e instalación de moto ventilador de unidad evaporadora.
- Suministro e instalación de tarjeta o modulo electrónico universal.
- Reparación de tarjeta o modulo electrónico universal.

- Suministro e instalación de válvula de control soldable.
 - Suministro e instalación de válvula de expansión termostática.
 - Suministro e instalación de válvula de descarga para compresor.
 - Suministro e instalación de válvula de succión para compresor.
- **Correctivo MENOR:**
- Detección y corrección de fugas de refrigerante incluye limpieza con nitrógeno, vacío y soldadura de plata; recarga de refrigerante hasta su capacidad nominal.
 - Suministro e instalación de filtro deshidratador soldable relleno de silica incluye válvula de control.
 - Suministro e instalación de protector térmico para compresor hermético.
 - Suministro e instalación de difusor móvil.
 - Suministro e instalación de aspas metálicas para ventilador-condensador.
 - Suministro e instalación de vibro aisladores para base de compresor.
 - Suministro e instalación de termostato.
 - Suministro e instalación de control remoto electrónico inalámbrico.
 - Suministro e instalación de interruptor de alta y baja presión.
 - Suministro e instalación de interruptor de alta y baja temperatura.
 - Suministro e instalación de display alfanumérico del módulo electrónico de control.
 - Suministro e instalación de mirilla para visualizar presencia de refrigerante.
 - Suministro e instalación de contactor auxiliar.
 - Suministro e instalación de relevador de tiempo (timer) para retraso de arranque de compresor.
 - Suministro e instalación de protección anticorrosiva.
 - Suministro e instalación de capacitor de arranque con relay integrado.
 - Suministro e instalación de filtro de aire (si la unidad no cuenta con el mismo).

- Suministro y completación de carga de refrigerante.

C. Actividades mínimas de mantenimiento correctivo en una unidad tipo Ventana de aire acondicionado

➤ Correctivo MAYOR:

- Suministro e instalación de serpentín de aluminio para evaporador.
- Reparación de serpentín de aluminio para evaporador.
- Suministro e instalación de serpentín de aluminio para condensador.
- Reparación de serpentín de aluminio para condensador.
- Reparación de tarjetas y/o módulos electrónicos.
- Suministro e instalación de moto ventilador.
- Suministro e instalación de compresor incluye recarga de refrigerante hasta su valor nominal.

➤ Correctivo MENOR:

- Detección y corrección de fugas de refrigerante incluye limpieza con nitrógeno, vacío y soldadura de plata; recarga de refrigerante hasta su capacidad nominal.
- Suministro e instalación de difusor móvil.
- Suministro e instalación de aspas metálicas.
- Suministro e instalación de termostato de características técnicas de acuerdo a especificación del fabricante o equivalente.
- Suministro e instalación de selector de velocidad.
- Suministro e instalación de perilla para control de temperatura.
- Suministro e instalación de rodamientos para moto ventilador.
- Suministro e instalación de capacitor.
- Suministro e instalación de protección anticorrosiva.
- Suministro e instalación de capacitor de arranque con relay integrado para compresor.
- Suministro e instalación de filtro de aire (si la unidad no cuenta con el mismo).
- Suministro y carga de refrigerante. Todo lo anterior según lo especificado en las bases de licitación.

SEGUNDA: MONTO DEL CONTRATO: El monto del contrato es por **SETECIENTOS DIECIOCHO MIL SETECIENTOS CUATRO LEMPIRAS EXACTOS (L. 718,704.00);** Oferta que incluye el Impuesto sobre ventas, el cual será retenido por el IPM.

TERCERA: FORMA DE PAGO: **EL INSTITUTO** pagará pagos mensuales según informe previamente revisado y aprobado por la División de Bienes y Seguridad Institucional del IPM.

CUARTA: SUPERVISIÓN POR PARTE DEL INSTITUTO: la División de Bienes y Seguridad Institucional del IPM nombrará un supervisor quien se encargará de verificar la calidad de los trabajos realizados y el cumplimiento del contrato por parte de **EL PROVEEDOR.-**

QUINTA: GARANTÍAS DEL PROVEEDOR: UNA GARANTÍA DE CUMPLIMIENTO DE CONTRATO por la cantidad de **CIENTO SIETE MIL OCHOCIENTOS CINCO LEMPIRAS CON 60/100 (L. 107,805.60)** en concepto del quince por ciento (15%) del monto total del Contrato, la cual tendrá una vigencia de quince (15) meses, contados a partir de la fecha en que se firme el presente contrato, dicha garantía deberá ser emitida al valor equivalente en Lempiras y por una Entidad Bancaria o Aseguradora establecida legalmente en el País, de reconocida experiencia y capacidad, y ser aceptada por **EL INSTITUTO.**

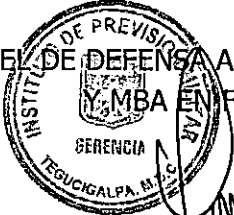
SEXTA: INCUMPLIMIENTO DEL CONTRATO: En caso de incumplimiento comprobado por parte del **PROVEEDOR** en las cláusulas convenidas y en el objeto del presente contrato, **EL INSTITUTO** hará efectiva la garantía de cumplimiento de contrato, con previa notificación a **EL PROVEEDOR.** De igual forma el Proveedor pagará la indemnización que conforme a Ley corresponda. - **SÉPTIMA: MULTAS:** **EL INSTITUTO** cobrará al **PROVEEDOR** una multa correspondiente al 0.036% del monto restante del contrato incumplido.

OCTAVA: CAUSAS DE DISOLUCIÓN DEL CONTRATO: Las partes contratantes podrán invocar cualesquiera de las causales de disolución del contrato tales como: **1)** El grave o reiterado incumplimiento de las cláusulas convenidas, **2)** La falta de constitución de las garantías a cargo del **PROVEEDOR** dentro de los plazos correspondientes; **3)** La declaración de quiebra o suspensión de pagos del **PROVEEDOR**, o su comprobada insolvencia financiera; **4)** Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor que surjan a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; **5)** El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; **6)** El mutuo acuerdo de las partes; **7)** Las demás que establezca expresamente este contrato, las especificaciones técnicas y las Leyes vigentes en la República; y, **8)** En caso de existir alguna orden de cambio y/o modificación no aprobada por la División de Bienes y Seguridad Institucional del IPM o alguna

modificación no contemplada por el **INSTITUTO**.- **NOVENA: CESIÓN, SUB CONTRATACIÓN, TRASPASO DEL CONTRATO: EL PROVEEDOR** no podrá ceder, subcontratar o traspasar lo estipulado en el presente contrato sin previo consentimiento por escrito del **INSTITUTO**. La aprobación de cualquier subcontratación no eximirá a **EL PROVEEDOR** de ninguna responsabilidad u obligación bajo los términos de este contrato. **EL PROVEEDOR** no podrá ceder su derecho a recibir pago conforme a lo estipulado en el presente contrato, sin previo consentimiento por escrito del **INSTITUTO**. - **DÉCIMA: SOLUCIÓN DE CONFLICTOS:** Si existiera alguna desavenencia en la interpretación y ejecución de este contrato y la misma no fuera solucionada por el buen entendimiento extrajudicial o la conciliación, ambas partes nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicarán las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. **DÉCIMA PRIMERA: CLAUSULA DE INTEGRIDAD:** Las partes en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y acceso a la información pública (LTAIP) y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a: 1. Mantener el más alto nivel de conducta, ética, moral y de respeto a las Leyes de la República así como los valores de: **INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS.** 2. Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia. 3. Que durante la ejecución del contrato ninguna persona que actué debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado autorizado o no, realizará a) **Prácticas Corruptivas:** entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) **Prácticas Colusorias:** entendiendo estas como aquellas en las que denoten, surjan o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de

alcanzar un propósito inadecuado incluyendo influenciar en forma inapropiada las acciones de la otra parte. 4. Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte, para efectos del contrato y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente, imprecisa o que no corresponda a la realidad para efectos de este contrato. 5. Mantener la debida confidencialidad sobre toda la información a la que se tenga acceso por razón del Contrato, y no proporcionarla, ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos. 6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta cláusula por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra. 7. Denunciar en forma oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al subcontratista, con los cuales el contratista o consultor contrate, así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar a: De parte del contratista o consultor: i. A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele a. La aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b. De parte del contratante a la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o que pudiendo hacerlo no denunciaron la irregularidad de su Registro de proveedores y contratistas que al efecto llevaré para no ser sujeto de elegibilidad futura en procesos de contratación. ii. A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. **DÉCIMA SEGUNDA:** **RESPONSABILIDADES: EL PROVEEDOR** se hace responsable por cualquier accidente de trabajo y pago de planilla de sus empleados. Además asume todas las responsabilidades legales, sociales y laborales prescritas en todas las leyes que se mantengan en vigencia en el país y que se deriven de las

relaciones obreras patronales que mantengan con todos los trabajadores que presten el servicio objeto del presente contrato de Servicios, obligaciones que correrán por cuenta de **EL PROVEEDOR**. - **DÉCIMA TERCERA:** **EL PROVEEDOR** se compromete a facilitar cualquier tipo de información de los Auditores Externos contratados por el **INSTITUTO**, referente a los montos y ejecución del presente contrato. **DÉCIMA CUARTA:** **VIGENCIA DEL CONTRATO:** La vigencia del presente contrato es de doce (12) meses a partir de la orden de inicio. En fe de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los un días del mes de julio del año dos mil veinticuatro.

CORONEL DE DEFENSA AEREA DEMA ACTUARIO
Y MBA EN FINANZAS

OTTO FABRICIO MEJIA HERCULES
EL INSTITUTO

LICENCIADO

JOSE ALEJANDRO JIMENEZ ROMERO
EL PROVEEDOR

"CONTRATO DE RENOVACIÓN DE LOS PRODUCTOS FORTINET DEL INSTITUTO DE PREVISIÓN MILITAR, SEGÚN LICITACIÓN PÚBLICA NO. IPM-LPN-GC-2024-002".

Nosotros, **OTTO FABRICIO MEJÍA HÉRCULES**, Coronel de Defensa Aérea D.E.M.A, Actuario y MBA en Finanzas, mayor de edad, casado, hondureño, con Documento Nacional de Identificación número 0501-1971-02586, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR (I.P.M.)** Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guion Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis (2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Ordinaria Número Quinientos Diecinueve (519) mediante Resolución Número Seis Mil Noventa y Siete (6097) de fecha Trece (13) de Diciembre del año Dos Mil Veintitrés (2023), y el Poder General de Representación y Administración otorgado mediante Instrumento Público Número dieciocho (18) autorizado en esta ciudad, ante los oficios del Notario David Alfonso Velásquez, el catorce (14) de Marzo del año dos mil veinticuatro (2024), e inscrito bajo el Número Treinta y Nueve (39) del Tomo Cuatrocientos Dieciséis (416) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO** y **JUAN CARLOS SORTO RIVERA**, mayor de edad, hondureño, casado, Ingeniero Industrial y en Sistemas, con domicilio en la Ciudad de Tegucigalpa; con Documento Nacional de Identificación número **0801-1978-04347**, RTN número **08011978043472** actuando en mi condición de Representante Legal de la Sociedad **JETSTEREO S.A. DE C.V.**, Sociedad con RTN No. **05019999400238** y constituida en escritura pública número 50 de fecha ocho (08) de agosto de mil novecientos sesenta y ocho (1968) autorizada por el Notario Arturo Humberto Montes, inscrita bajo el número 77, folio 345-349, Tomo 62 del Registro Mercantil de Tegucigalpa, Departamento de Francisco Morazán el 15 de diciembre de 1969, con facultades suficientes para la suscripción del presente contrato según Poder Especial de Administración otorgado mediante instrumento público número 21 de fecha 08 de agosto de 2019, por el Notario José Oswaldo Guillén Domínguez, inscrito número 55286 y Matricula 62846, del Registro Mercantil de Francisco Morazán, Centro Asociado al IP, y para efectos de este contrato me denominaré como **EL PROVEEDOR**, hemos convenido en celebrar el presente **CONTRATO DE RENOVACIÓN DE LOS PRODUCTOS FORTINET DEL INSTITUTO DE PREVISIÓN MILITAR, SEGÚN LICITACIÓN PÚBLICA NO. IPM-LPN-GC-2024-002**, Aprobado en Comité de Compras y Licitaciones No. 25-2024 celebrado el 26 de junio de 2024 y Resolución de fecha 26 de junio de 2024, el cual se regirá por las cláusulas y condiciones siguientes: **PRIMERA: OBJETO DEL CONTRATO:** la renovación de los productos Fortinet del IPM de acuerdo con los ítems siguientes:

I. ACTIVIDADES:

- 1. Analizar la infraestructura actual de los equipos de protección de redes con el objetivo de generar esquemas de trabajo para facilitar la transición de los equipos actuales a los nuevos equipos.
- 2. Desarrollar cronograma de tareas de cambio de equipos donde se especifique fecha, hora, actividades a realizar, tiempo de las actividades, responsables, insumos necesarios por parte del Instituto, posibles impactos, nivel de afectación del cambio.
- 3. Implementar las mejores prácticas en configuración para los equipos según normas internacionales.
- 4. Ejecutar pruebas de funcionalidad, de todos los servicios y conexiones del IPM.
- 5. Soporte local por parte del Proveedor, de todos los equipos Fortinet propiedad del IPM e informes mensuales. Esto posterior a la implementación.

II. PRODUCTOS ESPECIFICOS

- 1. Plan de Trabajo validado por el personal responsable del Instituto.
- 2. Documento de diagnóstico del estado actual de los equipos de protección de redes, este plan debe ser entregado dentro de los diez (10) días calendario posterior a la firma del contrato y debe ser aceptado por la Unidad de Seguridad de la Información del IPM, formando parte íntegra de este contrato.
- 3. Desarrollar un plan para la migración de equipos
- 4. Plan de montaje e implementación del hardware
- 5. Documentación sobre los cambios realizados y capacitación a los usuarios finales.
- 6. Evaluación de los cambios aplicados con el personal responsable del Instituto.
- 7. Diseño de la Red, con los equipos implementados.
- 8. Implementación de todos los equipos con la debida certificación de los servicios, mismo que será certificado por la Unidad de Seguridad de la Información.

III. CARACTERISTICAS FORTIGATE 600F

N° EQUIPO REQUISITOS TÉCNICOS		
1	Hardware Fortigate 600F (2)	Hardware Accelerated 10 GE SPF + Slots: 2
		Hardware Accelerated GE RJ45 Interfaces:8
		Hardware Accelerated GE SFP Slots:8
		GE RJ45 Management Ports:2
		USB Ports:2
		RJ45 Console Port :1



	Included Transceivers: 2x SFP (SX 1 GE)	
	IPS Throughput 10 Gbps:	
	NGFW Throughput: 9.5 Gbps	
	Threat Protection Throughput: 7 Gbps	
	IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP): 36 / 36 / 27 Gbps	
	IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP): 36 / 36 / 27 Gbps	
	Firewall Latency (64 byte, UDP): 1.54 μs	
	Firewall Throughput (Packet per Second): 40.5 Mpps	
	Concurrent Sessions (TCP): 8 Million New Sessions/Second (TCP) 450 000	
	Firewall Policies: 10 000	
	IPsec VPN Throughput (512 byte): 20 Gbps	
	Gateway-to-Gateway IPsec VPN Tunnels:2000	
	Client-to-Gateway IPsec VPN Tunnels: 50 000	
	SSL-VPN Throughput: 7 Gbps	
	Concurrent SSL-VPN Users: 10 000	
	SSL Inspection Throughput (IPS, avg. HTTPS): 8 Gbps	
	SSL Inspection CPS (IPS, avg. HTTPS):5500	
	SSL Inspection Concurrent Session (IPS, avg. HTTPS): 800 000	
	Application Control Throughput (HTTP 64K): 15 Gbps	
	CAPWAP Throughput (HTTP 64K): 18 Gbps	
	Virtual Domains (Default / Maximum): 10 / 10	
	Maximum Number of FortiSwitches Supported:96	
	Maximum Number of FortiAPs (Total / Tunnel): 1024 / 512	
	Maximum Number of FortiTokens:5000	
	High Availability Configurations: Active-Active, Active-Passive, Clustering	
	Height x Width x Length (inches): 1.75 x 17.0 x 15.0	
	Height x Width x Length (mm): 44.45 x 432 x 380	
	Weight: 16.1 lbs (7.3 kg)	
	Form Factor: Rack Mount, 1 RU	
	Power Source: 100–240V, 50/60 Hz	
	Power Consumption: (Average/ Maximum) 129 W / 244 W	
	Current (Maximum): 6A@100V	
	Heat Dissipation: 832 BTU/h	
Redundant Power Supplies: (Hot Swappable) Optional		
Características		
3	General	La solución debe consistir en una plataforma de protección de Red, basada en un

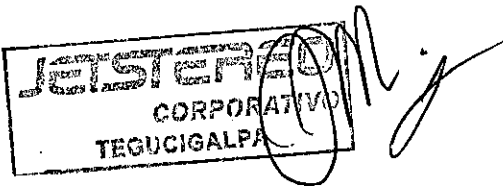
	dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo
	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7
	Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación
	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red
	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q
	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP
	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding
	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM)
	Los dispositivos de protección de red deben soportar DHCP Relay
	Los dispositivos de protección de red deben soportar DHCP Server
	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas
	Debe ser compatible con NAT dinámica (varios-a-1)
	Debe ser compatible con NAT dinámica (muchos-a-muchos)
	Debe soportar NAT estática (1-a-1)
	Debe admitir NAT estática (muchos-a-muchos);
	Debe soportar NAT de origen y NAT de destino de forma simultánea
	Debe soportar NAT de origen y NAT de destino en la misma política
	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico
	Debe soportar SD-WAN de forma nativa
	Debe soportar el balanceo de enlace hash por IP de origen
	Debe soportar el balanceo de enlace por hash de IP de origen y destino
	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
	Enviar logs a sistemas de gestión externos simultáneamente

	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red
	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL
	Debe soportar protección contra la suplantación de identidad (anti-spoofing)
	Implementar la optimización del tráfico entre dos dispositivos
	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP)
	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3)
	Soportar OSPF graceful restart
	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red
	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico
	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico
	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3
	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3
	La configuración de alta disponibilidad debe sincronizar: Sesiones;
	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red
	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN
	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace
	Debe soportar la creación de sistemas virtuales en el mismo equipo
	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.

		Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red
		La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad
		La consola de administración debe soportar como mínimo, inglés, Español y Portugués
		Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi
		La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas
		El Licenciamiento y soporte de la herramienta debe ser a 3 años. El soporte debe ser con Fabricante y a nivel local con el proveedor certificado. El proveedor, debe dar soporte presencial tanto preventivo como correctivo y generar informes relevantes de la herramienta Durante la vigencia del licenciamiento.
Firewall		
Funcionalidad		Debe soportar controles de zona de seguridad
		Debe contar con políticas de control por puerto y protocolo;
		Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones
		Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad
		Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
		Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall
		Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública
		Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
		Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes

		Debe soportar el protocolo estándar de la industria VXLAN;
		La solución debe permitir la implementación sin asistencia de SD-WAN
		En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN
		la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.
Threat Prevention		
	Protección contra amenazas	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
		Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware)
		Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante
		Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
		Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos
		Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
		Debe incluir la protección contra ataques de denegación de servicio
		Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo
		Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo
		Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP
		Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP
		Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc
		Detectar y bloquear los escaneos de puertos de origen
		Bloquear ataques realizados por gusanos (worms) conocidos
		Contar con firmas específicas para la mitigación de ataques DoS y DDoS
		Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow)

		Debe poder crear firmas personalizadas en la interfaz gráfica del producto
		Identificar y bloquear la comunicación con redes de bots
		Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo
		Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación
		Los eventos deben identificar el país que origino la amenaza
		Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
		Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP
		Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos
		En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles
		Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
URL Filter		
Filtrado de contenido	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	
	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito	
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL	
	Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL	



		Tener por lo menos 75 categorías de URL
		Debe tener la funcionalidad de exclusión de URLs por categoría
		Permitir página de bloqueo personalizada
		Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
		Explicit Web Proxy, soportar proxy web transparente
User Identity		
	Identificación y logueo de usuarios	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios
		Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
		Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios
		Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios
		Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD
		Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo)
		Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios
		Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD
		Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma



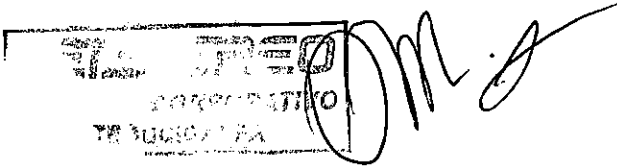
A handwritten signature in black ink, appearing to be "Mj" or similar, written in a cursive style.

		Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
QoS		
Calidad de Servicio	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming	
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen	
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino	
	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo	
	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube	
	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto	
	En QoS debe permitir la definición de tráfico con ancho de banda garantizado	
	En QoS debe permitir la definición de tráfico con máximo ancho de banda	
	En QoS debe permitir la definición de colas de prioridad	
	Soportar marcación de paquetes DiffServ, incluso por aplicación	
	Soportar la modificación de los valores de DSCP para Diffserv	
	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service)	
	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes	
Geo IP		
	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países	
	Debe permitir la visualización de los países de origen y destino en los registros de acceso	
	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de qusuario y la creación de políticas usando las mismas	
VPN		
	Soporte VPN de sitio-a-sitio y cliente-a-sitio	
	Soportar VPN IPSec	

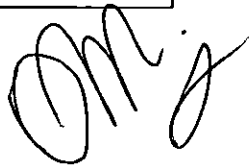
		Soportar VPN SSL
		La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
		La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14
		La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2)
		La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard)
		Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall
		Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec
		Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting
		Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy
		Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL
		Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local
		Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL
		El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS
		Deberá mantener una conexión segura con el portal durante la sesión

Wireless Controller		
		Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP)
		Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada
		Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador

	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor
	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS
	La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario
	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points
	El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico
	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC
	Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico
	Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica
	La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso
	La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso
	La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz


MINISTERIO DE EDUCACIÓN
DIRECCIÓN GENERAL DE ASesoría TÉCNICA
DIRECCIÓN DE ASesoría TÉCNICA

	La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm
	La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso
	La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y basada en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados
	La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;
	La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN
	La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming
	La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado
	La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitan para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac
	La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz
	La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID
	La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la

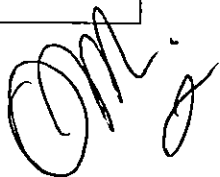


		actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución
--	--	---

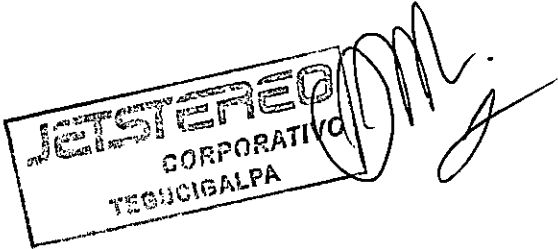
IV. CARACTERÍSTICAS FORTIMAIL 400F

N°	EQUIPO	REQUISITOS TÉCNICOS
	Hardware	10/100/1000 Interfaces (Copper, RJ45): 4
	FortiMail	Redundant Hot Swappable Power Supplies: No
	400F (1)	Storage: 2 x 1TB
		RAID Storage Management: Software 0,1
		Form Factor: Rack Mount, 1U
		Trusted Platform Module (TPM): Yes
Características		
	Generales	La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema
		La solución debe permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware.
		La solución debe poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
		La solución debe poder definir el reenvío de correo (relay) a una Ip específica con base a la IP origen del mensaje
		La solución debe proporcionar soporte para múltiples dominios de correo electrónico
		La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente.
		La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.
		La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web y POP3
		La solución debe ser capaz de programar el envío de informes de cuarentena
		La solución debe ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto

		La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega
		La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.
		La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP
		La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados.
		La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto.
		La solución debe tener características antispam, antivirus, anti-spyware y antiphishing
		La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente
		La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger
		La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb
		La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing
		El Licenciamiento y soporte de la herramienta debe ser a 3 años. El soporte debe ser con Fabricante y a nivel local con el proveedor certificado. El proveedor, debe dar soporte presencial tanto preventivo como correctivo y generar informes relevantes de la herramienta Durante la vigencia del licenciamiento.
Anti Spam		
	Filtro correo no deseado	La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam
		La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.
		La solución puede detectar si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante
		La revisión de URLs debe permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante.
		La solución debe contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correos recibidos y su posterior

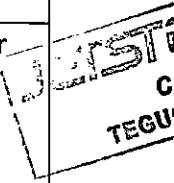


		correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM
		La solución debe ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo con el comportamiento del correo y así determinar si un correo es spam
		La solución debe ser capaz de realizar análisis Bayesiano para determinar si un correo es spam.
		La solución debe contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su comportamiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos.
		La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobre escribir el destinatario, Archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado
		La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP)
		La solución permite identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el analisis de las siguientes extenciones GIF, JPEG, PNG
		Configurar ambientes onpremise y en la nube de Microsoft.
Autenticación		
	Métodos	La solución debe poder validar si el destinatario del correo entrante es un buzón válido
		La solución debe ser compatible con Sender Policy Framework (SPF).
		La solución debe ser compatible con Domain Keys Identified Mail (DKIM)
		La solución debe ser compatible con Domain Based Message Authentication (DMARC)
		La solución debe identificar altos volúmenes de conexiones y aplicar limites basado en senders e Ips
		La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico
Administración		
	Métodos de Administración.	La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).
		mLa solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.



		La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)
		La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.
		La solución debe soportar doble factor de autenticación para el login de usuarios administradores

Alta Disponibilidad		
	Rendimiento de equipos.	La solución debe permitir esquemas de Alta disponibilidad, tanto Activo-Activo como Activo-Pasivo
		Cuando la solución se implementa para alta disponibilidad debe ser capaz de controlar el estado del enlace
		Cuando la solución se implementa para alta disponibilidad, para soportar la conmutación por falla de red.
		Cuando la solución se implementa para alta disponibilidad, debe ser capaz de sincronizar los mensajes de e-mails en cuarentena.
		Cuando la solución se implementa para alta disponibilidad activo / Pasivo debería ser posible sincronizar los mensajes de correo electrónico y configuraciones
		El modo de Activo-Pasivo debe soportar hasta 25 miembros en el cluster
		Cuando la solución se implementa para alta disponibilidad debe ser capaz de detectar y reportar el fallo de un dispositivo
Malware		
	Detección proactiva de amenazas	La solución debe contar con capacidades de evaluar, retener y/o bloquear correos que cuenten con amenazas avanzadas, Día zero mediante el análisis de archivos con herramientas de sandboxing
		Debe permitir el análisis de sandboxing con soluciones on premise o en la nube
		La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail
		La solución debe ser capaz de ejecutar el análisis antivirus / antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ, and RAR
		La solución debe contar con una base de datos de malware suministrada por el fabricante y Terceros aliados, la cual puede ser actualizada recurrentemente.

		Ante la detección de un malware, la solución puede ejecutar las siguientes acciones: enviar un mensaje de notificación en lugar del correo, reenviar el correo y el malware a una cuenta definida, reescribir el destinatario La solución debe poder re escanear los correos que son liberados de la cuarentena de SPAM por el usuario en busca de contenido malicioso
DLP		
	Data loss Prevention	También debe proporcionar una solución DLP para detectar la información sensible que puede estar llegando por e-mail. La funcionalidad DLP debe pemritir definir la información a detectar como palabras, frases y expresiones regulares. La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros. La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos. La funcionalidad DLP para permitir la creación de filtros por tipos de archivos; La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico. La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado
Logs		
	Registros y reportes	La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog). La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica. La solución debe generar informes por demanda o programados a intervalos de tiempo específicos La solución debe generar informes por demanda o programados a intervalos de tiempo específicos, ajustados a las necesidades del IPM.

V. RENOVACIÓN DE LICENCIAS

Dentro de los requerimientos, se encuentra la renovación de licencias de los equipos que se describen a continuación:

No.	Equipo	Renovación Hasta	Tipo
1	FortiAnalyzer	Jun-2027	Renovación
2	FortiGate-81E	Nov - 26	Renovación



3	FortiSwitch-224E	Jun-2027	Renovación
4	FortiSwitch-224E	Jun-2027	Renovación
5	FortiGate 600E	Jun-2027	Renovación
6	FortiGate 600E	Jun-2027	Renovación
7	FortiGate 80F	Jun-2027	Renovación
8	FortiGate 80F	Jun-2027	Renovación
9	FortiSwitch-224E	Jun-2027	Renovación

Durante la vigencia del licenciamiento: El Licenciamiento y soporte de todas las herramientas Fortinet propiedad del IPM debe ser a 3 años.

El proveedor, debe dar soporte presencial, preventivo como correctivo y generar informes relevantes de la herramienta con periodicidad mensual, el soporte y los informes deben ser **Durante la vigencia del licenciamiento.**

VI. LUGAR DE REALIZACION DE LOS SERVICIOS

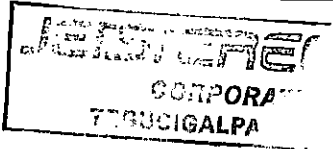
Los servicios se llevarán a cabo en las instalaciones del Instituto de Previsión Militar (SPS y TGU) en coordinación con la Unidad de Seguridad Información y Ciberseguridad y la División de Tecnología.

VII. PERFIL DEL PROVEEDOR

El proveedor deberá contar como mínimo con las siguientes calificaciones. plazo estimado para el cumplimiento, evidenciando con documentación lo siguiente:

- Se deberá contar con nivel más alto de partnership ante el fabricante.
- Tener certificación en los productos y representación, así como soporte local de los productos y servicios a otorgar a Grupo IPM.
- Evidenciar el Personal Certificado por el Fabricante para dar soporte a los equipos y tecnologías que se están adquiriendo y renovando.
- El personal que se somete como parte de los requisitos es el personal que va a atender el requerimiento.
- Se deberá crear un contrato de mantenimiento, el cual debe durar por la vigencia del licenciamiento, con informes mensuales.
- El proveedor deberá estar debidamente inscrito.
- El proveedor deberá asegurarse de tener toda la documentación vigente que los acredite como proveedores y lo que por normativa interna se les solicitará.

Todo lo anterior especificado en las bases de licitación. **SEGUNDA: MONTO DEL CONTRATO:** El monto del contrato es por **CUATRO MILLONES CINCUENTA Y CUATRO MIL QUINIENTOS SETENTA Y CUATRO LEMPIRAS CON 55/100 (L. 4,054,574.55).** Oferta que incluye el Impuesto sobre ventas y el cual será retenido por el Instituto. **TERCERA: FORMA**



DE PAGO: EL INSTITUTO realizará un pago único contra el informe de aceptación y satisfacción emitido por la Unidad de Seguridad de la Información del IPM. **CUARTA: SUPERVISIÓN POR PARTE DEL INSTITUTO:** La Unidad de Seguridad de la Información del IPM asignará una persona que se encargará de verificar la calidad de los servicios solicitados.- **QUINTA: GARANTÍAS DEL PROVEEDOR: UNA GARANTÍA DE CUMPLIMIENTO DE CONTRATO** por la cantidad de **SEISCIENTOS OCHO MIL CIENTO OCHENTA Y SEIS LEMPIRAS CON 18/100 (L. 608,186.18)** correspondiente al quince por ciento (15%) del monto total del Contrato, la cual tendrá una vigencia de nueve (9) meses, contados a partir de la fecha en que se inicie el presente contrato, **UNA GARANTÍA DE CALIDAD** por la cantidad de **DOSCIENTOS DOS MIL SETECIENTOS VEINTIOCHO LEMPIRAS CON 73/100 (L. 202,728.73)** correspondiente al cinco por ciento (5%) del monto total del Contrato, la cual tendrá una vigencia de doce (12) meses, contados a partir de la fecha en que se recepcionen a conformidad los bienes adquiridos. Ambas garantías deberán ser emitidas por una Institución Bancaria o Entidad Aseguradora establecida legalmente en el País, de reconocida experiencia y capacidad, y ser aceptada por EL INSTITUTO. - **SEXTA: INCUMPLIMIENTO DEL CONTRATO:** En caso de incumplimiento comprobado por parte del **PROVEEDOR** en las cláusulas convenidas y en el objeto del presente contrato, **EL INSTITUTO** hará efectiva la garantía de cumplimiento de contrato, con previa notificación a **EL PROVEEDOR**. De igual forma el Proveedor pagará la indemnización que conforme a Ley corresponda. - **SÉPTIMA: MULTAS:** EL INSTITUTO cobrará al **PROVEEDOR** una multa correspondiente al 0.036% del monto restante del contrato incumplido. **OCTAVA: CAUSAS DE RESOLUCIÓN DEL CONTRATO:** Las partes contratantes podrán invocar cualesquiera de las causales de disolución del contrato tales como: **1)** El grave o reiterado incumplimiento de las cláusulas convenidas, **2)** La falta de constitución de las garantías a cargo del **PROVEEDOR** dentro de los plazos correspondientes; **3)** En caso de muerte de **EL PROVEEDOR** y sus sucesores no pudieren concluir el Contrato; **4)** La declaración de quiebra o suspensión de pagos del **PROVEEDOR**, o su comprobada insolvencia financiera; **5)** Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor que surjan a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; **6)** El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; **7)** El mutuo acuerdo de las partes; **8)** Las demás que establezca expresamente este contrato, las especificaciones técnicas y las Leyes vigentes en la República; y, **9)** En caso de existir alguna orden de cambio y/o modificación no aprobada por la Unidad de Seguridad de la Información del IPM o alguna modificación no contemplada por el INSTITUTO.- **NOVENA: CESIÓN, SUB CONTRATACIÓN, TRASPASO DEL CONTRATO:** EL PROVEEDOR no podrá ceder, subcontratar o traspasar lo estipulado en el presente contrato sin previo consentimiento por escrito del INSTITUTO. La aprobación de cualquier subcontratación no eximirá a **EL PROVEEDOR** de ninguna responsabilidad u obligación bajo los términos de este contrato. **EL PROVEEDOR** no podrá ceder su derecho a recibir pago conforme a lo estipulado

en el presente contrato, sin previo consentimiento por escrito del INSTITUTO. - **DÉCIMA:**

SOLUCIÓN DE CONFLICTOS: Si existiera alguna desavenencia en la interpretación y ejecución de este contrato y la misma no fuera solucionada por el buen entendimiento extrajudicial o la conciliación, ambas partes nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicarán las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. **DÉCIMA PRIMERA: CLAUSULA DE INTEGRIDAD Y CONFIDENCIALIDAD:** Las partes en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y acceso a la información pública (LTAIP) y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a:

1. Mantener el más alto nivel de conducta, ética, moral y de respeto a las Leyes de la República así como los valores de: **INTEGRIDAD, CONFIDENCIALIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS.**
2. Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia.
3. Que durante la ejecución del contrato ninguna persona que actúe debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado autorizado o no, realizará a)

Prácticas Corruptivas: entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) **Prácticas Colusorias:** entendiendo estas como aquellas en las que denoten, surgieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado incluyendo influenciar en forma inapropiada las acciones de la otra parte.

4. Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte, para efectos del contrato y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente, imprecisa o que no corresponda a la realidad para efectos de este contrato.
5. Mantener la debida confidencialidad sobre toda la información a la que se tenga acceso por razón del Contrato, y no proporcionarla, ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos.
6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta cláusula por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra.
7. Denunciar en forma

oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al sub-contratista, con los cuales el contratista o consultor contrate así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar a: De parte del contratista o consultor: i. A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele a. La aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b. De parte del contratante a la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o que pudiendo hacerlo no denunciaron la irregularidad de su Registro de proveedores y contratistas que al efecto llevaré para no ser sujeto de elegibilidad futura en procesos de contratación. ii. A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. **DÉCIMA SEGUNDA:** EL **PROVEEDOR** se compromete a facilitar cualquier tipo de información a los Auditores Externos contratados por el **INSTITUTO**, referente a los montos y ejecución del presente contrato. **DÉCIMA TERCERA:** **VIGENCIA DEL CONTRATO:** La vigencia del presente contrato es de seis (6) meses a partir de la firma del contrato. En fé de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los diez (10) días del mes de julio del año Dos Mil veinticuatro (2024).

CORONEL DE DEFENSA AÉREA DEMA,
ACTUARIO Y MBA EN FINANZAS

OTTO FABRICIO MEJA HÉRCULES
EL INSTITUTO

INGENIERO

JUAN CARLOS SORTO RIVERA
EL PROVEEDOR
