MUNICIPIO DE TOCANCIPÁ

ADENDA No. 01

PROCESO DE SELECCIÓN ABREVIADA POR SUBASTA INVERSA No. SASI 006 MT 2026

El Municipio de Tocancipá se permite informar a los interesados y futuros oferentes dentro de la **SASI 006 MT 2026** cuyo objeto es **"ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE PLATAFORMAS DE CIBERSEGURIDAD QUE PERMITAN CORRELACIONAR SOLUCIÓN PROTECCIÓN DE ENDPOINT Y SERVIDORES CON EDR Y XDR Y PROTECCIÓN DE CORREO PARA LA ALCALDÍA DE TOCANCIPÁ"**, que de acuerdo a las observaciones presentadas al Pliego Definitivo de carácter técnico y la respuesta emitida por las dependencias responsables del proceso a través del memorando **823/26,** y según lo establecido en el cronograma, la entidad en aras de garantizar el principio de transparencia, economía y publicidad entre otros, a continuación y a través de la presente Adenda, se relacionara la información ajustada y que hará parte integral del Pliego Definitivo y las **ESTABLECIDAS EN LA PLATAFORMA DEL SISTEMA ELECTRONICO DE CONTRATACION PUBLICA - SECOP II.**

PRIMERO: MODIFICACIÓN DEL NUMERAL 3.3.2. — CERTIFICACIÓN DE DISTRIBUIDOR AUTORIZADO, QUEDARA DE LA SIGUIENTE MANERA:

El proponente deberá presentar certificación expedida por el fabricante de la solución de ciberseguridad ofertada (o por su mayorista autorizado en Colombia), con una fecha de expedición no superior a treinta (30) días calendario previos a la fecha de cierre del proceso. En dicho documento, El proponente deberá acreditar, mediante carta de la fabricante dirigida al proceso SASI 006 MT 2026 y expedida dentro del término previsto en el pliego, que mantiene una relación comercial vigente con el fabricante y señalar expresamente el nivel de membresía que ostenta en el programa de canales para Colombia. Para efectos de habilitación, se aceptará alguno de los dos (2) niveles más altos de membresía reconocidos por el fabricante para su programa de canales en Colombia.

La carta deberá identificar al proponente y al fabricante y permitir verificar el nivel certificado con capacidad para comercializar, implementar y prestar el soporte técnico oficial de las licencias requeridas.

Con el fin de garantizar la pluralidad de oferentes y la libre concurrencia, la solución o tecnología ofertada deberá contar con al menos dos (2) distribuidores, aliados o partners habilitados en Colombia que pertenezcan a alguno de los dos (2) niveles más altos de membresía establecidos por el fabricante para su programa de canales en Colombia.

Asimismo, la solución de ciberseguridad propuesta deberá figurar como reconocida o evaluada en el mercado dentro de informes o cuadrantes de firmas especializadas en análisis de tecnología (como Gartner, Forrester, IDC o equivalentes), correspondientes a las últimas dos (2) vigencias.

NOTA: En caso de proponentes plurales cualquiera de los integrantes del consorcio o unión temporal podrá acreditar dicho requisito.

SEGUNDO: MODIFICACIÓN DEL NUMERAL 3.3.3. — CARTAS Y CERTIFICACIONES, QUEDARÁ DE LA SIGUIENTE MANERA:

El proponente deberá aportar certificación expedida por el fabricante de cada solución ofertada o por su mayorista autorizado en Colombia, dirigida al presente proceso de selección SASI 006 MT 2026, en la cual se certifique expresamente que mantiene una relación comercial vigente y que pertenece a alguno de los dos (2) niveles más altos de membresía establecidos por el fabricante para su programa de canales en Colombia. La certificación deberá indicar expresamente el nivel de membresía que ostenta el proponente. No será suficiente acreditar únicamente la condición de distribuidor o partner autorizado sin especificar dicho nivel.

Las soluciones presentadas deben ser reconocidas en el mercado de ciberseguridad por evaluadores correspondientes.

Para contar con una solución reconocida en el mercado, confirmar que el fabricante de la solución ofertada debe tener cobertura sobre los entornos Windows y Linux, debe respaldar sus tácticas de ciberseguridad por MITRE ATT&CK. Capacidad de correlacionar o mapear detecciones y técnicas identificadas por la solución con la matriz MITRE ATT&CK se acreditará mediante documentación oficial del fabricante o documentación técnica verificable de la solución ofertada.

TERCERO: Se realizarán las siguientes modificaciones al **ANEXO No. 1 — FICHA TÉCNICA:**

1. ACLARACIÓN Y ARMONIZACIÓN
2. LA DLP BÁSICO PARA SERVIDORES.
3. ACLARACIÓN DE LA ARQUITECTURA DE PROTECCIÓN Y CONSOLAS.

La ficha técnica DEL ANEXO No. 01 y formulario 5 y 7, quedará de la siguiente manera:

DESCRIPCION DEL BIEN	CANT
SOLUCIÓN INTEGRAL Y UNIFICADA ANTIMALWARE PARA ENDPOINTS Solución integral de seguridad antimalware para endpoints, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar y aplicar políticas de seguridad para la prevención de amenazas, el control de acceso, la protección de datos, el despliegue y la actualización de agentes. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá cumplir, como mínimo, con las siguientes características: • **Gestión basada en la nube (SaaS):** deberá operar sin requerir infraestructura local dedicada para la administración de la solución. • **Consola de administración centralizada:** deberá permitir administrar las capacidades de protección de endpoints y servidores ofertadas, sus políticas de seguridad, informes, despliegue y actualización de agentes desde una misma consola SaaS centralizada. La protección del correo electrónico podrá ser suministrada por un fabricante diferente, con su propia consola SaaS, siempre que cumpla integralmente los requisitos establecidos para dicho componente y se acredite la integración mediante API o conectores para el intercambio de información y la correlación de eventos. • **Agente único:** la protección de endpoints y servidores deberá operar mediante un agente único que integre las funciones de prevención de amenazas, EDR, XDR, firewall de host y DLP básico, administradas desde una misma consola SaaS centralizada. La integración posterior de eventos mediante SIEM, Syslog o API no sustituye la exigencia de agente único ni la capacidad de respuesta y bloqueo unificado en tiempo real. Las funcionalidades complementarias deberán estar incluidas en la solución propuesta y su licenciamiento deberá identificarse claramente. • **Soporte multiplataforma:** deberá soportar, como mínimo, los sistemas operativos empresariales Windows (escritorio y servidor), macOS y Linux, de acuerdo con las versiones y condiciones de compatibilidad establecidas en la ficha técnica. • **Despliegue y actualizaciones centralizadas:** deberá permitir gestionar centralizadamente el despliegue, configuración y actualización de los agentes instalados en los endpoints protegidos. • **Alta disponibilidad y escalabilidad:** deberá contar con capacidades que permitan mantener la disponibilidad del servicio y ampliar la cobertura de protección según las necesidades de la Entidad. • **Prevención de ejecución de malware:** deberá detectar y bloquear amenazas conocidas mediante mecanismos de protección antimalware. • **Detección basada en análisis heurístico y comportamental:** deberá utilizar mecanismos de análisis heurístico, comportamiento, inteligencia artificial o aprendizaje automático para detectar y bloquear malware de día cero, amenazas polimórficas y otras amenazas avanzadas. • **Protección contra ransomware:** deberá detectar comportamientos asociados con procesos de cifrado malicioso y permitir su bloqueo o contención, así como las acciones de remediación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología o denominación comercial específica. • **Detección y respuesta en endpoints (EDR):** deberá recolectar y analizar telemetría de los endpoints, proporcionar visibilidad de la cadena de eventos de un ataque y permitir la investigación de incidentes de seguridad y la ejecución de las acciones de respuesta disponibles en la solución.	500

• **Análisis y control de aplicaciones:** deberá permitir identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas, conforme a las políticas de seguridad configuradas. • **Control de dispositivos periféricos:** deberá permitir gestionar y controlar el uso de dispositivos USB y otros medios removibles, conforme a las políticas definidas por la Entidad. • **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. • **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección por reputación de URL maliciosas, por sí sola, no acreditará el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y acreditar que está incluida en el licenciamiento propuesto. • **Prevención básica de pérdida de datos (DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles. El proponente deberá especificar los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria para cumplir este requisito deberá identificarse expresamente e incluirse en la oferta económica. • **Análisis de comportamiento, investigación de amenazas y protección anti-exploit:** cuando estas capacidades sean exigidas en los documentos del proceso, podrán acreditarse mediante funcionalidades equivalentes de la solución ofertada, siempre que la documentación oficial del fabricante demuestre el cumplimiento de las capacidades técnicas requeridas. • **Soporte técnico del fabricante:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana (24/7), durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. • El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas e identificar las funcionalidades y licencias incluidas en la solución. La aceptación de equivalencias funcionales no exime del cumplimiento de los requisitos técnicos mínimos establecidos en la presente ficha.	
SOLUCIÓN INTEGRAL DE PROTECCIÓN ANTIMALWARE PARA SERVIDORES Solución de seguridad antimalware para servidores, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar políticas de seguridad, prevenir amenazas, controlar el acceso, proteger los datos y gestionar el despliegue y las actualizaciones de los agentes desde la plataforma de administración. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá proporcionar capacidades de prevención, detección y respuesta en servidores, incluyendo EDR y correlación XDR con los endpoints protegidos, conforme a los requisitos técnicos establecidos en este ítem. Deberá cumplir, como mínimo, con las siguientes características: 1. **Soporte extendido para sistemas operativos de servidor:** deberá ser compatible con los sistemas operativos y versiones de servidor exigidos en la ficha técnica, proporcionando las funcionalidades de prevención, EDR y correlación XDR disponibles para cada versión. El proponente deberá acreditar la compatibilidad y las capacidades efectivamente soportadas mediante documentación oficial del fabricante. 2. **Visibilidad EDR en tiempo real:** deberá recolectar y permitir consultar telemetría de seguridad de los servidores protegidos, incluida la actividad de red entrante y saliente, de acuerdo con las capacidades de la solución y las limitaciones del sistema operativo.	10

3. **Correlación XDR y detección de movimiento lateral:** deberá permitir correlacionar eventos de seguridad entre los servidores protegidos y los endpoints de usuario, con el propósito de identificar incidentes, comportamientos sospechosos y posibles movimientos laterales dentro del entorno tecnológico de la Entidad. 4. **Control de aplicaciones mediante listas de permitidos (whitelisting):** deberá permitir establecer políticas para autorizar la ejecución de aplicaciones y servicios previamente aprobados y restringir aquellos que no estén autorizados, conforme a las capacidades de la solución ofertada. 5. **Control de acceso y puertos de red:** deberá permitir definir políticas de control de acceso y comunicaciones de red para los servidores, de acuerdo con sus funciones y roles, conforme a las capacidades de la solución y del sistema operativo. 6. **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. 7. **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección de URL maliciosas basada únicamente en reputación no acreditará, por sí sola, el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y demostrar que está incluida en el licenciamiento propuesto. 8. **Prevención básica de pérdida de datos (Data Loss Prevention — DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles, de acuerdo con las capacidades compatibles con el sistema operativo del servidor. El proponente deberá especificar las funcionalidades, los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria deberá identificarse expresamente e incluirse en la oferta económica. 9. **Soporte técnico del fabricante 24/7:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas, la compatibilidad con los sistemas operativos y versiones correspondientes, y las funcionalidades incluidas en el licenciamiento ofertado. La instalación del agente, por sí sola, no acreditará el cumplimiento de todas las capacidades requeridas.	
1. SOLUCIÓN INTEGRAL DE PROTECCIÓN DE CORREO ELECTRÓNICO Solución de seguridad para la protección del correo electrónico institucional, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que combine capacidades de filtrado multicapa y tecnologías de inteligencia artificial para detectar, prevenir y bloquear amenazas avanzadas, incluyendo phishing, ransomware, suplantación de identidad y ataques de compromiso de correo empresarial (BEC). Deberá incorporar mecanismos de análisis de archivos adjuntos y URL, sandbox en la nube, protección contra correo no deseado y malware, cifrado de mensajes, políticas de prevención de pérdida de datos (DLP), autenticación del remitente y administración de cuarentena. La solución deberá integrarse con Microsoft 365 mediante API, sin interrupción del flujo de correo electrónico, y contar con una consola de administración centralizada que permita configurar políticas, supervisar eventos de seguridad, gestionar mensajes sospechosos y generar informes de las actividades de protección. La solución deberá cumplir, como mínimo, con las siguientes características:	400

- **Protección contra phishing y suplantación de identidad:** deberá detectar y bloquear intentos de phishing, suplantación de identidad y ataques BEC mediante el análisis del contenido, contexto y características de los mensajes. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una técnica específica de procesamiento de lenguaje natural o una tecnología determinada de inteligencia artificial.
- **Autenticación del correo electrónico:** deberá soportar los mecanismos SPF, DKIM y DMARC para validar la autenticidad de los remitentes y contribuir a la detección de mensajes fraudulentos.
- **Análisis de reputación:** deberá disponer de mecanismos para analizar la reputación de remitentes, dominios y direcciones IP, con el propósito de identificar mensajes potencialmente maliciosos o no deseados.
- **Protección antispam y antimalware:** deberá incorporar filtrado antispam, análisis de malware y sandbox en la nube para el análisis dinámico de archivos adjuntos y otros elementos potencialmente maliciosos.
- **Detección y reescritura de URL:** deberá detectar URL maliciosas y permitir la reescritura de enlaces para verificar su seguridad en el momento en que el usuario haga clic. Asimismo, deberá detectar anomalías en los encabezados de los mensajes que puedan indicar suplantación o actividad sospechosa.
- **Filtrado por país e idioma:** deberá permitir aplicar reglas de filtrado o tratamiento de mensajes según el país de origen y el idioma, conforme a las capacidades de la solución ofertada.
- **Detección de suplantación de nombres visibles:** deberá permitir analizar los nombres para mostrar de los remitentes e identificar posibles suplantaciones de personas VIP, directivos, usuarios o marcas de la Entidad.
- **Detección de dominios similares:** deberá identificar dominios similares al dominio legítimo de la Entidad o a dominios de confianza, con el fin de detectar posibles intentos de suplantación y fraude.
- **Prevención de pérdida de datos (DLP):** deberá permitir configurar políticas DLP con múltiples reglas aplicables a grupos y usuarios individuales, incluyendo controles sobre información financiera, contenidos confidenciales, información relacionada con la salud y datos personales identificables (PII).
- **Cifrado de comunicaciones mediante TLS:** deberá soportar TLS para proteger las comunicaciones de correo electrónico durante el transporte, conforme a las capacidades de la solución y las condiciones de interoperabilidad aplicables.
- **Compatibilidad con S/MIME:** deberá soportar el estándar S/MIME para el cifrado y la firma digital de mensajes, de acuerdo con las funcionalidades y condiciones de licenciamiento ofertadas.
- **Autenticación del remitente:** deberá contar con mecanismos para verificar la autenticidad de los remitentes y detectar posibles falsificaciones, de acuerdo con las funcionalidades requeridas.
- **Cifrado de mensajes y archivos adjuntos:** deberá permitir proteger mensajes y archivos adjuntos sensibles mediante mecanismos de cifrado con entrega protegida al destinatario (push encryption), conforme a las políticas de seguridad configuradas.
- **Protección del correo entrante y saliente:** deberá analizar los mensajes entrantes para detectar amenazas, spam, suplantación y contenido malicioso, así como aplicar controles al correo saliente para prevenir fugas de información y el envío de mensajes maliciosos o no autorizados.
- **Administración granular de políticas:** deberá permitir configurar y aplicar políticas de seguridad a nivel de dominio, grupo y usuario individual.
- **Administración de cuarentena:** deberá permitir a los administradores revisar y liberar mensajes retenidos y ofrecer a los usuarios mecanismos para consultar y gestionar sus propios mensajes en cuarentena, de acuerdo con los permisos y políticas definidos por la Entidad.
- **Banners de seguridad en mensajes entrantes:** deberá permitir identificar los mensajes entrantes mediante avisos visuales configurables que indiquen, como mínimo, las categorías de remitente confiable, externo y no confiable.

• **Sincronización de directorios:** deberá permitir sincronizar usuarios y grupos desde Active Directory (AD) o Microsoft Entra ID (Azure AD), según la infraestructura de la Entidad y las capacidades de integración de la solución. • **Integración mediante API con Microsoft 365:** deberá disponer de integración mediante API con Microsoft 365, sin interrupción del flujo de correo electrónico, de acuerdo con las condiciones establecidas en los documentos del proceso. El proponente deberá acreditar el mecanismo de integración y las funcionalidades de protección disponibles mediante documentación técnica oficial del fabricante. • **Consola SaaS y generación de informes:** deberá disponer de una consola centralizada en la nube que permita administrar las políticas de seguridad, consultar eventos, gestionar la cuarentena y generar informes sobre amenazas detectadas, acciones ejecutadas y actividades relevantes para el seguimiento de la seguridad institucional. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar el cumplimiento integral de cada característica exigida, incluyendo los mecanismos de integración con Microsoft 365 y las funcionalidades disponibles en el licenciamiento ofertado. Los módulos o licencias adicionales necesarios para cumplir los requisitos deberán identificarse expresamente e incluirse en la oferta económica. La solución de protección de correo electrónico podrá corresponder a un fabricante diferente del utilizado para la protección de endpoints y servidores. En ese caso, se administrará desde la consola SaaS propia del fabricante de correo y deberá acreditarse la integración mediante API o conectores para el intercambio de información y la correlación de eventos. Esta condición no exime del cumplimiento integral de los requisitos técnicos aplicables a cada componente.	
2. **SOLUCIÓN DE PROTECCIÓN PARA SISTEMAS OPERATIVOS DE SERVIDORES, INCLUIDOS SISTEMAS FUERA DE SOPORTE** La solución deberá proporcionar protección antimalware para los equipos servidores que utilicen sistemas operativos actualmente soportados y para aquellos que se encuentren fuera del ciclo de soporte del fabricante, de acuerdo con las capacidades compatibles con cada sistema operativo. • **Protección de sistemas operativos fuera de soporte:** Para los servidores que utilicen versiones de Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, RHEL, CentOS u otros sistemas operativos que la Entidad identifique y que se encuentren fuera del soporte del fabricante, se deberá garantizar protección antimalware compatible, de acuerdo con las capacidades disponibles para cada versión. Para estos sistemas no será obligatorio disponer de funcionalidades EDR/XDR. • **Capacidades EDR/XDR para sistemas operativos soportados:** Los sistemas operativos que cuenten con soporte vigente del fabricante de la solución deberán disponer de las funcionalidades EDR/XDR exigidas en la ficha técnica, incluyendo detección de amenazas, análisis de eventos y correlación automática de eventos entre servidores y endpoints, según corresponda. • **Protección sin conexión:** La solución deberá indicar las capacidades de prevención y detección que puede mantener localmente cuando un servidor pierda temporalmente la conexión con la consola de administración SaaS, así como las limitaciones aplicables a cada sistema operativo. • **Detección de anomalías de comportamiento:** Para los sistemas operativos soportados que dispongan de las funcionalidades correspondientes, la solución deberá permitir identificar comportamientos anómalos y generar alertas para su investigación. • **Prevención de pérdida de datos (DLP):** La solución deberá permitir monitorear y bloquear, según las capacidades compatibles con el sistema operativo, las transferencias no autorizadas de información sensible. El proponente deberá identificar las funcionalidades, canales de control y licenciamiento requeridos para cumplir este requisito.	1

• **Soporte técnico:** Se deberá disponer del soporte técnico del fabricante 24/7, de acuerdo con las condiciones de soporte aplicables a la solución ofrecida y a los sistemas operativos correspondientes. • **Acreditación del cumplimiento:** El proponente deberá aportar documentación técnica oficial del fabricante que permita verificar la compatibilidad con los sistemas operativos ofertados y diferenciar las funcionalidades disponibles para sistemas operativos soportados y fuera de soporte. La instalación de un agente, por sí sola, no acreditará el cumplimiento de las funcionalidades exigidas. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar la compatibilidad con cada sistema operativo y versión identificados por la Entidad, así como las funcionalidades efectivamente disponibles para cada uno. La instalación del agente, por sí sola, no acreditará el cumplimiento de las capacidades de prevención, EDR, correlación XDR, protección sin conexión y detección de anomalías exigidas.	
3. SERVICIOS PROFESIONALES DE INGENIERÍA PARA IMPLEMENTACIÓN Y SOPORTE El contratista deberá prestar servicios profesionales de ingeniería para la implementación, configuración, puesta en funcionamiento y soporte de las soluciones de protección de endpoints, servidores y correo electrónico, así como para la gestión del inventario de activos tecnológicos, la gestión de vulnerabilidades y el control remoto. **5.1. Implementación y configuración:** Instalación, configuración y puesta en funcionamiento de las soluciones de protección de endpoints, servidores y correo electrónico, de acuerdo con las características técnicas de las soluciones ofertadas y los requerimientos de la Entidad. **5.2. Inventario centralizado de equipos:** La solución de protección de endpoints y servidores deberá disponer de una funcionalidad que permita descubrir, identificar, registrar, consultar y monitorear centralizadamente los equipos administrados. Como mínimo, deberá permitir visualizar el nombre del equipo, dirección IP, tipo de equipo, tipo y versión del sistema operativo, estado de administración, versión del agente o producto de seguridad instalado, problemas o alertas de seguridad detectados, fecha y hora de la última sincronización o comunicación con la consola, política de seguridad asignada y estado de aplicación de dicha política. Asimismo, deberá permitir buscar y filtrar los equipos por nombre, dirección IP, sistema operativo, estado de protección y estado de administración, así como generar o exportar reportes del inventario desde una consola de administración centralizada. La información deberá actualizarse de acuerdo con la detección y comunicación de los equipos con la solución. El proponente deberá acreditar estas capacidades mediante documentación técnica oficial del fabricante. El inventario comprenderá los equipos detectados o administrados por la solución y no implicará. **5.3. Gestión de vulnerabilidades:** La solución ofertada deberán permitir identificar, evaluar y realizar seguimiento a las vulnerabilidades de los activos tecnológicos incluidos en el alcance **5.4. Control remoto:** Se deberá disponer de funcionalidades o herramientas que permitan realizar actividades de asistencia y administración remota de los equipos incluidos en el alcance, de acuerdo con los permisos, procedimientos de seguridad y autorizaciones definidos por la Entidad. **5.5. Soporte técnico:** El contratista deberá proporcionar acompañamiento y soporte técnico para la implementación, configuración y operación de las soluciones objeto del contrato, conforme a las condiciones y el alcance establecidos en los documentos del proceso.	1

CUARTO: MODIFICACIÓN DE LA OBLIGACIÓN ESPECÍFICA No. 7 DE LA MINUTA CONTRACTUAL QUEDARÁ DE LA SIGUIENTE MANERA:

"Adquirir, configurar, implementar y poner en funcionamiento las soluciones de ciberseguridad para la protección de endpoints, servidores y correo electrónico, incluyendo las funcionalidades EDR y XDR exigidas en los documentos del proceso, por un periodo de un (1) año, conforme al objeto contractual y a las especificaciones técnicas establecidas en los Estudios Previos y el Anexo No. 1 — Ficha Técnica."

QUINTA: ASPECTOS QUE PERMANECEN SIN MODIFICACIÓN

Los demás requisitos, condiciones y disposiciones del pliego de condiciones definitivo, los Estudios Previos, el Anexo No. 1 — Ficha Técnica y los documentos del proceso que no hayan sido modificados o aclarados expresamente mediante la presente Adenda continúan vigentes.

En particular, se mantienen los umbrales de los indicadores financieros y de capacidad organizacional establecidos en el numeral 3.2, de acuerdo con la respuesta oficial a las observaciones.

La presente Adenda forma parte integral de los documentos del proceso **SASI 006 MT 2026**.

En caso de discrepancia entre los apartados aquí modificados y su redacción anterior, prevalecerá lo dispuesto en esta Adenda. Las aclaraciones se interpretarán de manera armónica con las respuestas oficiales a las observaciones y con los demás documentos del proceso.

ANEXO No. 1
FICHA TÉCNICA DE LOS BIENES Y SERVICIOS A ADQUIRIR

OBJETO: ADQUISICIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE PLATAFORMAS DE CIBERSEGURIDAD QUE PERMITAN CORRELACIONAR SOLUCIÓN PROTECCIÓN DE ENDPOINT Y SERVIDORES CON EDR Y XDR Y PROTECCIÓN DE CORREO PARA LA ALCALDÍA DE TOCANCIPÁ.

ÍTEM	BIEN	CODIGO UNSPSC	UNIDAD MEDIDA	DESCRIPCION DEL BIEN	CANT
1	Software de seguridad y protección	43233200	UNIDAD	Solución integral de seguridad antimalware para endpoints, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar y aplicar políticas de seguridad para la prevención de amenazas, el control de acceso, la protección de datos, el despliegue y la actualización de agentes. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá cumplir, como mínimo, con las siguientes características: • **Gestión basada en la nube (SaaS):** deberá operar sin requerir infraestructura local dedicada para la administración de la solución. • **Consola de administración centralizada:** deberá permitir administrar las capacidades de protección de endpoints y servidores ofertadas, sus políticas de seguridad, informes, despliegue y actualización de agentes desde una misma consola SaaS centralizada. La protección del correo electrónico podrá ser suministrada por un fabricante diferente, con su propia consola SaaS, siempre que cumpla integralmente los requisitos establecidos para dicho componente y se acredite la integración mediante API o conectores para el intercambio de información y la correlación de eventos. • **Agente único:** la protección de endpoints y servidores deberá operar mediante un agente único que integre las funciones de prevención de amenazas, EDR, XDR, firewall de host y DLP básico, administradas desde una misma consola SaaS centralizada. La integración posterior de eventos mediante SIEM, Syslog o API no sustituye la exigencia de agente único ni la capacidad de respuesta y bloqueo unificado en tiempo real. Las funcionalidades complementarias deberán estar incluidas en la solución propuesta y su licenciamiento deberá identificarse claramente. • **Soporte multiplataforma:** deberá soportar, como mínimo, los sistemas operativos empresariales Windows (escritorio y servidor), macOS y Linux, de acuerdo con las versiones y condiciones de compatibilidad establecidas en la ficha técnica. • **Despliegue y actualizaciones centralizadas:** deberá permitir gestionar centralizadamente el despliegue, configuración y actualización de los agentes instalados en los endpoints protegidos. • **Alta disponibilidad y escalabilidad:** deberá contar con capacidades que permitan mantener la disponibilidad del servicio y ampliar la cobertura de protección según las necesidades de la Entidad. • **Prevención de ejecución de malware:** deberá detectar y bloquear amenazas conocidas mediante mecanismos de protección antimalware. • **Detección basada en análisis heurístico y comportamental:** deberá utilizar mecanismos de análisis heurístico, comportamiento, inteligencia artificial o aprendizaje automático para detectar y bloquear malware de día cero, amenazas polimórficas y otras amenazas avanzadas. • **Protección contra ransomware:** deberá detectar comportamientos asociados con procesos de cifrado malicioso y permitir su bloqueo o contención, así como las acciones de remediación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología o denominación comercial específica.	500

				• **Detección y respuesta en endpoints (EDR):** deberá recolectar y analizar telemetría de los endpoints, proporcionar visibilidad de la cadena de eventos de un ataque y permitir la investigación de incidentes de seguridad y la ejecución de las acciones de respuesta disponibles en la solución. • **Análisis y control de aplicaciones:** deberá permitir identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas, conforme a las políticas de seguridad configuradas. • **Control de dispositivos periféricos:** deberá permitir gestionar y controlar el uso de dispositivos USB y otros medios removibles, conforme a las políticas definidas por la Entidad. • **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. • **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección por reputación de URL maliciosas, por sí sola, no acreditará el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y acreditar que está incluida en el licenciamiento propuesto. • **Prevención básica de pérdida de datos (DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles. El proponente deberá especificar los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria para cumplir este requisito deberá identificarse expresamente e incluirse en la oferta económica. • **Análisis de comportamiento, investigación de amenazas y protección anti-exploit:** cuando estas capacidades sean exigidas en los documentos del proceso, podrán acreditarse mediante funcionalidades equivalentes de la solución ofertada, siempre que la documentación oficial del fabricante demuestre el cumplimiento de las capacidades técnicas requeridas. • **Soporte técnico del fabricante:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana (24/7), durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. • El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas e identificar las funcionalidades y licencias incluidas en la solución. La aceptación de equivalencias funcionales no exime del cumplimiento de los requisitos técnicos mínimos establecidos en la presente ficha	
2	Software de seguridad y protección	43233200	UNIDAD	Solución de seguridad antimalware para servidores, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar políticas de seguridad, prevenir amenazas, controlar el acceso, proteger los datos y gestionar el despliegue y las actualizaciones de los agentes desde la plataforma de administración. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá proporcionar capacidades de prevención, detección y respuesta en servidores, incluyendo EDR y correlación XDR con los endpoints protegidos, conforme a los requisitos técnicos establecidos en este ítem. Deberá cumplir, como mínimo, con las siguientes características: 1. **Soporte extendido para sistemas operativos de servidor:** deberá ser compatible con los sistemas operativos y versiones de	10

				servidor exigidos en la ficha técnica, proporcionando las funcionalidades de prevención, EDR y correlación XDR disponibles para cada versión. El proponente deberá acreditar la compatibilidad y las capacidades efectivamente soportadas mediante documentación oficial del fabricante. 2. **Visibilidad EDR en tiempo real:** deberá recolectar y permitir consultar telemetría de seguridad de los servidores protegidos, incluida la actividad de red entrante y saliente, de acuerdo con las capacidades de la solución y las limitaciones del sistema operativo. 3. **Correlación XDR y detección de movimiento lateral:** deberá permitir correlacionar eventos de seguridad entre los servidores protegidos y los endpoints de usuario, con el propósito de identificar incidentes, comportamientos sospechosos y posibles movimientos laterales dentro del entorno tecnológico de la Entidad. 4. **Control de aplicaciones mediante listas de permitidos (whitelisting):** deberá permitir establecer políticas para autorizar la ejecución de aplicaciones y servicios previamente aprobados y restringir aquellos que no estén autorizados, conforme a las capacidades de la solución ofertada. 5. **Control de acceso y puertos de red:** deberá permitir definir políticas de control de acceso y comunicaciones de red para los servidores, de acuerdo con sus funciones y roles, conforme a las capacidades de la solución y del sistema operativo. 6. **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. 7. **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección de URL maliciosas basada únicamente en reputación no acreditará, por sí sola, el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y demostrar que está incluida en el licenciamiento propuesto. 8. **Prevención básica de pérdida de datos (Data Loss Prevention — DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles, de acuerdo con las capacidades compatibles con el sistema operativo del servidor. El proponente deberá especificar las funcionalidades, los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria deberá identificarse expresamente e incluirse en la oferta económica. 9. **Soporte técnico del fabricante 24/7:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas, la compatibilidad con los sistemas operativos y versiones correspondientes, y las funcionalidades incluidas en el licenciamiento ofertado. La instalación del agente, por sí sola, no acreditará el cumplimiento de todas las capacidades requeridas.	

3	Software de seguridad y protección	43233200	UNIDAD	Solución de seguridad para la protección del correo electrónico institucional, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que combine capacidades de filtrado multicapa y tecnologías de inteligencia artificial para detectar, prevenir y bloquear amenazas avanzadas, incluyendo phishing, ransomware, suplantación de identidad y ataques de compromiso de correo empresarial (BEC). Deberá incorporar mecanismos de análisis de archivos adjuntos y URL, sandbox en la nube, protección contra correo no deseado y malware, cifrado de mensajes, políticas de prevención de pérdida de datos (DLP), autenticación del remitente y administración de cuarentena. La solución deberá integrarse con Microsoft 365 mediante API, sin interrupción del flujo de correo electrónico, y contar con una consola de administración centralizada que permita configurar políticas, supervisar eventos de seguridad, gestionar mensajes sospechosos y generar informes de las actividades de protección. La solución deberá cumplir, como mínimo, con las siguientes características: • **Protección contra phishing y suplantación de identidad:** deberá detectar y bloquear intentos de phishing, suplantación de identidad y ataques BEC mediante el análisis del contenido, contexto y características de los mensajes. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una técnica específica de procesamiento de lenguaje natural o una tecnología determinada de inteligencia artificial. • **Autenticación del correo electrónico:** deberá soportar los mecanismos SPF, DKIM y DMARC para validar la autenticidad de los remitentes y contribuir a la detección de mensajes fraudulentos. • **Análisis de reputación:** deberá disponer de mecanismos para analizar la reputación de remitentes, dominios y direcciones IP, con el propósito de identificar mensajes potencialmente maliciosos o no deseados. • **Protección antispam y antimalware:** deberá incorporar filtrado antispam, análisis de malware y sandbox en la nube para el análisis dinámico de archivos adjuntos y otros elementos potencialmente maliciosos. • **Detección y reescritura de URL:** deberá detectar URL maliciosas y permitir la reescritura de enlaces para verificar su seguridad en el momento en que el usuario haga clic. Asimismo, deberá detectar anomalías en los encabezados de los mensajes que puedan indicar suplantación o actividad sospechosa. • **Filtrado por país e idioma:** deberá permitir aplicar reglas de filtrado o tratamiento de mensajes según el país de origen y el idioma, conforme a las capacidades de la solución ofertada. • **Detección de suplantación de nombres visibles:** deberá permitir analizar los nombres para mostrar de los remitentes e identificar posibles suplantaciones de personas VIP, directivos, usuarios o marcas de la Entidad. • **Detección de dominios similares:** deberá identificar dominios similares al dominio legítimo de la Entidad o a dominios de confianza, con el fin de detectar posibles intentos de suplantación y fraude. • **Prevención de pérdida de datos (DLP):** deberá permitir configurar políticas DLP con múltiples reglas aplicables a grupos y usuarios individuales, incluyendo controles sobre información financiera, contenidos confidenciales, información relacionada con la salud y datos personales identificables (PII). • **Cifrado de comunicaciones mediante TLS:** deberá soportar TLS para proteger las comunicaciones de correo electrónico durante el transporte, conforme a las capacidades de la solución y las condiciones de interoperabilidad aplicables.	400

				• **Compatibilidad con S/MIME:** deberá soportar el estándar S/MIME para el cifrado y la firma digital de mensajes, de acuerdo con las funcionalidades y condiciones de licenciamiento ofertadas. • **Autenticación del remitente:** deberá contar con mecanismos para verificar la autenticidad de los remitentes y detectar posibles falsificaciones, de acuerdo con las funcionalidades requeridas. • **Cifrado de mensajes y archivos adjuntos:** deberá permitir proteger mensajes y archivos adjuntos sensibles mediante mecanismos de cifrado con entrega protegida al destinatario (push encryption), conforme a las políticas de seguridad configuradas. • **Protección del correo entrante y saliente:** deberá analizar los mensajes entrantes para detectar amenazas, spam, suplantación y contenido malicioso, así como aplicar controles al correo saliente para prevenir fugas de información y el envío de mensajes maliciosos o no autorizados. • **Administración granular de políticas:** deberá permitir configurar y aplicar políticas de seguridad a nivel de dominio, grupo y usuario individual. • **Administración de cuarentena:** deberá permitir a los administradores revisar y liberar mensajes retenidos y ofrecer a los usuarios mecanismos para consultar y gestionar sus propios mensajes en cuarentena, de acuerdo con los permisos y políticas definidos por la Entidad. • **Banners de seguridad en mensajes entrantes:** deberá permitir identificar los mensajes entrantes mediante avisos visuales configurables que indiquen, como mínimo, las categorías de remitente confiable, externo y no confiable. • **Sincronización de directorios:** deberá permitir sincronizar usuarios y grupos desde Active Directory (AD) o Microsoft Entra ID (Azure AD), según la infraestructura de la Entidad y las capacidades de integración de la solución. • **Integración mediante API con Microsoft 365:** deberá disponer de integración mediante API con Microsoft 365, sin interrupción del flujo de correo electrónico, de acuerdo con las condiciones establecidas en los documentos del proceso. El proponente deberá acreditar el mecanismo de integración y las funcionalidades de protección disponibles mediante documentación técnica oficial del fabricante. • **Consola SaaS y generación de informes:** deberá disponer de una consola centralizada en la nube que permita administrar las políticas de seguridad, consultar eventos, gestionar la cuarentena y generar informes sobre amenazas detectadas, acciones ejecutadas y actividades relevantes para el seguimiento de la seguridad institucional. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar el cumplimiento integral de cada característica exigida, incluyendo los mecanismos de integración con Microsoft 365 y las funcionalidades disponibles en el licenciamiento ofertado. Los módulos o licencias adicionales necesarios para cumplir los requisitos deberán identificarse expresamente e incluirse en la oferta económica. La solución de protección de correo electrónico podrá corresponder a un fabricante diferente del utilizado para la protección de endpoints y servidores. En ese caso, se administrará desde la consola SaaS propia del fabricante de correo y deberá acreditarse la integración mediante API o conectores para el intercambio de información y la correlación de eventos. Esta condición no exime del cumplimiento integral de los requisitos técnicos aplicables a cada componente	
4	Software de seguridad y protección	43233200	UNIDAD	La solución deberá proporcionar protección antimalware para los equipos servidores que utilicen sistemas operativos actualmente soportados y para aquellos que se encuentren fuera del ciclo de soporte del fabricante, de acuerdo con las capacidades compatibles con cada sistema operativo.	1

				• Protección de sistemas operativos fuera de soporte: Para los servidores que utilicen versiones de Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, RHEL, CentOS u otros sistemas operativos que la Entidad identifique y que se encuentren fuera del soporte del fabricante, se deberá garantizar protección antimalware compatible, de acuerdo con las capacidades disponibles para cada versión. Para estos sistemas no será obligatorio disponer de funcionalidades EDR/XDR. • Capacidades EDR/XDR para sistemas operativos soportados: Los sistemas operativos que cuenten con soporte vigente del fabricante de la solución deberán disponer de las funcionalidades EDR/XDR exigidas en la ficha técnica, incluyendo detección de amenazas, análisis de eventos y correlación automática de eventos entre servidores y endpoints, según corresponda. • Protección sin conexión: La solución deberá indicar las capacidades de prevención y detección que puede mantener localmente cuando un servidor pierda temporalmente la conexión con la consola de administración SaaS, así como las limitaciones aplicables a cada sistema operativo. • Detección de anomalías de comportamiento: Para los sistemas operativos soportados que dispongan de las funcionalidades correspondientes, la solución deberá permitir identificar comportamientos anómalos y generar alertas para su investigación. • Prevención de pérdida de datos (DLP): La solución deberá permitir monitorear y bloquear, según las capacidades compatibles con el sistema operativo, las transferencias no autorizadas de información sensible. El proponente deberá identificar las funcionalidades, canales de control y licenciamiento requeridos para cumplir este requisito. • Soporte técnico: Se deberá disponer del soporte técnico del fabricante 24/7, de acuerdo con las condiciones de soporte aplicables a la solución ofrecida y a los sistemas operativos correspondientes. • Acreditación del cumplimiento: El proponente deberá aportar documentación técnica oficial del fabricante que permita verificar la compatibilidad con los sistemas operativos ofertados y diferenciar las funcionalidades disponibles para sistemas operativos soportados y fuera de soporte. La instalación de un agente, por sí sola, no acreditará el cumplimiento de las funcionalidades exigidas. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar la compatibilidad con cada sistema operativo y versión identificados por la Entidad, así como las funcionalidades efectivamente disponibles para cada uno. La instalación del agente, por sí sola, no acreditará el cumplimiento de las capacidades de prevención, EDR, correlación XDR, protección sin conexión y detección de anomalías exigidas.	
5	Ingeniería de software o hardware	81111500	UNIDAD	El contratista deberá prestar servicios profesionales de ingeniería para la implementación, configuración, puesta en funcionamiento y soporte de las soluciones de protección de endpoints, servidores y correo electrónico, así como para la gestión del inventario de activos tecnológicos, la gestión de vulnerabilidades y el control remoto. **5.1. Implementación y configuración:** Instalación, configuración y puesta en funcionamiento de las soluciones de protección de endpoints, servidores y correo electrónico, de acuerdo con las características técnicas de las soluciones ofertadas y los requerimientos de la Entidad.	1

				5.2. Inventario centralizado de equipos: La solución de protección de endpoints y servidores deberá disponer de una funcionalidad que permita descubrir, identificar, registrar, consultar y monitorear centralizadamente los equipos administrados. Como mínimo, deberá permitir visualizar el nombre del equipo, dirección IP, tipo de equipo, tipo y versión del sistema operativo, estado de administración, versión del agente o producto de seguridad instalado, problemas o alertas de seguridad detectados, fecha y hora de la última sincronización o comunicación con la consola, política de seguridad asignada y estado de aplicación de dicha política. Asimismo, deberá permitir buscar y filtrar los equipos por nombre, dirección IP, sistema operativo, estado de protección y estado de administración, así como generar o exportar reportes del inventario desde una consola de administración centralizada. La información deberá actualizarse de acuerdo con la detección y comunicación de los equipos con la solución. El proponente deberá acreditar estas capacidades mediante documentación técnica oficial del fabricante. El inventario comprenderá los equipos detectados o administrados por la solución y no implicará. **5.3. Gestión de vulnerabilidades:** La solución ofertada deberán permitir identificar, evaluar y realizar seguimiento a las vulnerabilidades de los activos tecnológicos incluidos en el alcance **5.4. Control remoto:** Se deberá disponer de funcionalidades o herramientas que permitan realizar actividades de asistencia y administración remota de los equipos incluidos en el alcance, de acuerdo con los permisos, procedimientos de seguridad y autorizaciones definidos por la Entidad. **5.5. Soporte técnico:** El contratista deberá proporcionar acompañamiento y soporte técnico para la implementación, configuración y operación de las soluciones objeto del contrato, conforme a las condiciones y el alcance establecidos en los documentos del proceso. .	

El presente Anexo Técnico establece las condiciones técnicas mínimas obligatorias que deberá cumplir el contratista seleccionado para la ejecución del objeto contractual. La verificación de cumplimiento de las especificaciones requeridas se adelantará durante la etapa de evaluación de ofertas y su seguimiento estará a cargo de la supervisión designada por el Municipio de Tocancipá.

FORMULARIO No. 5

CUMPLIMIENTO DE LA FICHA TÉCNICA

(Ciudad y fecha)

Doctor
WALFRANDO FORERO BEJARANO
ALCALDE MUNICIPAL
Calle 11 No.6 -12
Ciudad

REF: **SASI ____ MT 202__**
OBJETO: ***(INDICAR OBJETO)***,

El abajo firmante, actuando en nombre y representación de _____, de acuerdo con lo dispuesto en el pliego de condiciones, bajo la gravedad de juramento que se entiende prestado con la suscripción y firma de este documento, me permito ofertar los siguientes bienes que cumplen plenamente con la ficha técnica elaborada y publicada por el Municipio de Tocancipá, así:

4. PROTECCIÓN ENDPOINT

Se requiere una solución integral y unificada anti-malware de seguridad para endpoints, que combine múltiples capacidades de protección en un solo agente y consola de administración, la solución debe tener una consola para definir políticas de seguridad para la prevención de amenazas, control de acceso y cumplimiento, protección de datos, despliegue y actualizaciones de agentes del Endpoint, La solución debe incluir una Gestión Basada en nube en modalidad SaaS que permite gestionar equipos, con su debido licenciamiento, puesta en funcionamiento, soporte de fábrica y garantía. La solución requerida debe proveer como mínimo:

La solución propuesta debe ser capaz de unificar la visibilidad, detección, investigación y respuesta a amenazas a través de múltiples vectores de ataque, incluyendo endpoints, servidores, redes, correo electrónico y entornos en la nube.

Consola de Administración

La consola de administración debe ser una solución SaaS (Software as a Service) que proporcione capacidades robustas de informes y monitoreo. Debe ofrecer filtros preconstruidos para facilitar la visualización y corrección de equipos que requieran atención. Es fundamental que la consola genere un registro de auditoría seguro, supervisando toda la actividad para asegurar el cumplimiento normativo, facilitar auditorías de seguridad, análisis forenses y solución de problemas. Además, la consola debe permitir la gestión centralizada de políticas de seguridad y la visualización unificada de eventos de seguridad a través de múltiples vectores de ataque, incluyendo endpoints, red, correo electrónico y entornos en la nube. Debe contar con capacidades de gestión de casos colaborativa y mapeo automático a frameworks de amenazas como MITRE ATT&CK para una mejor contextualización de las detecciones.

Protección de Endpoint

La solución debe ofrecer protección de ciberseguridad para estaciones de trabajo, laptops, dispositivos móviles y servidores, operando en tiempo real y mediante escaneos programados. Debe ser capaz de detectar, bloquear y limpiar virus, troyanos, gusanos, spyware, aplicaciones potencialmente no deseadas (PUA), adware y comportamientos sospechosos en sistemas operativos Windows, Linux y Mac. La detección de malware debe incluir análisis en pre-ejecución y comprobación de comportamiento malicioso para identificar amenazas desconocidas. Es crucial que la solución impida la reconfiguración, deshabilitación o desinstalación no autorizada de sus componentes, incluso por parte de administradores locales, mediante mecanismos de protección como contraseñas.

Debe verificar todos los archivos accedidos en tiempo real, incluso durante el arranque del sistema, y realizar una limpieza automática de elementos maliciosos. La protección debe extenderse a funciones críticas en navegadores de Internet (Safe Browsing) y prevenir ataques de vulnerabilidades web a través de exploits. La solución debe aplicar análisis de comportamiento durante la ejecución para detectar desbordamientos de búfer y otras anomalías. Además, debe permitir la autorización de detecciones maliciosas y la exclusión de directorios y archivos específicos del escaneo.

Control de Dispositivos y Aplicaciones

La solución debe permitir el monitoreo y control de dispositivos extraíbles (USB, discos duros externos, CD/DVD, interfaces de red inalámbrica, módems, Bluetooth, infrarrojos, MTP, PTP) aplicando políticas tanto a usuarios como a dispositivos. Debe contar con control de aplicaciones para monitorear e impedir la ejecución o instalación de aplicaciones que puedan afectar la productividad o el rendimiento de la red, reconociendo y bloqueando automáticamente aplicaciones basadas en su huella digital (hash). La lista de aplicaciones controlables debe actualizarse automáticamente, permitiendo la liberación o bloqueo de aplicaciones o categorías específicas. Las detecciones de aplicaciones controladas deben ofrecer opciones de permitir y alertar o bloquear y alertar.

Prevención de Intrusiones y Fuga de Datos

La solución debe incluir prevención de intrusión en el host (HIPS) para monitorear y bloquear código con comportamiento malicioso antes de su ejecución. Debe poseer protección contra fugas o pérdida de datos sensibles (DLP) en el agente de protección, considerando el contenido, la extensión del archivo y múltiples destinos. Debe identificar información confidencial (números de tarjetas de crédito, cuentas bancarias, pasaportes, direcciones, teléfonos, correos electrónicos) incluso si los documentos no están clasificados, utilizando listas de control de contenido (CCL) preconfiguradas y permitiendo la adición de reglas personalizadas. Las acciones ante la detección de datos sensibles deben incluir bloqueo, registro del evento en la consola de administración web o consulta al usuario.

Control Web y Monitoreo de Cambios

La solución debe incluir control web para gestionar el acceso a sitios inapropiados, con al menos 12 categorías predefinidas y la posibilidad de crear listas blancas y negras. Debe monitorear cambios (creaciones o modificaciones) en carpetas y archivos críticos del sistema, basándose en una lista predefinida y personalizable para sistemas operativos Windows Server 2012 R2 o superior. Además, debe generar una lista blanca de aplicaciones para Windows Server 2008 R2 o superior, permitiendo la ejecución exclusiva de aplicaciones autorizadas.

Detección Proactiva de Nuevas Amenazas

La solución debe contener funcionalidad de protección contra amenazas de día cero mediante tecnología de deep learning (sin firmas). Debe ser capaz de detectar amenazas desconocidas en memoria y realizar detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria. Asimismo, debe detectar y bloquear troyanos y gusanos, entre otros malwares, por comportamiento de los procesos en memoria. La solución no debe requerir la descarga de firmas de ningún tipo. Debe analizar el comportamiento de nuevos procesos al ser ejecutados, complementando la exploración programada. Además, debe contar con funcionalidad de análisis forense para entender la causa raíz de los problemas, detallando procesos y subprocesos ejecutados, lectura y escritura de archivos, y claves de registro. Debe bloquear y proteger contra amenazas desconocidas potencialmente sospechosas (PUA) y permitir la generación de excepciones ante falsos positivos.

Protección Proactiva contra Ransomware

La solución deberá detectar comportamientos asociados con procesos de cifrado malicioso y permitir su bloqueo o contención, así como las acciones de remediación o recuperación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir protección específica del Master Boot Record ni restauración automática como mecanismo obligatorio.

Protección contra Vulnerabilidades y Técnicas de Explotación

La solución debe tener la capacidad de bloquear ataques basados en la explotación de vulnerabilidades conocidas o de día cero. Debe contar con detección y protección contra las siguientes técnicas de explotación:

Enforce Data Execution Prevention
Mandatory Address Space Layout Randomization
Bottom-up ASLR
Null Page (Null Deference Protection)
Heap Spray Allocation
Dynamic Heap Spray
Stack Pivot
Stack Exec (MemProt)
Stack-based ROP Mitigations (Caller)
Branch-based ROP Mitigations (Hardware Assisted)
Structured Exception Handler Overwrite (SEHOP)
Import Address Table Filtering (IAF)
Load Library
Reflective DLL Injection
Shellcode
VBScript God Mode
Wow64
Syscall

Además, la solución debe contar con mitigación de inyección de códigos en procesos, protección contra robo de credenciales, protección contra malware escondido en aplicaciones legítimas (code cave), prevención de migración de procesos maliciosos, prevención de escalamiento de privilegios y prevención de modificación de claves de registro para la ejecución de código arbitrario. Estas capacidades son cruciales para una defensa profunda contra ataques avanzados.

Reducción de la Superficie de Amenazas

La solución debe contribuir significativamente a la reducción de la superficie de ataque, incluyendo las siguientes funcionalidades:

- ✓ **Protección web y control web:** Bloqueo de acceso a sitios maliciosos o no autorizados, con categorización y políticas personalizadas. Debe permitir la creación de listas blancas y negras.
- ✓ **Reputación de descargas:** Evaluación automática del riesgo de archivos descargados mediante consultas en la nube, bloqueando archivos maliciosos antes de su ejecución.
- ✓ **Control de aplicaciones (Application Control):** Impedir que aplicaciones no autorizadas se ejecuten en los endpoints, utilizando listas blancas o bloqueo por hash. Debe actualizarse automáticamente y permitir la gestión de categorías de aplicaciones.
- ✓ **Control de periféricos (Device Control):** Permitir o bloquear el uso de dispositivos USB, almacenamiento externo, impresoras, y otros periféricos, aplicando políticas por usuario, grupo y ubicación. Debe soportar la integración con directorios de usuarios como Active Directory o Azure AD para aplicar controles contextuales.
- ✓ **Prevención de fuga de datos (DLP):** Detección y bloqueo del intento de extraer información confidencial según contenido y contexto (archivos, dispositivos, red). Debe incluir listas de control de contenido (CCL) preconfiguradas para información sensible (números de tarjetas de crédito, cuentas bancarias, pasaportes, direcciones, teléfonos, correos electrónicos) y permitir la adición de reglas personalizadas.
- ✓ **Bloqueo de servidor (Allowlisting):** Permitir la ejecución exclusiva de software previamente autorizado en sistemas críticos, protegiéndolos contra código no deseado. Esta funcionalidad es especialmente relevante para servidores Windows Server 2008 R2 o superior.

La solución debe asegurar la compatibilidad con políticas granulares por usuario, grupo y ubicación, y una integración fluida con servicios de directorio para la aplicación de controles contextuales. Además, debe soportar la generación de logs auditables centralizados para el cumplimiento de regulaciones.

Prevención de Amenazas (EDR/XDR)

La solución debe incorporar capacidades avanzadas de prevención de amenazas, tanto a nivel de Endpoint Detection and Response (EDR) como de Extended Detection and Response (XDR), para una defensa proactiva y adaptativa. Estas capacidades incluyen:

- ✓ **Protección contra ransomware:** la solución deberá detectar comportamientos asociados con procesos de cifrado malicioso en los equipos protegidos y permitir su bloqueo o contención, así como las acciones de remediación o recuperación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología, módulo o denominación comercial específica.
- ✓ **Defensas Contextuales Adaptativas:** La solución debe ajustar dinámicamente las medidas de defensa según la criticidad del endpoint, su ubicación y el nivel de amenaza detectado. Esto permite una protección más granular y eficiente.
- ✓ **Prevención basada en Inteligencia Artificial (Deep Learning):** Análisis de archivos antes de su ejecución sin necesidad de firmas, lo que es crucial para la protección contra amenazas de día cero y malware desconocido. Debe incluir la capacidad de detectar y bloquear aplicaciones potencialmente no deseadas (PUA), como adware o toolbars.
- ✓ **Live Protection (Cloud Lookup):** Verificación instantánea en la nube de archivos o URLs ante cualquier sospecha, utilizando inteligencia de amenazas actualizada.
- ✓ **Análisis de Comportamiento:** Monitoreo en tiempo real de la conducta de procesos para detectar comportamientos maliciosos que los antivirus tradicionales podrían pasar por alto. Esto incluye la detección de inyecciones de código, desbordamientos de búfer y otras técnicas de explotación.
- ✓ **Protección contra explotación de vulnerabilidades (anti-exploit):** la solución deberá detectar y bloquear, según las capacidades soportadas, técnicas de explotación que puedan comprometer aplicaciones o procesos legítimos, incluyendo técnicas como inyección de código, ROP, heap spray y desbordamiento de búfer. Se aceptarán capacidades funcionalmente equivalentes, acreditadas mediante documentación oficial del fabricante, sin exigir un número predeterminado de mitigaciones.
- ✓ **Integración AMSI:** Escaneo de scripts en tiempo real utilizando la interfaz antimalware de Windows para una detección temprana de amenazas basadas en scripts.
- ✓ **Detección de Tráfico Malicioso e IPS:** Visibilidad sobre conexiones de red maliciosas y protección activa contra exploits a nivel de red, actuando como un sistema de prevención de intrusiones (IPS).
- ✓ **Monitorización de Integridad de Archivos (FIM):** Detección de modificaciones no autorizadas en archivos del sistema o aplicaciones críticas, especialmente en servidores, para identificar actividades sospechosas o maliciosas.
- ✓ **Datos Exhaustivos en el Dispositivo y la Nube:** Recopilación de datos detallados para análisis en tiempo real o histórico, facilitando la investigación de incidentes.
- ✓ **Retención de Datos en la Nube:** Capacidad de retención de datos de eventos de seguridad por un período mínimo de 90 días, lo cual es fundamental para el cumplimiento de normativas forenses y de auditoría.

Es importante que el motor de protección funcione eficazmente sin conexión a internet (protección offline) y que los eventos y datos del endpoint se integren nativamente con una plataforma XDR para una correlación multivectorial completa.

Detección (EDR/XDR)

La solución debe proporcionar capacidades avanzadas de detección que abarquen tanto el EDR como el XDR, permitiendo una visibilidad integral y una identificación precisa de amenazas. Estas capacidades incluyen:

- ✓ **Detección de Eventos Sospechosos en Endpoint:** Identificación de cambios anómalos, ejecuciones inusuales o procesos ocultos en los dispositivos finales.
- ✓ **Priorización con Inteligencia Artificial:** Utilización de modelos de riesgo para jerarquizar alertas, lo que ayuda a los analistas a enfocarse en las amenazas más críticas y reales.
- ✓ **Asignación Automática a MITRE ATT&CK:** Cada detección debe ser contextualizada automáticamente dentro de la matriz MITRE ATT&CK, facilitando el análisis táctico y la comprensión del comportamiento del atacante.
- ✓ **Detección en Contenedores Linux:** Soporte específico para la detección de amenazas en ambientes modernos como Docker o Kubernetes, asegurando la protección de infraestructuras basadas en contenedores.
- ✓ **Correlación de Eventos entre Productos:** Capacidad clave para una plataforma XDR, que permite ver la progresión de un ataque a través de múltiples capas de seguridad (correo, red, endpoint, servidor, cloud), unificando la información para una visión completa del incidente.

Es fundamental que el sistema se integre con SIEMs (Security Information and Event Management) y otras herramientas SOC (Security Operations Center) para ampliar la visibilidad y mejorar la capacidad de respuesta. Además, debe soportar la detección en entornos híbridos y BYOD (Bring Your Own Device).

Investigación (EDR)

La solución debe proporcionar herramientas robustas para la investigación de incidentes, permitiendo a los analistas comprender a fondo la naturaleza y el alcance de las amenazas. Las capacidades clave incluyen:

- ✓ **Gráficos de Análisis de Causa Raíz (RCA):** Visualización completa del camino del ataque, desde la intrusión inicial hasta la carga útil final, facilitando la comprensión de la secuencia de eventos.
- ✓ **Casos Automáticos y Manuales:** Capacidad para agrupar eventos relacionados y tratarlos como un incidente completo, mejorando la organización y gestión de las investigaciones.
- ✓ **Live Discover y Consultas Programadas:** Herramientas potentes para buscar patrones de amenaza en tiempo real o con periodicidad, permitiendo la caza proactiva de amenazas.
- ✓ **Consultas e investigación de eventos:** la solución deberá permitir consultar y filtrar eventos de seguridad, buscar indicadores de compromiso (IoC) y apoyar la investigación de incidentes mediante las funciones de consulta disponibles en la plataforma. Las consultas podrán ejecutarse bajo demanda o de forma programada, de acuerdo con las necesidades de la Entidad y las capacidades documentadas por el fabricante.
- ✓ **Exportación de Datos Forenses:** Los eventos deben poder exportarse para cumplir con requerimientos regulatorios o peritajes externos, asegurando la cadena de custodia de la evidencia.
- ✓ **Información de Amenazas (Threat Intelligence):** Contextualización de las detecciones con indicadores de compromiso (IOC) y fuentes externas de inteligencia de amenazas, enriqueciendo la investigación.
- ✓ **Gestión de casos e incidentes:** la solución deberá permitir documentar, organizar y dar seguimiento a los casos o incidentes de seguridad, incluyendo la información y las acciones disponibles para su investigación y respuesta. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología específica de inteligencia artificial generativa.

Es crucial que la solución asegure soporte para inteligencia de amenazas en tiempo real y que los datos almacenados puedan ser exportados legalmente según las normativas locales aplicables.

Respuesta (EDR/XDR)

La solución debe ofrecer capacidades de respuesta rápidas y eficientes para contener y remediar las amenazas detectadas. Las funcionalidades clave incluyen:

- ✓ **Limpieza Automática de Malware:** La solución debe ser capaz de remover el malware y restaurar el sistema sin intervención manual, minimizando el impacto de los incidentes.
- ✓ **Remediación y recuperación frente a ransomware:** la solución deberá ofrecer las acciones de remediación o recuperación que soporte para incidentes de cifrado malicioso. El proponente deberá describir las capacidades disponibles y acreditarlas mediante documentación oficial del fabricante; no se exige restauración automática de archivos como mecanismo específico.
- ✓ **Finalización de Procesos:** El EDR debe detener procesos maliciosos activos tan pronto como se detectan, impidiendo su propagación y ejecución.
- ✓ **Aislamiento de Endpoints:** La solución debe permitir el aislamiento automático de endpoints cuando se detecta una amenaza grave, conteniendo el incidente y evitando la propagación lateral.
- ✓ **Respuesta Automatizada por Tipo de Amenaza:** La capacidad de automatizar la respuesta según el tipo de amenaza, permitiendo una acción en segundos en el caso de ataques severos, es crucial para minimizar el tiempo de permanencia de los atacantes.

5. PROTECCIÓN EMAIL

- La consola de administración debe ser Saas
- La solución deberá contar con protección contra phishing y suplantación de identidad, mediante el análisis del contenido, contexto y características de los mensajes para identificar y bloquear intentos de engaño. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una técnica específica de procesamiento de lenguaje natural.
- Manejo de protocolos SPF,DKIM y DMARC
- La solución debe realizar Análisis de reputación
- La solución brinda Protección de antispam, escaneo de malware y sandbox cloud

- Debe poder realizar Detección de URL maliciosas y Reescritura de URL en el momento del clic además de brindar Detección de anomalías del encabezado
- Debe permitir Filtrar por país de origen e idiomas
- Análisis de nombres para mostrar (VIP y marcas)
- Debe contar con Verificaciones de dominios similares
- Políticas DLP de múltiples reglas para grupos y usuarios individuales
- Debe contar con Listas de control de contenido (financieros, contenidos confidenciales, información de salud y PII)
- Cifrado TLS aplicado
- Estándar S/MIME
- Autenticación del remitente
- Cifrado de mensajes y archivos adjuntos basado en push
- La solución debe ofrecer un control integral sobre el flujo de correo electrónico, asegurando la seguridad en todas las direcciones. También escanear minuciosamente tanto los mensajes entrantes para detectar amenazas como los salientes para prevenir la fuga de datos y el spam.
- La solución debe permitir la implementación de políticas a nivel de dominio, grupo y usuario.
- Se debe ofrecer un control granular sobre el correo sospechoso a través de la cuarentena de administrador y usuario, permitiendo a los administradores revisar y liberar mensajes, mientras que los usuarios pueden gestionar sus propios correos en cuarentena.
- Debe tener Banners de correo electrónico entrante (remitente confiable, externo, no confiable)
- Debe permitir Sincronización de AD o sincronización de Azure AD
- Integración mediante API (sin interrupción de flujo de correo, Microsoft nube

Se debe contar con una única consola de administración para la protección de endpoints, servidores, email y firewall. Esta consolidación no es una opción, sino una necesidad estratégica para la ciberseguridad de la entidad y permite una visibilidad completa y correlacionada de todas las amenazas, una respuesta unificada y más rápida a incidentes, y una gestión drásticamente simplificada que reduce la complejidad operativa y los errores humanos, los cuales deben estar dados de acuerdo con la siguiente tabla técnica:

DESCRIPCION DEL BIEN	CANT
SOLUCIÓN INTEGRAL Y UNIFICADA ANTIMALWARE PARA ENDPOINTS Solución integral de seguridad antimalware para endpoints, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar y aplicar políticas de seguridad para la prevención de amenazas, el control de acceso, la protección de datos, el despliegue y la actualización de agentes. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá cumplir, como mínimo, con las siguientes características: • **Gestión basada en la nube (SaaS):** deberá operar sin requerir infraestructura local dedicada para la administración de la solución. • **Consola de administración centralizada:** deberá permitir administrar las capacidades de protección de endpoints y servidores ofertadas, sus políticas de seguridad, informes, despliegue y actualización de agentes desde una misma consola SaaS centralizada. La protección del correo electrónico podrá ser suministrada por un fabricante diferente, con su propia consola SaaS, siempre que cumpla integralmente los requisitos establecidos para dicho componente y se acredite la integración mediante API o conectores para el intercambio de información y la correlación de eventos. • **Agente único:** la protección de endpoints y servidores deberá operar mediante un agente único que integre las funciones de prevención de amenazas, EDR, XDR, firewall de host y DLP básico, administradas desde una misma consola SaaS centralizada. La integración posterior de eventos mediante SIEM, Syslog o API no sustituye la exigencia de agente único ni la capacidad de respuesta y bloqueo unificado en tiempo real. Las funcionalidades complementarias deberán estar incluidas en la solución propuesta y su licenciamiento deberá identificarse claramente. • **Soporte multiplataforma:** deberá soportar, como mínimo, los sistemas operativos empresariales Windows (escritorio y servidor), macOS y Linux, de acuerdo con las versiones y condiciones de compatibilidad establecidas en la ficha técnica.	500

- **Despliegue y actualizaciones centralizadas:** deberá permitir gestionar centralizadamente el despliegue, configuración y actualización de los agentes instalados en los endpoints protegidos.
- **Alta disponibilidad y escalabilidad:** deberá contar con capacidades que permitan mantener la disponibilidad del servicio y ampliar la cobertura de protección según las necesidades de la Entidad.
- **Prevención de ejecución de malware:** deberá detectar y bloquear amenazas conocidas mediante mecanismos de protección antimalware.
- **Detección basada en análisis heurístico y comportamental:** deberá utilizar mecanismos de análisis heurístico, comportamiento, inteligencia artificial o aprendizaje automático para detectar y bloquear malware de día cero, amenazas polimórficas y otras amenazas avanzadas.
- **Protección contra ransomware:** deberá detectar comportamientos asociados con procesos de cifrado malicioso y permitir su bloqueo o contención, así como las acciones de remediación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología o denominación comercial específica.
- **Detección y respuesta en endpoints (EDR):** deberá recolectar y analizar telemetría de los endpoints, proporcionar visibilidad de la cadena de eventos de un ataque y permitir la investigación de incidentes de seguridad y la ejecución de las acciones de respuesta disponibles en la solución.
- **Análisis y control de aplicaciones:** deberá permitir identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas, conforme a las políticas de seguridad configuradas.
- **Control de dispositivos periféricos:** deberá permitir gestionar y controlar el uso de dispositivos USB y otros medios removibles, conforme a las políticas definidas por la Entidad.
- **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante.
- **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección por reputación de URL maliciosas, por sí sola, no acreditará el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y acreditar que está incluida en el licenciamiento propuesto.
- **Prevención básica de pérdida de datos (DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles. El proponente deberá especificar los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria para cumplir este requisito deberá identificarse expresamente e incluirse en la oferta económica.
- **Análisis de comportamiento, investigación de amenazas y protección anti-exploit:** cuando estas capacidades sean exigidas en los documentos del proceso, podrán acreditarse mediante funcionalidades equivalentes de la solución ofertada, siempre que la documentación oficial del fabricante demuestre el cumplimiento de las capacidades técnicas requeridas.
- **Soporte técnico del fabricante:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana (24/7), durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado.
- El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas e identificar las funcionalidades y licencias

incluidas en la solución. La aceptación de equivalencias funcionales no exime del cumplimiento de los requisitos técnicos mínimos establecidos en la presente ficha.	
SOLUCIÓN INTEGRAL DE PROTECCIÓN ANTIMALWARE PARA SERVIDORES Solución de seguridad antimalware para servidores, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar políticas de seguridad, prevenir amenazas, controlar el acceso, proteger los datos y gestionar el despliegue y las actualizaciones de los agentes desde la plataforma de administración. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá proporcionar capacidades de prevención, detección y respuesta en servidores, incluyendo EDR y correlación XDR con los endpoints protegidos, conforme a los requisitos técnicos establecidos en este ítem. Deberá cumplir, como mínimo, con las siguientes características: 10. **Soporte extendido para sistemas operativos de servidor:** deberá ser compatible con los sistemas operativos y versiones de servidor exigidos en la ficha técnica, proporcionando las funcionalidades de prevención, EDR y correlación XDR disponibles para cada versión. El proponente deberá acreditar la compatibilidad y las capacidades efectivamente soportadas mediante documentación oficial del fabricante. 11. **Visibilidad EDR en tiempo real:** deberá recolectar y permitir consultar telemetría de seguridad de los servidores protegidos, incluida la actividad de red entrante y saliente, de acuerdo con las capacidades de la solución y las limitaciones del sistema operativo. 12. **Correlación XDR y detección de movimiento lateral:** deberá permitir correlacionar eventos de seguridad entre los servidores protegidos y los endpoints de usuario, con el propósito de identificar incidentes, comportamientos sospechosos y posibles movimientos laterales dentro del entorno tecnológico de la Entidad. 13. **Control de aplicaciones mediante listas de permitidos (whitelisting):** deberá permitir establecer políticas para autorizar la ejecución de aplicaciones y servicios previamente aprobados y restringir aquellos que no estén autorizados, conforme a las capacidades de la solución ofertada. 14. **Control de acceso y puertos de red:** deberá permitir definir políticas de control de acceso y comunicaciones de red para los servidores, de acuerdo con sus funciones y roles, conforme a las capacidades de la solución y del sistema operativo. 15. **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. 16. **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección de URL maliciosas basada únicamente en reputación no acreditará, por sí sola, el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y demostrar que está incluida en el licenciamiento propuesto. 17. **Prevención básica de pérdida de datos (Data Loss Prevention — DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles, de acuerdo con las capacidades compatibles con el sistema operativo del servidor. El proponente deberá especificar las funcionalidades, los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria deberá identificarse expresamente e incluirse en la oferta económica.	10

18. **Soporte técnico del fabricante 24/7:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas, la compatibilidad con los sistemas operativos y versiones correspondientes, y las funcionalidades incluidas en el licenciamiento ofertado. La instalación del agente, por sí sola, no acreditará el cumplimiento de todas las capacidades requeridas.	
6. SOLUCIÓN INTEGRAL DE PROTECCIÓN DE CORREO ELECTRÓNICO Solución de seguridad para la protección del correo electrónico institucional, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que combine capacidades de filtrado multicapa y tecnologías de inteligencia artificial para detectar, prevenir y bloquear amenazas avanzadas, incluyendo phishing, ransomware, suplantación de identidad y ataques de compromiso de correo empresarial (BEC). Deberá incorporar mecanismos de análisis de archivos adjuntos y URL, sandbox en la nube, protección contra correo no deseado y malware, cifrado de mensajes, políticas de prevención de pérdida de datos (DLP), autenticación del remitente y administración de cuarentena. La solución deberá integrarse con Microsoft 365 mediante API, sin interrupción del flujo de correo electrónico, y contar con una consola de administración centralizada que permita configurar políticas, supervisar eventos de seguridad, gestionar mensajes sospechosos y generar informes de las actividades de protección. La solución deberá cumplir, como mínimo, con las siguientes características: • **Protección contra phishing y suplantación de identidad:** deberá detectar y bloquear intentos de phishing, suplantación de identidad y ataques BEC mediante el análisis del contenido, contexto y características de los mensajes. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una técnica específica de procesamiento de lenguaje natural o una tecnología determinada de inteligencia artificial. • **Autenticación del correo electrónico:** deberá soportar los mecanismos SPF, DKIM y DMARC para validar la autenticidad de los remitentes y contribuir a la detección de mensajes fraudulentos. • **Análisis de reputación:** deberá disponer de mecanismos para analizar la reputación de remitentes, dominios y direcciones IP, con el propósito de identificar mensajes potencialmente maliciosos o no deseados. • **Protección antispam y antimalware:** deberá incorporar filtrado antispam, análisis de malware y sandbox en la nube para el análisis dinámico de archivos adjuntos y otros elementos potencialmente maliciosos. • **Detección y reescritura de URL:** deberá detectar URL maliciosas y permitir la reescritura de enlaces para verificar su seguridad en el momento en que el usuario haga clic. Asimismo, deberá detectar anomalías en los encabezados de los mensajes que puedan indicar suplantación o actividad sospechosa. • **Filtrado por país e idioma:** deberá permitir aplicar reglas de filtrado o tratamiento de mensajes según el país de origen y el idioma, conforme a las capacidades de la solución ofertada. • **Detección de suplantación de nombres visibles:** deberá permitir analizar los nombres para mostrar de los remitentes e identificar posibles suplantaciones de personas VIP, directivos, usuarios o marcas de la Entidad. • **Detección de dominios similares:** deberá identificar dominios similares al dominio legítimo de la Entidad o a dominios de confianza, con el fin de detectar posibles intentos de suplantación y fraude. • **Prevención de pérdida de datos (DLP):** deberá permitir configurar políticas DLP con múltiples reglas aplicables a grupos y usuarios individuales, incluyendo controles sobre información financiera, contenidos confidenciales, información relacionada con la salud y datos personales identificables (PII).	400

• **Cifrado de comunicaciones mediante TLS:** deberá soportar TLS para proteger las comunicaciones de correo electrónico durante el transporte, conforme a las capacidades de la solución y las condiciones de interoperabilidad aplicables. • **Compatibilidad con S/MIME:** deberá soportar el estándar S/MIME para el cifrado y la firma digital de mensajes, de acuerdo con las funcionalidades y condiciones de licenciamiento ofertadas. • **Autenticación del remitente:** deberá contar con mecanismos para verificar la autenticidad de los remitentes y detectar posibles falsificaciones, de acuerdo con las funcionalidades requeridas. • **Cifrado de mensajes y archivos adjuntos:** deberá permitir proteger mensajes y archivos adjuntos sensibles mediante mecanismos de cifrado con entrega protegida al destinatario (push encryption), conforme a las políticas de seguridad configuradas. • **Protección del correo entrante y saliente:** deberá analizar los mensajes entrantes para detectar amenazas, spam, suplantación y contenido malicioso, así como aplicar controles al correo saliente para prevenir fugas de información y el envío de mensajes maliciosos o no autorizados. • **Administración granular de políticas:** deberá permitir configurar y aplicar políticas de seguridad a nivel de dominio, grupo y usuario individual. • **Administración de cuarentena:** deberá permitir a los administradores revisar y liberar mensajes retenidos y ofrecer a los usuarios mecanismos para consultar y gestionar sus propios mensajes en cuarentena, de acuerdo con los permisos y políticas definidos por la Entidad. • **Banners de seguridad en mensajes entrantes:** deberá permitir identificar los mensajes entrantes mediante avisos visuales configurables que indiquen, como mínimo, las categorías de remitente confiable, externo y no confiable. • **Sincronización de directorios:** deberá permitir sincronizar usuarios y grupos desde Active Directory (AD) o Microsoft Entra ID (Azure AD), según la infraestructura de la Entidad y las capacidades de integración de la solución. • **Integración mediante API con Microsoft 365:** deberá disponer de integración mediante API con Microsoft 365, sin interrupción del flujo de correo electrónico, de acuerdo con las condiciones establecidas en los documentos del proceso. El proponente deberá acreditar el mecanismo de integración y las funcionalidades de protección disponibles mediante documentación técnica oficial del fabricante. • **Consola SaaS y generación de informes:** deberá disponer de una consola centralizada en la nube que permita administrar las políticas de seguridad, consultar eventos, gestionar la cuarentena y generar informes sobre amenazas detectadas, acciones ejecutadas y actividades relevantes para el seguimiento de la seguridad institucional. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar el cumplimiento integral de cada característica exigida, incluyendo los mecanismos de integración con Microsoft 365 y las funcionalidades disponibles en el licenciamiento ofertado. Los módulos o licencias adicionales necesarios para cumplir los requisitos deberán identificarse expresamente e incluirse en la oferta económica. La solución de protección de correo electrónico podrá corresponder a un fabricante diferente del utilizado para la protección de endpoints y servidores. En ese caso, se administrará desde la consola SaaS propia del fabricante de correo y deberá acreditarse la integración mediante API o conectores para el intercambio de información y la correlación de eventos. Esta condición no exime del cumplimiento integral de los requisitos técnicos aplicables a cada componente.	
7. SOLUCIÓN DE PROTECCIÓN PARA SISTEMAS OPERATIVOS DE SERVIDORES, INCLUIDOS SISTEMAS FUERA DE SOPORTE La solución deberá proporcionar protección antimalware para los equipos servidores que utilicen sistemas operativos actualmente soportados y para aquellos que se encuentren fuera del ciclo de soporte del fabricante, de acuerdo con las capacidades compatibles con cada sistema operativo. • **Protección de sistemas operativos fuera de soporte:** Para los servidores que utilicen versiones de Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, RHEL,	1

CentOS u otros sistemas operativos que la Entidad identifique y que se encuentren fuera del soporte del fabricante, se deberá garantizar protección antimalware compatible, de acuerdo con las capacidades disponibles para cada versión. Para estos sistemas no será obligatorio disponer de funcionalidades EDR/XDR. • **Capacidades EDR/XDR para sistemas operativos soportados:** Los sistemas operativos que cuenten con soporte vigente del fabricante de la solución deberán disponer de las funcionalidades EDR/XDR exigidas en la ficha técnica, incluyendo detección de amenazas, análisis de eventos y correlación automática de eventos entre servidores y endpoints, según corresponda. • **Protección sin conexión:** La solución deberá indicar las capacidades de prevención y detección que puede mantener localmente cuando un servidor pierda temporalmente la conexión con la consola de administración SaaS, así como las limitaciones aplicables a cada sistema operativo. • **Detección de anomalías de comportamiento:** Para los sistemas operativos soportados que dispongan de las funcionalidades correspondientes, la solución deberá permitir identificar comportamientos anómalos y generar alertas para su investigación. • **Prevención de pérdida de datos (DLP):** La solución deberá permitir monitorear y bloquear, según las capacidades compatibles con el sistema operativo, las transferencias no autorizadas de información sensible. El proponente deberá identificar las funcionalidades, canales de control y licenciamiento requeridos para cumplir este requisito. • **Soporte técnico:** Se deberá disponer del soporte técnico del fabricante 24/7, de acuerdo con las condiciones de soporte aplicables a la solución ofrecida y a los sistemas operativos correspondientes. • **Acreditación del cumplimiento:** El proponente deberá aportar documentación técnica oficial del fabricante que permita verificar la compatibilidad con los sistemas operativos ofertados y diferenciar las funcionalidades disponibles para sistemas operativos soportados y fuera de soporte. La instalación de un agente, por sí sola, no acreditará el cumplimiento de las funcionalidades exigidas. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar la compatibilidad con cada sistema operativo y versión identificados por la Entidad, así como las funcionalidades efectivamente disponibles para cada uno. La instalación del agente, por sí sola, no acreditará el cumplimiento de las capacidades de prevención, EDR, correlación XDR, protección sin conexión y detección de anomalías exigidas.	
8. SERVICIOS PROFESIONALES DE INGENIERÍA PARA IMPLEMENTACIÓN Y SOPORTE El contratista deberá prestar servicios profesionales de ingeniería para la implementación, configuración, puesta en funcionamiento y soporte de las soluciones de protección de endpoints, servidores y correo electrónico, así como para la gestión del inventario de activos tecnológicos, la gestión de vulnerabilidades y el control remoto. **5.1. Implementación y configuración:** Instalación, configuración y puesta en funcionamiento de las soluciones de protección de endpoints, servidores y correo electrónico, de acuerdo con las características técnicas de las soluciones ofertadas y los requerimientos de la Entidad. **5.2. Inventario centralizado de equipos:** La solución de protección de endpoints y servidores deberá disponer de una funcionalidad que permita descubrir, identificar, registrar, consultar y monitorear centralizadamente los equipos administrados. Como mínimo, deberá permitir visualizar el nombre del equipo, dirección IP, tipo de equipo, tipo y versión del sistema operativo, estado de administración, versión del agente o producto de seguridad instalado, problemas o alertas de seguridad detectados, fecha y hora de la última sincronización o comunicación con la consola, política de seguridad asignada y estado de aplicación de dicha política. Asimismo, deberá permitir buscar y filtrar los equipos por nombre, dirección IP, sistema operativo, estado de protección y estado de administración, así como generar o exportar reportes del	1

inventario desde una consola de administración centralizada. La información deberá actualizarse de acuerdo con la detección y comunicación de los equipos con la solución. El proponente deberá acreditar estas capacidades mediante documentación técnica oficial del fabricante. El inventario comprenderá los equipos detectados o administrados por la solución y no implicará. **5.3. Gestión de vulnerabilidades:** La solución ofertada deberán permitir identificar, evaluar y realizar seguimiento a las vulnerabilidades de los activos tecnológicos incluidos en el alcance **5.4. Control remoto:** Se deberá disponer de funcionalidades o herramientas que permitan realizar actividades de asistencia y administración remota de los equipos incluidos en el alcance, de acuerdo con los permisos, procedimientos de seguridad y autorizaciones definidos por la Entidad. **5.5. Soporte técnico:** El contratista deberá proporcionar acompañamiento y soporte técnico para la implementación, configuración y operación de las soluciones objeto del contrato, conforme a las condiciones y el alcance establecidos en los documentos del proceso.	

De ustedes atentamente,

NOMBRE DEL PROPONENTE: _____
DIRECCIÓN: _____ CIUDAD _____
TELÉFONO: _____ FAX: _____
NOMBRE DEL REPRESENTANTE LEGAL: _____
FIRMA DEL REPRESENTANTE LEGAL O APODERADO: _____

FORMULARIO No. 7

CARTA DE PRESENTACIÓN DE LA PROPUESTA ECONÓMICA
(Este formato se debe presentar en el sobre No 2 Propuesta Económica, debidamente cerrado)

Ciudad, _____ del 20__

Doctor
WALFRANDO FORERO BEJARANO
ALCALDE MUNICIPAL DE TOCANCIPA
Calle 11 No. 6-12
Tocancipá - Cundinamarca

REF: **SASI ____ MT 202__**
OBJETO: ***(INDICAR OBJETO)***,

El abajo firmante, actuando en nombre y representación de _____ de acuerdo con el pliego de condiciones, hacemos la siguiente propuesta económica:

DESCRIPCION DEL BIEN	CANT
SOLUCIÓN INTEGRAL Y UNIFICADA ANTIMALWARE PARA ENDPOINTS Solución integral de seguridad antimalware para endpoints, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar y aplicar políticas de seguridad para la prevención de amenazas, el control de acceso, la protección de datos, el despliegue y la actualización de agentes. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente. La solución deberá cumplir, como mínimo, con las siguientes características: • **Gestión basada en la nube (SaaS):** deberá operar sin requerir infraestructura local dedicada para la administración de la solución. • **Consola de administración centralizada:** deberá permitir administrar las capacidades de protección de endpoints y servidores ofertadas, sus políticas de seguridad, informes, despliegue y actualización de agentes desde una misma consola SaaS centralizada. La protección del correo electrónico podrá ser suministrada por un fabricante diferente, con su propia consola SaaS, siempre que cumpla integralmente los requisitos establecidos para dicho componente y se acredite la integración mediante API o conectores para el intercambio de información y la correlación de eventos. • **Agente único:** la protección de endpoints y servidores deberá operar mediante un agente único que integre las funciones de prevención de amenazas, EDR, XDR, firewall de host y DLP básico, administradas desde una misma consola SaaS centralizada. La integración posterior de eventos mediante SIEM, Syslog o API no sustituye la exigencia de agente único ni la capacidad de respuesta y bloqueo unificado en tiempo real. Las funcionalidades complementarias deberán estar incluidas en la solución propuesta y su licenciamiento deberá identificarse claramente. • **Soporte multiplataforma:** deberá soportar, como mínimo, los sistemas operativos empresariales Windows (escritorio y servidor), macOS y Linux, de acuerdo con las versiones y condiciones de compatibilidad establecidas en la ficha técnica. • **Despliegue y actualizaciones centralizadas:** deberá permitir gestionar centralizadamente el despliegue, configuración y actualización de los agentes instalados en los endpoints protegidos. • **Alta disponibilidad y escalabilidad:** deberá contar con capacidades que permitan mantener la disponibilidad del servicio y ampliar la cobertura de protección según las necesidades de la Entidad. • **Prevención de ejecución de malware:** deberá detectar y bloquear amenazas conocidas mediante mecanismos de protección antimalware.	500

• **Detección basada en análisis heurístico y comportamental:** deberá utilizar mecanismos de análisis heurístico, comportamiento, inteligencia artificial o aprendizaje automático para detectar y bloquear malware de día cero, amenazas polimórficas y otras amenazas avanzadas. • **Protección contra ransomware:** deberá detectar comportamientos asociados con procesos de cifrado malicioso y permitir su bloqueo o contención, así como las acciones de remediación disponibles en la solución. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una tecnología o denominación comercial específica. • **Detección y respuesta en endpoints (EDR):** deberá recolectar y analizar telemetría de los endpoints, proporcionar visibilidad de la cadena de eventos de un ataque y permitir la investigación de incidentes de seguridad y la ejecución de las acciones de respuesta disponibles en la solución. • **Análisis y control de aplicaciones:** deberá permitir identificar y bloquear la ejecución de aplicaciones no autorizadas o potencialmente no deseadas, conforme a las políticas de seguridad configuradas. • **Control de dispositivos periféricos:** deberá permitir gestionar y controlar el uso de dispositivos USB y otros medios removibles, conforme a las políticas definidas por la Entidad. • **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. • **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección por reputación de URL maliciosas, por sí sola, no acreditará el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y acreditar que está incluida en el licenciamiento propuesto. • **Prevención básica de pérdida de datos (DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles. El proponente deberá especificar los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria para cumplir este requisito deberá identificarse expresamente e incluirse en la oferta económica. • **Análisis de comportamiento, investigación de amenazas y protección anti-exploit:** cuando estas capacidades sean exigidas en los documentos del proceso, podrán acreditarse mediante funcionalidades equivalentes de la solución ofertada, siempre que la documentación oficial del fabricante demuestre el cumplimiento de las capacidades técnicas requeridas. • **Soporte técnico del fabricante:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana (24/7), durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. • El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas e identificar las funcionalidades y licencias incluidas en la solución. La aceptación de equivalencias funcionales no exime del cumplimiento de los requisitos técnicos mínimos establecidos en la presente ficha.	
SOLUCIÓN INTEGRAL DE PROTECCIÓN ANTIMALWARE PARA SERVIDORES Solución de seguridad antimalware para servidores, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que permita configurar políticas de seguridad, prevenir amenazas, controlar el acceso, proteger los datos y gestionar el despliegue y las actualizaciones de los agentes desde la plataforma de administración. La solución deberá incluir el licenciamiento requerido, la puesta en funcionamiento, el soporte del fabricante y la garantía correspondiente.	10

La solución deberá proporcionar capacidades de prevención, detección y respuesta en servidores, incluyendo EDR y correlación XDR con los endpoints protegidos, conforme a los requisitos técnicos establecidos en este ítem. Deberá cumplir, como mínimo, con las siguientes características: 19. **Soporte extendido para sistemas operativos de servidor:** deberá ser compatible con los sistemas operativos y versiones de servidor exigidos en la ficha técnica, proporcionando las funcionalidades de prevención, EDR y correlación XDR disponibles para cada versión. El proponente deberá acreditar la compatibilidad y las capacidades efectivamente soportadas mediante documentación oficial del fabricante. 20. **Visibilidad EDR en tiempo real:** deberá recolectar y permitir consultar telemetría de seguridad de los servidores protegidos, incluida la actividad de red entrante y saliente, de acuerdo con las capacidades de la solución y las limitaciones del sistema operativo. 21. **Correlación XDR y detección de movimiento lateral:** deberá permitir correlacionar eventos de seguridad entre los servidores protegidos y los endpoints de usuario, con el propósito de identificar incidentes, comportamientos sospechosos y posibles movimientos laterales dentro del entorno tecnológico de la Entidad. 22. **Control de aplicaciones mediante listas de permitidos (whitelisting):** deberá permitir establecer políticas para autorizar la ejecución de aplicaciones y servicios previamente aprobados y restringir aquellos que no estén autorizados, conforme a las capacidades de la solución ofertada. 23. **Control de acceso y puertos de red:** deberá permitir definir políticas de control de acceso y comunicaciones de red para los servidores, de acuerdo con sus funciones y roles, conforme a las capacidades de la solución y del sistema operativo. 24. **Firewall de host bidireccional:** la solución deberá integrar en el mismo agente único de protección para endpoints y servidores la funcionalidad de firewall de host, permitiendo definir y administrar centralizadamente políticas de control del tráfico de red entrante y saliente desde la consola SaaS ofertada. El alcance corresponde exclusivamente al firewall a nivel de host; no se exige firewall perimetral. El cumplimiento deberá acreditarse mediante documentación oficial del fabricante. 25. **Control de contenido web y filtrado de URL:** deberá permitir aplicar políticas de filtrado web por categorías de contenido o grupos de URL. La detección de URL maliciosas basada únicamente en reputación no acreditará, por sí sola, el cumplimiento del filtrado por categorías. El proponente deberá identificar la funcionalidad ofertada y demostrar que está incluida en el licenciamiento propuesto. 26. **Prevención básica de pérdida de datos (Data Loss Prevention — DLP):** deberá permitir monitorear y bloquear transferencias de datos sensibles e incluir Listas de Control de Contenido (CCL), identificación de tipos de datos sensibles —como tarjetas de crédito, información de identificación personal (PII) y cuentas bancarias— y control sobre múltiples destinos y dispositivos extraíbles, de acuerdo con las capacidades compatibles con el sistema operativo del servidor. El proponente deberá especificar las funcionalidades, los canales cubiertos, las acciones de control disponibles y los módulos o licencias requeridos. Toda licencia necesaria deberá identificarse expresamente e incluirse en la oferta económica. 27. **Soporte técnico del fabricante 24/7:** deberá contar con soporte técnico del fabricante disponible las veinticuatro (24) horas del día, los siete (7) días de la semana, durante la vigencia del licenciamiento, conforme a las condiciones del servicio ofertado. El proponente deberá presentar documentación oficial del fabricante que permita verificar el cumplimiento de las características exigidas, la compatibilidad con los sistemas operativos y versiones correspondientes, y las funcionalidades incluidas en el licenciamiento ofertado. La instalación del agente, por sí sola, no acreditará el cumplimiento de todas las capacidades requeridas.	
9. SOLUCIÓN INTEGRAL DE PROTECCIÓN DE CORREO ELECTRÓNICO	400

Solución de seguridad para la protección del correo electrónico institucional, administrada mediante una consola centralizada en la nube bajo modalidad SaaS, que combine capacidades de filtrado multicapa y tecnologías de inteligencia artificial para detectar, prevenir y bloquear amenazas avanzadas, incluyendo phishing, ransomware, suplantación de identidad y ataques de compromiso de correo empresarial (BEC). Deberá incorporar mecanismos de análisis de archivos adjuntos y URL, sandbox en la nube, protección contra correo no deseado y malware, cifrado de mensajes, políticas de prevención de pérdida de datos (DLP), autenticación del remitente y administración de cuarentena. La solución deberá integrarse con Microsoft 365 mediante API, sin interrupción del flujo de correo electrónico, y contar con una consola de administración centralizada que permita configurar políticas, supervisar eventos de seguridad, gestionar mensajes sospechosos y generar informes de las actividades de protección. La solución deberá cumplir, como mínimo, con las siguientes características: • **Protección contra phishing y suplantación de identidad:** deberá detectar y bloquear intentos de phishing, suplantación de identidad y ataques BEC mediante el análisis del contenido, contexto y características de los mensajes. El cumplimiento se acreditará mediante documentación oficial del fabricante, sin exigir una técnica específica de procesamiento de lenguaje natural o una tecnología determinada de inteligencia artificial. • **Autenticación del correo electrónico:** deberá soportar los mecanismos SPF, DKIM y DMARC para validar la autenticidad de los remitentes y contribuir a la detección de mensajes fraudulentos. • **Análisis de reputación:** deberá disponer de mecanismos para analizar la reputación de remitentes, dominios y direcciones IP, con el propósito de identificar mensajes potencialmente maliciosos o no deseados. • **Protección antispam y antimalware:** deberá incorporar filtrado antispam, análisis de malware y sandbox en la nube para el análisis dinámico de archivos adjuntos y otros elementos potencialmente maliciosos. • **Detección y reescritura de URL:** deberá detectar URL maliciosas y permitir la reescritura de enlaces para verificar su seguridad en el momento en que el usuario haga clic. Asimismo, deberá detectar anomalías en los encabezados de los mensajes que puedan indicar suplantación o actividad sospechosa. • **Filtrado por país e idioma:** deberá permitir aplicar reglas de filtrado o tratamiento de mensajes según el país de origen y el idioma, conforme a las capacidades de la solución ofertada. • **Detección de suplantación de nombres visibles:** deberá permitir analizar los nombres para mostrar de los remitentes e identificar posibles suplantaciones de personas VIP, directivos, usuarios o marcas de la Entidad. • **Detección de dominios similares:** deberá identificar dominios similares al dominio legítimo de la Entidad o a dominios de confianza, con el fin de detectar posibles intentos de suplantación y fraude. • **Prevención de pérdida de datos (DLP):** deberá permitir configurar políticas DLP con múltiples reglas aplicables a grupos y usuarios individuales, incluyendo controles sobre información financiera, contenidos confidenciales, información relacionada con la salud y datos personales identificables (PII). • **Cifrado de comunicaciones mediante TLS:** deberá soportar TLS para proteger las comunicaciones de correo electrónico durante el transporte, conforme a las capacidades de la solución y las condiciones de interoperabilidad aplicables. • **Compatibilidad con S/MIME:** deberá soportar el estándar S/MIME para el cifrado y la firma digital de mensajes, de acuerdo con las funcionalidades y condiciones de licenciamiento ofertadas. • **Autenticación del remitente:** deberá contar con mecanismos para verificar la autenticidad de los remitentes y detectar posibles falsificaciones, de acuerdo con las funcionalidades requeridas. • **Cifrado de mensajes y archivos adjuntos:** deberá permitir proteger mensajes y archivos adjuntos sensibles mediante mecanismos de cifrado con entrega protegida al destinatario (push encryption), conforme a las políticas de seguridad configuradas.	

• **Protección del correo entrante y saliente:** deberá analizar los mensajes entrantes para detectar amenazas, spam, suplantación y contenido malicioso, así como aplicar controles al correo saliente para prevenir fugas de información y el envío de mensajes maliciosos o no autorizados. • **Administración granular de políticas:** deberá permitir configurar y aplicar políticas de seguridad a nivel de dominio, grupo y usuario individual. • **Administración de cuarentena:** deberá permitir a los administradores revisar y liberar mensajes retenidos y ofrecer a los usuarios mecanismos para consultar y gestionar sus propios mensajes en cuarentena, de acuerdo con los permisos y políticas definidos por la Entidad. • **Banners de seguridad en mensajes entrantes:** deberá permitir identificar los mensajes entrantes mediante avisos visuales configurables que indiquen, como mínimo, las categorías de remitente confiable, externo y no confiable. • **Sincronización de directorios:** deberá permitir sincronizar usuarios y grupos desde Active Directory (AD) o Microsoft Entra ID (Azure AD), según la infraestructura de la Entidad y las capacidades de integración de la solución. • **Integración mediante API con Microsoft 365:** deberá disponer de integración mediante API con Microsoft 365, sin interrupción del flujo de correo electrónico, de acuerdo con las condiciones establecidas en los documentos del proceso. El proponente deberá acreditar el mecanismo de integración y las funcionalidades de protección disponibles mediante documentación técnica oficial del fabricante. • **Consola SaaS y generación de informes:** deberá disponer de una consola centralizada en la nube que permita administrar las políticas de seguridad, consultar eventos, gestionar la cuarentena y generar informes sobre amenazas detectadas, acciones ejecutadas y actividades relevantes para el seguimiento de la seguridad institucional. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar el cumplimiento integral de cada característica exigida, incluyendo los mecanismos de integración con Microsoft 365 y las funcionalidades disponibles en el licenciamiento ofertado. Los módulos o licencias adicionales necesarios para cumplir los requisitos deberán identificarse expresamente e incluirse en la oferta económica. La solución de protección de correo electrónico podrá corresponder a un fabricante diferente del utilizado para la protección de endpoints y servidores. En ese caso, se administrará desde la consola SaaS propia del fabricante de correo y deberá acreditarse la integración mediante API o conectores para el intercambio de información y la correlación de eventos. Esta condición no exime del cumplimiento integral de los requisitos técnicos aplicables a cada componente.	
10. SOLUCIÓN DE PROTECCIÓN PARA SISTEMAS OPERATIVOS DE SERVIDORES, INCLUIDOS SISTEMAS FUERA DE SOPORTE La solución deberá proporcionar protección antimalware para los equipos servidores que utilicen sistemas operativos actualmente soportados y para aquellos que se encuentren fuera del ciclo de soporte del fabricante, de acuerdo con las capacidades compatibles con cada sistema operativo. • **Protección de sistemas operativos fuera de soporte:** Para los servidores que utilicen versiones de Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, RHEL, CentOS u otros sistemas operativos que la Entidad identifique y que se encuentren fuera del soporte del fabricante, se deberá garantizar protección antimalware compatible, de acuerdo con las capacidades disponibles para cada versión. Para estos sistemas no será obligatorio disponer de funcionalidades EDR/XDR. • **Capacidades EDR/XDR para sistemas operativos soportados:** Los sistemas operativos que cuenten con soporte vigente del fabricante de la solución deberán disponer de las funcionalidades EDR/XDR exigidas en la ficha técnica, incluyendo detección de amenazas, análisis de eventos y correlación automática de eventos entre servidores y endpoints, según corresponda. • **Protección sin conexión:** La solución deberá indicar las capacidades de prevención y detección que puede mantener localmente cuando un servidor pierda temporalmente la	1

conexión con la consola de administración SaaS, así como las limitaciones aplicables a cada sistema operativo. • **Detección de anomalías de comportamiento:** Para los sistemas operativos soportados que dispongan de las funcionalidades correspondientes, la solución deberá permitir identificar comportamientos anómalos y generar alertas para su investigación. • **Prevención de pérdida de datos (DLP):** La solución deberá permitir monitorear y bloquear, según las capacidades compatibles con el sistema operativo, las transferencias no autorizadas de información sensible. El proponente deberá identificar las funcionalidades, canales de control y licenciamiento requeridos para cumplir este requisito. • **Soporte técnico:** Se deberá disponer del soporte técnico del fabricante 24/7, de acuerdo con las condiciones de soporte aplicables a la solución ofrecida y a los sistemas operativos correspondientes. • **Acreditación del cumplimiento:** El proponente deberá aportar documentación técnica oficial del fabricante que permita verificar la compatibilidad con los sistemas operativos ofertados y diferenciar las funcionalidades disponibles para sistemas operativos soportados y fuera de soporte. La instalación de un agente, por sí sola, no acreditará el cumplimiento de las funcionalidades exigidas. El proponente deberá presentar documentación técnica oficial del fabricante que permita verificar la compatibilidad con cada sistema operativo y versión identificados por la Entidad, así como las funcionalidades efectivamente disponibles para cada uno. La instalación del agente, por sí sola, no acreditará el cumplimiento de las capacidades de prevención, EDR, correlación XDR, protección sin conexión y detección de anomalías exigidas.	
11. SERVICIOS PROFESIONALES DE INGENIERÍA PARA IMPLEMENTACIÓN Y SOPORTE El contratista deberá prestar servicios profesionales de ingeniería para la implementación, configuración, puesta en funcionamiento y soporte de las soluciones de protección de endpoints, servidores y correo electrónico, así como para la gestión del inventario de activos tecnológicos, la gestión de vulnerabilidades y el control remoto. **5.1. Implementación y configuración:** Instalación, configuración y puesta en funcionamiento de las soluciones de protección de endpoints, servidores y correo electrónico, de acuerdo con las características técnicas de las soluciones ofertadas y los requerimientos de la Entidad. **5.2. Inventario centralizado de equipos:** La solución de protección de endpoints y servidores deberá disponer de una funcionalidad que permita descubrir, identificar, registrar, consultar y monitorear centralizadamente los equipos administrados. Como mínimo, deberá permitir visualizar el nombre del equipo, dirección IP, tipo de equipo, tipo y versión del sistema operativo, estado de administración, versión del agente o producto de seguridad instalado, problemas o alertas de seguridad detectados, fecha y hora de la última sincronización o comunicación con la consola, política de seguridad asignada y estado de aplicación de dicha política. Asimismo, deberá permitir buscar y filtrar los equipos por nombre, dirección IP, sistema operativo, estado de protección y estado de administración, así como generar o exportar reportes del inventario desde una consola de administración centralizada. La información deberá actualizarse de acuerdo con la detección y comunicación de los equipos con la solución. El proponente deberá acreditar estas capacidades mediante documentación técnica oficial del fabricante. El inventario comprenderá los equipos detectados o administrados por la solución y no implicará. **5.3. Gestión de vulnerabilidades:** La solución ofertada deberán permitir identificar, evaluar y realizar seguimiento a las vulnerabilidades de los activos tecnológicos incluidos en el alcance **5.4. Control remoto:** Se deberá disponer de funcionalidades o herramientas que permitan realizar actividades de asistencia y administración remota de los equipos incluidos en el alcance, de acuerdo con los permisos, procedimientos de seguridad y autorizaciones definidos por la Entidad.	1

5.5. Soporte técnico: El contratista deberá proporcionar acompañamiento y soporte técnico para la implementación, configuración y operación de las soluciones objeto del contrato, conforme a las condiciones y el alcance establecidos en los documentos del proceso.	

Atentamente,

NOMBRE DEL PROPONENTE: _____

DIRECCIÓN: _____

CIUDAD _____

TELÉFONO: _____FAX:_____

NOMBRE DEL REPRESENTANTE LEGAL: _____