| | |
|---|---|
| AGENCIA NACIONAL DE MINERÍA | **ANEXO 2**<br>**ESPECIFICACIONES Y REQUERIMIENTOS TÉCNICOS MÍNIMOS** |

## 1. OBJETO

Contratar la suscripción de Endpoints de última generación para la protección de los servidores donde se ejecutan las aplicaciones y herramientas de la agencia nacional de minería, y su administración centralizada (Línea del PAA 130007426).

### 1.1. ALCANCE DEL OBJETO:

El alcance de la presente contratación comprende la adquisición, implementación y puesta en operación de una suscripción de solución de seguridad de Endpoints de última generación, orientada a la protección de los servidores donde se ejecutan las aplicaciones y herramientas tecnológicas de la Agencia Nacional de Minería, durante la vigencia contractual.

En desarrollo del objeto, el contratista deberá suministrar una solución que cubra, como mínimo, los siguientes componentes:

- **Suscripción y licenciamiento**

  Suministro de las suscripciones requeridas para la protección de los servidores institucionales, incluyendo ambientes físicos, virtuales y/o en infraestructura en la nube, conforme a las necesidades definidas por la Entidad.

  El alcance contractual también contempla la disponibilidad permanente de actualizaciones, parches y soporte especializado del fabricante.

- **Protección avanzada de Endpoints (XDR)**

  La solución deberá contar con una plataforma unificada de ciberseguridad basada en IA que combine la gestión de exposición a riesgos cibernéticos, **IPS o mecanismos funcionalmente equivalentes** de prevención de intrusiones y/o explotación y/o comportamiento malicioso y capacidades de prevención, detección y respuesta frente a amenazas de ciberseguridad, incluyendo, entre otras, malware, ransomware, ataques sin archivos, monitoreo de cambios no autorizados en archivos críticos de los sistemas, binarios, librerías y configuraciones. Análisis inteligente de los logs de aplicaciones y sistemas operativos para detectar patrones de ataque y comportamientos anómalos, así como mecanismos de actualización automática y en tiempo real. Ofreciendo visibilidad completa de las identidades, dispositivos, activos en la nube y red, gestión proactiva de amenazas con inteligencia predictiva de riesgos, respuesta rápida a incidentes en todos los endpoints y sistemas.

- **Compatibilidad e integración**

  La solución deberá ser compatible con los sistemas operativos y plataformas tecnológicas existentes en la Entidad, permitiendo su integración sin afectar la disponibilidad, estabilidad y continuidad de los servicios institucionales.

- **Administración centralizada**

  Provisión de una **consola de administración centralizada** que permita la gestión unificada de los servidores protegidos, la definición y aplicación de políticas de seguridad, la visualización y correlación de eventos, la generación de alertas, la asignación de un **score de riesgo** por servidor o activo descubierto, la detección de comportamientos en tiempo real, la investigación de la cadena de ataque, la ejecución de respuestas automatizadas (por ejemplo, aislamiento, bloqueo y cuarentena) y la elaboración de reportes técnicos; así mismo, deberá habilitar, **de manera integrada**, las capacidades de **gestión de exposición**, **identificación y priorización contextual de vulnerabilidades basada en riesgos reales**, **evaluación de riesgos de identidad y acceso** (usuarios, cuentas y privilegios) y **descubrimiento de activos** (incluyendo identificación de puertos y servicios expuestos), las cuales podrán acreditarse mediante **módulos, servicios o componentes del mismo fabricante** de la solución ofertada, siempre que sean gestionables desde dicha consola y permitan obtener el resultado funcional requerido.
  Nota: esa consola puede ser suministrada en la infraestructura on premise de la entidad o como un servicio de software software (SaaS), por lo cual el ofetende debe suministrar el medio de instalación y asistir en dicha para realizar dicha tarea.

| Modalidad | Qué significa |
|---|---|
| SaaS | La consola de administración está alojada en la nube del fabricante o proveedor. La ANM accede por internet para administrar políticas, alertas, eventos y reportes. |
| On premise | La consola se instala dentro de la infraestructura de la ANM, por ejemplo en servidores propios, centro de datos o nube privada. |

- **Implementación y configuración**

  El oferente **se obliga** a prestar acompañamiento técnico especializado para la **instalación, configuración y puesta en funcionamiento integral de la solución mediante sesiones pactadas con la supervisión del contrato**, garantizando que dichas actividades se realicen de manera controlada y sin interrupciones significativas de los servicios misionales o afectación de la infraestructura. Este acompañamiento deberá realizarse **en todos los servidores establecidos por el supervisor** y durante **todas las sesiones técnicas que sean necesarias para la correcta implementación**, incluyendo, como mínimo, las actividades de instalación de componentes, configuración de parámetros, validación de funcionamiento, ejecución de pruebas y ajustes requeridos para la estabilización de la plataforma.

  La implementación, instalación, configuración y puesta en operación de la solución deberá ser ejecutada o liderada por al menos un profesional en ingeniera de sistemas, electrónica o afines con certificación oficial vigente del fabricante de la solución propuesta

- **Soporte y mantenimiento**

  Prestación del soporte técnico 7*24 durante la vigencia de la suscripción, incluyendo acceso a actualizaciones, parches de seguridad y asistencia especializada del fabricante o del proveedor autorizado.

  El oferente deberá prestar el servicio de atención de requerimientos e incidentes de primer nivel de lunes a viernes 5*8 durante la vigencia de la suscripción sin limitar el número de necesidades establecidos por la Agencia Nacional de Minería y que involucren directa o indirectamente la solución adquirida, acorde con los Acuerdos de Nivel de Servicios establecidos.

- **Transferencia de conocimiento**

  Realización de tres sesiones de capacitación o transferencia de conocimiento de 2 horas dirigidas al personal técnico designado por la Entidad, orientadas al uso, administración y operación básica de la solución implementada.

- **Cumplimiento normativo**

  La solución y los servicios asociados deberán cumplir con la normativa vigente en materia de seguridad de la información, protección de datos personales y ciberseguridad, así como con los lineamientos y políticas internas de la Entidad[1]

  Así las cosas, el alcance de esta contratación se extiende mucho más allá del simple aprovisionamiento de licencias de software. Implica el aseguramiento integral de los servidores donde residen las aplicaciones y herramientas nucleares de la Agencia, incluyendo ambientes físicos, virtuales y con proyección a nubes híbridas o públicas. La solución adquirida debe ser compatible con la diversidad de plataformas operativas, integrándose de manera transparente en el entorno tecnológico existente.

  Desde una perspectiva técnica, el alcance contempla funcionalidades avanzadas propias de soluciones de protección, detección y respuesta extendida —**EPP, EDR y/o XDR**—, incluyendo capacidades de prevención, detección, análisis y respuesta proactiva ante amenazas emergentes, protección frente a malware, ransomware, ataques sin archivos, explotación de vulnerabilidades y comportamientos maliciosos, junto con mecanismos de actualización automática y continua de los componentes de detección, prevención, inteligencia de amenazas,

[1] https://anm.gov.co/politicas-de-gestion-de-seguridad-de-la-informacion

reputación, reglas, modelos analíticos y demás elementos requeridos para su operación.

En este sentido, la solución deberá incorporar capacidades orientadas a la **gestión, reducción o mitigación del riesgo asociado a vulnerabilidades**, las cuales podrán acreditarse mediante funcionalidades nativas, módulos integrados o componentes complementarios de la solución ofertada. Para estos efectos, serán aceptables mecanismos tales como **parcheo virtual**, **Patch Management**, prevención de explotación de vulnerabilidades, control de aplicaciones, análisis de exposición, priorización basada en riesgo, endurecimiento de configuración adaptado por usuario/equipo según su comportamiento, bloqueo de comportamientos maliciosos, reglas de prevención de intrusiones, inteligencia de amenazas, aislamiento preventivo u otros enfoques funcionalmente equivalentes que permitan disminuir la superficie de ataque y reducir la probabilidad de explotación de vulnerabilidades conocidas o emergentes.

La acreditación de estas capacidades podrá realizarse mediante documentación técnica oficial del fabricante, fichas técnicas, manuales, guías de arquitectura, certificaciones, reportes de laboratorio, demostraciones técnicas o cualquier otro soporte verificable que evidencie que la solución propuesta permite identificar, priorizar, prevenir, mitigar o remediar riesgos derivados de vulnerabilidades en los servidores protegidos. No se exigirá que la funcionalidad corresponda exclusivamente a una tecnología específica, siempre que el oferente demuestre que el enfoque propuesto cumple de manera equivalente con el objetivo de reducir la exposición institucional frente a amenazas y vulnerabilidades.

Un valor fundamental en el alcance es la **administración centralizada**, habilitada por consolas que ofrezcan visibilidad y control sobre todos los servidores protegidos. Esta centralización deberá facilitar la gestión unificada de políticas, la configuración de controles de prevención y respuesta, la supervisión del estado de protección, la generación automatizada de alertas e informes, y la trazabilidad de eventos relevantes para la toma de decisiones y la reacción oportuna ante incidentes de seguridad.

## 2. CUADRO DE CANTIDADES:

Para el desarrollo y ejecución del objeto contractual, corresponde al contratista prestar los servicios enunciados en las especificaciones técnicas y características que se encuentran establecidas en el Anexo de Especificaciones y Requerimientos Técnicos Mínimos, en el que se mencionan los lineamientos para la ejecución del contrato.

A continuación, se especifican el producto y las cantidades a adquirir:

| Ítem | COD UNSPSC | DESCRIPCIÓN DEL PRODUCTO | UNIDAD DE MEDIA | CANTIDAD | MESES |
|---|---|---|---|---|---|
| 1 | 43231500, 43233200, 81111800, 81112200, 81112300; 80101500, 81111500; 81161500 | Suscripción de solución de seguridad de end point para servidores | Unidad | 300 | 12 |

## 3. ESPECIFICACIONES TECNICAS

Se requiere la adquisición de una solución de seguridad de endpoints de última generación para servidores integrados con herramientas de seguridad como firewalls, SIEM, entre otros. La protección integral de la infraestructura tecnológica de la Agencia Nacional de Minería exige implementar una estrategia de defensa en profundidad, en la que converjan diversas capas y herramientas de seguridad especializadas. La adquisición de una solución de seguridad de endpoints de última generación para servidores es un componente crítico dentro de este ecosistema de seguridad, y se justifica desde varias perspectivas técnicas y operativas:

### 3.1. Defensa Contra Amenazas Avanzadas

Los servidores constituyen el núcleo operativo y el repositorio de información crítica institucional. Son blancos recurrentes de ataques avanzados como ransomware, malware polimórfico, fileless attacks y movimientos laterales. Las soluciones modernas de protección de endpoints (EPP/XDR) ofrecen capacidades de monitoreo, detección y respuesta en tiempo real, complementando la protección perimetral proporcionada por firewalls y otras herramientas de seguridad tradicionales.

### 3.2. Integración y Orquestación de Seguridad

La solución debe permitir la integración mecanismos tales como API/Syslog/CEF/conectores con herramientas como:

- **Firewall**: La solución deberá contar con capacidad nativa de aislamiento (cuarentena) del endpoint afectado a nivel de host, y con capacidad de transmitir, mediante API, Syslog o CEF, los eventos y alertas de seguridad relevantes hacia el SIEM/SOAR y/o el firewall institucional. Las acciones de contención perimetral (bloqueo de direcciones IP, cierre de puertos) serán ejecutadas por el SIEM/SOAR institucional, con base en los eventos transmitidos por la solución de endpoint, garantizando su ejecución automatizada sin intervención manual.

- **SIEM** SIEM (Security Information and Event Management): la consola centralizada de endpoints deberá transmitir logs y alertas en tiempo real al SIEM institucional (Fortinet y Microsoft Sentinel), mediante conectores nativos, API, Syslog o CEF, permitiendo la correlación, auditoría y orquestación de eventos de seguridad a partir de múltiples fuentes. La capacidad de integración se acreditará mediante documentación técnica oficial del fabricante de la solución ofertada y/o documentación de integración publicada oficialmente por el fabricante del SIEM receptor

**Otros sistemas de seguridad**: La solución debera permitir la integración mediante API/Syslog/CEF/conectores con soluciones DLP, IDS/IPS y sistemas de escaneo de vulnerabilidades, creando un ecosistema de seguridad cohesionado y automatizable.

- Nota: la versión actual de firewall es FORTIGATE 1100E

### 3.3. Visibilidad y Control Centralizado

La administración centralizada de la protección de endpoints facilita el monitoreo de la postura de seguridad de todos los servidores desde un único panel. Esto optimiza la gestión de incidentes, el despliegue de políticas unificadas y la generación automática de alertas combinadas con otras fuentes de seguridad empresarial.

### 3.4. Cumplimiento Normativo y Reducción de Superficie de Ataque

La solución debe permitir integrar la defensa de endpoints en los servidores con firewalls y sistemas SIEM, en cumplimiento de las mejores prácticas internacionales (ISO 27001, NIST, etc.) y lineamientos del gobierno corporativo de TI, mitigando riesgos y facilitando auditorías de seguridad.

Todas las funcionalidades, gestión y procesamiento de información deberán cumplir con la normatividad vigente sobre protección de datos, ciberseguridad y lineamientos institucionales aplicables.

### 3.5. Respuesta Acelerada y Automatización

Se requiere la conjunción de endpoints inteligentes con un SIEM y firewall para: automatizar respuestas ante incidentes aislamiento del endpoint afectado a nivel de host (ejecutado de forma nativa por la solución de endpoint) y bloqueo de direcciones IP o cierre de puertos (ejecutado por el SIEM/SOAR institucional con base en los eventos recibidos de la solución de endpoint), entre otras acciones , disminuir el tiempo de detección y remediación, proporcionar trazabilidad completa

- 
- Visor de incidentes con línea de tiempo basado en modelos de Mitre ATT&CK que documentan tácticas, técnicas y procedimientos utilizados por atacantes en ciberseguridad.

La adquisición de una solución de endpoints de última generación para servidores, integrada a

los demás componentes del ecosistema de ciberseguridad institucional, responde a la necesidad de fortificar la defensa activa, lograr reacción coordinada y aumentar la resiliencia ante amenazas, alineándose con los lineamientos regulatorios y los objetivos estratégicos de protección de activos críticos de la Agencia.

### 3.6. Desempeño del antivirus en los equipos:

La solución de protección de endpoints EPP/EDR/XDR ofertada deberá estar diseñada y soportada por el fabricante para su operación en ambientes empresariales de servidores y deberá ser compatible con los sistemas operativos y demás componentes tecnológicos definidos por la Agencia Nacional de Minería en el presente Anexo.

### 3.7. Cobertura y compatibilidad multiplataforma

La solución deberá ofrecer cobertura integral de los servidores de la ANM, incluyendo ambientes físicos, virtuales y, en caso de requerirse, nubes privadas y públicas. El software deberá ser compatible con los principales sistemas operativos institucionales tales como Windows 2019 @ Windows 2025, Linux RHEL y sus distribuciones derivadas**,** acorde a la siguiente distribución, sin limitarse a ella:

| Sistema Operativo | Cantidad |
|---|---|
| Windows 2016/19 | 133 |
| Oracle Linux | 52 |
| Linux | 30 |
| Otros Linux | 85 |
| **TOTAL** | 300 |

Los Sistemas Operativos institucionales son los siguiente:

| Sistema operativo | Cantidad |
|---|---|
| Debian GNU/Linux 10 (64-bit) | 1 |
| Debian GNU/Linux 9 (64-bit) | 1 |
| Microsoft Windows Server 2016 (64-bit) | 16 |
| Microsoft Windows Server 2016 or later (64-bit) | 54 |
| Microsoft Windows Server 2019 (64-bit) | 35 |
| Microsoft Windows Server 2022 (64-bit) | 24 |
| Microsoft Windows Server 2025 (64-bit) | 22 |
| Oracle Linux 7 (64-bit) | 3 |
| Oracle Linux 8 (64-bit) | 13 |
| Oracle Linux 9 (64-bit) | 9 |
| Oracle Linux Server 7.9 | 9 |
| Oracle Linux Server 8.10 | 1 |
| Oracle Linux Server release 7.9 | 7 |
| Red Hat Enterprise Linux 7 (64-bit) | 24 |
| Red Hat Enterprise Linux 8 (64-bit) | 7 |
| Red-hat 7,4 | 4 |
| Rocky Linux (64-bit) | 1 |
| SUSE Linux Enterprice 15 | 1 |
| SUSE Linux Enterprise 12 (64-bit) | 1 |
| Ubuntu Linux (64-bit) | 7 |

| | |
|---|---|
| Crecimeinto esperado 2027 | 20 |

El producto ofertado deberá disponer de, al menos, las siguientes capacidades:

- Prevención, detección y respuesta ante amenazas avanzadas (XDR).
- Protección contra código malicioso, ransomware y ataques sin archivos.
- Funcionalidades de control de aplicaciones. Preferiblemente que permita la detección de vulnerabilidades y protección o contención de estas sin aplicar parches físicos en los servidores.
- Actualizaciones automatizadas y entrega de inteligencia de amenazas en tiempo real.
- Capacidad de aislamiento y contención en caso de incidente.
- Integración con sistemas de eventos y monitoreo de seguridad (SIEM), conforme a las prácticas del sector.

### 3.8. Administración centralizada

La solución debe incorporar una consola para administración centralizada y unificada, que permita:

- Supervisar el estado y la seguridad de todos los activos protegidos de manera consolidada.
- Implantar y ajustar políticas de protección y configuración.
- Generar reportes, alertas y auditoría de actividades.
- Permitir trazabilidad en la gestión de incidentes y acciones de remediación.

### 3.9. Soporte especializado

El contratista proveerá soporte remoto y/o presencial de nivel especializado durante la vigencia de la suscripción. Se deberá tener en cuenta los Acuerdos de Niveles de Servicio señalados en el presente documento.

### 3.10. Transferencia de conocimiento:

Realizar la transferencia tecnológica de conocimiento en instalación, configuración, administración del endpoint y su consola de administración centralizada instaladas en la ANM a por lo menos a dos (2) personas de la Oficina de Tecnología e Información que sean designados para tal fin por un periodo mínimo de diez (10) horas. La transferencia tecnológica de conocimiento no tendrá costo adicional para la Entidad.

### 3.11. Vigencia y mantenimiento de la suscripción:

La suscripción contratada deberá estar vigente por el término de doce (12) meses, contados a partir de la activación, garantizando acceso continuo a actualizaciones, nuevas versiones, parches de seguridad y soporte del fabricante.

## 4. ACTIVIDADES A REALIZAR:

1. Suministro y habilitación de suscripciones: El contratista será responsable de suministrar suscripciones activas de una solución de protección de endpoints (EPP/EDR/XDR) de última generación, diseñadas para ser implementadas en los servidores que soportan las aplicaciones y herramientas de la Agencia Nacional de Minería, la cantidad estipulada en este proceso es de trescientas (300) unidades durante doce (12) meses contados a partir del día de de la activación.

En todo caso, la activación del antivirus deberá llevarse a cabo durante los treinta (30) días siguiente a la suscripción del acta de inicio. Durante este término, se deberán realizar todas las tareas de preparación para el inicio de instalación y despliegue.

2. Suministro y habilitación de suscripciones de administración centralizada: El contratista será responsable de suministrar suscripciones activas de una solución o consola de administración centralizada, que permita: Supervisar el estado y la seguridad de todos los activos protegidos de manera consolidada, la cantidad estipulada en este proceso es de una unidad.

3. Implementación y despliegue El proveedor será responsable de la instalación, configuración inicial y puesta en producción de la solución, asegurando continuidad operacional y mitigan-do

interferencias sobre los servicios implementados en los servidores, sin superar los 60 dias después de la activación de la suscripción de los endpoints.

## 6. ACUERDOS DE NIVELES DE SERVICIOS

El oferente para la respuesta de primer nivel deberá acogerse a los Acuerdos de Niveles de Servicio de la Entidad, los cuales son:

| PRIORIDAD | DESCRIPCIÓN | TIEMPO DE RESPUESTA | TIEMPO MÁXIMO DE SOLUCIÓN |
|---|---|---|---|
| ALTA | Falla que afecte la disponibilidad de uno de los servicios tecnológicos de la ANM 7x24 | Inmediato, Máximo 15 minutos | 1 hora |
| MEDIA | Falla que afecte alguna de las funcionalidades del servicio 5x8 | Máximo 1 hora | 2 horas |
| BAJA | Reporte, consulta o solicitud que no afecte la prestación de los servicios tecnológicos 5x8 | Máximo 12 horas | 12 horas |

Para el caso de incidentes la ANM realizará la priorización del requerimiento con base en la siguiente metodología:

**Definición de prioridades**

El nivel de prioridad se basa esencialmente en el impacto y la urgencia así:

**Impacto:**

| Nivel de impacto | Descripción | Puntaje |
|---|---|---|
| Crítico | Afectación total del servicio o información en cualquiera de las sedes. El incidente afecta activos de información considerados de impacto catastrófico y mayor, que influyen directamente a los objetivos misionales. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata. | 4 |
| Alto | Afecta a un usuario VIP (servicio o información del mismo) o un servicio crítico; afecta una dependencia completa o toda una sede. | 3 |
| Medio | Afectación tecnológica o de información de muchos usuarios, el incidente afecta activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado. | 2 |
| Bajo | Afectación tecnológica o de información de un único usuario. El incidente afecta activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto. | 1 |

***Tabla 1 Niveles de Impacto***

**Urgencia:**

| Nivel de urgencia | Descripción | Puntaje |
|---|---|---|
| Crítico | El incidente afecta el servicio o información que involucra a varias de las partes interesadas(por ejemplo, entes de control, ciudadanos). | 4 |
| Alto | El incidente afecta gravemente el servicio o la información que involucra uno o varios procesos de la ANM. | 3 |
| Medio | El incidente interrumpe actividades o afecta información que no son criticas para la entidad y afecta a una persona o a un grupo máximo 3 personas pequeño de personas. | 2 |
| Bajo | El incidente no afecta el normal funcionamiento de la ANM | 1 |

***Tabla 2 Niveles de Urgencia***

**Priorización:**

La priorización se realiza a través de una operación matemática resultante de la multiplicación entre el valor asignado a la urgencia y al impacto; el resultado obtenido determina el nivel de prioridad de acuerdo con el mapa de calor de la siguiente imagen.:
Priorización= impacto x urgencia




| | | IMPACTO | | | |
|---|---|---|---|---|---|
| | | Menor (Bajo) | Moderado (Medio) | Mayor (Alta) | Bloqueante (Crítico) |
| URGENCIA | | 1 | 2 | 3 | 4 |
| Crítica | 4 | 4 | 8 | 12 | 16 |
| Alta | 3 | 3 | 6 | 9 | 12 |
| Media | 2 | 2 | 4 | 6 | 8 |
| Baja | 1 | 1 | 2 | 3 | 4 |

*Tabla 3 Manejo de Prioridad*

**7. CONDICIONES GENERALES**

El proponente que resulte adjudicatario de este proceso se deberá comprometer a:

**7.1.** Garantizar que las actividades desarrolladas durante la ejecución del contrato no interferirán en la continuidad, disponibilidad, integridad e interoperabilidad de los servicios de TI de la Agencia.

**7.2.** Garantizar la integridad y confidencialidad de la información institucional a la que tenga acceso -directamente o por intermedio de terceros- durante la ejecución del contrato y adoptar todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración o utilización indebida.

**7.3.** Presentar los informes que requiera la entidad, a través del supervisor del contrato o desu apoyo.

**7.4.** Asumir los gastos de desplazamiento a los centros de datos principal y alterno de la Agencia, para la realización del mantenimiento preventivo o correctivo, el cambio y/o configuración que se requiera para la solución del problema y/o falla presentada, sin costo adicional para la Entidad.

**7.5.** Garantizar que el soporte y actualización sea prestado por un especialista, debidamente certificado por el fabricante, que garantice su idoneidad para la prestación de estos servicios.

**8. CERTIFICACIONES DEL OFERTENTE:**

**8.1. ANEXO ESPECIFICACIONES TÉCNICAS MÍNIMOS REQUERIDOS**

Serán habilitados los proponentes que cumplan con todas las especificaciones y requisitos establecidos en el ANEXO ESPECIFICACIONES Y REQUERIMIENTOS TÉCNICOS MÍNIMOS, para lo cual el proponente deberá adjuntar dicho documento debidamente diligenciado y firmado, en el que declare su conocimiento y aceptación de las condiciones y requerimientos técnicos aplicables al mismo.

**NOTA 1:** Con la presentación de la oferta, el proponente deberá aportar la ficha técnica (datasheet) o documentación técnica oficial del fabricante de la solución ofertada, que permita verificar el cumplimiento de las especificaciones técnicas mínimas establecidas en el ANEXO ESPECIFICACIONES Y REQUERIMIENTOS TÉCNICOS MÍNIMOS del proceso

**8.2. CERTIFICACIONES DEL PROPONENTE:**

8.4.2.1. El proponente deberá aportar certificado emitido directamente por el fabricante donde exprese que el proponente es canal o distribuidor autorizado de la solución ofertada. La

mencionada certificación debe encontrarse vigente al momento de cierre del proceso.

8.4.2.2.

NOTA 1: En caso de Unión Temporal, consorcio o cualquier otra figura de proponente plural, las certificaciones podrán ser aportadas por cualquiera de sus integrantes.

**CONOCEMOS, ACEPTAMOS Y NOS COMPROMETEMOS A CUMPLIR CON TODOS LOS REQUERIMIENTOS MÍNIMOS OBLIGATORIOS, ESTABLECIDOS EN ESTE DOCUMENTO, LOS CUALESSE ENTIENDEN COMO OFERTA TÉCNICA MÍNIMA.**

**RAZON SOCIAL OFERENTE:** _____
**NOMBRE DEL OFERENTE:** _____
**DIRECCIÓN DE CONTACTO:** _____
**TELEFONO DE CONTACTO** _____
**CORREO ELECTRÓNICO DE CONTACTO:** _____
**FIRMA DEL OFERENTE:** _____