Versión: 2 Fecha de vigencia: 12 de junio de 2025

ALCALDÍA DE PEREIRA

Secretaría de Tecnologías de la Información y las Comunicaciones

ANEXO TÉCNICO

ADQUISICIÓN DE LICENCIAMIENTO DE SOLUCIÓN INTEGRAL DE CIBERSEGURIDAD

(EDR, SIEM, XDR, SOAR, protección de correo electrónico y plataforma de concienciación)

Versión: 2 Fecha de vigencia: 12 de junio de 2025

Tabla de contenido

1 OBJETO 5

2 **OBJETIVO DEL ANEXO TÉCNICO** 5

3 **INTRODUCCIÓN** 5

3.1 **Contexto reciente de amenazas** 7

3.1.1 Registro de Ciberataques Notables y sus Daños (2025 – 2026) 7

3.2 **Evolución del panorama de ciberataques y necesidad de adaptación tecnológica** 9

4 **JUSTIFICACIÓN** 10

4.1 **Justificación Técnica y Legal de la Adquisición de una Plataforma integral de Ciberseguridad** 14

4.2 **Marco de Acción y Fundamentación Técnica** 17

5 **CONDICIONES DE ENTREGA Y REQUISITOS TÉCNICOS DE LA ADQUISICIÓN** 19

5.1 **EDR Avanzado — Administración Central de la Alcaldía de Pereira** 21

5.1.1 ***Requerimientos Técnicos Mínimos — Licencia Avanzada (Alcaldía de Pereira)*** 21

5.2 Gestión, Administración y Capacidades Complementarias de la consola de administración de las licencias EDR Avanzadas 25

5.2.1 Compatibilidad tecnológica de la consola de administración 27

5.3 **Plataforma de ciberseguridad para Protección de Correo Electrónico Institucional** 27

5.3.1 Implementación 28

5.3.2 ***Integración de eventos de correo con la plataforma SIEM Cloud*** 29

5.3.3 ***Requerimientos Técnicos Mínimos de la Solución de Protección de Correo Electrónico*** 30

5.4 **SIEM — Plataforma Cloud con Capacidades XDR, Correlación de Correo y SOAR** 33

5.4.1 ***Alcance del monitoreo de seguridad*** 34

5.4.2 ***Capacidades mínimas de la plataforma*** 34

5.4.3 ***Requerimientos Técnicos Mínimos de la Plataforma SIEM Cloud con capacidades XDR y SOAR*** 35
5.4.4 Interfaz de Gestión y Análisis 41
5.4.5 ***Actividades mínimas de soporte técnico especializado*** 42
5.5 **Plataforma de Concienciación en Ciberseguridad (Capacitaciones)** 43
5.5.1 ***Requerimientos Técnicos Mínimos de la Plataforma de Concienciación*** 43
5.5.2 ***Recibo y auditoría de la plataforma de concienciación*** 46
6 **LICENCIAMIENTO Y COBERTURA** 47
6.1 **Cantidad de licencias y componentes requeridos** 47
6.2 **Vigencia del licenciamiento** 47
6.3 **Alcance del licenciamiento** 48
6.4 **Generalidades** 48
7 **OBLIGACIONES DEL CONTRATISTA** 49
7.1 **Obligaciones Específicas** 51
7.2 **Acuerdos de Niveles de Servicio (ANS) para el Soporte Técnico Especializado** 54
7.2.1 ***Tabla de Severidad y Tiempos de Atención*** 55
8 **CONDICIONES GENERALES** 56
8.1 **Capacitación y transferencia de conocimiento** 56
8.2 **Información técnica sobre inteligencia de amenazas** 56
8.3 **El proponente deberá garantizar** 58
9 **REQUISITOS DEL EQUIPO DE TRABAJO** 59
9.1 **Perfiles y Capacidad de Respuesta del Equipo de Seguridad** 59
9.2 **Certificación técnica del producto ofertado** 60
9.3 **Certificaciones requeridas para el Ingeniero de Sistemas** 60
9.4 **Certificaciones requeridas para los Tecnólogos en Sistemas o afines** 61
9.5 Capacidades complementarias del equipo 61
9.6 **Requisitos del proponente** 61
10 VIGENCIA 63

11 GLOSARIO DE TÉRMINOS Y SIGLAS 63

Versión: 2 Fecha de vigencia: 12 de junio de 2025

1 OBJETO

ADQUIRIR LICENCIAS DE SOFTWARE ANTIMALWARE DE ULTIMA GENERACION PARA LOS EQUIPOS DE COMPUTO DE LA ALCALDIA DE PEREIRA Y LICENCIA DE PLATAFORMA CLOUD PARA EL MONITOREO DE ALERTAS Y OPERACIONES DE CIBERSEGURIDAD

2 OBJETIVO DEL ANEXO TÉCNICO

Establecer los requerimientos técnicos, funcionales, operativos, de implementación, administración, monitoreo y soporte para la adquisición de una solución integral de ciberseguridad, conformada por:

- Una plataforma de protección avanzada para endpoints (EDR).
- Una solución de seguridad para correo electrónico institucional.
- Una plataforma cloud de gestión y correlación de eventos de seguridad (SIEM) con capacidades de detección y respuesta extendida (XDR), automatización y orquestación de respuesta ante incidentes (SOAR), monitoreo de los dispositivos de seguridad perimetral (firewalls) y funcionalidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad.
- Una plataforma de concienciación en ciberseguridad para usuarios finales.

La solución deberá fortalecer la postura de ciberseguridad mediante herramientas tecnológicas que permitan la prevención, detección, correlación, priorización y gestión de eventos e incidentes de seguridad de la información, incluyendo capacidades de inteligencia de amenazas y correlación avanzada que faciliten la labor de investigación por parte del personal designado por la Entidad, apoyando la toma de decisiones, la protección de los activos tecnológicos, la continuidad de los servicios institucionales y el cumplimiento de la normatividad vigente.

3 INTRODUCCIÓN

La transformación digital de las entidades públicas ha incrementado significativamente la superficie de exposición frente a amenazas cibernéticas cada vez más sofisticadas, dirigidas no solo contra los equipos de cómputo, sino también contra el correo electrónico, las identidades digitales, las aplicaciones, los servicios en la nube y la infraestructura tecnológica institucional. En este contexto, las organizaciones requieren adoptar una estrategia de ciberseguridad basada en múltiples capas de protección que permita prevenir, detectar, correlacionar y responder oportunamente a los incidentes de seguridad de la información, protegiendo de esta manera el activo más importante de cualquier entidad u organización en los tiempos actuales como son los datos y cualquier otro activo tecnológico que soporte la operación y mantenimiento en el tiempo de los procesos.

Versión: 2 Fecha de vigencia: 12 de junio de 2025

En el marco de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Ley 1581 de 2012 sobre Protección de Datos Personales, la Ley 527 de 1999 y demás disposiciones aplicables en materia de seguridad de la información y protección de datos, la Alcaldía de Pereira requiere fortalecer sus capacidades de ciberseguridad mediante la implementación de una solución integral que incorpore protección avanzada para endpoints (EPP/EDR), seguridad para el correo electrónico institucional, una plataforma cloud para la gestión y correlación de eventos de seguridad (SIEM) con capacidades de detección y respuesta extendida (XDR), automatización y orquestación de respuesta ante incidentes (SOAR), y funcionalidades tipo Centro de Operaciones de Seguridad (SOC).

Los equipos de cómputo, los buzones institucionales de correo electrónico y los demás activos tecnológicos utilizados en los procesos administrativos, financieros, misionales y de atención al ciudadano requieren mecanismos de protección que permitan prevenir, detectar, analizar y gestionar frente a amenazas como malware, ransomware, phishing, spear phishing, compromiso de cuentas (Account Takeover), Business Email Compromise (BEC), explotación de vulnerabilidades, ataques dirigidos e intentos de acceso no autorizado, preservando la confidencialidad, integridad y disponibilidad de la información institucional.

La solución objeto del presente proceso deberá implementar una arquitectura de defensa en profundidad mediante una plataforma cloud que integre diferentes capas de seguridad para la recolección, normalización, correlación, análisis y visualización de eventos de seguridad, así como capacidades de automatización, generación de alertas, administración de incidentes y soporte a la toma de decisiones, permitiendo fortalecer las capacidades institucionales de ciberseguridad.

Con la implementación de esta solución, la Alcaldía de Pereira busca:

- Fortalecer la protección de los equipos de cómputo y demás activos tecnológicos frente a amenazas avanzadas.
- Incorporar mecanismos especializados para la protección del correo electrónico institucional contra phishing, malware, spam y otras amenazas dirigidas.
- Centralizar la recolección, correlación y análisis de eventos de seguridad mediante una plataforma SIEM.
- Mejorar las capacidades tecnológicas institucionales para detectar, correlacionar, analizar y gestionar eventos e incidentes de seguridad, mediante capacidades de automatización y orquestación de respuesta (SOAR).
- Incrementar el nivel de concienciación de los usuarios frente a los riesgos asociados a la seguridad de la información.
- Contribuir al cumplimiento de las políticas, lineamientos y buenas prácticas nacionales e internacionales en materia de seguridad digital y protección de la información.
- Proteger el activo más importante de la organización, que son los datos.
- Fortalecer los procesos de continuidad del negocio mediante herramientas tecnológicas que mitiguen las pérdidas de información y la afectación de

disponibilidad de los servicios, a través de protección con herramientas antimalware de última generación.
- Mitigar las vulnerabilidades encontradas durante los periodos anteriores y trabajar sobre lecciones aprendidas.
- Disponer de mecanismos de soporte técnico incluidos en el licenciamiento para la atención de contingencias tecnológicas relacionadas con la plataforma.
- Contar con tecnología y herramientas capaces de reaccionar y evolucionar frente a los constantes cambios, estrategias y modelos de ataque de los ciberdelincuentes actuales, los cuales centran o fortalecen sus amenazas con modelos y herramientas dinámicas de IA, que han evolucionado tanto que adicional a los constantes ataques externos recibidos, ahora orquestan sus ataques desde el interior de la infraestructura.

3.1 Contexto reciente de amenazas

Con posterioridad al ciberataque de ransomware sufrido por IFX Networks en septiembre de 2023 (que afectó a más de 760 entidades públicas y privadas en Colombia), el panorama de amenazas ha continuado agravándose. En septiembre de 2024, la empresa Air-e, distribuidora y comercializadora de energía eléctrica en los departamentos de Atlántico, Magdalena y La Guajira, sufrió un ataque de ransomware que comprometió sus sistemas operativos, financieros y de atención al usuario, y que evidenció que los ataques de ransomware modernos logran evadir esquemas de protección tradicionales mediante combinaciones complejas de vectores de entrada, demostrando que ninguna solución por sí sola garantiza inmunidad absoluta frente a atacantes suficientemente sofisticados. Por su parte, el Centro Cibernético Policial y el ColCERT reportaron 1.427 incidentes de seguridad digital gestionados en 2024, cifra que descendió a 697 en 2025 (una reducción del 48,8 %), lo que si bien refleja una mejora en la capacidad de respuesta institucional del país, no disminuye la necesidad de mantener actualizadas las capacidades de prevención y detección de la Entidad, dado el incremento simultáneo en la sofisticación de los ataques.

A continuación se detallan ataques ocurridos en los años 2025 y 2026, que lograron vulnerar los esquemas de seguridad y causaron daños en las organizaciones:

3.1.1 Registro de Ciberataques Notables y sus Daños (2025 – 2026)

Durante el año 2025 y los primeros meses de 2026, el panorama global de la ciberseguridad registró un incremento crítico en incidentes de alto impacto. A diferencia de épocas anteriores centradas principalmente en la exfiltración de información, los ataques recientes se caracterizaron por causar parálisis operativa severa, pérdidas financieras multimillonarias e interrupciones directas en la cadena de suministro física y logística mundial.

3.1.1.1 Incidentes de Ciberseguridad en 2025

El año 2025 estuvo marcado por ciberataques de ransomware altamente destructivos dirigidos a sectores clave como la manufactura, la logística alimentaria, el comercio al por

menor y la administración pública. Uno de los incidentes más graves del periodo afectó al fabricante automotriz **Jaguar Land Rover (JLR)** a través de un ataque atribuido al grupo Scattered Lapsus$ Hunters. Este ciberataque paralizó las líneas de producción industrial en plantas de Reino Unido, Eslovaquia y Brasil durante aproximadamente cinco semanas, interrumpiendo las operaciones de más de 5.000 proveedores y generando pérdidas económicas astronómicas.

De manera similar, la distribuidora de alimentos **United Natural Foods (UNFI)** en Estados Unidos y Canadá fue víctima de un ataque de ransomware que inhabilitó sus sistemas informáticos de logística y procesamiento de pedidos electrónicos. La parálisis causó desabastecimiento directo en cadenas de supermercados, dejando góndolas vacías y provocando un impacto económico multimillonario en el sector alimentario.

En el ámbito minorista, grandes cadenas como **Marks & Spencer** sufrieron ciberataques coordinados mediante ingeniería social que comprometieron sus plataformas de comercio electrónico, procesamiento de pagos e inventarios durante semanas, afectando significativamente sus ingresos en temporadas operativas clave.

El sector del transporte aéreo también experimentó disrupciones severas tras el ataque a la plataforma **vMUSE de Collins Aerospace**, la cual gestiona los sistemas informáticos de check-in e itinerarios en múltiples aeropuertos de Europa. El incidente provocó retrasos masivos en vuelos, desorganización en el procesamiento de pasajeros y pérdidas operativas a nivel continental.

Por su parte, el sector público registró emergencias significativas como la del **Ayuntamiento de St. Paul** en Estados Unidos, donde el grupo de ransomware Interlock inhabilitó los sistemas de facturación municipal, la coordinación de servicios de emergencia y la atención ciudadana, obligando a las autoridades locales a declarar el estado de emergencia operacional.

Asimismo, durante 2025 se registraron ataques dirigidos a las cadenas de suministro SaaS y plataformas CRM integradas (como la campaña que afectó integraciones entre Salesloft y Salesforce), donde cibercriminales utilizaron credenciales comprometidas para eludir autenticaciones de múltiples factores y acceder a datos transaccionales de empresas a nivel internacional.

3.1.1.2 Incidentes de Ciberseguridad en 2026

A inicios de 2026, la tendencia destructiva continuó evolucionando hacia ataques dirigidos a la integridad de los datos y la explotación masiva de plataformas SaaS. Un caso emblemático fue el ciberataque sufrido por la corporación de tecnología médica **Stryker**, donde los atacantes desplegaron código malicioso de tipo *data wiper* (borrado masivo de datos). Este incidente provocó la eliminación en tiempo real de archivos corporativos clave y obligó a la suspensión inmediata de operaciones administrativas y de soporte en varias de sus sedes globales.

A continuación se detallan las fuentes donde se pueden consultar estos datos:

Las fuentes principales donde se documentan y detallan los eventos de ciberseguridad descritos son:

1. **Jaguar Land Rover (2025):**
   - **Reuters & BBC News:** Cobertura de las declaraciones oficiales de la empresa, el Ministerio de Negocios y Comercio del Reino Unido (gov.uk) y los informes macroeconómicos del Banco de Inglaterra sobre el impacto productivo.
   - **Wired Magazine & CyCraft Intelligence:** Reportes técnicos sobre la suspensión de operaciones globales y el análisis del grupo de ciberseguridad *Scattered Lapsus$ Hunters*.
2. **United Natural Foods - UNFI (2025):**
   - **Comisión de Bolsa y Valores de EE. UU. (SEC - Form 8-K):** Presentaciones financieras oficiales de la compañía donde se reportó la parálisis operativa, la pérdida estimada de $400 millones en ventas y los costos directos de respuesta.
   - **CyberScoop & Alliant Cyber Risk:** Artículos especializados que analizan las fallas en la cadena de suministro alimentario y los enlaces con grupos de cibercrimen.
3. **Marks & Spencer y Sector Retail (2025):**
   - **Financial Times & Retail Week:** Análisis del impacto financiero e interrupción de la infraestructura transaccional de minoristas en Reino Unido durante el ejercicio fiscal 2025.
4. **Collins Aerospace / vMUSE (2025):**
   - **Eurocontrol & Aviation Week:** Comunicados y reportes del sector aeronáutico europeo sobre las fallas de IT en servicios de aeropuerto.
5. **Ayuntamiento de St. Paul (2025):**
   - **Declaración Oficial de Emergencia Ciudadana de St. Paul:** Documento público del gobierno municipal sobre la inhabilitación de sus sistemas.
   - **BleepingComputer:** Cobertura de la atribuida participación del grupo de ransomware *Interlock*.
6. **Stryker Corporation (2026):**
   - **Coalition Security Labs:** Análisis forense e informe sobre el ataque de borrado masivo (*data wiper*) a sus plataformas corporativas.
   - **The Record by Recorded Future:** Reporte de ciberseguridad sobre la inhabilitación de endpoints de tecnología médica en marzo de 2026

3.2 Evolución del panorama de ciberataques y necesidad de adaptación tecnológica

Los mecanismos de ataque actuales han evolucionado de forma acelerada mediante la incorporación de inteligencia artificial, tanto para automatizar la generación de campañas

de phishing altamente personalizadas y difíciles de distinguir de comunicaciones legítimas, como para acelerar el descubrimiento y explotación de vulnerabilidades, y para evadir mecanismos de detección basados únicamente en firmas conocidas. Este dinamismo exige que la solución adquirida por la Entidad no se limite a una protección estática, sino que incorpore capacidades de detección basadas en comportamiento, analítica avanzada y aprendizaje automático, actualizadas de forma continua por el fabricante, de manera que la arquitectura de defensa pueda adaptarse con la misma velocidad con la que evolucionan las técnicas de ataque.

4 JUSTIFICACIÓN

La transformación digital de la Administración Municipal ha incrementado significativamente la virtualización y digitalización de sus procesos a través de una mayor oferta de servicios tecnológicos para la ejecución de las actividades administrativas, financieras, misionales y de atención al ciudadano. Esta evolución ha permitido optimizar la prestación de los servicios públicos y fortalecer la interacción con la ciudadanía; sin embargo, también ha ampliado la superficie de exposición frente a amenazas cibernéticas cada vez más sofisticadas, dirigidas contra los activos tecnológicos, la información institucional y la continuidad de la operación.

En este contexto, la ciberseguridad constituye un componente estratégico para garantizar la confidencialidad, integridad y disponibilidad de la información administrada por la Alcaldía de Pereira. Las amenazas actuales han evolucionado desde ataques basados en malware tradicional hacia campañas altamente especializadas que incluyen ransomware, phishing, spear phishing, compromiso de cuentas institucionales, explotación de vulnerabilidades de día cero (Zero-Day), robo de credenciales, ataques dirigidos contra servicios en la nube y otras modalidades que pueden afectar la continuidad de los servicios institucionales y comprometer la información pública.

La Alcaldía de Pereira requiere fortalecer su postura de ciberseguridad mediante la adquisición de una solución integral en modalidad Cloud que incorpore capacidades avanzadas de prevención, detección, análisis, correlación, automatización y gestión de eventos de seguridad, permitiendo consolidar información proveniente de múltiples fuentes, generar alertas, apoyar la toma de decisiones y facilitar la administración de incidentes mediante funcionalidades nativas de la plataforma. La solución deberá incluir el licenciamiento junto con las actividades de implementación, configuración, integración, soporte técnico especializado y actualización durante la vigencia del contrato.

Actualmente, la solución de protección instalada en la Entidad tiene fecha de vencimiento el 26 de diciembre de 2026, razón por la cual resulta indispensable garantizar la continuidad de la protección de los equipos de cómputo de la Administración Municipal. No obstante, la presente contratación no corresponde únicamente a la renovación del licenciamiento existente, sino a la evolución de las capacidades institucionales de ciberseguridad mediante la incorporación de mecanismos especializados para la protección de los diferentes vectores de ataque que actualmente enfrentan las entidades públicas y privadas. Las

amenazas cibernéticas evolucionan de forma constante, incluso fortaleciéndose a través de la expansión y democratización de la inteligencia artificial, lo que presenta un escenario cada vez más complejo para la protección de los datos; en consecuencia, el modelo y las herramientas de protección definidas e implementadas deben adaptarse a este escenario dinámico y evolutivo de las amenazas.

En consecuencia, la solución requerida deberá implementar un modelo de defensa en profundidad, integrando diferentes capas de seguridad que permitan proteger los equipos de usuario, el correo electrónico institucional, la infraestructura tecnológica y los demás activos de información, centralizando la gestión de eventos de seguridad, facilitando su correlación y fortaleciendo las capacidades institucionales mediante una plataforma Cloud que integre funcionalidades de SIEM, SOAR y XDR para la administración centralizada de eventos, correlación de información, generación de alertas, automatización de procesos y gestión de incidentes de seguridad.

La implementación de una solución integral de estas características permitirá a la Entidad evolucionar desde un esquema tradicional basado únicamente en protección antimalware hacia un modelo moderno de ciberseguridad, orientado al análisis, defensa en profundidad, automatización y gestión coordinada frente a amenazas avanzadas, contribuyendo a la continuidad de los servicios institucionales y a la protección de la información pública.

De manera particular, la solución deberá aportar beneficios institucionales tales como:

- Fortalecer la protección de los equipos de cómputo, servidores y demás activos tecnológicos frente a amenazas conocidas y emergentes.
- Incorporar mecanismos especializados para la protección del correo electrónico institucional, reduciendo el riesgo asociado a campañas de phishing, malware, spam, fraude electrónico y compromiso de cuentas.
- Mejorar la capacidad de detección temprana mediante el monitoreo continuo realizado por el personal designado por la Entidad con apoyo de la plataforma, el análisis automatizado de comportamiento y la identificación de actividades anómalas.
- Centralizar la recolección, normalización y correlación de eventos de seguridad provenientes de múltiples fuentes tecnológicas, facilitando el análisis y la gestión de eventos e incidentes.
- Optimizar los tiempos de identificación y gestión de eventos de seguridad mediante las capacidades de correlación, automatización, priorización y generación de alertas de la plataforma.
- Fortalecer la capacidad institucional para la gestión de amenazas mediante el uso de inteligencia de amenazas (Threat Intelligence), enriquecimiento de eventos y análisis contextual de incidentes.
- Incrementar la disponibilidad y continuidad de los servicios institucionales, minimizando el impacto operativo derivado de incidentes de ciberseguridad.
- Disminuir los riesgos económicos, operacionales, reputacionales y legales asociados a la materialización de incidentes de seguridad de la información.

- Fortalecer la cultura de ciberseguridad mediante mecanismos de concienciación orientados a los usuarios institucionales, promoviendo buenas prácticas para la protección de la información.
- Garantizar el cumplimiento de los lineamientos establecidos en la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las demás disposiciones aplicables en materia de seguridad de la información y protección de datos personales.

Por lo anterior, la presente contratación constituye una inversión estratégica orientada a fortalecer la resiliencia cibernética de la Alcaldía de Pereira, mejorar la capacidad institucional para gestionar los riesgos tecnológicos y garantizar la continuidad de los servicios digitales que soportan la gestión pública y la atención a la ciudadanía.

Panorama Nacional e Internacional de Ciberamenazas

La transformación digital, la adopción de servicios en la nube, el incremento del trabajo colaborativo y la creciente interconexión entre plataformas tecnológicas han ampliado significativamente la superficie de ataque de las organizaciones públicas y privadas. En consecuencia, el panorama actual de ciberseguridad evidencia un aumento sostenido en la frecuencia, complejidad y sofisticación de las amenazas cibernéticas, las cuales evolucionan continuamente mediante el uso de nuevas técnicas de evasión, automatización e inteligencia artificial.

Las entidades públicas constituyen uno de los principales objetivos de los ciberdelincuentes debido a la naturaleza de la información que administran, la criticidad de los servicios que prestan y el alto impacto que un incidente de seguridad puede generar sobre la continuidad institucional y la atención a la ciudadanía. En este contexto, los organismos gubernamentales enfrentan un escenario de riesgo permanente que exige fortalecer sus capacidades de prevención, detección, monitoreo, investigación y respuesta frente a incidentes de seguridad informática.

Entre las principales amenazas que afectan actualmente a las entidades públicas y a las infraestructuras críticas se encuentran:

- Ransomware dirigido al cifrado y secuestro de información institucional.
- Campañas de phishing, spear phishing y compromiso de cuentas institucionales (Business Email Compromise - BEC).
- Robo de credenciales y ataques contra mecanismos de autenticación.
- Explotación de vulnerabilidades conocidas y de día cero (Zero-Day).
- Malware orientado al robo de información, espionaje y acceso persistente.
- Amenazas Persistentes Avanzadas (APT) dirigidas contra entidades gubernamentales.
- Ataques contra servicios en la nube, plataformas colaborativas y entornos híbridos.
- Ataques distribuidos de denegación de servicio (DDoS) orientados a afectar la disponibilidad de los servicios.

- Técnicas avanzadas de ingeniería social apoyadas en inteligencia artificial para aumentar la efectividad de los ataques.
- Compromiso de identidades digitales, accesos remotos y credenciales privilegiadas.

La evolución de estas amenazas demuestra que los mecanismos tradicionales de protección basados exclusivamente en antimalware ya no son suficientes para enfrentar los riesgos actuales. Los ataques modernos suelen combinar múltiples vectores de compromiso, iniciando frecuentemente mediante campañas de correo electrónico malicioso, continuando con el robo de credenciales o la explotación de vulnerabilidades y finalizando con movimientos laterales, escalamiento de privilegios, exfiltración de información o despliegue de ransomware.

En este escenario, resulta indispensable adoptar un modelo de defensa en profundidad que integre múltiples capacidades de seguridad complementarias para proteger los diferentes componentes de la infraestructura tecnológica institucional, contemplando mecanismos especializados para la protección de endpoints, seguridad del correo electrónico, correlación de eventos, inteligencia de amenazas, automatización de procesos, administración de incidentes y herramientas de análisis que fortalezcan las capacidades institucionales de ciberseguridad.

En consecuencia, las entidades territoriales requieren fortalecer permanentemente sus capacidades institucionales mediante la implementación de soluciones integrales de ciberseguridad que permitan reducir los riesgos tecnológicos, proteger los activos de información, garantizar la continuidad de los servicios institucionales y dar cumplimiento a los lineamientos definidos por la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las demás disposiciones aplicables en materia de seguridad de la información.

Estrategia Nacional de Seguridad Digital y Fortalecimiento de las Capacidades Institucionales

El Gobierno Nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), ha venido fortaleciendo las políticas públicas orientadas a incrementar las capacidades nacionales de ciberseguridad y ciberdefensa. La Estrategia Nacional de Seguridad Digital 2025–2027, presentada por el MinTIC en junio de 2025, constituye la hoja de ruta vigente para fortalecer las capacidades institucionales y técnicas del país, orientando a las entidades públicas hacia la implementación de modelos modernos de gestión de riesgos de seguridad digital y protección de la infraestructura tecnológica, en un contexto en el que Colombia se ubicó en 2024 como el segundo país con más intentos de ciberataque en Latinoamérica (según reportes de ciberamenazas de Fortinet / FortiGuard Labs 2024 y datos de seguimiento del ColCERT).

Dicha estrategia promueve el fortalecimiento de cuatro ejes fundamentales:

- Gobernanza de la seguridad digital, mediante el fortalecimiento de la coordinación institucional, la gestión del riesgo y la adopción de políticas de seguridad de la información.
- Ciberresiliencia, incrementando las capacidades de prevención, detección, monitoreo, respuesta y recuperación frente a incidentes de ciberseguridad.
- Desarrollo de capacidades y talento humano, impulsando la formación especializada y la consolidación de una cultura organizacional orientada a la seguridad digital.
- Fortalecimiento del marco normativo y de las capacidades institucionales, promoviendo la actualización permanente de políticas, procedimientos y controles de seguridad acordes con la evolución del entorno tecnológico.

La presente contratación se encuentra alineada con estos principios, al contemplar la implementación de una solución integral de ciberseguridad que fortalezca la protección de los activos tecnológicos institucionales, incremente las capacidades tecnológicas para la detección, análisis, correlación y gestión de eventos e incidentes de seguridad frente a amenazas avanzadas, mejore la resiliencia operacional y contribuya a la continuidad de los servicios digitales prestados por la Alcaldía de Pereira.

4.1 Justificación Técnica y Legal de la Adquisición de una Plataforma integral de Ciberseguridad

La evolución del panorama de amenazas ha llevado a que las organizaciones públicas adopten plataformas tecnológicas con capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad, las cuales permiten centralizar la recolección, normalización, correlación y visualización de eventos de seguridad provenientes de múltiples fuentes, poniendo a disposición del personal designado por la Entidad herramientas para la detección temprana de amenazas, la gestión de incidentes y la toma de decisiones.

Para garantizar la efectividad del modelo de defensa en profundidad y la resiliencia operativa de la infraestructura municipal ante amenazas de alta velocidad (tales como ataques de ransomware, exfiltración masiva de datos o explotación de vulnerabilidades de día cero), resulta indispensable que el núcleo de protección de endpoints (EDR), la plataforma de correlación centralizada (SIEM Cloud) y los mecanismos de respuesta orquestada (SOAR) conformen una arquitectura XDR unificada de un mismo origen tecnológico. Esta integración nativa de fábrica asegura la ejecución automática e instantánea de playbooks de contención y aislamiento en tiempo real, eliminando la latencia operativa, las incompatibilidades de versiones y la necesidad de desarrollar o mantener middleware y conectores de terceros a cargo de la Entidad. Asimismo, esta aproximación de ecosistema único consolida la responsabilidad técnica de detección, análisis y mitigación en una sola casa matriz, garantizando la estabilidad del servicio y la continuidad del soporte especializado bajo un esquema de atención eficiente y sin brechas de integración.

Desde el punto de vista normativo, el Decreto 1078 de 2015, como Decreto Único Reglamentario del Sector TIC, en desarrollo de la Política de Gobierno Digital, establece que las entidades públicas deben implementar medidas orientadas a garantizar la

confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como fortalecer la gestión del riesgo de seguridad digital y la continuidad de los servicios soportados por las tecnologías de la información, a través del Modelo de Seguridad y Privacidad de la Información (MSPI). Adicionalmente, las iniciativas nacionales para el fortalecimiento de las capacidades de monitoreo y respuesta lideradas por el ColCERT y por el MinTIC evidencian la importancia de contar con mecanismos permanentes de vigilancia de la infraestructura tecnológica y gestión especializada de incidentes, como parte de una estrategia integral de protección de los activos digitales del Estado.

En concordancia con estos lineamientos, la Alcaldía de Pereira requiere disponer de una plataforma cloud que incorpore capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad, permitiendo centralizar la administración de eventos de seguridad, integrar información proveniente de múltiples fuentes, generar alertas, automatizar procesos y poner a disposición del personal designado por la Entidad las herramientas necesarias para la gestión de incidentes de ciberseguridad.

Estas capacidades se consolidan como un componente estratégico dentro de la arquitectura integral de ciberseguridad de la Entidad, habilitando las actividades de prevención, detección, investigación, análisis y respuesta que realice el personal designado por la Alcaldía, mediante la integración de información proveniente de múltiples fuentes tecnológicas, la correlación de eventos y la priorización de incidentes con base en su nivel de criticidad.

La plataforma de ciberseguridad permitirá entre otros aspectos:

- Contar con capacidades tecnológicas de monitoreo continuo de la infraestructura institucional bajo un esquema de disponibilidad 24x7x365.
- Centralizar la recolección y correlación de eventos provenientes de endpoints, servidores, servicios de correo electrónico, dispositivos de red, plataformas en la nube y demás activos tecnológicos integrados a la solución.
- Facilitar la identificación oportuna de comportamientos anómalos, indicadores de compromiso (IOC) y actividades maliciosas por parte del personal designado por la Entidad.
- Priorizar y clasificar alertas de seguridad mediante procesos estructurados de análisis e investigación de incidentes.
- Incorporar información de inteligencia de amenazas (Threat Intelligence) para enriquecer el análisis de eventos y fortalecer la capacidad de identificación de amenazas emergentes.
- Reducir los tiempos de detección (MTTD) y respuesta (MTTR), minimizando el impacto operativo derivado de incidentes de seguridad informática.
- Facilitar la generación de reportes técnicos e indicadores de gestión orientados al fortalecimiento continuo de la postura de ciberseguridad institucional.
- Apoyar el cumplimiento de las políticas institucionales de seguridad de la información, de la Política de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI).

Adicionalmente, el fabricante de la solución deberá disponer de laboratorios propios o de acceso a redes de inteligencia de amenazas especializadas en la investigación permanente de nuevas variantes de malware, campañas de phishing y técnicas de explotación, cuyos hallazgos alimenten de forma continua y automática los motores de detección de la plataforma ofertada, sin que ello represente un componente o costo adicional para la Entidad.

La incorporación de estas capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad no solo incrementa la capacidad institucional para identificar amenazas conocidas y emergentes, sino que también fortalece la resiliencia organizacional, mejora la visibilidad sobre los eventos de seguridad y proporciona información oportuna para la toma de decisiones del personal designado por la Entidad, orientadas a la protección de los activos tecnológicos y la continuidad de los servicios prestados a la ciudadanía.

Desafíos Actuales de la Ciberseguridad y Fortalecimiento de Capacidades Institucionales

La evolución permanente de las amenazas cibernéticas plantea importantes desafíos para las entidades públicas, las cuales deben fortalecer continuamente sus capacidades de prevención, detección, monitoreo, investigación y respuesta frente a incidentes que puedan comprometer la prestación de los servicios institucionales y la protección de la información pública.

Entre los principales retos que actualmente enfrentan las organizaciones del sector público se destacan:

- El incremento en la sofisticación de los ataques cibernéticos y la utilización de inteligencia artificial para automatizar campañas de ataque y evasión de controles de seguridad.
- El crecimiento de la superficie de exposición derivado de la adopción de servicios en la nube, plataformas colaborativas, trabajo remoto y transformación digital.
- La necesidad de fortalecer las capacidades institucionales para el monitoreo continuo, la gestión de eventos de seguridad y la respuesta oportuna frente a incidentes.
- La creciente demanda de talento especializado en ciberseguridad, situación que ha impulsado el desarrollo de estrategias nacionales de formación y fortalecimiento de capacidades técnicas.
- La necesidad de consolidar modelos de gestión del riesgo cibernético que permitan integrar personas, procesos y tecnología bajo un enfoque de mejora continua.
- El fortalecimiento de los procesos para garantizar la continuidad del negocio.

En respuesta a estos desafíos, el MinTIC, en conjunto con entidades públicas, instituciones académicas y aliados estratégicos, ha promovido diferentes iniciativas orientadas al fortalecimiento del talento humano, la adopción de buenas prácticas de seguridad digital y

el incremento de las capacidades institucionales para la gestión de riesgos de ciberseguridad.

Es importante resaltar que continuamente estamos expuestos a ciberataques cada vez más especializados y con mayor efectividad y daños gracias a la IA, tal cual como se indicó en el numeral 3.1 de este documento, donde se evidencian todos los ataques que lograron causar daños en entidades, tanto públicas como privadas, ocurridos de manera reciente.

4.2 Marco de Acción y Fundamentación Técnica

La estrategia de ciberseguridad propuesta para la Alcaldía de Pereira se fundamenta en un modelo de Defensa en Profundidad (Defense in Depth), reconocido internacionalmente como una de las mejores prácticas para la gestión del riesgo cibernético. Este enfoque consiste en implementar múltiples capas de protección complementarias que permitan prevenir, detectar, contener, investigar y responder oportunamente a las amenazas que puedan afectar la infraestructura tecnológica, los servicios institucionales y los activos de información.

Este modelo de defensa en profundidad ha demostrado un desempeño adecuado según los informes de seguimiento e indicadores de la Dirección de Infraestructura Tecnológica de la Alcaldía de Pereira durante las vigencias anteriores, logrando la contención de eventos de seguridad y protegiendo la disponibilidad de los activos de información institucional, evitando que los ataques recibidos pudieran sobrepasar las líneas de defensa y causar daños.

A diferencia de los modelos tradicionales basados exclusivamente en mecanismos preventivos, la defensa en profundidad integra controles tecnológicos, operativos y administrativos orientados a proteger los diferentes vectores de ataque utilizados por los ciberdelincuentes. Este enfoque garantiza que, en caso de que una capa de seguridad sea comprometida, existan controles adicionales capaces de facilitar la detección de la actividad maliciosa por parte del personal de la Entidad, limitar su propagación, apoyar la investigación del incidente y reducir su impacto sobre la operación institucional.

En este contexto, la solución integral de ciberseguridad requerida por la Alcaldía de Pereira deberá estar conformada por una arquitectura interoperable, escalable y modular, capaz de integrar diferentes componentes tecnológicos especializados que actúen de manera coordinada para fortalecer las capacidades del personal designado por la Entidad en materia de prevención, detección, análisis, correlación, investigación, contención y respuesta frente a incidentes de seguridad de la información.

Para alcanzar estos objetivos, la arquitectura deberá incorporar, como mínimo, las siguientes capacidades funcionales:

1. *Protección avanzada de endpoints*: mecanismos especializados para la prevención, detección y respuesta frente a amenazas dirigidas a estaciones de trabajo, equipos

portátiles, servidores y demás activos tecnológicos, mediante el análisis de comportamiento, la identificación de actividades maliciosas y la contención de amenazas, con herramientas que apoyen los procesos de investigación de incidentes por parte del personal de la Entidad.

2. *Protección del correo electrónico institucional*: mecanismos especializados para proteger los servicios de correo electrónico institucional frente a phishing, spear phishing, malware, ransomware, spam, Business Email Compromise (BEC), suplantación de identidad, archivos adjuntos maliciosos y enlaces fraudulentos, considerado actualmente uno de los principales vectores de compromiso de las entidades públicas.
3. *Gestión y correlación centralizada de eventos de seguridad (SIEM)*: una plataforma especializada para la recolección, normalización, almacenamiento, correlación y análisis de eventos provenientes de múltiples fuentes tecnológicas, que permita identificar patrones de ataque, enriquecer los eventos de seguridad, priorizar alertas según su criticidad y facilitar la investigación de incidentes por parte del personal de la Entidad. Esta plataforma SIEM debe incluir entre otros lo siguiente:

   Capacidades de detección y respuesta extendida (XDR): consolidación de información proveniente de los diferentes componentes de seguridad implementados por la Entidad, con el propósito de incrementar la visibilidad sobre el entorno tecnológico, mejorar la capacidad de detección de amenazas avanzadas y facilitar investigaciones más rápidas y precisas frente a incidentes que involucren múltiples vectores de ataque.

   Automatización y orquestación de procesos de respuesta (SOAR): capacidades que permitan automatizar tareas repetitivas asociadas al análisis, clasificación y gestión de incidentes, optimizando los tiempos de respuesta, reduciendo la intervención manual en actividades operativas y fortaleciendo la eficiencia de las labores de monitoreo de seguridad realizadas por el personal de la Entidad.

4. *Fortalecimiento del factor humano*: programas permanentes de concienciación y sensibilización dirigidos a los usuarios institucionales, orientados a fortalecer las buenas prácticas en seguridad de la información, reducir los riesgos asociados a la ingeniería social y promover una cultura organizacional enfocada en la ciberseguridad.

Interoperabilidad de la arquitectura: la solución deberá garantizar la interoperabilidad entre todos sus componentes mediante mecanismos de integración estandarizados, tales como APIs, Syslog u otros protocolos ampliamente utilizados en la industria, permitiendo el intercambio de información, la correlación centralizada de eventos y la gestión unificada de incidentes dentro de la plataforma. La protección de endpoints y la plataforma SIEM Cloud con sus capacidades XDR y SOAR deberán provenir de un mismo fabricante, por las razones técnicas expuestas en el numeral 4.1; la plataforma de concienciación y la plataforma de protección del correo electrónico institucional podrán ser de fabricantes distintos, integrados a la plataforma SIEM Cloud mediante los mecanismos estándar antes descritos.

La implementación de esta arquitectura permitirá fortalecer significativamente la postura de ciberseguridad de la Alcaldía de Pereira, incrementando la capacidad institucional para identificar oportunamente actividades maliciosas, correlacionar eventos provenientes de diferentes componentes tecnológicos, reducir los tiempos de detección y respuesta frente a incidentes, mejorar la eficiencia operativa de la plataforma y garantizar la continuidad de los servicios institucionales.

De igual manera, este enfoque se encuentra alineado con los principios establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, la Política de Gobierno Digital, las buenas prácticas definidas en la familia de normas ISO/IEC 27000 — especialmente ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27035 — así como con los lineamientos del NIST Cybersecurity Framework (NIST CSF), los cuales promueven la adopción de capacidades integrales para identificar, proteger, detectar, responder y recuperar la operación frente a riesgos de ciberseguridad.

En consecuencia, la presente contratación responde a la necesidad de evolucionar las capacidades de ciberseguridad de la Alcaldía de Pereira hacia un modelo capaz de responder al dinamismo de las amenazas actuales, mediante la implementación de una solución integral, interoperable y escalable, conformada por mecanismos especializados para la protección de endpoints, seguridad del correo electrónico institucional, gestión y correlación de eventos de seguridad, capacidades de detección y respuesta extendida, automatización y orquestación de respuesta, capacidades tecnológicas Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad y fortalecimiento de la cultura de ciberseguridad. Esta evolución resulta necesaria porque los atacantes actuales incorporan inteligencia artificial para automatizar y personalizar sus campañas, acelerar la explotación de vulnerabilidades y evadir controles basados únicamente en firmas, por lo que la arquitectura institucional debe migrar hacia capacidades de detección basadas en comportamiento, correlación multiplataforma y automatización de respuesta, garantizando la continuidad operativa y la protección de la información institucional frente a un panorama de amenazas cada vez más sofisticado y cambiante.

5 CONDICIONES DE ENTREGA Y REQUISITOS TÉCNICOS DE LA ADQUISICIÓN

La Alcaldía de Pereira requiere la adquisición, implementación, configuración, integración, puesta en funcionamiento y soporte técnico especializado de una solución integral de ciberseguridad, orientada al fortalecimiento de las capacidades institucionales para la prevención, detección, investigación, correlación, visualización y respuesta frente a eventos e incidentes de seguridad de la información.

La solución deberá estar conformada por componentes tecnológicos especializados que operen de manera integrada e interoperable, permitiendo una administración centralizada y el intercambio automático de información, eventos y alertas, con el fin de fortalecer la protección de la infraestructura tecnológica de la Entidad.

Como evolución de la plataforma actualmente implementada, la nueva solución deberá incorporar capacidades avanzadas de detección y respuesta extendida (XDR), orquestación y automatización de respuestas (SOAR), así como la integración de la protección del correo electrónico institucional y de los dispositivos de seguridad perimetral (Firewall) dentro de la plataforma SIEM Cloud, fortaleciendo la capacidad institucional para identificar, correlacionar y gestionar eventos de ciberseguridad desde una visión unificada.

La solución deberá proporcionar, como mínimo, las siguientes capacidades funcionales:

- Protección avanzada para estaciones de trabajo, equipos portátiles y servidores mediante tecnologías de Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR), de acuerdo con los niveles de licenciamiento requeridos por la Entidad.
- Protección especializada para el correo electrónico institucional frente a amenazas como phishing, malware, ransomware, Business Email Compromise (BEC), spam y demás amenazas dirigidas al servicio de correo electrónico, mediante una solución especializada integrada con la plataforma SIEM Cloud a través de APIs o conectores oficialmente soportados por los fabricantes involucrados.
- Plataforma SIEM Cloud para la recepción, almacenamiento, normalización, correlación, visualización y gestión centralizada de eventos de ciberseguridad, con capacidades nativas de XDR y SOAR, permitiendo la integración de múltiples fuentes de información y la automatización de acciones de respuesta mediante mecanismos soportados por el fabricante.
- Integración de los eventos generados por los dispositivos Firewall y demás componentes de seguridad definidos por la Entidad, permitiendo su correlación y visualización centralizada dentro de la plataforma SIEM Cloud.
- Plataforma oficial de concienciación y capacitación en ciberseguridad, orientada al fortalecimiento de la cultura de seguridad de los usuarios institucionales, permitiendo la ejecución de campañas de sensibilización, simulaciones de phishing, asignación de contenidos, evaluación de resultados y generación de reportes.

La solución de protección de endpoints (EDR avanzado) y la plataforma SIEM Cloud con sus capacidades XDR y SOAR deberán provenir del mismo fabricante, garantizando la integración nativa entre estos componentes sin necesidad de desarrollos, middleware o conectores personalizados. La plataforma de protección de correo electrónico institucional, por tratarse de un componente especializado, podrá ser suministrada por un fabricante distinto al del EDR/SIEM, integrado a la plataforma SIEM Cloud mediante APIs o conectores oficialmente soportados por el proveedor del SIEM, garantizando la interoperabilidad, el intercambio automático de eventos y la correlación centralizada de dicha información dentro de la plataforma SIEM Cloud. Para garantizar que la plataforma de protección de correo electrónico institucional si se encuentra habilitado por el fabricante de la plataforma SIEM, se deberá adjuntar una certificación emitida directamente por el fabricante de la plataforma SIEM, que avale la integración con la plataforma de protección de correos electrónicos institucionales ofertada.

La solución deberá integrarse con la infraestructura tecnológica existente de la Entidad sin afectar la operación normal de los servicios institucionales, garantizando la compatibilidad con la infraestructura de seguridad perimetral, los dispositivos Firewall, la infraestructura SD-WAN y los demás componentes tecnológicos que sean definidos durante la implementación.

El contratista será responsable del suministro del licenciamiento, la implementación, configuración, parametrización, integración, puesta en funcionamiento, actualización, transferencia de conocimiento y soporte técnico especializado de todos los componentes de la solución, garantizando su correcta interoperabilidad y funcionamiento durante toda la vigencia del contrato. La implementación deberá ejecutarse de manera presencial en las sedes de la Alcaldía de Pereira, de acuerdo con el plan de trabajo aprobado por la supervisión del contrato.

5.1 EDR Avanzado — Administración Central de la Alcaldía de Pereira

Componente destinado a mil (1.000) activos tecnológicos de la Administración Central del Municipio de Pereira, bajo licenciamiento de nivel avanzado, con capacidades ampliadas de investigación, búsqueda de amenazas (threat hunting) y respuesta. El alcance de las 1.000 licencias cubre de forma explícita: (i) servidores físicos y virtuales, y (ii) equipos de cómputo de escritorio y portátiles, Las licencias podrán reasignarse entre los activos de la Administración Central dentro del cupo de mil (1.000), sin costo adicional para la Entidad.

5.1.1 *Requerimientos Técnicos Mínimos — Licencia Avanzada (Alcaldía de Pereira)*

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Información general	El fabricante deberá acreditar al menos veinte (20) años de experiencia global en ciberseguridad empresarial y disponer de soporte para organizaciones públicas y privadas.		
	El fabricante deberá contar con un equipo propio de investigación e inteligencia de amenazas, cobertura global y presencia permanente en América Latina; la inteligencia generada deberá alimentar de forma nativa los motores de prevención y detección.		
	El fabricante deberá aportar evidencia pública reciente de investigación sobre APT, malware avanzado y vulnerabilidades de día cero, incluyendo al menos dos (2) vulnerabilidades registradas en CVE durante los veinticuatro (24) meses anteriores al cierre del proceso.		
Plataforma y administración	La licencia deberá incluir protección EPP de nueva generación y capacidades esenciales de EDR basada en IA, con análisis de causa raíz y visualización gráfica de la cadena de desarrollo de la amenaza.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La solución deberá ofrecer administración web centralizada en nube o en infraestructura local, según el modelo ofertado, con segregación administrativa, control de acceso basado en roles, auditoría y administración mediante políticas.		
	La solución deberá proteger estaciones de trabajo y servidores Windows, Linux y macOS.		
	La consola deberá integrar descubrimiento de dispositivos y directorio corporativo, puntos de distribución, despliegue remoto, actualización de bases y módulos, inventario de activos y verificación continua del estado de protección.		
Prevención multicapa	La detección deberá combinar firmas, aprendizaje automático, análisis heurístico y de comportamiento, reputación en la nube e inteligencia de amenazas para identificar amenazas conocidas, desconocidas y avanzadas.		
	La solución deberá incluir protección de archivos, web, correo y red, con inspección de tráfico HTTP/HTTPS y protocolos soportados, bloqueo de sitios maliciosos, phishing, descargas maliciosas y ataques de red.		
	La solución deberá detectar y bloquear ransomware, ataques sin archivos, scripts maliciosos, abuso de herramientas legítimas, exploits, macros y contenido examinado mediante AMSI, e incorporar remediación o reversión automática de cambios maliciosos cuando aplique.		
	La solución deberá incorporar autoprotección, protección mediante contraseña y mecanismos anti manipulación que impidan la desactivación o modificación no autorizada de procesos, archivos, servicios y configuración.		
Controles de seguridad	La solución deberá incluir firewall de host y prevención de intrusiones, con reglas por aplicación, red, protocolo, puerto y nivel de confianza.		
	La solución deberá incluir control de aplicaciones en modos de lista permitida y lista denegada, inventario de ejecutables y reglas por usuarios, grupos, firmas, rutas, hash u otros criterios soportados.		
	La solución deberá incluir control web y control de dispositivos por tipo, bus, usuario y dispositivo de confianza, así como prevención de Bad USB y bloqueo de puentes de red no autorizados.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La solución deberá incluir análisis de vulnerabilidades y software, identificación de aplicaciones vulnerables y generación de información para la reducción de la superficie de ataque.		
	La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación		
EDR esencial y análisis	La consola deberá generar alertas centralizadas con severidad, objeto detectado, host, usuario, proceso, archivo, conexión de red y demás evidencia disponible.		
	La solución deberá mostrar gráficamente la causa raíz y la cadena de desarrollo de la amenaza, incluyendo relaciones entre procesos, archivos, bibliotecas, conexiones de red y cambios relevantes en el registro.		
	La solución deberá permitir consulta histórica, exportación de evidencias y reportes técnicos, operativos y ejecutivos sobre amenazas, cobertura, políticas, vulnerabilidades e inventario.		
Interoperabilidad	La solución deberá integrarse de manera nativa con la plataforma SIEM Cloud.		
Telemetría y detección	La solución deberá recopilar y conservar telemetría de procesos, archivos, registro, scripts, módulos, usuarios, conexiones y actividad de red de los endpoints protegidos, conforme a la matriz de sistemas operativos soportados.		
	La detección deberá combinar EPP, análisis de comportamiento, aprendizaje automático, firmas, heurística, reputación, indicadores de compromiso (IoC), indicadores de ataque (IoA) y reglas personalizables, incluyendo reglas YARA cuando sean soportadas.		
Telemetría y detección Investigación	Las detecciones y los incidentes deberán mapearse a tácticas y técnicas de MITRE ATT&CK y permitir reglas propias del fabricante y reglas personalizadas para escenarios específicos de la Entidad.		
	La solución deberá agrupar alertas relacionadas en incidentes, priorizarlas por criticidad y mostrar línea de tiempo, causa raíz, cadena de ataque, activos, usuarios, procesos, conexiones y objetos afectados.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La solución deberá permitir búsquedas sobre telemetría histórica, consultas por múltiples atributos, investigación retrospectiva y búsqueda de indicadores en el conjunto de endpoints licenciados.		
Investigación Respuesta en endpoints	La solución deberá permitir consultar, recuperar y conservar evidencias para análisis forense, incluyendo archivos, metadatos, eventos, telemetría y resultados de las acciones de respuesta.		
	La solución deberá permitir aislar de la red un endpoint comprometido, conservando únicamente las comunicaciones necesarias para su administración, investigación y respuesta.		
	La solución deberá permitir terminar procesos, eliminar o poner en cuarentena archivos, bloquear objetos por hash u otros indicadores e impedir su ejecución en los endpoints administrados.		
Respuesta en endpoints Análisis avanzado Inteligencia y servicios	La solución deberá permitir ejecutar acciones remotas, tareas, scripts o comandos autorizados y recopilar archivos o información del endpoint, con trazabilidad, permisos y registro de auditoría.		
	Las acciones de respuesta deberán poder ejecutarse manualmente, de forma guiada o mediante playbooks de la plataforma integrada, de acuerdo con los permisos y flujos de aprobación definidos por la Entidad.		
	El alcance ofertado deberá incluir análisis de objetos sospechosos mediante sandbox o servicio avanzado del mismo fabricante, en nube o local, y utilizar sus veredictos para enriquecer detecciones e investigaciones. Este debe estar incluido en el licenciamiento de endpoint propuesto y no como licenciamiento adicional.		
	La solución debe integrarse nativamente con los servicios de reputación e inteligencia de amenazas del fabricante y deberá tener la capacidad de permitir la integración oficial con servicios MDR del mismo fabricante cuando sean contratados.		
Integridad y reducción de superficie	La solución deberá incluir monitoreo de integridad de archivos, inspección de eventos del sistema, control de anomalías adaptativo y controles de aplicaciones, dispositivos y navegación, dentro del licenciamiento o de los componentes oficialmente asociados.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Protección de datos	La solución deberá admitir cifrado de disco o administración centralizada del cifrado nativo del sistema operativo en los sistemas expresamente soportados por el fabricante.		
Integración SIEM/XDR/SOAR	La telemetría, alertas, incidentes y acciones de respuesta del EDR deberán integrarse de forma nativa con la plataforma SIEM/XDR/SOAR del mismo fabricante, sin middleware, scripts ni conectores personalizados para la integración principal.		
Protección de datos	Desde la interfaz operativa integrada deberán poder consultarse incidentes, ejecutar búsquedas, lanzar playbooks y ordenar acciones de respuesta sobre los endpoints administrados, manteniendo trazabilidad y auditoría.		
Capacitación	El proponente deberá garantizar la transferencia de conocimiento y el entrenamiento técnico especializado (que abarque mínimo 5 temáticas clave como identificación de amenazas, análisis de alertas EDR, mitigación de incidentes, seguridad para servidores e integración con directorio activo) para el equipo de administradores de seguridad de la Alcaldía de Pereira, el cual podrá ser impartido de forma directa por personal certificado del oferente como parte de los servicios de implementación.		
Licenciamiento	El licenciamiento avanzado deberá cubrir mil (1.000) endpoints de la Alcaldía de Pereira durante toda la vigencia contractual, incluyendo actualizaciones y soporte del fabricante.		

5.2 Gestión, Administración y Capacidades Complementarias de la consola de administración de las licencias EDR Avanzadas

La solución deberá proporcionar una consola web centralizada que permita administrar de manera segregada la infraestructura de la Alcaldía de Pereira, facilitando la operación, monitoreo y administración de los componentes de seguridad implementados. Como mínimo deberá permitir:

- Consola de administración centralizada, disponible en modalidad cloud que permita la administración remota de todos los dispositivos protegidos.

- Administración de políticas, tareas, licencias, actualizaciones, instalación, desinstalación, inventario y estado de protección de estaciones de trabajo, portátiles y servidores incluidos en el alcance.

- Despliegue remoto de agentes, instalación, actualización y desinstalación desde la consola administrativa.
- Transición y migración de agentes: Durante la etapa inicial de implementación, de máximo quince (15) días calendario contados a partir del acta de inicio y sin superar el 26 de diciembre de 2026, el contratista deberá efectuar la migración y el despliegue de la nueva solución por grupos de equipos, garantizando la continuidad de la protección institucional. Para ello, una vez suscritos los compromisos de confidencialidad y reserva correspondientes, la Entidad suministrará la información técnica necesaria del entorno existente y los accesos temporales autorizados. Se permitirá la coexistencia temporal de los agentes de protección saliente y entrante exclusivamente durante las pruebas de validación por grupos de equipos, siempre que no se generen conflictos de funcionamiento o consumo de recursos. Verificada la correcta comunicación con la plataforma Cloud, la transmisión de telemetría y la aplicación de las políticas de seguridad, deberá procederse a la remoción desatendida de la solución anterior mediante los mecanismos técnicamente disponibles y autorizados por la Entidad.}

- Control de acceso basado en roles, autenticación segura, registro de auditoría y perfiles diferenciados para administradores, operadores, analistas y usuarios de consulta.
- Descubrimiento de equipos por directorio activo corporativo, segmentos de red o mecanismos soportados; despliegue remoto, puntos de distribución y actualización optimizada para sedes con conectividad limitada.
- Generación automática de alertas frente a eventos relevantes de seguridad.
- Generación de reportes técnicos, operativos y ejecutivos sobre amenazas detectadas, estado de protección, cumplimiento de políticas, inventario de activos y tendencias de seguridad.
- Inventario centralizado de activos administrados.
- Alertas, paneles y reportes técnicos, operativos y ejecutivos sobre amenazas, incidentes, vulnerabilidades, cobertura, cumplimiento de políticas e inventario.
- Integración nativa con la plataforma SIEM Cloud y sus capacidades XDR y SOAR del mismo fabricante, permitiendo el intercambio automático de telemetría, eventos, alertas y acciones de respuesta.
- Capacidad para intercambiar de forma segura eventos, alertas e indicadores de compromiso con la solución de protección del correo electrónico implementada por la Entidad, mediante APIs o conectores oficialmente soportados por los fabricantes, permitiendo enriquecer los procesos de correlación, investigación y respuesta desarrollados desde la plataforma SIEM Cloud.

5.2.1 Compatibilidad tecnológica de la consola de administración

Las licencias EDR avanzado deberán ser compatibles con versiones vigentes de Microsoft Edge, Google Chrome, Mozilla Firefox, Safari y navegadores basados en Chromium expresamente soportados por el fabricante.

Los agentes deberán soportar, como mínimo, versiones vigentes de Windows 10/11, Windows Server 2016 o superior, macOS y distribuciones empresariales de Linux oficialmente incluidas en la matriz de compatibilidad del fabricante.
Para sistemas operativos en estado End of Life o sin soporte oficial, el contratista deberá realizar un diagnóstico, identificar las capacidades técnicamente disponibles y presentar un plan de transición; no se exigirá al fabricante soporte sobre plataformas descontinuadas.

5.3 Plataforma de ciberseguridad para Protección de Correo Electrónico Institucional

Componente especializado destinado a proteger los seiscientos cuarenta (640) buzones institucionales de Google Workspace de la Alcaldía de Pereira. A diferencia del EDR avanzado y el SIEM, que deben provenir de un mismo fabricante, este componente **podrá ser de un fabricante especializado distinto**, integrado a la plataforma SIEM Cloud mediante un conector basado en interfaces de programación de aplicaciones (API).

La solución de protección de correo electrónico deberá estar basada en una plataforma especializada en seguridad de correo en la nube (distinta y complementaria a la plataforma SIEM), la cual será la responsable directa de analizar el contenido de los mensajes y sus archivos adjuntos y de decidir si un correo se entrega, se pone en cuarentena o se bloquea. Dicha plataforma deberá contar con integración con Google Workspace mediante interfaces de programación de aplicaciones (API), sin requerir la modificación de los registros de intercambio de correo (MX) del dominio institucional ni la instalación de agentes adicionales en los equipos de los usuarios.

La solución deberá proporcionar, protección frente a las siguientes amenazas:

- Phishing.
- Spear Phishing.
- Business Email Compromise (BEC).
- Malware.
- Ransomware.
- Archivos adjuntos maliciosos.
- Enlaces maliciosos (URL Protection).
- Suplantación de identidad (Spoofing).
- Spam.
- Ataques dirigidos al correo electrónico.
- Compromiso de cuentas de usuario.
- Amenazas emergentes identificadas mediante inteligencia de amenazas del fabricante.

Esta plataforma de protección de los correos electrónicos institucionales deberá basarse, como mínimo, en los siguientes elementos:

- Autenticación delegada: acceso mediante una cuenta de servicio autorizada por el administrador de Google Workspace de la Alcaldía de Pereira, con permisos (scopes de OAuth) limitados estrictamente a las funciones necesarias para la protección del correo, sin requerir credenciales de usuarios individuales.
- Ingesta de alertas de seguridad de Google: consumo de la interfaz de alertas de Google Workspace (Alert Center API), que permite recibir las alertas de seguridad que la propia plataforma de Google genera (inicios de sesión sospechosos, reglas de reenvío anómalas, fuga de datos, entre otras).
- Visibilidad de actividad y auditoría: consumo de la interfaz de reportes administrativos de Google (Admin SDK Reports API), para obtener registros de auditoría de la actividad de correo (inicios de sesión, cambios de configuración, accesos administrativos).
- Análisis y remediación de mensajes: la plataforma especializada de correo utiliza la interfaz de mensajería de Google (Gmail API) para analizar el contenido de los mensajes de forma casi inmediata y, cuando sea necesario, retirar de los buzones mensajes ya entregados que posteriormente se determine que son maliciosos, sin necesidad de intervención manual del usuario.
- Envío de eventos hacia el SIEM Cloud: una vez la plataforma de correo emite su veredicto sobre un mensaje, el conector transmite dicho evento hacia la plataforma SIEM Cloud mediante API, Syslog, CEF, JSON u otro mecanismo estándar de integración, para su correlación con las demás fuentes de información de la solución.

La plataforma de protección de correo electrónico institucional, por tratarse de un componente especializado, podrá ser suministrada por un fabricante distinto al del EDR/SIEM, integrado a la plataforma SIEM Cloud mediante APIs o conectores oficialmente soportados pór el proveedor del SIEM, garantizando la interoperabilidad, el intercambio automático de eventos y la correlación centralizada de dicha información dentro de la plataforma SIEM Cloud. Para garantizar que la plataforma de protección de correo electrónico institucional si se encuentra habilitado por el fabricante de la plataforma SIEM, se deberá adjuntar una certificación emitida directamente por el fabricante de la plataforma SIEM, que avale la integración con la plataforma de protección de correos electrónicos institucionales ofertada.

5.3.1 Implementación

El contratista deberá realizar la configuración, parametrización, pruebas, afinamiento, puesta en producción y acompañamiento, garantizando continuidad de la protección y sin afectar la disponibilidad de Google Workspace.

La configuración deberá ejecutarse sin afectar la disponibilidad del servicio de correo electrónico institucional.

Durante la etapa de implementación, el contratista entregará a la Secretaría TIC la relación de los permisos (scopes de OAuth) y de las interfaces de Google Workspace que utilizará la

solución, indicando la función de protección que justifica cada uno, para su autorización por el administrador de Google Workspace de la Entidad.

5.3.2 *Integración de eventos de correo con la plataforma SIEM Cloud*

La solución de protección de correo electrónico deberá permitir el envío de eventos, alertas, registros de auditoría e indicadores de seguridad hacia la plataforma SIEM Cloud, mediante APIs o conectores oficialmente soportados por los fabricantes involucrados, utilizando mecanismos estándar como JSON, Syslog, CEF u otros formatos compatibles con la plataforma de correlación implementada por la Entidad.

El contratista deberá implementar y dejar en funcionamiento la integración entre la solución de protección de correo electrónico y la plataforma SIEM Cloud, incluyendo, cuando aplique, los componentes necesarios para la recolección, transporte, normalización, enriquecimiento y correlación de los eventos, garantizando su correcta visualización, consulta e investigación desde la plataforma centralizada.

La integración deberá permitir correlacionar los eventos de seguridad del correo electrónico con la información proveniente de la solución de protección para endpoints, las capacidades XDR, los procesos de orquestación y automatización (SOAR), las identidades digitales y las demás fuentes de información integradas a la plataforma SIEM Cloud.

No se entenderá como cumplimiento de este requisito la simple exportación de registros o archivos de auditoría. El proponente deberá describir el mecanismo de integración ofertado, indicando los componentes, licencias, conectores y dependencias requeridas, así como demostrar durante las pruebas de aceptación el correcto envío, recepción, normalización, búsqueda y correlación de los eventos dentro de la plataforma SIEM Cloud.

Como mínimo, deberán integrarse los siguientes eventos cuando sean soportados por la solución ofertada:

- Detección de phishing, spear phishing y Business Email Compromise (BEC).
- Detección de malware, ransomware, archivos adjuntos y enlaces maliciosos.
- Mensajes puestos en cuarentena, eliminados o remediados.
- Eventos relacionados con compromiso o sospecha de compromiso de cuentas de usuario.
- Cambios administrativos relevantes sobre la plataforma.
- Eventos asociados con autenticación, configuración y auditoría.
- Fallas o indisponibilidad de la plataforma de protección de correo electrónico.
- Demás registros de auditoría y eventos de seguridad disponibles.

Todos los componentes, licencias, conectores, desarrollos de configuración y demás elementos requeridos para implementar esta integración deberán estar incluidos dentro de la oferta económica, sin generar costos adicionales para la Entidad.

5.3.3 *Requerimientos Técnicos Mínimos de la Solución de Protección de Correo Electrónico*

Categoría	Características Técnicas Mínimas Requeridas	Cumple	No Cumple
Características Generales de Arquitectura y Modelo de despliegue	Solución nativa en la nube que se integre mediante API con la plataforma de correo de la entidad, sin requerir modificación de registros, ni redireccionamiento del flujo de correo		
	Modelo de arquitectura en la nube (SaaS), sin necesidad de instalar componentes de hardware o software adicionales en las instalaciones de la Entidad, con segregación lógica de la información de la Entidad.		
	Integración con conector nativo vía API con Google Workspace.		
	Debe permitir tiempo de aprovisionamiento en minutos sin requerir configuración adicional posterior al alta del tenant		
	Análisis de correo entrante, saliente e interno, incluyendo archivos adjuntos y enlaces embebidos		
	El fabricante de la solución debe proveer mantenimiento y optimización continua de los motores de decisión.		
Administración	Consola web centralizada para administrar la seguridad del correo electrónico, con posibilidad de administración delegada y visibilidad para la entidad con módulo de monitoreo		
	Consola de administración 100 % Cloud/SaaS basada en la web, sin instalación de agentes en las estaciones de trabajo ni en los servidores de la Entidad.		
	Análisis se seguridad de correos para el 100 % del tráfico entrante, saliente e interno. Correos, archivos adjuntos y URL.		
	La plataforma debe permitir extraer de manera continua la información, para la generación de Informes periódicos a la entidad (semanal, mensual o bajo demanda)		
	Detección de phishing, spear phishing, BEC, suplantación, spam, malware, ransomware, URLs y adjuntos maliciosos, amenazas internas y compromiso de cuentas		
	Análisis de mensajes entrantes, salientes e internos, y remediación mediante cuarentena,		

Protección contra amenazas de correo	eliminación o retiro de mensajes ya entregados cuando se determine posteriormente que son maliciosos		
	Filtrado Antispam de alta precisión basado en reputación, análisis heurístico de contenido, inteligencia de amenazas y modelos de aprendizaje automático para la detección y neutralización de correo no deseado y phishing en Google Workspace		
	Protección de URLs y enlaces en tiempo real con capacidad de análisis dinámico en tiempo de clic (Time-of-Click), reescritura preventiva de enlaces y verificación en entorno aislado (sandboxing) para neutralizar phishing, redirecciones maliciosas y sitios web fraudulentos		
	La solución de protección frente a amenazas en el correo debe garantizar la compatibilidad con el estándar SMTP y la integración nativa y directa mediante APIs con la suite de productividad y correo electrónico en la nube de la entidad (Google Workspace), asegurando la inspección y remediación de todo el tráfico de correo electrónico		
	Validación y verificación estricta de protocolos de autenticación de correo (SPF, DKIM y DMARC) respaldada en análisis de reputación y aprendizaje automático (Machine Learning) para la prevención de suplantación de identidad (Anti-spoofing) y fraude electrónico.		
	Análisis del tráfico interno bajo un enfoque de confianza cero para protección ante Phishing interno o lateral		
	Debe contar con mecanismos de protección anti-evasión que permitan la descompresión recursiva de archivos, extracción de URLs embebidas en cualquier nivel de anidamiento y el análisis independiente de cada componente extraído.		
	Protección contra usurpación de cuentas (ATO) con monitoreo continuo de anomalías de comportamiento, como inicios de sesión desde ubicaciones atípicas o creación de reglas de reenvío no autorizadas.		
	La solución debe brindar Supervisión permanente del tráfico de correo protegido		
	La solución debe incluir cobertura de técnicas de exploit avanzadas y posibilidad de gestión de		

	falsos positivos, así como remediación y liberación de mensajes cuando corresponda.		
	Protección antiphishing mediante múltiples mecanismos de reputación y análisis de URL, incluida la validación de la legitimidad de la página de destino		
	Detección suplantación de identidad, Protección BEC (Business Email Compromise), protección ante posible suplantación ejecutiva y dominios similares		
	Detección y prevención estática y dinámica anti-malware y ransomware mediante múltiples motores antimalware basados en firmas, tecnología de análisis de firmas complejas y motores de próxima generación para la identificación de contenido malicioso oculto en mensajes y archivos adjuntos.		
	Análisis dinámico en entorno aislado (sandbox) capaz de detectar exploits y malware de día cero en mensajes y archivos adjuntos.		
	Aplicación de inteligencia de amenazas global en tiempo real integrada mediante la correlación continuada de múltiples fuentes de información (Threat Intelligence) para la identificación y mitigación proactiva de vectores de ataque emergentes en mensajes de correo		
	Debe admitir la integración de fuentes externas.		
	Operación analítica directa vía API en la nube con procesamiento dinámico de mensajes que no genera latencia ni afecta el flujo ni el rendimiento de Google Workspace.		
Integridad del contenido	A diferencia de las soluciones CDR, la plataforma debe garantizar que el archivo entregado al usuario conserva su funcionalidad original tras el análisis		
	Registro de auditoría centralizado: Bitácora centralizada de eventos e incidentes, con exportación para efectos de investigación y evidencia		
	El fabricante de la solución deberá acreditar, como mínimo, una (1) certificación vigente correspondiente a las normas ISO 27001 (Sistema de Gestión de Seguridad de la Información), ISO 27017 (Controles de seguridad para servicios en la nube) o ISO 27018 (Protección de información de identificación personal en la nube), expedida		

Módulos complementarios y Cumplimiento Normativo	por una entidad u organismo independiente, cuyo alcance comprenda el servicio ofertado. Para acreditar el cumplimiento de este requisito será suficiente cualquiera de las certificaciones mencionadas, sin que se exija contar con las tres simultáneamente. El proponente deberá anexar la certificación correspondiente.		
	Servicio de respuesta ante incidentes de correo electrónico, incluido sin costo adicional con ciberanalistas del proveedor de servicios.		
	Transmisión de eventos e indicadores hacia la consola SIEM Cloud mediante conectores o APIs en formato estándar.		
	Modelo de Seguridad y Privacidad de la Información (MSPI - MinTIC): La solución debe aportar los controles de gestión de incidentes, protección contra código malicioso y monitoreo.		
	Ley 1273 de 2009 (Delitos informáticos): Debe generar evidencia técnica de accesos abusivos, suplantación y transferencia no consentida de activos por correo.		
	CONPES 3995 de 2020 (Confianza y seguridad digital): Debe permitir fortalecer las capacidades de prevención y respuesta frente a incidentes digitales.		
	Lineamientos de reporte a ColCERT: El registro de auditoría exportable debe permitir soportar el reporte de incidentes a las instancias de coordinación nacional.		

5.4 SIEM — Plataforma Cloud con Capacidades XDR, Correlación de Correo y SOAR

Componente central de la solución, encargado de recibir, normalizar y correlacionar los eventos generados por el EDR avanzado, la protección de correo electrónico y los dispositivos de seguridad perimetral, bajo un único punto de administración. La plataforma SIEM, sus capacidades nativas de XDR y SOAR deberán provenir del mismo fabricante que el EDR avanzado.

La Entidad requiere el suministro, implementación, configuración y puesta en funcionamiento de una plataforma SIEM Cloud con capacidades XDR y SOAR, adquirida bajo modalidad de licenciamiento, que permita la recepción, almacenamiento, normalización, correlación, investigación y gestión centralizada de los eventos de ciberseguridad generados por la infraestructura tecnológica de la Alcaldía de Pereira.

La plataforma deberá integrar de manera centralizada la información proveniente de la solución de protección para endpoints, la solución de protección de correo electrónico, los

dispositivos de seguridad perimetral, la infraestructura tecnológica y las demás fuentes de eventos definidas por la Entidad, permitiendo su correlación, análisis e investigación desde una única consola de administración.

El licenciamiento ofertado, deberá permitir el monitoreo técnico especializado de la plataforma durante la vigencia del contrato, incluyendo la recepción y análisis de eventos, la identificación de amenazas, la generación de alertas. El contratista deberá brindar acompañamiento técnico en la investigación de incidentes y el apoyo en las actividades de contención y mitigación, conforme a los Acuerdos de Niveles de Servicio (ANS) establecidos por la Entidad.

La implementación deberá comprender la configuración de los mecanismos de recolección, normalización, correlación e integración de las diferentes fuentes de eventos soportadas por la solución, garantizando su correcta visualización, análisis e investigación desde la plataforma SIEM Cloud.

5.4.1 *Alcance del monitoreo de seguridad*

La plataforma SIEM Cloud deberá permitir el monitoreo, recepción, correlación y análisis de eventos de seguridad provenientes, como mínimo, de las siguientes fuentes de información:

- Mil (1.000) endpoints incluyendo servidores físicos y virtualizados, protegidos mediante licenciamiento avanzado EDR.
- Seiscientos cuarenta (640) buzones institucionales de Google Workspace protegidos por la solución especializada de seguridad de correo electrónico.
- Se deberá realizar la integración de los 2 firewalls perimetrales Fortinet implementados en la Alcaldía de Pereira, a la plataforma SIEM.

5.4.2 *Capacidades mínimas de la plataforma*

La plataforma SIEM Cloud con capacidades XDR y SOAR deberá proporcionar, como minimo, las siguientes funcionalidades:

- Recolección, normalización, enriquecimiento, almacenamiento, correlación en tiempo real y retrospectiva, búsqueda, visualización, gestión de alertas e incidentes e inteligencia de amenazas.
- Capacidades nativas de orquestación y automatización mediante playbooks, con acciones manuales, automáticas o sujetas a aprobación, trazabilidad y control de acceso.

Integración nativa de la información y las acciones de respuesta del EDR avanzado con el SIEM/XDR/SOAR del mismo fabricante, sin middleware ni conectores personalizados para esta integración principal.

Dimensionamiento de la plataforma SIEM Cloud sin restricción de Eventos por Segundo (EPS) ni límite de volumen diario para la totalidad de las fuentes contratadas (1.000 endpoints/servidores, 640 buzones de correo y 2 firewalls perimetrales), garantizando un periodo de retención de datos en línea de mínimo treinta (30) días calendario, sin cobros adicionales por picos de tráfico de eventos durante los doce (12) meses de vigencia.

- Enriquecimiento de eventos mediante inteligencia de amenazas (Threat Intelligence).
- Identificación de indicadores de compromiso (IoC).
- Visualización de cadenas de ataque basadas en MITRE ATT&CK.
- Gestión centralizada de alertas e incidentes.
- Análisis de comportamiento de usuarios y entidades (UEBA - User and Entity Behavior Analytics) para la detección de anomalías y amenazas internas.
- Motor de correlación en tiempo real, con capacidad de creación y ajuste de reglas de correlación personalizadas.

5.4.3 *Requerimientos Técnicos Mínimos de la Plataforma SIEM Cloud con capacidades XDR y SOAR*

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Integración tecnológica	La plataforma SIEM Cloud deberá integrar y correlacionar los eventos de seguridad provenientes de la totalidad de las fuentes delimitadas en el alcance contractual (1.000 endpoints/servidores con EDR avanzado, 640 buzones de Google Workspace y 2 firewalls perimetrales Fortinet). La integración de servicios de identidad y servidores se entenderá circunscrita a la telemetría generada por los dispositivos y cuentas que forman parte de dicho alcance.		
	La integración principal entre EDR, SIEM, XDR y SOAR deberá estar soportada nativamente por el mismo fabricante.		
	El contratista deberá implementar, configurar y validar la integración de todas las fuentes de información definidas por la Entidad, garantizando el correcto flujo, normalización y correlación de los eventos de seguridad.		
Monitoreo 24x7	La plataforma deberá recibir, almacenar, normalizar, correlacionar y visualizar eventos de seguridad en tiempo real, generando alertas de acuerdo con las reglas de correlación configuradas.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La plataforma deberá permitir el análisis, clasificación, priorización y seguimiento de alertas e incidentes de seguridad conforme a los niveles de criticidad definidos por la Entidad.		
	La plataforma deberá incorporar capacidades de detección, análisis y respuesta mediante SIEM Cloud, XDR y SOAR, permitiendo automatizar procesos de investigación y respuesta frente a incidentes de seguridad.		
Investigación y hunting	La plataforma deberá permitir la construcción de líneas de tiempo, análisis de causa raíz, visualización gráfica de la cadena de ataque, consultas históricas, búsqueda de indicadores de compromiso (IoC), indicadores de ataque (IoA) y el mapeo de eventos bajo el marco MITRE ATT&CK.		
	La plataforma deberá permitir investigaciones retrospectivas sobre la información almacenada, conservando evidencias, consultas realizadas y resultados obtenidos.		
	En la Investigación de Incidentes se integrarán además componentes como: Visualización gráfica de la cadena de ataque. Gestión avanzada de alertas de seguridad. Detección de amenazas avanzadas. Gestión de vulnerabilidades. Capacidades de gestión y respuesta ante incidentes integradas en la plataforma. Cacería de amenazas e inteligencia de amenazas. • Visualización gráfica de la cadena de ataque. • Gestión avanzada de alertas de seguridad • Detección de amenazas avanzadas • Gestión de vulnerabilidades • Cacería de amenazas e inteligencia de amenazas		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Correlación y casos de uso	La plataforma deberá permitir la creación, edición y afinamiento de reglas de correlación, casos de uso, listas, modelos de detección, paneles y mecanismos de enriquecimiento de eventos provenientes de múltiples fuentes de información.		
	Correlación de eventos provenientes de múltiples fuentes (endpoints, red, correo, servidores, nube, etc.).		
SOAR y respuesta	La plataforma deberá ejecutar playbooks con condiciones, aprobaciones, ramificaciones y registro de resultados, permitiendo automatizar enriquecimiento, notificación, creación de casos y acciones de contención.		
	Las acciones sobre endpoints deberán incluir, según autorización, aislamiento de red, bloqueo de objetos, terminación de procesos, cuarentena, recuperación de evidencia y ejecución de tareas o scripts soportados.		
Gestión de incidentes	Cada incidente deberá contar con identificador, criticidad, estado, responsable, evidencias, comunicaciones, acciones, tiempos, recomendaciones y cierre; la plataforma deberá integrarse con ITSM mediante API o webhook.		
Inteligencia de amenazas	La plataforma deberá consumir inteligencia de amenazas del fabricante y permitir la incorporación de fuentes adicionales oficialmente soportadas para enriquecer los procesos de correlación, investigación y respuesta.		
Detección Avanzada	• Uso de inteligencia artificial y machine learning para la detección de amenazas sin firma. • Análisis de comportamiento, heurística avanzada y correlación de eventos. • Monitoreo de procesos, librerías (DLLs) y accesos al registro del sistema.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Prevención	• Bloqueo de scripts sospechosos, macros maliciosas, exploits y ransomware. • Control de dispositivos extraíbles (USB) y descargas no autorizadas • Aislamiento lógico de endpoints comprometidos a nivel de EDR e integración con firewalls perimetrales mediante playbooks de respuesta automatizada (SOAR) para la contención rápida y prevención de movimientos laterales		
Administración de plataforma	La solución debe poder ser administrada desde una consola web. No se aceptarán soluciones que dispongan de consola adicional a la consola web (por ejemplo, una consola de escritorio)		
Reportes y métricas	La plataforma deberá incorporar capacidades de análisis mediante inteligencia artificial, aprendizaje automático, comportamiento, heurística e indicadores de compromiso soportados por el fabricante.		
Seguridad del servicio	La operación deberá aplicar RBAC (Role-Based Access Control), mínimo privilegio, segregación de funciones, auditoría, cifrado de comunicaciones, custodia de evidencias y controles de acceso físico y lógico.		
Aceptación	La solución debe recibir eventos, admitir normalizadores y conectores nativos para formatos y protocolos estándar de la industria (Syslog RFC3164/RFC5424, CEF, JSON, XML, CSV, NetFlow v5/v9, IPFIX, SNMP, WMI/WEC, bases de datos SQL estándar), con capacidad de incorporar fuentes adicionales según necesidad de la Entidad.		
	El proponente deberá demostrar en pruebas de aceptación la ingesta, normalización, correlación, investigación, ejecución de playbooks y acciones de respuesta sobre una muestra representativa de fuentes.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Plataforma integrada	La solución deberá proporcionar un núcleo empresarial integrado de SIEM, XDR y SOAR, desarrollado y soportado oficialmente por el mismo fabricante de la solución EDR avanzada.		
	La totalidad de la administración, monitoreo, investigación de incidentes, ejecución de playbooks y acciones de respuesta deberán realizarse de manera unificada desde una interfaz web basada en la nube (SaaS), sin requerir consolas locales, aplicaciones cliente ni herramientas de escritorio adicionales		
Arquitectura y despliegue	La solución SIEM Cloud podrá ser provista bajo un modelo de arquitectura centralizada en la nube (SaaS) o arquitectura híbrida. En caso de ofertarse componentes colectores o nodos locales, estos deberán desplegarse sobre la infraestructura de virtualización existente en la Entidad, incluyendo el 100% de los conectores y componentes requeridos, garantizando que el modelo propuesto no exija capacidades adicionales de cómputo o almacenamiento no previstas por el Municipio.		
	El licenciamiento de la plataforma SIEM ofertada deberá cubrir el 100% de la ingesta de eventos generada por las fuentes del alcance (1.000 endpoints, 640 buzones de correo y 2 firewalls Fortinet) sin límite de EPS ni cobro por Gigabytes diarios, incluyendo todos los componentes de cómputo, almacenamiento Cloud y licenciamiento indispensables para su operación.		
Recolección y normalización	La solución deberá recibir eventos mediante agentes, Syslog, CEF, LEEF, JSON, archivos, bases de datos, APIs, Kafka, NetFlow/IPFIX u otros mecanismos oficialmente soportados.		
	Los colectores deberán permitir transporte, parsing, normalización, filtrado, agregación, enriquecimiento y enrutamiento, con monitoreo de estado, almacenamiento temporal y recuperación ante interrupciones.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La solución deberá incluir normalizadores predefinidos y personalizables, esquema de eventos extensible y enriquecimiento con activos, identidades, geolocalización, listas e inteligencia de amenazas.		
Correlación y analítica	La plataforma deberá ejecutar correlación en tiempo real, listas activas, modelos analíticos y detecciones alineadas con MITRE ATT&CK, con versionamiento, trazabilidad y auditoría de cambios.		
	Las reglas de detección deberán poder aplicarse retrospectivamente sobre eventos almacenados para identificar amenazas o patrones que no hubieran sido detectados inicialmente.		
Investigación y hunting	La plataforma deberá agrupar alertas en incidentes, mostrar cronología, entidades y relaciones, permitir búsquedas estructuradas sobre eventos y telemetría y conservar consultas, notas y evidencias de investigación.		
	La solución deberá permitir buscar IoC, IoA, hashes, dominios, direcciones IP, usuarios, procesos y otros atributos tanto en los eventos centralizados como en los endpoints integrados.		
Almacenamiento y retención	El almacenamiento deberá soportar búsqueda en línea, particionamiento temporal, políticas de retención, respaldo, restauración y almacenamiento de largo plazo, garantizando el rendimiento definido en los SLA.		
	La solución deberá garantizar el almacenamiento y retención de datos de registro (logs) en línea por un período mínimo obligatorio de treinta (30) días calendario para la totalidad de las fuentes contratadas, asegurando la capacidad de consulta, búsqueda e investigación histórica durante dicho periodo		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
SOAR y playbooks	La plataforma deberá disponer de diseñador visual de playbooks con acciones secuenciales y paralelas, condiciones, ramificaciones, variables, aprobaciones, manejo de errores y registro completo de cada ejecución.		
	Los playbooks deberán iniciarse manualmente o por eventos, alertas, incidentes, reglas, API o programación, y permitir integración con correo, mensajería, ITSM y sistemas de terceros.		
Respuesta nativa	La plataforma deberá ejecutar sobre los endpoints del mismo fabricante acciones nativas de aislamiento, bloqueo, terminación de procesos, cuarentena o eliminación, recuperación de evidencia y tareas o scripts oficialmente soportados.		
Interoperabilidad	La plataforma deberá exponer APIs y webhooks documentados para consultar y actualizar alertas, incidentes, activos, indicadores, playbooks y acciones, con autenticación, autorización y auditoría.		
Multitenant y acceso	La plataforma deberá ser multitenant o soportar segregación lógica equivalente, RBAC granular, acceso a uno o varios entornos según permisos y separación de eventos, recursos y configuraciones.		
5.4.4 Interfaz de Gestión y Análisis	La solución debe proporcionar una interfaz web para la gestión y el análisis, que incluya datos de incidentes, estado del sistema y comprobaciones de funcionamiento, configuración y mucho más.		
Continuidad y operación	La solución deberá incluir monitoreo, métricas, alertas de capacidad, respaldo de configuraciones y procedimientos documentados de actualización, recuperación, alta disponibilidad y continuidad.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Licenciamiento	El licenciamiento deberá cubrir capacidad de ingesta, almacenamiento, componentes SIEM/XDR/SOAR, conectores, normalizadores, playbooks, usuarios operativos y demás elementos indispensables, sin costos ocultos por fuentes o colectores requeridos. Los cambios en la configuración de registro (logging) de las fuentes del alcance que la Entidad realice durante la vigencia no generarán costos adicionales.		

5.4.5 *Actividades mínimas de soporte técnico especializado*

Como parte de la asistencia técnica posventa y la garantía de funcionamiento inherentes al licenciamiento por suscripción de la plataforma SIEM Cloud con capacidades XDR y SOAR, el contratista deberá ejecutar, como mínimo, las siguientes actividades durante los doce (12) meses de cobertura de las suscripciones:

- Monitorear el correcto funcionamiento de la plataforma, verificando la recepción, normalización, correlación y visualización de los eventos de seguridad provenientes de las fuentes de información integradas.
- Realizar el análisis técnico de las alertas e incidentes de seguridad que la Entidad escale, así como de aquellos que, por falla o anomalía en el funcionamiento de la plataforma, requieran su intervención, apoyando a la Entidad en su investigación, clasificación, priorización y seguimiento, de acuerdo con los Acuerdos de Niveles de Servicio (ANS) establecidos.
- Administrar y mantener actualizados los componentes de la plataforma, incluyendo colectores, conectores, reglas de correlación, casos de uso, paneles de control, reportes, playbooks, integraciones y demás configuraciones necesarias para garantizar su correcta operación.
- Ejecutar el afinamiento continuo de las reglas de correlación y de los mecanismos de detección, con el fin de optimizar la identificación de amenazas y reducir la generación de falsos positivos.
- Mantener actualizados los indicadores de compromiso (IoC), las fuentes de inteligencia de amenazas y demás mecanismos de enriquecimiento soportados por la plataforma.
- Generar, cuando sea requerido por la Entidad, informes técnicos sobre el estado de la plataforma, eventos relevantes, incidentes analizados, indicadores de desempeño, tendencias de amenazas y recomendaciones orientadas al fortalecimiento de la postura de ciberseguridad.

5.5 Plataforma de Concienciación en Ciberseguridad (Capacitaciones)

La oferta deberá incluir una plataforma automatizada de concienciación y capacitación para **doscientos (200) usuarios**, con licenciamiento vigente durante toda la ejecución contractual, orientada a reducir el riesgo humano mediante formación continua, pruebas, refuerzo y simulaciones de phishing. Esta plataforma podrá ser de un fabricante distinto al del EDR avanzado y el SIEM, y deberá integrarse con la plataforma SIEM Cloud mediante API o conector oficialmente soportado.

Requerimientos Técnicos Mínimos de la Plataforma de Concienciación

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Información general	La plataforma de concienciación deberá integrarse con la plataforma SIEM Cloud mediante API o conector oficialmente soportado y permitir el intercambio de información con dicha plataforma o con la consola de endpoints para fortalecer los procesos de capacitación y reducción del riesgo humano.		
Metodología de formación	La plataforma deberá basarse en un modelo de competencias con aprendizaje continuo, secuencial y progresivo, dividido como mínimo en cuatro niveles de dificultad, con lecciones breves, pruebas y refuerzo sistemático del conocimiento.		
	La plataforma deberá incluir rutas principal y exprés, y generar automáticamente el calendario de formación según intensidad, temas, fecha de inicio, fecha objetivo y nivel de dominio requerido, recalculándolo cuando cambien estos parámetros.		
	La formación deberá asignarse por rol, grupo, nivel inicial de conocimiento y riesgo, permitiendo pausar, reanudar o cambiar al usuario de grupo sin perder su progreso.		

Versión: 2 Fecha de vigencia: 12 de junio de 2025

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Contenido	Los contenidos deberán cubrir como mínimo correo y phishing, contraseñas y cuentas, navegación web, redes sociales y mensajería, seguridad de equipos y móviles, datos confidenciales y personales, trabajo remoto, pagos y fraude, inteligencia artificial para usuario final e incidentes de ingeniería social.		
	La plataforma deberá permitir incorporar contenido personalizado mediante un editor que admita texto, imágenes y archivos, y disponer de contenidos en formatos SCORM 1.2 y SCORM 2004 para interoperabilidad con plataformas de aprendizaje.		
Phishing simulado	La plataforma deberá integrar simulaciones de phishing dentro de la ruta de aprendizaje y permitir campañas independientes, con biblioteca de plantillas multitemática, personalización de texto, imágenes y logotipos y páginas educativas de destino.		
	Cuando un usuario falle una simulación, la plataforma deberá asignar o repetir automáticamente actividades de refuerzo y registrar correos enviados, interacciones, clics, reportes, tasa de fallos y estado de la campaña.		
Gestión de usuarios	La plataforma deberá permitir alta, edición, archivo, restauración e importación masiva de usuarios, sincronización con directorios de identidad corporativos y en la nube (incluyendo Google Workspace / Google Directory, Active Directory o Microsoft Entra ID), autenticación SSO (Single Sign-On), campos personalizados y reglas automáticas de asignación a grupos.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
Administración y roles	La plataforma deberá incluir RBAC con perfiles diferenciados de superadministrador, administrador, administrador de formación y observador, separando la capacidad de configurar la formación del acceso a los informes personales.		
Personalización	La Entidad deberá poder personalizar nombre, logotipo, dominio o subdominio, mensajes, invitaciones, recordatorios, recomendaciones, idiomas, campos de usuario y certificados, incluyendo su adaptación al contexto cultural y organizacional.		
Licenciamiento	Las licencias deberán administrarse como una cuota reutilizable y no quedar vinculadas permanentemente a una persona; al suspender, finalizar o archivar la formación de un usuario, la licencia deberá quedar disponible para reasignación.		
Reportes y certificación	La plataforma deberá generar paneles e informes automáticos por usuario, grupo y organización, con categorías de desempeño, avance, unidades atrasadas, pruebas, previsión de finalización, recomendaciones y exportación a XLSX.		
	El certificado electrónico deberá emitirse cuando el usuario alcance los criterios definidos de aprendizaje, incluyendo aprobación de pruebas y superación de la simulación de phishing aplicable, y deberá ser personalizable y descargable.		
Integración	La plataforma deberá disponer de API HTTP documentada, autenticación mediante token y respuestas en JSON para automatizar usuarios, grupos, asignaciones y reportes, e integrarse con la plataforma SIEM mediante mecanismo oficialmente soportado.		

Categoría	Características Técnicas Mínimas Requeridas	CUMPLE	NO CUMPLE
	La plataforma deberá contar con integración oficialmente documentada con la plataforma SIEM Cloud o con la consola cloud de administración de endpoints ofertada, para asignar formación y consultar el estado de los usuarios.		
Disponibilidad y soporte	La solución deberá operar en modalidad cloud, actualizaciones durante la vigencia sin afectar la disponibilidad, soporte técnico y registro de cambios funcionales.		

5.5.1 *Recibo y auditoría de la plataforma de concienciación*

Con el fin de garantizar el cumplimiento efectivo de este componente, la recepción y auditoría de la plataforma de concienciación se regirá por las siguientes condiciones:

- Recibo a satisfacción: el contratista deberá entregar, dentro de los plazos definidos en el cronograma de implementación, un acta de puesta en producción de la plataforma que evidencie la activación de las doscientas (200) licencias, la carga del listado nominal de usuarios suministrado por la Secretaría TIC y la asignación de al menos una ruta de formación inicial a la totalidad de los usuarios cargados.
- Población objeto de capacitación: los doscientos (200) usuarios corresponden a personal de la Administración Central de la Alcaldía de Pereira designado por la Secretaría TIC; no se exige que esta cifra coincida con el número de buzones de correo de Google Workspace (640), dado que la plataforma de concienciación y la protección de correo tienen alcances y poblaciones independientes, aunque complementarios.
- Auditoría periódica: el contratista deberá poner a disposición de la supervisión del contrato, con periodicidad mensual, un reporte que permita verificar el listado de usuarios activos frente al listado nominal aprobado, el avance de formación, la tasa de finalización de rutas, los resultados de las simulaciones de phishing ejecutadas y las licencias disponibles para reasignación.
- Sustitución de usuarios: cuando un usuario designado deje de pertenecer a la población objeto de capacitación (retiro, cambio de dependencia u otra causa), la Entidad podrá solicitar su reemplazo por otro usuario sin costo adicional, conforme a la condición de licenciamiento por cuota reutilizable establecida en la tabla de requerimientos técnicos.
- Evidencia de aceptación final: al finalizar cada trimestre de ejecución, el contratista deberá presentar un informe consolidado de cobertura (usuarios formados, pendientes y tasa de aprobación) que servirá como soporte para la verificación del cumplimiento de este componente por parte de la supervisión del contrato.

6 LICENCIAMIENTO Y COBERTURA

6.1 Cantidad de licencias y componentes requeridos

Con el propósito de fortalecer la postura de ciberseguridad del Municipio de Pereira, garantizar la continuidad operativa de la infraestructura tecnológica institucional y proteger los activos de información frente a amenazas cibernéticas actuales y emergentes, la Entidad requiere el suministro, implementación, configuración, puesta en operación, soporte y actualización de una solución integral de ciberseguridad, conformada por los siguientes componentes:

La solución deberá suministrarse completamente licenciada durante la vigencia contractual, incluyendo la totalidad de los componentes tecnológicos, licencias de software, suscripciones, infraestructura en la nube cuando aplique, actualizaciones, soporte técnico del fabricante, mantenimiento, configuración, acompañamiento técnico y todos los elementos necesarios para su correcta operación, sin que la Entidad deba adquirir componentes adicionales para cumplir con el alcance funcional establecido en el presente Anexo Técnico.

Componente requerido	Cantidad
1. Licencias de protección avanzada para endpoints con capacidades EDR, integradas a la plataforma institucional de correlación y respuesta, destinadas a la Administración Central.	1.000
2. Integración de dispositivos de seguridad perimetral (firewalls) institucionales a la plataforma SIEM Cloud, para la correlación de sus eventos de seguridad.	2
3. Protección especializada de correo electrónico institucional (Google Workspace), con capacidades de análisis de malware, phishing, BEC y cuarentena, integradas a la plataforma SIEM Cloud para la correlación de sus eventos.	640
4 Plataforma centralizada cloud tipo SIEM con capacidades XDR y SOAR para la recolección, normalización, almacenamiento, correlación e investigación de eventos de seguridad.	1
5 Plataforma cloud de capacitación y concienciación en ciberseguridad, con cursos interactivos, simulacros controlados de phishing, contenido en español y métricas de desempeño por usuario.	200

6.2 Vigencia del licenciamiento

Todas las licencias y suscripciones suministradas deberán contar con una cobertura efectiva de doce (12) meses, contados a partir de la puesta en producción y recibo a satisfacción de la solución por parte de la supervisión del contrato, sin que el periodo de alistamiento, implementación, configuración e integración disminuya dicha cobertura.

El derecho de uso de las plataformas, el acceso a actualizaciones de firmas/motores, la disponibilidad de la consola en la nube y el soporte técnico especializado 7x24 forman parte integral del licenciamiento adquirido y estarán amparados bajo la garantía técnica de la solución durante dicho periodo.

Durante dicho periodo, el contratista deberá garantizar, como mínimo:

- Derecho al uso de la totalidad de las funcionalidades licenciadas.
- Actualizaciones automáticas de motores de detección, firmas, reglas, inteligencia de amenazas y nuevas versiones liberadas por el fabricante.
- Acceso al soporte técnico del fabricante y del contratista.
- Corrección de vulnerabilidades y actualizaciones de seguridad.
- Disponibilidad permanente de la infraestructura en la nube requerida para la operación de la plataforma.
- Acompañamiento técnico especializado durante la implementación, configuración y estabilización de la solución.

6.3 Alcance del licenciamiento

El licenciamiento deberá permitir la operación integrada de todos los componentes de la solución de ciberseguridad, garantizando la interoperabilidad entre las plataformas de protección de endpoints, protección de correo electrónico, SIEM, capacidades XDR, SOAR, plataforma de concienciación y las Capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad.

La solución deberá operar como una arquitectura integral de ciberseguridad, permitiendo la centralización de eventos, la correlación de alertas, el enriquecimiento de incidentes, la investigación de amenazas por parte del personal designado por la Entidad y el fortalecimiento de las capacidades institucionales de detección y respuesta.

6.4 Generalidades

La solución integral de ciberseguridad deberá cumplir, como mínimo, con las siguientes condiciones generales:

- Ser totalmente compatible con la infraestructura tecnológica actual del Municipio de Pereira, incluyendo estaciones de trabajo, servidores, plataformas de virtualización, servicios en la nube y la infraestructura de seguridad perimetral existente, sin afectar la operación institucional.
- Soportar la totalidad del licenciamiento requerido por la Entidad, permitiendo su administración en múltiples sedes y garantizando la escalabilidad de la solución para futuros crecimientos de la infraestructura tecnológica.
- Permitir la administración centralizada de la solución mediante las consolas de gestión correspondientes a cada uno de sus componentes, garantizando la

interoperabilidad entre las diferentes plataformas que conforman la arquitectura integral de ciberseguridad.

- Permitir la integración de los diferentes componentes de la solución mediante mecanismos estándar soportados por los fabricantes, tales como APIs, Syslog, conectores nativos u otros mecanismos equivalentes, facilitando la centralización y correlación de eventos dentro de la plataforma SIEM y de las Capacidades Avanzadas de Detección, Correlación e Investigación.
- Todos los componentes de la solución deberán operar de manera integrada, permitiendo el intercambio seguro de información entre las plataformas de protección de endpoints, protección del correo electrónico, SIEM, capacidades XDR, SOAR, plataforma de concienciación y las Capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad, con el fin de fortalecer las capacidades institucionales de prevención, detección, investigación y respuesta frente a incidentes de ciberseguridad.

7 OBLIGACIONES DEL CONTRATISTA

El contratista deberá ejecutar el objeto contractual garantizando el suministro, implementación, configuración, integración, puesta en funcionamiento y soporte técnico especializado de la solución integral de ciberseguridad, incluyendo la plataforma SIEM Cloud, las capacidades de detección y respuesta extendida (XDR), automatización y orquestación de respuestas (SOAR), la protección de los endpoints, la protección del correo electrónico institucional y los demás componentes que conforman la solución, asegurando su correcto funcionamiento e interoperabilidad durante toda la vigencia del contrato.

Como mínimo deberá cumplir con las siguientes obligaciones:

1. Suministrar la totalidad de las licencias, suscripciones, plataformas y componentes tecnológicos requeridos para el correcto funcionamiento de la solución integral de ciberseguridad.
2. Implementar, configurar y poner en operación todos los componentes de la solución, garantizando su integración con la infraestructura tecnológica existente de la Entidad.
3. Realizar el aprovisionamiento, implementación, parametrización y puesta en producción de la nueva plataforma especializada de protección para los seiscientos cuarenta (640) buzones de correo electrónico institucional de Google Workspace, configurando las políticas de seguridad para la prevención y remediación de phishing, malware, ransomware y suplantación de identidad (BEC), e integrando la telemetría de eventos con la plataforma SIEM Cloud, sin generar interrupciones en la disponibilidad ni en el flujo del servicio de correo institucional de la Entidad.
4. Configurar las políticas de seguridad de acuerdo con las necesidades de la Alcaldía de Pereira.
5. Garantizar la puesta en funcionamiento y operación de la plataforma SIEM Cloud con capacidades de correlación, investigación y gestión de eventos de ciberseguridad, con funcionamiento continuo 7x24 de la plataforma, permitiendo la

recolección, normalización, correlación y análisis permanente de los eventos generados por los diferentes componentes de la solución, incluyendo los endpoints protegidos, la plataforma de seguridad de correo electrónico, los dispositivos de seguridad perimetral, así como cualquier otra fuente de eventos integrada por la Entidad. La plataforma deberá incorporar capacidades XDR para la correlación de eventos provenientes de múltiples dominios de seguridad y capacidades SOAR que permitan la automatización de procesos de respuesta mediante flujos de trabajo (playbooks), contribuyendo a la reducción de los tiempos de detección, análisis y contención de incidentes de ciberseguridad.

6. Garantizar la recolección, normalización, almacenamiento, correlación, análisis e investigación de eventos de ciberseguridad mediante la plataforma SIEM Cloud suministrada, integrando la telemetría proveniente de los endpoints, la solución de protección del correo electrónico, los dispositivos de seguridad perimetral y demás fuentes de eventos definidas por la Entidad. La plataforma deberá incorporar capacidades de detección y respuesta extendida (XDR) para correlacionar eventos de múltiples dominios de seguridad y capacidades de automatización de respuesta (SOAR) que permitan ejecutar flujos de respuesta automatizados (playbooks) frente a incidentes de ciberseguridad.
7. La plataforma SIEM Cloud deberá proporcionar una vista unificada y contextualizada de las alertas y eventos de ciberseguridad, permitiendo su clasificación y priorización de acuerdo con el nivel de riesgo, el impacto sobre los activos tecnológicos y el contexto de la amenaza, facilitando la gestión oportuna de los incidentes de seguridad.
8. La plataforma SIEM Cloud deberá permitir la gestión y trazabilidad de los incidentes de ciberseguridad identificados, registrando su ciclo de vida, estado, criticidad, acciones ejecutadas y evidencias asociadas, así como la generación de notificaciones y reportes para apoyar la toma de decisiones por parte de la Entidad.
9. Garantizar el soporte y acompañamiento técnico para la gestión y seguimiento de los incidentes de ciberseguridad identificados mediante la plataforma SIEM Cloud, permitiendo el registro de las acciones ejecutadas, el seguimiento de su estado, la generación de notificaciones y reportes, así como la entrega de recomendaciones para su contención y mitigación durante la ejecución del contrato.
10. Garantizar, durante toda la vigencia contractual, el soporte, mantenimiento y actualización de la plataforma SIEM Cloud y de los componentes que integran la solución de ciberseguridad suministrada, incluyendo motores de detección, inteligencia de amenazas, reglas de correlación, playbooks de automatización, políticas de seguridad, firmas, conectores, integraciones y demás actualizaciones, mejoras funcionales y de seguridad liberadas por los fabricantes, sin costo adicional para la Entidad.
11. Garantizar el soporte técnico especializado durante toda la ejecución del contrato para la solución de ciberseguridad suministrada, atendiendo oportunamente incidentes, requerimientos y solicitudes de soporte relacionadas con la plataforma SIEM Cloud, la protección de endpoints, la protección del correo electrónico, las integraciones implementadas y los demás componentes que conforman la solución.
12. Presentar, cuando sea requerido por la Entidad o de acuerdo con la periodicidad definida por el supervisor del contrato, reportes técnicos generados por la plataforma, relacionados con el estado de la solución, eventos de seguridad,

incidentes registrados, actividades de soporte realizadas y recomendaciones de mejora para la operación de la infraestructura protegida.

13. Brindar acompañamiento técnico especializado para el uso y operación de la plataforma SIEM Cloud y de los componentes que conforman la solución de ciberseguridad suministrada, apoyando a la Entidad en el seguimiento de eventos e incidentes de seguridad, el análisis de riesgos y la implementación de recomendaciones orientadas al fortalecimiento de su postura de ciberseguridad.
14. Garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso con ocasión de la ejecución del contrato, implementando las medidas de seguridad administrativas, técnicas y organizacionales necesarias para su protección, en cumplimiento de la normatividad vigente en materia de protección de datos personales, seguridad de la información y Gobierno Digital.
15. Designar el personal técnico especializado requerido para la implementación, configuración, integración, puesta en funcionamiento y soporte de la solución de ciberseguridad suministrada, garantizando que cuente con la experiencia, competencias y certificaciones necesarias para la correcta ejecución del contrato.
16. Garantizar el correcto funcionamiento de la solución integral de ciberseguridad suministrada durante toda la vigencia contractual, ejecutando las actividades de implementación, configuración, integración, actualización, mantenimiento y soporte técnico que sean necesarias para su adecuada operación, sin generar costos adicionales para la Entidad.

7.1 Obligaciones Específicas

- Designar un equipo técnico responsable de la implementación, configuración, integración, puesta en funcionamiento y soporte especializado de la solución integral de ciberseguridad, conformado por profesionales y/o tecnólogos con formación y experiencia en plataformas de ciberseguridad, así como con las certificaciones técnicas vigentes exigidas para los perfiles definidos en el numeral de Certificaciones del presente Anexo Técnico, quienes deberán estar vinculados directamente con el contratista durante toda la ejecución del contrato. El oferente deberá adjuntar las certificaciones técnicas vigentes del personal propuesto como parte de su oferta.
- Garantizar soporte técnico especializado durante la vigencia del contrato sobre la totalidad de los componentes que conforman la solución integral de ciberseguridad suministrada, incluyendo la protección de endpoints, la plataforma SIEM Cloud, las capacidades de detección y respuesta extendida (XDR), automatización y orquestación de respuestas (SOAR), la protección del correo electrónico institucional, la integración de los dispositivos perimetrales definidos por la Entidad y la plataforma de capacitación en concienciación de ciberseguridad, garantizando su correcto funcionamiento e interoperabilidad.
- Garantizar el funcionamiento continuo 7x24 de la plataforma SIEM Cloud, permitiendo la recepción, normalización, correlación y gestión de los eventos de seguridad generados por los diferentes componentes de la solución integral de ciberseguridad, así como el soporte especializado para la atención, investigación y

seguimiento de los incidentes escalados por la Entidad durante la vigencia del contrato.

- Garantizar un tiempo máximo de respuesta inicial de una (1) hora para la atención de incidentes críticos reportados o escalados por la Entidad, conforme a la Tabla de Severidad y Tiempos de Atención del numeral 7.2.1, brindando el soporte técnico especializado requerido para su diagnóstico, análisis y definición de las acciones de mitigación correspondientes.
- Garantizar la prestación del soporte técnico especializado sobre la solución integral de ciberseguridad, asegurando la atención oportuna de los incidentes y requerimientos reportados por la Entidad, dentro de los tiempos de respuesta e inicio de acciones establecidos en la Tabla de Severidad y Tiempos de Atención del numeral 7.2.1.
- Brindar soporte técnico especializado y acompañamiento a la Entidad para el adecuado funcionamiento de la solución integral de ciberseguridad, proporcionando asistencia en el análisis de eventos e incidentes identificados por la plataforma, la gestión de riesgos asociados, la validación de las integraciones implementadas y la formulación de recomendaciones para fortalecer la postura de ciberseguridad de la Entidad.
- Cuando el soporte técnico remoto no sea suficiente para atender un incidente o requerimiento asociado a la solución integral de ciberseguridad, y previa solicitud del supervisor del contrato, el contratista deberá disponer de acompañamiento técnico presencial en las instalaciones de la Entidad, en un tiempo máximo de una (1) hora.
- El oferente deberá contar con un Sistema de Gestión de Calidad certificado conforme a la Norma ISO 9001:2015, vigente a la fecha de cierre del proceso y durante la ejecución del contrato, cuyo alcance incluya la comercialización e implementación de soluciones TIC, garantizando que los procesos asociados al suministro, implementación y puesta en operación de la solución integral de ciberseguridad se ejecuten bajo procedimientos documentados y sujetos a mejora continua. Para acreditar este requisito, deberá aportar copia del certificado vigente expedido por un organismo certificador acreditado.
- Garantizar que el personal técnico asignado para la implementación, administración, configuración, integración y soporte de la solución integral de ciberseguridad preste la totalidad del soporte técnico especializado, atención de requerimientos y acompañamiento a la Entidad en idioma español durante la ejecución del contrato.
- Mantener comunicación permanente con el supervisor del contrato, informando oportunamente sobre incidentes críticos, vulnerabilidades de alto impacto, eventos relevantes identificados mediante la solución integral de ciberseguridad o situaciones que puedan afectar la disponibilidad, integridad o confidencialidad de la información institucional, brindando el soporte técnico y las recomendaciones necesarias para su atención y mitigación.
- Presentar, cuando sea requerido por la Entidad o en las oportunidades definidas durante la ejecución del contrato, informes sobre el estado y funcionamiento de la solución integral de ciberseguridad, incluyendo como mínimo los eventos relevantes identificados, el estado de la infraestructura protegida, las actualizaciones realizadas, el cumplimiento de los Acuerdos de Niveles de Servicio (ANS) del

soporte técnico y las recomendaciones para fortalecer la postura de ciberseguridad de la Entidad.

- Garantizar el soporte técnico especializado para la configuración, actualización y ajuste de los parámetros de operación de la plataforma SIEM Cloud suministrada, así como el correcto funcionamiento de las integraciones con los diferentes componentes que conforman la solución integral de ciberseguridad, asegurando la estabilidad, interoperabilidad y desempeño de la plataforma durante la ejecución del contrato.
- Cuando, en ejecución de las actividades de soporte o en la atención de incidentes escalados, el contratista tenga conocimiento de alertas clasificadas como críticas o de alto impacto que puedan comprometer la disponibilidad, integridad o confidencialidad de los activos tecnológicos de la Entidad, deberá informar oportunamente al Municipio de Pereira, de conformidad con el plan de comunicaciones y los Acuerdos de Niveles de Servicio (ANS) establecidos, suministrando la información técnica y las recomendaciones necesarias para su atención.
- La gestión de las acciones de contención, mitigación, remediación y recuperación sobre los activos de información continuará siendo responsabilidad de los administradores designados por el Municipio de Pereira. El contratista brindará el acompañamiento y soporte técnico especializado requerido para apoyar el análisis del incidente, la identificación de su causa y la implementación de las recomendaciones técnicas correspondientes, dentro del alcance del contrato.
- Los informes periódicos de estado de la solución deberán indicar, como mínimo, el estado de cada evento o incidente relevante (en atención, resuelto o pendiente) y su nivel de criticidad.
- El contratista deberá realizar la transferencia de conocimiento sobre la administración y aprovechamiento de la plataforma oficial de capacitación del fabricante, dirigida al personal designado por la Entidad, incluyendo la gestión de usuarios, la creación y seguimiento de campañas de concienciación, la asignación de contenidos, la consulta de indicadores y la generación de reportes.
- La consola centralizada de gestión de la plataforma SIEM Cloud operará en la nube, admitiendo esquemas de arquitectura híbrida con colectores locales cuando la solución del fabricante lo requiera. Todos los componentes de la arquitectura ofertada, independientemente de su esquema de despliegue, estarán cubiertos por la garantía técnica y la asistencia posventa 7x24 del fabricante y del contratista durante la vigencia de las suscripciones.
- Al finalizar el contrato, el contratista deberá entregar a la Entidad, en formato estándar e interoperable (como JSON, CSV o CEF), la totalidad de los registros, eventos, incidentes, alertas, evidencias de investigación y configuraciones almacenados en la plataforma durante la ejecución, sin costo adicional. La información es de propiedad de la Entidad, y el contratista no podrá retenerla, utilizarla para fines distintos a la ejecución del contrato ni conservar copias una vez cumplida la entrega y obtenida la autorización de la Entidad. Cumplida la entrega y obtenida la conformidad de la supervisión,

el contratista suprimirá las copias de la información que conserve y expedirá una certificación de borrado seguro, de conformidad con la Ley 1581 de 2012.

7.2 Acuerdos de Niveles de Servicio (ANS) para el Soporte Técnico Especializado

El presente numeral establece el Acuerdo de Nivel de Servicio (ANS) aplicable a la asistencia técnica posventa y garantía de la solución integral de ciberseguridad. Dicho soporte corresponde a la atención 7x24 para la atención de solicitudes, investigación de incidentes sobre la plataforma y acompañamiento técnico a la Entidad. La ejecución directa de las acciones de contención y remediación sobre la infraestructura institucional será responsabilidad del personal de la Alcaldía de Pereira, con el soporte técnico del contratista conforme a los tiempos del ANS.

Aclaración de Alcance de Soporte: El servicio de soporte técnico especializado 7x24 exigido en el presente numeral corresponde al soporte operativo, mantenimiento, atención de incidentes escalados por la Entidad y garantía de disponibilidad y estabilidad de las plataformas contratadas, cuya operación y revisión de consolas permanece a cargo del personal de la Secretaría TIC de la Alcaldía de Pereira.

El contratista deberá prestar el servicio de soporte técnico especializado bajo un esquema de atención 7x24 sobre la plataforma SIEM Cloud y los demás componentes de la solución, garantizando el monitoreo del correcto funcionamiento de la plataforma, el análisis técnico de las alertas escaladas por la Entidad y de aquellas que, por falla o anomalía en el funcionamiento de la plataforma, requieran su intervención, el apoyo en la investigación de incidentes, la gestión de casos de soporte y el acompañamiento durante las actividades de contención, mitigación y recuperación que ejecute la Entidad.

Los incidentes de seguridad serán clasificados de acuerdo con su criticidad de la siguiente manera:

Crítico: Incidentes que comprometan la disponibilidad de servicios esenciales, la confidencialidad o integridad de la información institucional, ataques de ransomware, compromiso de cuentas privilegiadas, accesos no autorizados, campañas activas de malware, compromiso de buzones de correo electrónico institucional, explotación activa de vulnerabilidades o cualquier evento que represente un riesgo alto para la operación de la Entidad.

Alto: Incidentes con afectación parcial de los servicios, detección de amenazas con alto potencial de explotación, intentos reiterados de compromiso, vulnerabilidades críticas identificadas o eventos que requieran atención prioritaria.

Medio: Incidentes con impacto limitado sobre la operación, eventos que requieran análisis técnico, ajustes de configuración o validaciones de seguridad sin afectación inmediata de los servicios institucionales.

Bajo: Solicitudes de soporte, consultas técnicas, ajustes menores de configuración, requerimientos administrativos o actividades preventivas que no representen riesgo inmediato para la operación.

Acuerdo de Nivel de Servicio (ANS)

Para efectos del presente contrato:

- *Tiempo de respuesta inicial:* corresponde al primer contacto técnico efectivo por parte del equipo especializado del contratista, incluyendo el registro, clasificación y asignación del incidente.
- *Inicio de acciones de contención o mitigación:* corresponde al momento en que el contratista inicia las actividades técnicas orientadas a reducir el impacto del incidente, contener la amenaza o implementar medidas de mitigación. La solución definitiva podrá depender de la complejidad del incidente, de la participación de terceros, de decisiones de la Entidad o de actividades de recuperación que excedan el alcance del servicio contratado.

El contratista deberá mantener comunicación permanente con la Entidad durante la atención del incidente, suministrando información sobre el estado del caso, las acciones ejecutadas, las recomendaciones emitidas y las actividades pendientes hasta su cierre.

El incumplimiento reiterado e injustificado de los niveles de servicio (ANS) establecidos podrá dar lugar a la aplicación de las medidas contractuales y sanciones previstas en la normatividad vigente y en el contrato.

7.2.1 *Tabla de Severidad y Tiempos de Atención*

Severidad	Tiempo máximo de respuesta inicial	Inicio de acciones de contención o mitigación
Crítico	1 hora	4 horas
Alto	2 horas	8 horas
Medio	4 horas	24 horas
Bajo	8 horas	48 horas

8 CONDICIONES GENERALES

El contratista deberá garantizar el suministro, instalación, configuración, parametrización, puesta en funcionamiento y correcto funcionamiento de la solución integral de ciberseguridad objeto del presente proceso, incluyendo las licencias de protección para endpoints, la plataforma de protección de correo electrónico, la plataforma SIEM Cloud, las capacidades de detección y respuesta extendida (XDR) y de automatización y orquestación de respuesta (SOAR), la plataforma de concienciación y capacitación, y las Capacidades Avanzadas de Detección, Correlación e Investigación de Eventos de Ciberseguridad.

Así mismo, deberá garantizar la integración entre los diferentes componentes tecnológicos de la solución, asegurando la correcta interoperabilidad entre las plataformas de protección de endpoints, protección de correo electrónico, SIEM Cloud, capacidades XDR y SOAR, los dispositivos de seguridad perimetral integrados y demás fuentes de eventos de la solución.

El contratista deberá implementar las consolas de administración requeridas, realizar las configuraciones necesarias, efectuar las pruebas funcionales y de aceptación, y brindar acompañamiento técnico durante toda la ejecución contractual, garantizando la continuidad operativa de la solución.

8.1 Capacitación y transferencia de conocimiento

Durante la ejecución del contrato, el contratista deberá desarrollar, como mínimo, las siguientes actividades de capacitación y transferencia de conocimiento, conforme a las condiciones, duraciones, participantes, modalidades, entregables y criterios de aceptación establecidos:

Actividad	Duración mínima	Participantes	Modalidad	Entregables exigidos	Criterio de aceptación
Jornada de capacitación técnica a administradores (EDR, SIEM, XDR y SOAR)	4 horas	Administradores e ingenieros de la Secretaría TIC	Presencial o virtual	Material técnico, registro de asistencia y memorias	Acta suscrita por la supervisión
Charla sobre buenas prácticas de ciberseguridad	4 horas	Servidores públicos y contratistas designados	Presencial o virtual	Registro de asistencia y presentación ejecutiva	Acta suscrita por la supervisión
Capacitación en protección de datos	4 horas	Servidores públicos y funcionarios	Presencial o virtual	Registro de asistencia y	Acta suscrita por

personales, Modelo de Seguridad y Privacidad de la Información (MSPI) y Gobierno Digital				material educativo	la supervisión
Capacitación en amenazas emergentes, ransomware, phishing y autenticación multifactor (MFA)	4 horas	Servidores públicos y usuarios designados	Presencial o virtual	Registro de asistencia y material didáctico	Acta suscrita por la supervisión
Campaña de concienciación con simulación controlada de phishing	Una (1) campaña completa	Población licenciada de hasta doscientos (200) usuarios	Plataforma Cloud	Informe detallado de resultados con las métricas previstas en el numeral 5.5	Informe aprobado por la supervisión

La capacitación técnica a administradores deberá comprender, como mínimo, la identificación de amenazas, el análisis de alertas EDR, la mitigación de incidentes, la configuración y utilización de flujos automatizados de respuesta (playbooks), la seguridad de servidores y la integración con Directorio Activo.

Las duraciones y actividades señaladas constituyen requisitos mínimos obligatorios. El contratista podrá ofrecer intensidades superiores sin costo adicional para la Entidad.

Los costos asociados a estas actividades se entienden incluidos en el valor de los componentes contratados y no darán lugar a facturación independiente.

La campaña de concienciación basada en simulación controlada de phishing deberá ejecutarse mediante la plataforma especializada adquirida, la cual deberá permitir, como mínimo:

- Simulación de campañas de phishing personalizables.

- Asignación automática de cursos o microcursos de concienciación según el comportamiento del usuario.
- Biblioteca de contenidos de formación en ciberseguridad.
- Seguimiento y evaluación del desempeño de los usuarios.
- Generación de indicadores, estadísticas y reportes de resultados.
- Emisión de certificados de participación o finalización.
- Administración centralizada de campañas y usuarios.

8.2 Información técnica sobre inteligencia de amenazas

Durante la ejecución del contrato, el contratista deberá suministrar a la Entidad, cuando se identifiquen amenazas relevantes o cuando sea requerido por el supervisor del contrato, información técnica relacionada con el panorama actual de ciberseguridad, orientada a fortalecer la administración de la solución implementada y la adopción de medidas preventivas. Esta información podrá ser obtenida de los fabricantes de las soluciones ofertadas, de la inteligencia de amenazas integrada en las plataformas suministradas y de organismos oficiales especializados en ciberseguridad.

Como mínimo, la información técnica deberá contemplar:

- Amenazas emergentes y tendencias de ciberseguridad con posible impacto sobre la infraestructura tecnológica de la Entidad.
- Vulnerabilidades críticas que puedan afectar los componentes protegidos por la solución implementada.
- Campañas activas de phishing, ransomware, malware y demás amenazas relevantes.
- Indicadores de compromiso (IoC), cuando sean publicados por los fabricantes u organismos especializados.
- Recomendaciones técnicas para la mitigación de riesgos y fortalecimiento de los controles de seguridad.
- Alertas, avisos de seguridad y boletines técnicos emitidos por los fabricantes de las soluciones suministradas y por organismos oficiales o especializados en ciberseguridad, tales como ColCERT, MinTIC, el Centro Cibernético Policial (CCP), FIRST, CISA u otros organismos equivalentes, cuando resulten aplicables.

8.3 El contratista deberá garantizar

- Que la totalidad de las licencias suministradas se encuentren correctamente implementadas, configuradas, activadas y en funcionamiento durante la vigencia del contrato.
- Que todas las licencias y componentes de la solución permanezcan durante la vigencia contractual con las versiones actualizadas y soportadas por el fabricante,

incluyendo las actualizaciones de motores de detección, firmas, políticas, inteligencia de amenazas, reglas de correlación, funcionalidades, parches de seguridad y demás componentes liberados oficialmente.

- Que toda instalación, implementación, configuración o actualización realizada sobre los componentes de la solución quede debidamente documentada mediante las actas o registros de implementación correspondientes, indicando como mínimo las actividades ejecutadas, los componentes intervenidos, la fecha de ejecución y la aceptación por parte del personal designado por la Entidad.
- Implementar, configurar y dejar en funcionamiento las consolas de administración de la solución, incluyendo la creación de políticas, perfiles, grupos, roles administrativos, parametrización de la plataforma SIEM Cloud, configuración de las integraciones y demás elementos necesarios para su correcta operación.
- Realizar las pruebas funcionales, de integración y validación necesarias para verificar el correcto funcionamiento de todos los componentes suministrados, incluyendo las capacidades de detección, correlación, visualización de eventos, automatización de respuestas, integración de fuentes de información y administración centralizada.
- Garantizar que dispone de un equipo de ingeniería debidamente certificado por el fabricante de la solución ofertada, con experiencia comprobable en implementación, integración y soporte técnico especializado de soluciones de ciberseguridad para entornos corporativos o institucionales. Dicho equipo deberá atender los incidentes y requerimientos de soporte de manera remota y, cuando por la naturaleza del caso sea necesaria la atención presencial y esta sea solicitada por la Entidad, deberá desplazarse a las instalaciones de la Alcaldía de Pereira en un tiempo máximo de una (1) hora.

9 REQUISITOS DEL EQUIPO DE TRABAJO

9.1 Perfiles y Capacidad de Respuesta del Equipo de Seguridad

El proponente deberá contar con personal certificado por el fabricante de la solución ofertada y con experiencia comprobable en implementación, administración y soporte de soluciones de ciberseguridad de nivel corporativo o institucional.

El proponente deberá acreditar como mínimo el siguiente equipo de trabajo:

- El equipo deberá estar conformado como mínimo por un (1) ingeniero en sistemas, con experiencia profesional mínima de dos (2) años, contados a partir de la expedición de su tarjeta profesional y dos (2) Tecnólogos en Sistemas o carreras afines.
- El ingeniero deberá contar con certificaciones vigentes emitidas por el fabricante correspondiente a los productos o tecnologías que se implementarán en el marco del contrato.
- Con el fin de garantizar la idoneidad y alineación con los lineamientos nacionales de seguridad digital, el proponente deberá acreditar que su equipo de trabajo posee certificaciones oficiales expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), específicamente en los siguientes ámbitos:

✓ Certificación en Seguridad y Privacidad de la Información Gobierno Digital (MinTIC): Acredita conocimientos en buenas prácticas de gestión de activos digitales, liderazgo en seguridad de la información y cumplimiento de políticas y normativas vigentes.

✓ Certificación en el Modelo de Seguridad y Privacidad de la Información (MSPI vigente): Acredita competencias en la implementación de controles, políticas y estrategias de seguridad alineadas con el Modelo de Seguridad y Privacidad de la Información del Gobierno Digital y los lineamientos nacionales vigentes en materia de ciberseguridad y protección de la información.

9.2 Certificación técnica del producto ofertado

- El equipo técnico deberá contar con certificación vigente en las tecnologías específicas de la solución propuesta, emitida directamente por el fabricante. Esto garantiza el dominio integral del producto, su correcta implementación y la capacidad de brindar soporte experto durante todo el ciclo del contrato.
- El personal técnico asignado deberá estar certificado en las líneas de productos de nueva generación del fabricante, incluyendo componentes de protección avanzada, detección, respuesta y gestión centralizada.
- El personal deberá contar adicionalmente con certificación en plataformas o módulos de concienciación y capacitación en ciberseguridad, orientadas a la implementación de campañas automatizadas para usuarios finales, con el fin de fortalecer la cultura organizacional de seguridad digital.
- Las certificaciones de producto exigidas en los numerales 9.3 y 9.4 del Anexo Técnico se entenderán acreditadas con la certificación oficial que el fabricante de la solución ofertada tenga establecida para la respectiva tecnología (XDR, EDR, SIEM, MDR, concienciación y preventa), vigente a la fecha de cierre, acompañada de documento del fabricante que indique su alcance. No se aceptarán certificaciones de terceros ni de fabricantes distintos al de la solución ofertada. La certificación ITIL 4 y las certificaciones MinTIC se acreditan en los términos señalados, sin equivalencias.
-

9.3 Certificaciones requeridas para el Ingeniero de Sistemas

- Certificación vigente como Sales Specialist o equivalente, emitida por el fabricante, que respalde competencias en gestión comercial, preventa y conocimiento integral de las soluciones de ciberseguridad ofertadas. El personal técnico asignado deberá estar certificado en las líneas de productos de nueva generación del fabricante, incluyendo componentes de protección avanzada, detección, respuesta y gestión centralizada.
- Certificación vigente como Certified Professional en soluciones de Managed Detection and Response (MDR), que evidencie dominio técnico y comercial sobre la arquitectura, funcionalidades y beneficios de servicios avanzados de detección y respuesta administrada.
- Certificación vigente como Certified Professional en plataformas SIEM (Security Information and Event Management), que acredite conocimiento en configuración, integración, correlación de eventos y gestión de incidentes.

- Certificación vigente en soluciones avanzadas de protección de endpoints, detección y respuesta ante amenazas, y plataformas de concienciación y capacitación en ciberseguridad.
- Certificación vigente ITIL 4 Foundation o superior, que acredite competencias en gestión de servicios TI, operación de servicios tecnológicos, gestión de incidentes, mejora continua y buenas prácticas orientadas a la calidad y eficiencia operativa de los servicios de tecnología y ciberseguridad.
-

9.4 Certificaciones requeridas para los Tecnólogos en Sistemas o afines

- Certificación vigente como Certified Professional en soluciones de Extended Detection and Response (XDR), que valide su conocimiento avanzado en integración de múltiples fuentes de telemetría, correlación de eventos, investigación de incidentes y automatización de respuestas.
- Certificación vigente en plataformas de capacitación automatizada en concienciación de seguridad, orientada a la gestión de contenidos, interpretación de reportes y fortalecimiento de la cultura de ciberseguridad institucional.
- Certificación vigente como Sales Specialist o equivalente, emitida por el fabricante, que respalde competencias comerciales, preventa e integración de soluciones de seguridad en entornos corporativos.
- Certificación vigente en Managed Detection and Response (MDR) y plataformas de monitoreo y análisis unificado de eventos de seguridad (SIEM), que validen sus conocimientos para administrar, optimizar y responder a incidentes en tiempo real.

9.5 Capacidades complementarias del equipo

- El proponente deberá presentar certificación suscrita por su Representante Legal, mediante la cual acredite que el equipo de trabajo asignado al proyecto cuenta con las certificaciones y experiencia requeridas para la implementación y gestión integral de la solución de seguridad ofertada.

  La certificación deberá relacionar, para cada integrante del equipo: nombre completo, cargo, certificaciones, y experiencia en mínimo dos (2) proyectos similares, indicando entidad contratante, objeto o alcance, actividades realizadas y período de ejecución.

  La experiencia del equipo de trabajo deberá comprender actividades de planificación, despliegue, gestión de incidentes, implementación de políticas y acompañamiento técnico en ciberseguridad en entidades públicas o empresas del sector privado

9.6 Requisitos del proponente

- El proponente debe adjuntar una certificación del fabricante donde se evidencie que cuenta con algún nivel de membresía como distribuidor autorizado, no debe ser mayor a 30 días y será validada por la entidad, directamente en el directorio oficial de Partners del fabricante, y no será válido el respaldo emitido por mayoristas.

- El proponente deberá anexar una certificación expedida directamente por el fabricante o fabricantes de las soluciones ofertadas, en la que se acredite que el personal técnico propuesto para la ejecución del contrato cuenta con el entrenamiento y las certificaciones técnicas vigentes necesarias para la implementación, configuración, integración y soporte de los componentes que conforman la solución integral de ciberseguridad objeto del presente proceso, de conformidad con las tecnologías ofertadas. Este requisito se entenderá cumplido con las certificaciones individuales vigentes de cada integrante del equipo, expedidas directamente por el fabricante de la solución ofertada y verificables por la Entidad. No se aceptan declaraciones del proponente sin soporte documental del fabricante
- Cuando para la atención de incidentes, requerimientos o actividades de soporte técnico sea necesario realizar acceso remoto a la infraestructura tecnológica de la Entidad, el proponente deberá suministrar la licencia de uso de la herramienta tecnológica que utilizará para dicho acceso, garantizando que esta sea legalmente licenciada, original y cuente con los derechos de uso vigentes, de conformidad con las disposiciones sobre propiedad intelectual y licenciamiento de software aplicables en Colombia, incluyendo la Ley 603 de 2000. El acceso remoto únicamente podrá realizarse con autorización previa de la Entidad y bajo los mecanismos de seguridad definidos por esta. Cuando la Entidad disponga o designe el mecanismo de acceso remoto, por ejemplo una VPN o una herramienta provista por ella, el contratista utilizará dicho mecanismo y no estará obligado a suministrar una licencia propia. Si el contratista utiliza una herramienta propia, esta deberá contar con autenticación multifactor, registro de auditoría de las sesiones y autorización previa de la Entidad para cada acceso.
- El proponente deberá disponer de un Centro de Operación y Soporte Especializado, desde el cual se ejecuten las actividades de soporte técnico especializado, atención de requerimientos e incidentes de la plataforma y acompañamiento asociados a la solución integral de ciberseguridad ofertada.

  Como mínimo, deberá cumplir las siguientes condiciones:

  - El Centro de Operación y Soporte Especializado deberá encontrarse bajo la administración directa y permanente del proponente, sea propio, arrendado o contratado.
  - Deberá estar ubicado en el territorio colombiano, indicando la ciudad donde opera, con el fin de garantizar la oportunidad en la prestación del soporte técnico, el monitoreo de la solución y el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos en el presente proceso.
  - El proponente deberá acreditar la disponibilidad del Centro de Operación y Soporte Especializado mediante certificación suscrita por su Representante Legal, indicando su dirección de funcionamiento y declarando que permanecerá disponible durante toda la ejecución del contrato.
  - El Centro de Operación y Soporte Especializado deberá contar con la infraestructura tecnológica, herramientas de gestión, mecanismos de control de acceso físico y

lógico, conectividad y demás recursos necesarios para garantizar la administración, monitoreo, soporte y continuidad operativa de la solución integral de ciberseguridad.

- El personal técnico encargado de la administración, monitoreo, soporte especializado y atención de incidentes deberá prestar la totalidad de estos servicios en idioma español.
- La Entidad podrá verificar, durante la evaluación de las ofertas o en cualquier momento de la ejecución contractual, la existencia, disponibilidad y condiciones operativas del Centro de Operación y Soporte Especializado declarado por el proponente

- Dado que el contratista podrá tener acceso a información y activos tecnológicos de la Alcaldía de Pereira durante las actividades de implementación, configuración, integración y soporte técnico de la solución integral de ciberseguridad, deberá garantizar la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso, adoptando las medidas técnicas, administrativas y organizacionales necesarias para su protección, en cumplimiento de la Ley 1581 de 2012, la Ley 1266 de 2008, la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y demás normas aplicables.

  El proponente deberá presentar certificación suscrita por el Representante Legal, en la cual manifieste que:

  1. Cuenta con políticas y procedimientos internos vigentes para la protección y manejo seguro de la información.
  2. Dichas políticas y procedimientos son aplicables al personal que participe en la ejecución del contrato.
  3. Cuenta con mecanismos de control de acceso orientados a prevenir el acceso, uso, divulgación, modificación o pérdida no autorizada de la información de la Entidad.
  4. Se compromete a garantizar la confidencialidad y protección de la información de la Entidad a la que tenga acceso con ocasión de la ejecución contractual.
  5. Dará cumplimiento a la normatividad vigente aplicable en materia de protección de datos personales, seguridad y confidencialidad de la información.

  La certificación deberá indicar expresamente que estas medidas se encuentran implementadas y vigentes a la fecha de presentación de la oferta y que las mantendrá durante toda la ejecución del contrato.

10VIGENCIA

El plazo de ejecución del contrato será de hasta un (1) año y quince (15) días calendario, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de ejecución contractual, sin exceder el 31 de diciembre de 2027.

La ejecución comprenderá una etapa inicial de alistamiento, suministro, instalación, configuración, integración, implementación y puesta en funcionamiento de la solución, de máximo quince (15) días calendario, contados a partir de la suscripción del acta de inicio. Esta etapa deberá finalizar, en todo caso, a más tardar el 26 de diciembre de 2026.

Posteriormente, las licencias, suscripciones, actualizaciones, soporte técnico especializado y asistencia técnica posventa deberán contar con una cobertura efectiva de doce (12) meses, contados a partir de la puesta en producción y recibo a satisfacción de la solución por parte de la supervisión del contrato, sin que el periodo de implementación disminuya dicha cobertura.

El cumplimiento de estas obligaciones estará amparado por las garantías de cumplimiento y calidad del servicio, en las condiciones establecidas en el contrato y demás documentos del proceso.

11 GLOSARIO DE TÉRMINOS Y SIGLAS

ANS (Acuerdo de Nivel de Servicio): Compromiso contractual que define, según el nivel de severidad del incidente, los tiempos máximos de respuesta inicial y de inicio de acciones de contención o mitigación, conforme al numeral 7.2.1. No incluye tiempos de solución definitiva.
API (Application Programming Interface): Interfaz de programación que permite que dos plataformas distintas —por ejemplo, la solución de correo y Google Workspace, o el correo y el SIEM— intercambien información de forma automatizada y segura, sin intervención manual.
APT (Advanced Persistent Threat): Amenaza persistente avanzada: ataque prolongado y sigiloso, normalmente dirigido, en el que el atacante permanece en la infraestructura de la víctima buscando pasar inadvertido durante un periodo extendido.
ATO (Account Takeover): Compromiso o usurpación de una cuenta de usuario legítima por parte de un atacante, generalmente mediante robo de credenciales.
BEC (Business Email Compromise): Fraude por suplantación de identidad ejecutiva o de proveedores mediante correo electrónico, orientado a inducir transferencias de dinero o divulgación de información sensible.
CEF (Common Event Format): Formato estándar de la industria para estructurar eventos de seguridad, utilizado para que distintas plataformas puedan enviarse información entre sí de forma comprensible.
CDP (Certificado de Disponibilidad Presupuestal): Documento que certifica la existencia de apropiación presupuestal disponible para respaldar un proceso de contratación pública en Colombia.
EDR (Endpoint Detection and Response): Tecnología de protección de estaciones de trabajo, portátiles y servidores que, además de prevenir amenazas, permite detectar comportamientos sospechosos, investigar incidentes y ejecutar acciones de respuesta (aislamiento, contención, remediación).
EPP (Endpoint Protection Platform): Plataforma de protección de endpoints orientada principalmente a la prevención (antivirus, antimalware de nueva generación), complementaria al EDR.

IoC (Indicador de Compromiso): Evidencia técnica (dirección IP, hash de archivo, dominio, etc.) que sugiere que un sistema ha sido comprometido o está siendo objeto de un ataque.
IoA (Indicador de Ataque): Evidencia de comportamiento que sugiere que un ataque está en curso, independientemente de si ya se identificó un indicador de compromiso específico.
MDR (Managed Detection and Response): Servicio gestionado de detección y respuesta, prestado por un tercero especializado que monitorea y responde a amenazas en nombre del cliente.
MITRE ATT&CK: Catálogo público y gratuito de tácticas y técnicas reales utilizadas por atacantes, empleado como referencia estándar para etiquetar y mapear la cobertura de detección de una plataforma de ciberseguridad.
Multitenant (arquitectura multiinquilino): Modelo de arquitectura en la nube en el que un mismo proveedor atiende a múltiples entidades clientes sobre una infraestructura compartida, garantizando la segregación lógica de los datos y configuraciones de cada una, sin necesidad de hardware o software dedicado en las instalaciones del cliente.
MSPI (Modelo de Seguridad y Privacidad de la Información): Modelo de referencia del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que orienta a las entidades públicas colombianas en la gestión de la seguridad y privacidad de la información.
MTTD (Mean Time to Detect): Tiempo promedio que tarda una organización en detectar un incidente de seguridad desde que ocurre.
MTTR (Mean Time to Respond): Tiempo promedio que tarda una organización en responder y contener un incidente de seguridad una vez detectado.
Playbook: Procedimiento de respuesta automatizado y predefinido que una plataforma SOAR ejecuta —de forma automática o con aprobación de un analista— ante un tipo específico de incidente, encadenando acciones como aislar un equipo, bloquear un archivo o notificar al equipo de soporte.
RBAC (Role-Based Access Control): Control de acceso basado en roles: modelo que permite definir perfiles de usuario dentro de una consola (administrador, analista, auditor de solo lectura, etc.) con permisos diferenciados sobre lo que cada uno puede ver y hacer.
SIEM (Security Information and Event Management): Plataforma centralizada de gestión de información y eventos de seguridad, encargada de recibir, normalizar, correlacionar y visualizar eventos provenientes de múltiples fuentes (EDR, correo, firewalls, etc.), sin realizar por sí misma el análisis de contenido de dichas fuentes.
SOAR (Security Orchestration, Automation and Response): Capacidades de orquestación, automatización y respuesta que permiten ejecutar playbooks y reducir la intervención manual del analista frente a incidentes repetitivos.
SOC (Security Operations Center): Centro de Operaciones de Seguridad: conjunto de personas, procesos y tecnología dedicados al monitoreo, detección, investigación y respuesta ante incidentes de ciberseguridad de una organización.
Syslog: Protocolo estándar utilizado para el envío de mensajes de registro (logs) desde un sistema hacia un servidor centralizado, comúnmente usado para integrar fuentes de datos con una plataforma SIEM.
UEBA (User and Entity Behavior Analytics): Analítica del comportamiento de usuarios y entidades, orientada a detectar anomalías que puedan indicar una amenaza interna o una cuenta comprometida, mediante el aprendizaje de patrones de comportamiento normal.

XDR (Extended Detection and Response): Detección y respuesta extendida: capacidad que consolida y correlaciona información proveniente de múltiples fuentes de seguridad (endpoints, correo, red, nube) para ampliar la visibilidad y precisión frente a amenazas que involucran varios vectores de ataque simultáneamente.

CARLOS FERNANDO GARCÍA C
Director de Infraestructura tecnológica

Apoyo técnico: Héctor F. Arias Cardona, contratista Secretaria de las TIC