

ALCALDÍA DE PEREIRA

Secretaría de Tecnologías de la Información y las Comunicaciones

FORMATO DE COTIZACIÓN

Solución integral de ciberseguridad (protección de endpoints, correo electrónico, correlación de eventos)

El presente formato debe ser diligenciado por el proponente y presentado dentro del proceso de invitación a cotizar adelantado por la Alcaldía de Pereira. La descripción de los ítems es de carácter general y funcional; no se exige ni se hace referencia a marca o fabricante específico, en garantía de la pluralidad de oferentes. El proveedor debe indicar el elemento que ofrece para cada ítem en la tabla de la página siguiente. El Anexo Técnico incluido al final de este formato detalla las condiciones mínimas que debe cumplir cada ítem.

1. Datos del proponente

Razón social: SPECTRA INGENIERIA SAS

NIT: 805.027.282-8

Representante legal: Guillermo Andrés González Vélez

Contacto / Teléfono / Correo: jorgecifuentes@spectra.com.co

Ciudad: Cali

Fecha de la oferta: 17 Septiembre del 2026

2. Oferta económica

Ítem	Descripción del componente / servicio requerido	Métrica de licenciamiento	Cantidad	Vigencia	Elemento ofertado por el proveedor (marca / referencia / descripción del producto propuesto)	Valor unitario	Valor total	Observaciones
1	Protección avanzada para endpoints (EDR): estaciones de trabajo, portátiles, servidores físicos/virtuales y	Por endpoint / dispositivo protegido	1.000	12 meses	Kaspersky Next EDR Expert License	\$73.000	\$73.000.000	

Ítem	Descripción del componente / servicio requerido	Métrica de licenciamiento	Cantidad	Vigencia	Elemento ofertado por el proveedor (marca / referencia / descripción del producto propuesto)	Valor unitario	Valor total	Observaciones
	dispositivos móviles corporativos.							
2	Integración de dispositivos de seguridad perimetral (firewalls) a la plataforma centralizada de correlación de eventos.	Por dispositivo integrado	2	12 meses	Kaspersky KUMA Servicio de conexión y configuración de 2 firewalls con la plataforma KUMA para la centralización de registros y eventos de seguridad. Incluye parametrización de las fuentes, habilitación y verificación del envío de logs, comprobación de la comunicación con la plataforma, pruebas de recepción de información y validación de la adecuada correlación y procesamiento de los eventos generados por los dispositivos.	\$13.100.000	\$26.200.000	
3	Protección especializada de correo electrónico institucional (plataforma de nube corporativa) frente a phishing, malware, ransomware, suplantación y demás amenazas dirigidas al correo.	Por buzón protegido	640	12 meses	Acronis Acronis Advanced Email Security Servicio de seguridad para 640 cuentas de correo electrónico institucional, orientado a fortalecer la protección del correo frente a amenazas cibernéticas. Incluye la configuración y habilitación de controles de seguridad en la nube para la identificación y bloqueo de phishing, malware, ransomware,	\$220.312,5	\$141.000.000	

Ítem	Descripción del componente / servicio requerido	Métrica de licenciamiento	Cantidad	Vigencia	Elemento ofertado por el proveedor (marca / referencia / descripción del producto propuesto)	Valor unitario	Valor total	Observaciones
					suplantación de identidad y demás técnicas maliciosas, junto con la validación de la correcta operación y cobertura del servicio.			
4	Plataforma centralizada para la recepción, correlación, investigación y automatización de respuesta ante eventos e incidentes de seguridad (tipo SIEM, con capacidades de detección extendida y orquestación).	Por plataforma / suscripción	1	12 meses	Kaspersky Unified Monitoring and Analysis Platform Servicio de monitoreo y análisis centralizado de seguridad Plataforma destinada a consolidar y procesar información de seguridad proveniente de múltiples fuentes, permitiendo la supervisión, correlación, análisis e investigación de eventos para la detección y gestión oportuna de incidentes. La solución contempla funcionalidades SIEM, capacidades de detección extendida XDR y mecanismos de automatización, orquestación y respuesta ante eventos de seguridad mediante SOAR.	\$311.000.000	\$311.000.000	
5	Plataforma de concienciación y	Por usuario licenciado	200	12 meses	Kaspersky Plataforma de concienciación y formación	\$99.000	\$19.800.000	

Ítem	Descripción del componente / servicio requerido	Métrica de licenciamiento	Cantidad	Vigencia	Elemento ofertado por el proveedor (marca / referencia / descripción del producto propuesto)	Valor unitario	Valor total	Observaciones
	capacitación en ciberseguridad para usuarios institucionales, con simulaciones de phishing y seguimiento de resultados.				en ciberseguridad Servicio de sensibilización dirigido a usuarios mediante programas de capacitación, campañas de seguridad, simulaciones de ataques de phishing y actividades de evaluación, con herramientas para el monitoreo de la participación, medición de conocimientos y seguimiento de los resultados obtenidos.			
SUBTOTAL							\$571.000.000	
IVA							0	
VALOR TOTAL DE LA OFERTA							\$571.000.000	

3. Condiciones generales del servicio

Los siguientes lineamientos generales aplican a la totalidad del licenciamiento y servicios ofertados; el Anexo Técnico incluido a continuación detalla las condiciones mínimas de cada componente.

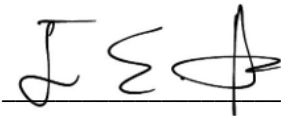
- Licenciamiento vigente por un período mínimo de doce (12) meses, incluyendo actualizaciones, soporte del fabricante y corrección de vulnerabilidades, sin costos adicionales.
- Los componentes de protección de endpoints, correlación de eventos y concienciación deberán operar de manera integrada y nativa entre sí, permitiendo el intercambio automático de información. El componente de protección de correo electrónico podrá integrarse mediante mecanismos estándar (API u otros oficialmente soportados).
- Soporte técnico especializado bajo esquema de atención continua (7x24) para la plataforma de correlación de eventos, con los tiempos máximos de atención detallados en el Anexo Técnico.
- Implementación presencial en las sedes de la Alcaldía de Pereira, con transferencia de conocimiento y capacitación técnica incluidas para el personal designado por la Entidad.
- Equipo técnico certificado en las tecnologías ofertadas, con centro de soporte propio ubicado en Colombia y atención en idioma español.
- Todos los componentes, licencias, conectores e integraciones necesarios para el cumplimiento del alcance deberán quedar incluidos en la oferta económica, sin generar costos ocultos para la Entidad.

4. Condiciones comerciales

Validez de la oferta	90 días
Forma de pago	Firmada acta de recibido a satisfacción
Tiempo de implementación	45 días
Moneda y tratamiento de IVA	Pesos

5. Declaración y firma

El proponente manifiesta que la presente oferta cumple con las condiciones técnicas y comerciales señaladas en la invitación a cotizar y en el Anexo Técnico del proceso, incluido a continuación de este formato.



Firma

Nombre: Jorge Cifuentes

Empresa: SPECTRA INGENIERIA SAS

ANEXO TÉCNICO PARA COTIZACIÓN — Solución Integral de Ciberseguridad

Documento de apoyo al Formato de Cotización. Describe de forma general y funcional las condiciones mínimas de cada componente, sin referencia a marca o fabricante, en garantía de la pluralidad de oferentes.

La Alcaldía de Pereira requiere la adquisición, implementación, configuración, integración y soporte técnico especializado de una solución integral de ciberseguridad para la Administración Central, compuesta por los cinco (5) componentes descritos a continuación. Los componentes de protección de endpoints, correlación de eventos (SIEM/XDR/SOAR) y concienciación deberán operar de forma integrada y nativa entre sí; el componente de protección de correo electrónico podrá integrarse mediante mecanismos estándar (API u otros oficialmente soportados).

Ítem / cantidad / vigencia	Condiciones técnicas mínimas que debe cumplir la oferta (sin marca ni fabricante específico)
1. Protección avanzada de endpoints (EDR) Cantidad: 1.000 Vigencia: 12 meses	● Protección de nueva generación (EPP + EDR) con detección basada en inteligencia artificial, análisis de comportamiento y visualización de la causa raíz de la amenaza. ● Cobertura de estaciones de trabajo, portátiles, servidores físicos y virtuales, y dispositivos móviles corporativos (Windows, Linux, macOS; Android/iOS cuando el alcance lo requiera). ● Prevención multicapa: firmas, aprendizaje automático, análisis heurístico y de comportamiento, y reputación en la nube. ● Controles de seguridad: firewall de host, control de aplicaciones (listas permitidas/denegadas), control web y de dispositivos USB, análisis de vulnerabilidades del software instalado. ● Capacidades de investigación y respuesta: aislamiento de red del equipo comprometido, terminación de procesos, cuarentena de archivos, análisis forense y ejecución de acciones remotas con trazabilidad y auditoría. ● Consola web centralizada con administración basada en roles, despliegue remoto de agentes, descubrimiento de equipos e inventario de activos protegidos. ● Integración nativa con la plataforma central de correlación de eventos (ítem 4), sin necesidad de desarrollos o conectores personalizados. ● Transferencia de conocimiento y capacitación técnica incluida para el equipo de administradores de la Entidad.
2. Integración de firewalls perimetrales Cantidad: 2 Vigencia: 12 meses	● Integración de los eventos de seguridad generados por los firewalls institucionales hacia la plataforma central de correlación (ítem 4). ● Correlación y visualización centralizada de dichos eventos junto con las demás fuentes de información de la solución. ● Sin licenciamiento adicional de hardware, software ni costos adicionales para la Entidad.
3. Protección de correo electrónico institucional Cantidad: 640 buzones Vigencia: 12 meses	● Solución nativa en la nube (SaaS), integrada mediante API con la plataforma de correo institucional, sin requerir modificación de registros de intercambio (MX) ni instalación de agentes en los equipos de usuario. ● Protección frente a phishing, spear phishing, compromiso de correo corporativo (BEC), malware, ransomware, archivos adjuntos y enlaces maliciosos, suplantación de identidad (spoofing), spam y compromiso de cuentas de usuario. ● Análisis del 100% del tráfico de correo entrante, saliente e interno, incluyendo archivos adjuntos y enlaces embebidos. ● Capacidad de cuarentena, eliminación o remediación de mensajes, incluso después de haber sido entregados al usuario. ● Motor antispam y validación de autenticidad del remitente mediante los protocolos estándar de la industria (SPF, DKIM, DMARC). ● Inteligencia de amenazas correlacionada de múltiples fuentes especializadas del mercado, con capacidad de incorporar fuentes adicionales. ● El fabricante de la solución deberá contar con certificaciones de gestión de seguridad de la información reconocidas internacionalmente (tipo ISO 27001 o equivalente). ● Envío de eventos, alertas y registros de auditoría hacia la plataforma central de correlación mediante mecanismos estándar (API, Syslog, CEF, JSON u otros equivalentes).
4. Plataforma central de correlación de eventos (tipo SIEM, con capacidades de detección extendida —XDR— y automatización de respuesta —SOAR—) Cantidad: 1 Vigencia: 12 meses	● Recepción, normalización, almacenamiento y correlación de los eventos generados por los 1.000 endpoints, los 640 buzones de correo y los 2 firewalls integrados. ● Capacidades nativas de detección extendida (correlación de eventos de múltiples dominios de seguridad) y de automatización de respuesta mediante flujos de trabajo (playbooks) con acciones manuales, automáticas o sujetas a aprobación. ● Monitoreo continuo bajo esquema 7x24, con gestión centralizada de alertas e incidentes, líneas de tiempo, análisis de causa raíz y búsqueda de indicadores de compromiso. ● Retención de eventos mínima de 30 días en línea, con posibilidad de ampliación según necesidad de la Entidad. ● Arquitectura de despliegue flexible (nube, local o híbrida), con soporte multiusuario y control de acceso basado en roles (RBAC). ● APIs y conectores documentados para la integración con otras fuentes de información y con sistemas de gestión de incidentes (ITSM) de la Entidad. ● Generación de reportes técnicos, operativos y ejecutivos sobre el estado de la plataforma, los eventos gestionados y el cumplimiento de los niveles de servicio.

Ítem / cantidad / vigencia	Condiciones técnicas mínimas que debe cumplir la oferta (sin marca ni fabricante específico)
5. Plataforma de concienciación y capacitación en ciberseguridad Cantidad: 200 usuarios Vigencia: 12 meses	- Plataforma de formación continua estructurada por niveles de dificultad, con contenidos que cubran, como mínimo, correo y phishing, contraseñas y cuentas, navegación segura, dispositivos móviles, datos personales y buenas prácticas de trabajo remoto. - Simulaciones controladas de phishing integradas a la ruta de formación, con asignación automática de actividades de refuerzo cuando un usuario falle una simulación. - Generación de reportes de desempeño por usuario, grupo y organización, con emisión de certificados de finalización. - Gestión de usuarios con posibilidad de sincronización con directorios corporativos y autenticación de inicio de sesión único (SSO). - Licencias administradas como cuota reutilizable: al finalizar o archivar la formación de un usuario, la licencia debe quedar disponible para su reasignación sin costo adicional. - Integración con la plataforma central de correlación de eventos y con la consola de administración de endpoints, para el intercambio de información y el fortalecimiento de los procesos de reducción de riesgo humano.

Soporte técnico y Acuerdo de Niveles de Servicio (ANS)

- Esquema de atención continua (7x24) sobre la plataforma central de correlación y los demás componentes de la solución, incluyendo monitoreo, recepción de eventos, análisis de alertas e investigación de incidentes.
- Clasificación de incidentes por severidad, con los siguientes tiempos máximos de atención:

Severidad	Respuesta inicial	Inicio de contención/mitigación
Crítico	1 hora	4 horas
Alto	2 horas	8 horas
Medio	4 horas	24 horas
Bajo	8 horas	48 horas

- Atención presencial cuando el soporte remoto no sea suficiente, en un tiempo máximo de una (1) hora de desplazamiento a las sedes de la Entidad.
- Informes periódicos de estado, afinamiento continuo de las reglas de detección y actualización permanente de los indicadores de compromiso.

Capacitación y transferencia de conocimiento (actividades mínimas durante la ejecución)

- Una (1) campaña de concienciación con simulación controlada de phishing, dirigida como mínimo a treinta (30) usuarios.
- Una (1) jornada de capacitación técnica para los administradores de la solución.
- Una (1) charla sobre buenas prácticas de ciberseguridad dirigida a funcionarios de la Entidad.
- Una (1) capacitación sobre protección de datos personales, seguridad de la información y Gobierno Digital.
- Una (1) capacitación sobre amenazas emergentes, autenticación multifactor y buenas prácticas para la protección de la información.

Requisitos del equipo de trabajo y del proponente

- Equipo técnico mínimo: un (1) Ingeniero de Sistemas (mínimo 2 años de experiencia profesional) y dos (2) Tecnólogos en Sistemas o afines, con certificaciones vigentes en las tecnologías ofertadas.
- Certificaciones del personal en Seguridad y Privacidad de la Información / Gobierno Digital y en el Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos nacionales vigentes.
- Certificación vigente como distribuidor autorizado de las soluciones ofertadas, validable directamente en el directorio oficial de aliados del fabricante (no se aceptan respaldos emitidos por mayoristas).
- Sistema de Gestión de Calidad certificado (ISO 9001:2015) vigente, con alcance en comercialización e implementación de soluciones TIC.
- Centro de Operación y Soporte Especializado propio del proponente, ubicado en territorio colombiano, disponible durante toda la ejecución del contrato.
- Atención y soporte técnico prestados en idioma español durante toda la ejecución del contrato.
- En caso de requerirse acceso remoto a la infraestructura de la Entidad, la herramienta utilizada deberá estar debidamente licenciada y su uso requerirá autorización previa de la Entidad.

Vigencia

- Licenciamiento con vigencia mínima de doce (12) meses desde la suscripción del acta de inicio, incluyendo actualizaciones, soporte del fabricante y corrección de vulnerabilidades, sin costo adicional.
- Vigencia del contrato: doce (12) meses, contados a partir del acta de inicio.