DATOS DE LA DEPENDENCIA SOLICITANTE			
DEPENDENCIA/PROCESO SOLICITANTE:		OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	**FECHA DE SOLICITUD:**6/11/2026
NOMBRE DEL RESPONSABLE DE DEPENDENCIA/PROCESO:		YENNY HASLEY YAZO LOZADA	**TELÉFONO:** (601) 377 9555
CORREO INSTITUCIONAL DE CONTACTO:		Yenny.yazo@umv.gov.co	
FECHA ESTIMADA DE APERTURA DEL PROCESO DEFINIDO EN EL PLAN DE ADQUISICIONES:			
FUENTE DE LOS RECURSOS	**FUNCIONAMIENTO**		
	INVERSIÓN	Proyecto 8089	
	OTRA FUENTE DE RECURSOS		
ÍTEM PLAN DE ADQUISICIONES:		8089-053	
RUBRO PRESUPUESTAL QUE AMPARA LA CONTRATACIÓN:		O2301174599202401610900 7 Fortalecimiento de los componentes tecnológicos	

DESCRIPCIÓN DE LA NECESIDAD:

OBJETO DE LA CONTRATACION: SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA PROTECCIÓN INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCIÓN, DETECCIÓN Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCIÓN DE PÉRDIDAS DE DATOS

PRESUPUESTO ESTABLECIDO EN EL PLAN DE ADQUISICIONES PARA LA NECESIDAD: QUINIENTOS VEINTITRÉS MILLONES SEISCIENTOS CINCUENTA Y DOS MIL CUATROCIENTOS CUARENTA Y OCHO PESOS M/CTE ($523.652.448,00).

PLAZO DE EJECUCION DEL CONTRATO:
Duración del contrato: DOS (2) MESES.
Duración de las licencias: DOCE (12) MESES

JUSTIFICACIÓN DE LA NECESIDAD A CONTRATAR:

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial está organizada como una Unidad Administrativa Especial del orden distrital del Sector Descentralizado, de carácter técnico, con personería jurídica, autonomía administrativa y presupuestal y con patrimonio propio, adscrita a la Secretaría Distrital de Movilidad, y tiene por objeto *"programar y ejecutar las obras necesarias para garantizar la rehabilitación y el mantenimiento periódico de la malla vial local, intermedia y rural; así como la atención inmediata de todo el subsistema de la malla vial cuando se presenten situaciones que dificulten la movilidad en el Distrito Capital."*

En concordancia con lo anterior y al tenor del artículo 109 del Acuerdo Distrital 257 de 2006, modificado por el Art. 95 del Acuerdo Distrital 761 de 2020, la UAERMV tiene las siguientes funciones:

- *Programar, ejecutar y realizar el seguimiento a la programación e información de los planes y proyectos de rehabilitación y mantenimiento de la malla vial intermedia, local y rural construidas y ejecutar las acciones de*

mantenimiento que se requieran para atender situaciones que dificulten la movilidad en la red vial de la ciudad.

- *Suministrar la información para mantener actualizado el Sistema de Gestión de la Malla Vial del Distrito Capital, con toda la información de las acciones que se ejecuten.*
- *Atender la construcción y desarrollo de obras específicas que se requieran para complementar la acción de otros organismos y UAERMV es del Distrito.*
- *Ejecutar las obras necesarias para el manejo del tráfico, el control de la velocidad, señalización horizontal y la seguridad vial, para obras de mantenimiento vial, cuando se le requiera.*
- *Ejecutar las acciones de adecuación y desarrollo de las obras necesarias para la circulación peatonal, rampas y andenes, alamedas, separadores viales, zonas peatonales, pasos peatonales seguros y tramos de ciclorrutas cuando se le requiera.*
- *Ejecutar las actividades de conservación de la cicloinfraestructura de acuerdo con las especificaciones técnicas y metodologías vigentes y su clasificación de acuerdo con el tipo de intervención y tratamiento requerido (intervenciones superficiales o profundas).*

Parágrafo 1. *En el caso de las intervenciones para mejoramiento de la movilidad de la red vial arterial, éstas deberán ser planeadas y priorizadas de manera conjunta con el Instituto de Desarrollo Urbano.*

Parágrafo 2. *Las obras a las que hacen mención los literales c, d y e responderán a la priorización que haga la Secretaría Distrital de Movilidad y deberán cumplir con las especificaciones técnicas establecidas por esta y/o por el Instituto de Desarrollo Urbano cuando no existan las especificaciones técnicas requeridas. Así mismo la Secretaría Distrital de Movilidad regulará lo pertinente frente a las características de los proyectos de acuerdo con la escala de intervención.*

Parágrafo 3. . *De conformidad con lo previsto en los artículos 2.2.1.2.1.2.7 y 2.2.1.2.1.2.8 del Decreto 1082 de 2015, modificado por los Decretos 2106 de 2019 y 1860 de 2021, y en atención a que el objeto contractual corresponde a la suscripción de licencias, soporte y servicios tecnológicos de seguridad informática, la contratación se adelantará bajo la modalidad de Selección Abreviada en la modalidad de Subasta Inversa, conforme a la causal establecida en el numeral 2 del artículo 2 de la Ley 1150 de 2007. El contrato soporte tendrá una duración de* ***dos (2) meses****, contados a partir del acta de inicio.*

Normatividad de soporte

La presente contratación se fundamenta en el siguiente marco normativo:

- Constitución Política de 1991: artículos 209 y 315 numeral 3, relativos a los principios de la función administrativa y a las competencias de los alcaldes y sus entidades.
- Ley 80 de 1993 y Ley 1150 de 2007: régimen general de contratación estatal y causales de selección abreviada.
- Decreto 1082 de 2015: compilatorio reglamentario del sistema de compras y contratación pública.
- Decretos 2106 de 2019 y 1860 de 2021: disposiciones sobre simplificación de trámites y modalidades de selección.
- Ley 2294 de 2023 – Plan Nacional de Desarrollo 2022-2026 y Plan Distrital de Desarrollo 2024-2027 “Bogotá Camina Segura”: lineamientos en materia de fortalecimiento institucional, seguridad digital y sostenibilidad del MIPG.
- Resolución 2710 de 2017 del MinTIC: adopción de IPv6 en entidades públicas.
- CONPES 3975 de 2019 – Política de Gobierno Digital y lineamientos de ciberseguridad del MinTIC/ColCERT (2020-2024).
- Decreto Distrital 761 de 2020, que modifica el Acuerdo Distrital 257 de 2006, sobre competencias de la UAERMV.

Concepto Ambiental

De acuerdo con el concepto emitido por la Oficina de Servicios y Control Ambiental – OSCS de la UAERMV, no se requieren licencias ambientales para la ejecución de este contrato**,** dado que el objeto contractual corresponde a la suscripción, implementación y soporte de una plataforma tecnológica y no implica obras, intervenciones físicas ni actividades con impacto ambiental directo.

No obstante, el contratista deberá cumplir la cláusula ambiental institucional**,** dando cumplimiento a lo dispuesto en el Plan Institucional de Gestión Ambiental (PIGA)**,** observando las normas sobre protección y conservación del medio ambiente, uso eficiente de los recursos, adecuada segregación de residuos y participación en actividades de sensibilización y cuidado ambiental

En cumplimiento de dichos lineamientos, la Oficina de Tecnologías de la Información de la UMV adelanta acciones de fortalecimiento de la infraestructura de ciberseguridad institucional, dentro de las cuales se encuentra la suscripción y modernización integral del soporte y servicios asociados a la plataforma de seguridad de endpoint y proteger la información confidencial de la UAERMV detectando, monitoreando y bloqueando el uso o transferencia no autorizada de información sensible.

Esta actuación garantiza la continuidad del servicio, la protección de la información institucional y el cumplimiento de los objetivos estratégicos de la UAERMV.

En conclusión, la presente actuación contractual se enmarca en los principios de la función administrativa previstos en el artículo 209 de la Constitución Política, y en los principios de planeación, economía, transparencia, responsabilidad y selección objetiva consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, asegurando la eficiencia en el uso de los recursos públicos y la continuidad de los servicios tecnológicos que soportan la operación misional de la UAERMV.

De conformidad con lo establecido en el Acuerdo 2 de 2023 “Por el cual se establece la estructura organizacional de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial y las funciones de sus dependencias”, la Oficina de Tecnologías de la Información tendrá las siguientes funciones:

- Proponer a la Dirección General la formulación de las políticas, planes, programas y proyectos en materia de tecnologías de la información, conforme a los lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones, la Alta Consejería Distrital y en cumplimiento de los requisitos normativos vigentes.
- Formular y ejecutar acciones para el diseño, transición, provisión y mejora de los servicios que son soportados por las Tecnologías de la Información, de conformidad con los requisitos y acuerdos de nivel de servicio trazados por la Entidad y entidades competentes.
- Dirigir e implementar y hacer seguimiento a las políticas de seguridad de la información, de acuerdo con los lineamientos de las entidades distritales y nacionales competentes.
- Formular, ejecutar y actualizar el Plan Estratégico de Tecnologías de la Información, de acuerdo con las necesidades identificadas.
- Administrar el proceso de operación, mantenimiento y actualización del hardware, software y sistemas de información, de conformidad con la evaluación e identificación de necesidades.
- Prestar el soporte técnico requerido en la Entidad, de conformidad con los requisitos y acuerdos de nivel de servicio trazados.
- Desarrollar e implementar soluciones y servicios de tecnologías de la información, basados en estándares y buenas prácticas.
- Fortalecer la arquitectura empresarial, conforme a las directrices de orden nacional y distrital sobre la materia.
- Gestionar la conectividad, el mantenimiento y actualización de las redes internas y externas, las comunicaciones

fijas y móviles de la entidad, conforme a las necesidades identificadas.
- Administrar las aplicaciones institucionales de uso en la entidad y el desarrollo de nuevos aplicativos, basados en estándares y buenas prácticas.
- Gestionar alianzas estratégicas con otras entidades públicas o privadas para el desarrollo de las Tecnologías de la Información de la Entidad.
- Las demás que le sean asignadas y que correspondan a la naturaleza de la dependencia.

Para el actual gobierno Distrital se presenta El Plan de Desarrollo Distrital 2024-2027, “Bogotá Camina Segura”, fue aprobado en junio de 2024, en este se estableció el objetivo estratégico, “05 Bogotá confía en su gobierno", con el programa 33 Fortalecimiento institucional para un gobierno confiable y donde la entidad aporta al cumplimiento de la meta Plan de Desarrollo: Desarrollar el 100% de la estrategia de mejora y sostenibilidad del Modelo Integrado De Planeación y Gestión - MIPG en las entidades del Sector Movilidad.

Como parte de ejecución del plan de desarrollo, la UAERMV en el marco de sus funciones y misión institucional, formuló el Proyecto de inversión “8089 “Fortalecimiento de los Componentes tecnológicos para garantizar la demanda en la operación de la UAERMV de Bogotá D.C.”, y su cumplimiento se adelanta a través de las metas de inversión 1. Mantener, optimizar y modernizar un (1) Modelo Integrado de Planeación y Gestión - MIPG en la Entidad y 2. Adecuación y mantenimiento de 2 Sedes de la UAERMV. Su cumplimiento se adelanta a través de las metas de inversión: 1. Ejecutar 12 Proyectos encaminados a actualizar los módulos de los sistemas de información SIGMA, Calíope y Orfeo e Implementar el plan de mantenimiento de sistemas de información. 2. Actualizar (4) documentos que enmarquen la estrategia de TI en el Plan Estratégico de Tecnologías de la Información de la UAERMV para la vigencia 2025-2027 y 3. Garantizar la disponibilidad del 94% de los servicios tecnológicos que intervienen en los sistemas SIGMA, Calíope, Orfeo y Portales Web.

En el desarrollo de sus funciones, la UAERMV genera y procesa información sensible que reside y circula en los equipos de cómputo de la entidad, tanto propios como rentados (estaciones de trabajo, portátiles y servidores), así como en las aplicaciones misionales y administrativas soportadas en la arquitectura Cloud. Para salvaguardar esta información se cuenta con herramientas de seguridad perimetral, monitoreo, correlacionador de eventos, entre otros, sin embargo, estos controles no cubren la totalidad de amenazas ciberseguridad actuales. Por un lado, el antivirus tradicional nativo de los equipos de cómputo no detecta ni responde ante amenazas avanzadas que operan directamente sobre los equipos, por lo que se requiere una solución de **detección y respuesta en el endpoint (EDR)** que brinde visibilidad y protección continua sobre la totalidad de los equipos propios y rentados de la Unidad. Por otro lado, la entidad **no dispone actualmente de una herramienta de prevención de fuga de información (DLP)**, lo que la expone a la pérdida, extracción o divulgación no autorizada de datos sensibles. En consecuencia, es necesario incorporar capas adicionales de seguridad informática y ciberseguridad que fortalezcan la gestión de la confidencialidad, integridad y disponibilidad de los activos de información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Bajo los lineamientos enunciados por el Ministerio de las Tecnologías y las Comunicaciones - MINTIC -, definen las necesidades para que las entidades usen herramientas que velen por la seguridad de la información; estos dispositivos deben contar con sistemas operativos actualizados y con la capacidad de soportar los protocolos de red IPv6, tal y como se establece en la **Resolución 2710 de 2017 del MINTIC**.

Adicionalmente, las soluciones adquiridas deben integrarse con las herramientas de administración de la Unidad y ser totalmente compatibles e interoperables con los ecosistemas de seguridad perimetral ya implementados, de manera que aporten a la operación conjunta de los controles de seguridad. Todo ello en cumplimiento de las políticas de seguridad EGTI-DI-001 V4 – Políticas generales de tecnología y seguridad de la información.

Estas herramientas están orientadas al análisis constante y a la ejecución proactiva de acciones de detección, identificando de forma temprana las falencias o vulnerabilidades que puedan derivar en un evento o incidente de seguridad de la información. La materialización de estos riesgos puede comprometer los activos de información de la entidad y ocasionar

afectaciones a la imagen corporativa, así como repercusiones legales y económicas, entre otras. En este sentido, el uso de soluciones como el EDR y el DLP permite implementar ambientes controlados de monitoreo continuo, detectar oportunamente posibles amenazas —incluida la fuga de información— y establecer mecanismos de defensa adecuados al interior de la entidad. Asimismo, facilitan la identificación de patrones de comportamiento de las amenazas, de manera que la UAERMV pueda responder de forma proactiva y evitar la materialización de riesgos de seguridad de la información.

En conclusión, mediante estas adquisiciones la entidad implementará medidas técnicas que fortalecerán la protección de sus equipos, datos e infraestructura tecnológica, la cual soporta la operación misional de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

La Oficina de Tecnologías de la Información de la UAERMV, en cumplimiento de la normativa vigente en materia de seguridad digital y gestión de riesgos tecnológicos, adelanta iniciativas de fortalecimiento de su arquitectura de ciberseguridad, que incluyen la actualización de políticas, procedimientos y controles, así como la renovación de componentes críticos de su infraestructura tecnológica.

La Entidad cuenta en la actualidad con una plataforma de seguridad integral compuesta por firewalls de nueva generación desplegados tanto en instalaciones físicas como en su infraestructura de nube pública (Oracle Cloud), una solución de control de acceso a la red con capacidad para gestionar más de setecientos (700) dispositivos concurrentes, un motor de análisis dinámico de amenazas mediante sandboxing, una plataforma centralizada de correlación de eventos e inteligencia de seguridad, un analizador de registros con capacidad analítica sostenida de dos mil (2.000) logs por segundo, una solución de protección avanzada del correo institucional con integración nativa a Microsoft 365, y una consola de gestión centralizada de políticas incorporada recientemente como parte de la modernización tecnológica en curso. Esta arquitectura, construida sobre un ecosistema de fabricante único y consolidada a lo largo de varios ciclos de inversión institucional, genera condiciones estructurales que hacen que la adquisición de capacidades de detección, respuesta y prevención en los endpoints, así como de prevención avanzada de fuga de información, deban articularse de forma nativa con la infraestructura existente, y no como capas tecnológicas aisladas. La incorporación de soluciones del mismo ecosistema sobre esta base instalada produce economías de escala concretas y verificables: elimina la necesidad de desarrollar conectores de integración a medida, descarta costos de middleware y evita licenciamientos adicionales de plataformas de orquestación para hacer interoperar tecnologías de distintos fabricantes. A ello se suma que el personal técnico de la Entidad ha acumulado conocimiento operativo, certificaciones de fabricante y experiencia de configuración sobre esta plataforma, lo cual reduce de forma significativa la curva de adopción, el riesgo de configuración incorrecta y los tiempos de respuesta ante incidentes, factores que en entornos de seguridad representan variables críticas y no meramente administrativas. En términos de protección efectiva, la integración nativa de la capa de endpoint con el firewall perimetral, el control de acceso a la red, el sandbox de análisis dinámico y el correlacionador de eventos permite construir flujos de respuesta automatizada y coordinada: una alerta generada en el endpoint puede derivar en una cuarentena de red ejecutada automáticamente por el control de acceso, un bloqueo de tráfico aplicado por el firewall, una detonación de muestra sospechosa en el sandbox y un evento correlacionado en tiempo real en el SIEM, todo ello dentro del mismo ecosistema tecnológico y sin dependencia de integraciones de terceros que introduzcan latencia, brechas de visibilidad o puntos de falla adicionales. Esta capacidad de respuesta orquestada no es replicable con el mismo nivel de eficacia y confiabilidad cuando se combinan soluciones de fabricantes distintos, dado que las integraciones entre ecosistemas heterogéneos dependen de APIs públicas con cobertura funcional limitada, acuerdos de interoperabilidad sujetos a cambios de versión y tiempos de sincronización que deterioran la efectividad de la respuesta en los primeros minutos críticos de un incidente. En consecuencia, la adquisición de las capacidades de protección de endpoint y prevención de fuga de información bajo los parámetros técnicos definidos en los presentes estudios no constituye una restricción a la pluralidad de oferentes sino la expresión técnicamente fundamentada del principio de planeación eficiente: preservar y potenciar una inversión institucional acumulada, reducir el riesgo operativo y maximizar la cobertura de protección sobre la infraestructura tecnológica de la Entidad con el menor costo total de integración.

Evaluación de soluciones existentes en la arquitectura actual

La entidad realizó un análisis técnico de las capacidades de las soluciones actualmente implementadas en su arquitectura de seguridad, particularmente aquellas orientadas a la protección perimetral y control del tráfico de red.
Si bien dichas soluciones cumplen un papel fundamental dentro del esquema de defensa perimetral y segmentación de la red, su alcance funcional está orientado principalmente a:

- inspección y control del tráfico de red,
- prevención de intrusiones,
- segmentación y control de acceso a nivel de red,
- monitoreo del tráfico perimetral.

No obstante, las amenazas modernas han evolucionado significativamente y actualmente se caracterizan por técnicas como:

- uso indebido de credenciales legítimas,
- movimiento lateral dentro de la red,
- ataques sin archivos (fileless),
- abuso de herramientas del sistema operativo,
- compromisos de identidades y privilegios.

En este contexto, las buenas prácticas internacionales de arquitectura de ciberseguridad, tales como ISO/IEC 27001:2022, NIST Cybersecurity Framework y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC, recomiendan complementar los controles perimetrales con capacidades especializadas de protección en endpoints y datos, dado que estos constituyen actualmente uno de los principales vectores de ataque en las organizaciones.
Durante el análisis de mercado se identificó que algunos fabricantes que cuentan con soluciones perimetrales también ofrecen módulos adicionales orientados a protección de endpoints y datos. En consecuencia, la entidad concluyó que la adopción de plataformas especializadas para la protección de endpoint y datos resulta más adecuada para fortalecer la postura de ciberseguridad institucional, complementando los controles perimetrales existentes y alineándose con las mejores prácticas internacionales de arquitectura de seguridad.

Madurez operativa de la entidad

La arquitectura tecnológica propuesta busca mantener un equilibrio entre:

- Fortalecimiento de seguridad,
- Sostenibilidad operativa,
- Capacidad de gestión interna.

En este sentido, los requerimientos técnicos definidos se orientan a seleccionar soluciones que sean proporcionales al nivel de riesgo institucional, pero que al mismo tiempo puedan ser administradas eficientemente con los recursos humanos disponibles.

Este enfoque permite evitar tanto el subdimensionamiento de los controles de seguridad como la adopción de arquitecturas excesivamente complejas que puedan generar dificultades operativas.

Justificación de la solución propuesta

Con base en el análisis técnico, el estudio de mercado y la evaluación de la arquitectura actual, la entidad concluye que la implementación de plataformas modernas de protección de endpoint y protección de fuga de datos es necesaria para:

- Fortalecer la postura de ciberseguridad institucional,
- Reducir el riesgo de incidentes de seguridad,
- Mejorar la capacidad de detección y respuesta ante amenazas,
- Proteger la información institucional y los servicios misionales.

Las soluciones propuestas permitirán evolucionar desde un modelo de protección basado en antivirus tradicional hacia una arquitectura de seguridad moderna basada en telemetría, análisis de comportamiento y respuesta automatizada, alineada con las mejores prácticas internacionales.

Análisis de riesgo institucional asociado a la protección de endpoint y datos

El análisis de riesgos tecnológicos realizado por la entidad evidencia que los endpoints y los datos digitales representan actualmente uno de los principales vectores de ataque en los entornos tecnológicos modernos**.**

De acuerdo con estudios internacionales de ciberseguridad y marcos de referencia como el NIST Cybersecurity Framework, una proporción significativa de los incidentes de seguridad actuales se origina a partir de:

- Robo o abuso de credenciales legítimas,
- Ejecución de código malicioso en estaciones de trabajo,
- Explotación de vulnerabilidades en equipos finales,
- Movimiento lateral dentro de la red institucional,
- Uso indebido de cuentas privilegiadas.

En este contexto, los controles tradicionales basados únicamente en antivirus y protección perimetral resultan insuficientes para detectar amenazas avanzadas que operan mediante técnicas como:

- Ataques sin archivos (fileless),
- Uso de herramientas administrativas del sistema,
- Ejecución de scripts maliciosos,
- Ataques dirigidos a servicios de identidad.

Estas amenazas pueden permanecer durante largos periodos dentro de la infraestructura tecnológica sin ser detectadas, comprometiendo progresivamente la confidencialidad, integridad y disponibilidad de la información institucional.

Riesgos identificados

En ausencia de mecanismos avanzados de detección y respuesta en endpoint y datos, la entidad se expone a riesgos relevantes tales como:

Compromiso de estaciones de trabajo y servidores

Los equipos de usuario y servidores constituyen el punto de entrada más frecuente para ataques de **ransomware,** malware avanzado y explotación de vulnerabilidades.

Un compromiso exitoso de estos dispositivos puede permitir a un atacante:

- Ejecutar código malicioso,
- Acceder a información sensible,
- Instalar herramientas de persistencia,
- Expandir el ataque hacia otros sistemas.

Movimiento lateral dentro de la red

Una vez que un atacante compromete un equipo o una identidad, puede desplazarse lateralmente dentro de la infraestructura tecnológica con el objetivo de:

- Comprometer servidores críticos,
- Acceder a bases de datos,
- Obtener información sensible,
- Interrumpir servicios institucionales.

La ausencia de visibilidad sobre el comportamiento de los endpoint dificulta la detección temprana de estas actividades.

Interrupción de servicios institucionales

La materialización de un incidente de seguridad puede generar impactos operativos significativos, tales como:

- Indisponibilidad de sistemas de información institucionales,
- Afectación de servicios misionales,
- Pérdida o alteración de información,
- Impacto reputacional para la entidad.

Dado que la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial es responsable de procesos asociados

a la gestión y mantenimiento de la infraestructura vial de la ciudad, la continuidad de sus sistemas de información resulta fundamental para el cumplimiento de sus funciones institucionales.

Marco normativo y buenas prácticas

La necesidad de implementar capacidades avanzadas de protección en endpoint y datos se encuentra alineada con diversos marcos de referencia y lineamientos institucionales, entre los cuales se destacan:

ISO/IEC 27001:2022

La norma establece controles relacionados con:
- Protección contra malware,
- Monitoreo de actividades,
- Control de acceso,
- Detección de eventos de seguridad.

Estos controles requieren que las organizaciones cuenten con mecanismos que permitan detectar comportamientos anómalos y responder oportunamente ante incidentes de seguridad.

Modelo de Seguridad y Privacidad de la Información – MSPI

El MSPI del Ministerio TIC establece que las entidades públicas deben implementar controles que permitan:
- Monitorear permanentemente los activos tecnológicos,
- Detectar eventos de seguridad,
- Gestionar incidentes de manera oportuna.

La adopción de soluciones avanzadas de protección de endpoints y datos contribuye directamente al cumplimiento de estos lineamientos.

NIST Cybersecurity Framework

Este marco establece que las organizaciones deben desarrollar capacidades en las funciones de:
- Detect (Detectar)
- Respond (Responder)
- Recover (Recuperar)

Las plataformas modernas de protección de endpoints permiten fortalecer estas capacidades mediante:
- Telemetría avanzada,
- Análisis de comportamiento,
- Correlación de eventos,
- Respuesta automatizada.

Basados en lo anterior, con el fin de contar con plataformas con el mejor posicionamiento en el mercado para la protección de endpoints y datos, la entidad requiere cubrir la necesidad a través de un proceso de selección que le permita contratar soluciones que aporten e integren capacidades operativas a las plataformas ya existentes en el ecosistema de ciberseguridad de la Entidad, para generar valor por medio de la interoperabilidad, detección, protección y respuesta automatizadas ante amenazas cibernéticas de la siguiente manera:

SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR).

Generalidades

- La Entidad requiere del licenciamiento de la solución EDR Avanzado para 450 Endpoints.
- La solución de EDR debe proporcionar a la Entidad un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la

amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas.
- La solución debe ser desplegada en la Nube del Fabricante (SaaS).
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

A continuación, se detallan y describen cada uno de estos mecanismos de protección requeridos:

Funcionalidades de Prevención

- El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad Antivirus de Nueva Generación (Next-Generation Anti-Virus - NGAV) viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional.
- Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML).
- Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube que se actualiza continuamente.
- Proteger los endpoints desconectados de la red con una protección fuera de línea; este modo de operación se denomina modo autónomo.
- Proporcionar un control de dispositivos USB basado en múltiples parámetros.
- Debe estar en capacidad de eliminar tiempos de permanencia y Fatigas por exceso de alarmas (falsos positivos).
- Identificación, evaluación y mitigación de vulnerabilidades (incluyendo detalle de códigos CVE aplicables, recomendaciones de remediación y aplicación de parches virtuales / Virtual Patching) para sistemas operativos Windows, macOS y Linux, sin exigir la distribución o instalación directa de actualizaciones sobre los sistemas operativos.
-
-

Funcionalidades de Descubrimiento

- El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad.
- Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT.
- Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad.
- Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicación con el exterior.
- Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables.
- Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo.

Funcionalidades de Detección y Protección

El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado, debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes items:

- Se debe basar en la detección integrada de forma profunda en el sistema operativo, permitiendo la detección de ataques de infiltración sigilosa, los ataques basados en la memoria y los ataques “living off the land”.
- Debe proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows).

- Debe poder detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoint desconectados de la red corporativa.
- Debe bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control.
- Debe impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros.
- Debe permitir definir listas blancas y negras para personalizar mediante exclusiones estas protecciones (por hash, nombre y/o ruta de archivo, o por aplicación, incluyendo datos de versión y fabricante).
- Debe proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares.
- Debe Proporcionar un análisis de todo el historial de eventos.
- Debe realizar la validación continua de la clasificación de amenazas.

Funcionalidades de Protección contra Ransomware

La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes.

Dichas estrategias deben incluir como mínimo:

1. Debug de Procesos.
2. Código dinámico.
3. Formato de archivo ejecutable incorrecto.
4. Una pila con código ejecutable.
5. El programa ejecutado no tiene instalador.
6. Programa crítico falso.
7. Empaquetador falso.
8. File Encryptor.
9. Proceso oculto.
10. Ejecutable inyectado.
11. Proceso inyectado.
12. Hilo inyectado.
13. Suma de comprobación no válida.
14. Ejecución no válida.
15. Puntero no válido.
16. Inyección de kernel.
17. Empaquetador conocido.
18. Archivo malicioso detectado.
19. Proceso malicioso.
20. Ejecutable modificado.
21. Stack Parcialmente asignado.
22. Exploit de escalamiento de privilegios.
23. Proceso vacío.
24. Manipulación de pilas.
25. Aplicación sospechosa.
26. Empaquetador sospechoso.
27. Ejecutable manipulado.
28. Ejecutable no confirmado.
29. Ejecutable sin asignar.
30. Código grabable.
31. Prevención automatizada en tiempo real encriptación de Ransomware.

Funcionalidades de Remediación

La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los

cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos:

- Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta.
- Debe estandarizar los procedimientos de respuesta a incidentes con la automatización de playbooks.
- Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la apertura de tickets.
- Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (como, por ejemplo, grupos de estaciones de trabajo).
- Debe proporcionar visibilidad completa de la cadena de ataque y los cambios maliciosos, mediante el seguimiento de código.
- Debe permitir automatizar la limpieza y reversión de los cambios maliciosos preservando así la integridad del sistema.
- La solución de EDR Se debe contar un servicio de respuesta y detección gestionada (MDR) ante incidentes, proporcionado por técnicos del propio fabricante.
- Debe realizar la contención y respuesta de forma automática.

Funcionalidades de Investigación

La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoint infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos:

- Debe desactivar y bloquear automáticamente las amenazas, lo que permite a los analistas de seguridad cazar marcando sus propios tiempos.
- Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el “paciente cero”, incluso si el dispositivo está fuera de línea.
- Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria.
- La interfaz gráfica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense.

Funcionalidades de EDR

La solución de EDR debe tener la capacidad de poder integrarse con diferentes plataformas de seguridad, creando así un marco robusto que pueda identificar y responder eficiente y eficazmente frente a los ataques como es recomendado por Gartner.

La solución de EDR deberá integrarse al menos con las siguientes plataformas con las que cuenta la Entidad:

1. Next Generation Firewall (FortiGate).
2. Control de Acceso a la Red (FortiNAC).
3. SandBox (Fortisandbox).
4. Correlacionador de Eventos (FortiSIEM).

- Debe contar con una Gestión Unificada.
- Debe contar con la funcionalidad de identificación de incidentes entre productos.
- Debe contar con la funcionalidad de investigación impulsada por inteligencia artificial.
- Debe contar con la funcionalidad de respuesta automatizada.

Componentes de la Solución EDR

La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de un agente en software compatible con los sistemas operativos y entornos con los que cuenta la Entidad (estaciones de trabajo, portátiles y servidores que conforman los 450 endpoints), en las arquitecturas (32 y/o 64 bits según corresponda a cada sistema operativo) oficialmente soportadas por el fabricante: Windows (incluyendo Windows 11), macOS (Ventura 13 y superior), Windows Server (2019, 2022 y superior) y Linux (Oracle Linux, Ubuntu Server LTS y CentOS/RHEL en las versiones soportadas oficialmente en la hoja de datos del fabricante).
En cuanto al hardware, debe ser un agente ligero, el cual no debe requerir más de 350 MB de memoria RAM y 1 GB de espacio en disco, de acuerdo con la documentación oficial del fabricante, garantizando una operación eficiente y mínima afectación al rendimiento de los equipos protegidos

SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

Generalidades

- Se requiere una solución DLP que permita a la Entidad anticipar y prevenir la fuga y/o perdida de datos.
- La solución debe contar con licenciamiento avanzado para 450 Endpoints, incluido conector para Microsoft Office 365.
- La solución debe ser desplegada en la Nube del Fabricante (SaaS).
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

Requerimientos técnicos

- La solución debe prevenir la exfiltración y pérdida accidental de datos.
- La solución debe ser SaaS, en cloud, sin instalación de equipos ni colectores en tierra.
- La solución debe ser una sola licencia, que incluya todo lo solicitado sin módulos adicionales de componentes de seguridad no solicitados que puedan generar administraciones o coexistencia con diferentes configuraciones que no permitan centrarse en la función de DLP. No se permiten soluciones que deban incluir infraestructura en sitio como servidores o bases de datos.
- La solución debe inspeccionar y clasificar comportamientos aun sin crear reglas mediante el uso de Machine Learning.
- La solución debe tener la posibilidad de incluir analistas dedicados a detectar fugas de información en caso de requerirse directamente de fábrica.
- La solución debe proporcionar visibilidad inmediata sobre el movimiento y la actividad de los datos.
- La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
- La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
- La solución debe tener capacidades de inteligencia artificial y aprendizaje automático.
- La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
- La solución debe proporcionar capacidades adicionales de análisis y analítica para ofrecer insights a nivel organizacional.
- La solución debe permitir a las organizaciones activar servicios y obtener visibilidad de riesgos de datos en minutos para proteger datos sensibles desde el primer día.
- La solución debe detectar y responder a la manipulación de datos y actividades anómalas utilizando IA y ML.
- La solución debe ser capaz de monitorear amenazas internas y empleados de alto riesgo.
- La solución debe aplicar políticas de riesgo interno con acciones de seguridad proactivas en tiempo real.
- La solución debe mapear las actividades en un formato de MITRE.
- La solución debe identificar y mitigar amenazas internas a través de análisis avanzados de comportamiento de usuarios.
- La solución debe asegurar los datos en uso por aplicaciones SaaS y otras aplicaciones.
- La solución debe permitir políticas de protección de privacidad de datos como almacenamiento de datos y logs forenses en datacenters de la compañía, colocar seudónimos a los nombres de las cuentas que se están investigando para que el analista no sepa a quien se hace la revisión e incluir la autorización de investigaciones

fuera de la caja (out-of-the-box) por parte de analistas.

- La solución debe proporcionar visibilidad integral de las interacciones de los usuarios con los datos en la nube y mantener la protección a medida que los datos se mueven fuera de la nube, asegurando la protección continua de la información sensible, independientemente de su ubicación o método de acceso.
- La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Hotmail, Yahoo, entre otros).
- La solución debe fortalecer las defensas contra posibles brechas de datos derivadas de la exposición de datos empresariales a través del uso no autorizado de aplicaciones, incentivando a los empleados a usar herramientas autorizadas.
- La solución debe diferenciar entre datos sensibles transferidos a soluciones en la nube empresariales y soluciones en la nube personales (por ejemplo, Microsoft oneDrive para Empresas vs. Microsoft oneDrive Personal).
- La solución debe identificar el uso de Shadow AI y detener la carga de datos sensibles.
- La solución debe monitorear el uso de aplicaciones SaaS, incluyendo herramientas de Shadow AI como Gen-AI, e incorporar educación de usuarios basada en riesgos en el punto de acceso a datos sensibles.
- La solución debe cumplir con los requisitos de residencia de datos.
- La solución debe construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización, con información sobre el ingreso, egreso y credenciales de datos.
- La plataforma debe monitorear la actividad en aplicaciones de inteligencia artificial (Por ejemplo, ChatGPT, Gemini, entre otros).
- La solución debe aplicar análisis de comportamiento de usuarios y entidades a gran escala.
- La solución debe incluir un asistente de IA que resuma y contextualice los datos asociados con actividades de alto riesgo para acelerar el análisis de incidentes.
- La solución debe analizar qué datos se están utilizando y cómo, permitiendo determinar la mejor respuesta.
- La solución debe clasificar y rastrear datos en tiempo real para proporcionar visibilidad y protección de datos inmediata, sin necesidad de políticas predefinidas.
- La solución debe estar disponible en la nube para facilitar su implementación y escalabilidad, como un servicio SaaS.
- La solución debe funcionar independientemente de la conexión de red y la ubicación.
- La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos.
- La solución debe utilizar un agente escalable y ligero para recopilar y registrar datos.
- La solución debe permitir reducir los costos de ancho de banda, al no depender de un motor de escaneo de archivos basado en la nube.
- La solución debe utilizar agentes, extensiones de navegador y conectores en la nube para recopilar, enriquecer e indexar automáticamente la actividad a través de diferentes tipos de eventos (autenticación, web, email, aplicaciones, USB, creación de archivos, compartición y descarga de archivos).
- La solución debe proporcionar visibilidad profunda en las actividades de los usuarios, el acceso a datos y los sistemas para prevenir la salida de datos sensibles.
- La solución debe incorporar funcionalidades que permitan educar a los usuarios sobre el manejo adecuado de datos.
- La solución debe proporcionar capacitación basada en riesgos para entrenar a los empleados a tomar las decisiones correctas basadas en la detección de comportamientos inaceptables, reforzar las políticas de seguridad corporativa y promover una buena higiene cibernética.
- La solución debe proporcionar notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas. Las notificaciones deben poder enviarse a través de diálogos en el Endpoint, correo electrónico, y mensajería (por ejemplo: Microsoft Teams, Slack, etc).
- La solución debe aplicar políticas adaptativas basadas en riesgos que consideren factores de riesgo y permitan decidir qué acciones tomar, como notificar a los usuarios a través de mensajería (por ejemplo: Microsoft Teams, Slack, etc), capturar forenses de archivos y pantallas, aislar o bloquear un endpoint, terminar un proceso o bloquear actividades de alto riesgo.
- La solución debe integrarse fácilmente con los sistemas y plataformas existentes en la organización.
- La solución debe ser compatible con dispositivos y plataformas de colaboración.
- La solución debe proporcionar perfiles MDM, transmisión de eventos, webhooks y una API abierta para la

integración con herramientas MDM, SIEM, SOAR, de automatización y de mesa de servicio existentes.

- La solución debe identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección.
- La solución debe aplicar políticas de DLP y de riesgo interno basadas en el origen de los datos y si se utilizó una cuenta corporativa o no corporativa para la salida de datos.
- La solución debe incorporar conectores de Microsoft Office 365.
- La solución debe mapear las actividades a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas.
- La solución debe proporcionar visibilidad de datos, evaluación de riesgos y políticas de protección de datos listas para usar para proteger los activos de información críticos dentro y fuera de la red.
- La solución debe ayudar a cumplir con requisitos clave de cumplimiento, incluyendo PCI DSS, HIPAA, ISO 27001, NIST, PII, PHI, entre otros.
- La solución debe abordar los controles de cumplimiento normativo relacionados con la prevención de pérdida de datos con un esfuerzo mínimo utilizando políticas predefinidas de PII/PHI/PCI.
- La solución debe priorizar la privacidad bajo regulaciones como GDPR y CCPA.
- La solución debe utilizar técnicas de minimización de datos integradas, como la seudonimización y el almacenamiento forense localizado, para ayudar a los equipos de seguridad a detectar y mitigar amenazas mientras se protege la confidencialidad de los empleados.
- La solución debe minimizar los conjuntos de datos de investigación seudonimizados.
- La solución debe mapear las detecciones de actividades de alto riesgo a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas y secuenciarlas automáticamente en incidentes con puntuación de riesgo para priorizar las investigaciones.
- La solución debe almacenar los registros forenses en centros de datos controlados por el cliente en la región.
- La solución debe incluir flujos de trabajo de autorización de investigación listos para usar para los analistas.
- La solución debe proporcionar un feed de actividad detallado y secuenciado en el tiempo que permita a los analistas ver la actividad de usuarios, datos y dispositivos antes, durante y después de un incidente.
- La solución debe permitir a los analistas de seguridad tomar acciones según la gravedad del riesgo, como mostrar un mensaje en pantalla al empleado, tomar una captura de pantalla, terminar un proceso, bloquear conexiones a un dispositivo o bloquear el teclado y el ratón de un dispositivo.
- La solución debe incluir gestión de casos integrada y reportes de riesgos que destaquen comportamientos descuidados, maliciosos y accidentales a lo largo del tiempo, permitiendo evaluar la efectividad de los controles de seguridad e identificar áreas de mejora.
- Los reportes deben poder exportarse fácilmente para compartir con la alta dirección.
- La solución debe proporcionar un dashboard para cumplimiento y auditoría.
- La solución debe soportar la generación de reportes personalizados basados en usuarios específicos.
- La solución debe soportar la generación de reportes personalizados basados en tipos específicos de datos.
- La solución debe soportar la generación de reportes personalizados basados en períodos específicos.
- Los reportes deben poder exportarse fácilmente para compartir con otras áreas de la entidad.
- La solución debe incluir reglas predefinidas para detectar prácticas de higiene cibernética deficientes, como la carga de archivos confidenciales a ubicaciones inesperadas, la conexión a redes Wi-Fi no seguras, la inserción de dispositivos de hardware maliciosos o el uso de aplicaciones no autorizadas para almacenamiento en la nube o dispositivos USB.
- La solución debe monitorear y bloquear datos sensibles transferidos a dispositivos USB.
- La solución debe monitorear datos sensibles transferidos a través de aplicaciones de terceros (por ejemplo, Putty).
- La solución debe monitorear datos sensibles copiados mediante capturas de pantalla.
- La solución debe monitorear datos sensibles copiados a través de pulsaciones de teclas (por ejemplo, imprimir pantalla).
- La solución debe monitorear datos sensibles copiados a nivel de archivo/carpeta.
- La solución debe monitorear datos sensibles copiados a nivel de comando (por ejemplo, símbolo del sistema, terminal).
- La solución debe monitorear datos sensibles copiados/descargados a una máquina virtual sin agente de punto final.
- La solución debe soportar el rastreo de múltiples archivos compartidos por un usuario.
- La solución debe soportar el monitoreo del movimiento de datos sensibles fuera de un conjunto definido de usuarios.

- La solución debe exportar un historial de todo el movimiento de datos dentro de la empresa, incluyendo datos provenientes de fuentes externas.
- La solución debe monitorear la descarga de datos sensibles por un usuario directamente desde una aplicación/servidor de aplicaciones.
- La solución debe proporcionar detalles de los datos sensibles descargados por un usuario durante un período especificado, incluyendo el número total de archivos, volumen de descarga, nombres de archivos y origen.
- La solución debe monitorear servicios y plataformas de correo electrónico (por ejemplo, MS Exchange, Office 365, Outlook, entre otros).
- La solución debe bloquear el montaje de unidades de almacenamiento removibles (por ejemplo, USB, HDD externo).
- La solución debe monitorear y bloquear datos sensibles impresos en impresoras físicas y/o PDF.
- La solución debe integrarse con otras herramientas de ciberseguridad (por ejemplo, SIEM).
- La solución debe integrarse con Active Directory, Azure AD y soluciones LDAP de terceros.
- La solución debe soportar MFA (Autenticación Multifactor).
- La solución debe soportar SSO (Inicio de Sesión Único) con Active Directory, Entra ID, GCP, Amazon, AWS.

La solución de DLP deberá integrarse al menos con las siguientes plataformas con las que cuenta la Entidad:

1. Correlacionador de Eventos (FortiSIEM).
2. Analizador (Fortianalyzer)
3. Microsoft Office 365.

Componentes de la Solución DLP

La plataforma de seguridad de DLP debe ser una arquitectura distribuida, la cual debe constar de un agente ligero en software compatible con sistemas operativos Windows, macOS y Linux, acreditado conforme a las versiones, distribuciones y arquitecturas oficialmente soportadas en la documentación técnica o matriz de compatibilidad oficial del fabricante para los endpoints objeto de protección.

Servicios y soporte

- La solución debe incluir soporte directo con el fabricante en modalidad 7x24.
- La solución debe incluir acceso a un equipo especializado directo de fábrica que brinde orientación remota sobre implementación, actualizaciones y operaciones de la solución DLP.
- La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante que incluya el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones y seguimiento durante el primer mes de implementación y seguimiento mensual y final de la solución implementada. Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.
- La solución requerida debe incluir la licencia para Control de dispositivos integrada, DLP en línea para web, correo, Cloud Drive y conectores de medio, Clasificación de datos en tiempo real, análisis de riesgo de aplicaciones SaaS y de Inteligencia Artificial generativa, Entrenamiento de riesgos a usuarios finales, Soporte de librerías de cumplimiento regulatorio, etiquetas de Microsoft MIP/AIP, archivos forenses, gestión de incidentes y secuencia de tiempo de actividad. El entrenamiento debe incluir permitir hacer una evaluación de la justificación de incumplimiento.
- La solución requerida debe incluir las licencias necesarias para monitoreo de actividades de usuario y equipo final, analítica de comportamiento con Machine learning, detección de manipulación de datos, aislamiento de usuarios finales y bloqueo en tiempo real, detección de incidentes con puntuación de riesgo, captura de pantalla para análisis forense, gestión de caso, librería de detección de riesgo asociado a mapas de Mitre ATT&ck, conectores de integración con Google workspace, Microsoft office 365 y controles de compartir archivos.
- La solución debe ser ofertada con un soporte de 24x7x365 por un periodo de doce (12) meses.

La suscripción de las plataformas de protección de nueva generación basadas en la nube del fabricante incluye la implementación y el soporte por doce (12) meses, a partir de la firma del acta de inicio, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista. El oferente debe incluir todo el software requerido para el cumplimiento

de lo solicitado por la entidad.

El desarrollo del futuro contrato tiene como fin realizar el cumplimiento de la meta 3 “Garantizar la disponibilidad del 94% de los servicios tecnológicos que intervienen en los sistemas SIGMA, Calíope, Orfeo y Portales Web”. Bajo esta perspectiva, de conformidad con el numeral 2 del artículo 2 de la Ley 1150 de 2007 y lo establecido en el artículo 2.2.1.2.1.2.4.5 del Decreto 1082 de 2015, esta contratación se adelanta bajo la modalidad de **Selección Abreviada**, por tratarse de bienes y servicios de características técnicas estandarizadas, respecto de los cuales existe pluralidad de oferentes, lo que permite fomentar la competencia y seleccionar la oferta más favorable en términos de precio.

Como parte del análisis se dio cumplimiento al Decreto 310 en cuanto a la verificación de los Acuerdos Marco de Precio e Instrumentos de Agregación de Demanda para el presente proceso, el cual, no existe un mecanismo de compra aplicable para la suscripción de una solución de ciberseguridad con las funcionalidades descritas en el presente proceso para la protección de equipos y datos para la UAERMV. Sin embargo, en el numeral 4.4 normatividad del presente documento se hace el análisis respectivo.

En conclusión, la presente actuación contractual se enmarca en los principios de la función administrativa previstos en el artículo 209 de la Constitución Política, y en los principios de planeación, economía, transparencia, responsabilidad y selección objetiva consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007, asegurando la eficiencia en el uso de los recursos públicos y la continuidad de los servicios tecnológicos que soportan la operación misional de la UAERMV.

Cabe resaltar que esta adquisición se encuentra contemplada en la línea 8089-053 dentro del plan anual de adquisiciones de la UAERMV del 2026.

LOCALIZACIÓN Y ÁREA DE INFLUENCIA:

El lugar de entrega de los productos será en las instalaciones de las sedes de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, Ubicadas en:
Sede Administrativa: Calle 26 # 69-76, Piso 3, Edificio Elemento, Torre Aire, Bogotá D.C.
Sede Operativa: Calle 22d # 120 – 40, Predio La Elvira, Localidad Fontibón, Bogotá D.C.
Sede Producción: Parque Minero Industrial “El Mochuelo”, Km. 3 vía a Pasquilla, Localidad Ciudad Bolívar, Bogotá D.C.
Lo anterior, sujeto a previa coordinación del almacén y de la Supervisión o quien hace sus veces.

LUGAR DE EJECUCIÓN O ENTREGA: El lugar de entrega de los productos será en las instalaciones de las sedes de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, Ubicadas en:
Sede Administrativa: Calle 26 # 69-76, Piso 3, Edificio Elemento, Torre Aire, Bogotá D.C.
Sede Operativa: Calle 22d # 120 – 40, Predio La Elvira, Localidad Fontibón, Bogotá D.C.
Sede Producción: Parque Minero Industrial “El Mochuelo”, Km. 3 vía a Pasquilla, Localidad Ciudad Bolívar, Bogotá D.C.
Lo anterior, sujeto a previa coordinación del almacén y de la Supervisión o quien hace sus veces.

CÓDIGOS UNSPSC

Clasificación UNSPSC	Segmento	Familia	Clase	Productos
43222501	(43000000) Difusión de tecnologías de información y telecomunicaciones	[43230000] Software	[43233200] Software de seguridad y protección	[43233200] Software de seguridad informática
43222502	(43000000) Difusión de tecnologías de información y telecomunicaciones	(43220000) Equipos o plataformas y accesorios de redes de datos, voz o multimedia	(43222500) Equipos de seguridad de red	(43222502) Equipos y soluciones de seguridad
43233200	(43000000) Difusión de tecnologías de	[43230000] Software	[43233200] Software de seguridad y	[43233200] Software de seguridad informática

	información y telecomunicaciones		protección	
43233205	(43000000) Difusión de tecnologías de información y telecomunicaciones	[43230000] Software	[43233200] Software de seguridad y protección	[43233205] Software de seguridad de transacciones y de protección contra virus

DESCRIPCIÓN TÉCNICA DE LA NECESIDAD (Si aplica):

ÍTEM Requerido en el Proceso o Contractual	SERVICIO / ELEMENTO	DESCRIPCIÓN ESPECÍFICA DEL ÍTEM	CANT	UNIDAD	MODALIDAD NORMA TÉCNICA	HORAS DE INTENSIDAD IMAGEN DE REFERENCIA	SOPORTES
Solución EDR Avanzada	Servicio	SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR). La solución deberá ser una plataforma integral de seguridad para endpoints diseñada desde cero para detectar amenazas avanzadas y detener intrusion	450	Endpoints	Administración centralizada en nube del fabricante (SaaS).	N/A	N/A

		es y ataques de ransomware en tiempo real, incluso en dispositivos ya comprometidos. La solución deberá permitir mitigación proactiva de riesgos en tiempo real y seguridad de IoT, reduciendo considerablemente la superficie de ataque mediante evaluaciones de vulnerabilidad y políticas de mitigación de riesgos, como la aplicación de parches virtuales, la detección de dispositivos y el control de aplicaciones.					

		La solución deberá permitir protección previa a la infección, proporcionando una primera capa de defensa probada mediante un motor antivirus de próxima generación (NGAV) basado en aprendizaje automático (CML) personalizado y a nivel de kernel, que previene la infección por ataques avanzados como el ransomware en tiempo real. La solución deberá permitir protección posterior a la infección, Detecta					

		ndo y detenien do ataques avanzad os en tiempo real, incluso cuando el endpoint ha sido compro metido. Sin brechas de segurida d, sin pérdida de datos, sin problem as. Además , eliminar el tiempo de espera y proporci ona un conjunto de funcione s automati zadas de detecció n y respuest a de endpoint s (EDR) para detectar , neutraliz ar, investig ar, respond er y remedia r incident es. La					

		solución deberá permitir responder y remediar incidentes automáticamente para proteger los datos, garantizar la disponibilidad del sistema y preservar la continuidad del negocio. La solución deberá integrarse con las plataformas del ecosistema de ciberseguridad con el que cuenta actualmente la Entidad. La solución deberá ser desplegada en la Nube del Fabricante (SaaS). Tiempo: El término de					

		cobertura de las suscripciones de la plataforma que incluye la implementación y el soporte debe ser por doce (12) meses, con esquema de soporte 24x7 con fabricante y soporte local por parte del Contratista.					
Solución DLP Avanzada	Servicio	SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) La solución deberá ofrecer un enfoque moderno y unificado para la seguridad de los datos al combinar la prevenci	450	Endpoints	Administración centralizada en nube del fabricante (SaaS).	N/A	N/A

		ón de pérdida de datos, la gestión de riesgos internos, la protección de datos GenAI y SaaS, y la formación de usuarios basada en riesgos. Ademar, proporcionar visibilidad en tiempo real del movimiento y la actividad de los datos en los endpoints, el almacenamiento en la nube, las aplicaciones SaaS (incluidas las herramientas GenAI) y las plataformas de colaboración. La solución deberá detectar con precisión la propied					

		ad intelectual y los datos confidenciales mediante la clasificación avanzada de datos, el origen de los datos y el seguimiento de datos basado en la identidad. La solución deberá proporcionar seguimiento de datos desde su origen con visibilidad completa de la manipulación posterior de datos a lo largo del tiempo mediante las funciones de flujo de datos seguro y linaje de datos. La solución deberá permitir					

		secuencia automática de la actividad de amenazas internas de alto riesgo y genera un incidente con puntuación de riesgo para priorizar la actividad de exfiltración de datos para su investigación y gestión de casos. La solución deberá supervisar el uso de aplicaciones de GenAI y SaaS, incluido el uso de credenciales corporativas y personales. La solución deberá admitir etiquetas de confidencialidad de Microsoft, así					

		como integración a través de conector Microsoft Office 365. La solución deberá integrarse con las plataformas del ecosistema de ciberseguridad con el que cuenta actualmente la Entidad. La solución deberá ser nativa de la nube del fabricante, lo que permitirá a la Entidad activar servicios y obtener visibilidad inmediata y sin políticas sobre los flujos de datos corporativos y los riesgos, con acceso a análisis y					

		detecciones. Tiempo: El término de cobertura de las suscripciones de la plataforma que incluye la implementación y el soporte debe ser por doce (12) meses, con esquema de soporte 24x7 con fabricante y soporte local por parte del Contratista					

OTRAS ESPECIFICACIONES TÉCNICAS PARA TENER EN CUENTA:

1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR).

La solución EDR avanzada deberá incluir:

Higiene de TI

- Descubrimiento de activos
- Evaluación de activos
- Reducción de la superficie de ataque
- Control de aplicaciones
- Control de dispositivos USB

Protección de endpoints

- NGAV (pre-ejecución)
- Protección posterior a la ejecución
- Análisis de sandbox
- Inteligencia de amenazas en la nube
- Visualización de la cadena de ataque

- Análisis forense avanzado de incidentes
- Etiquetado MITRE
- Navegador seguro
- Cortafuegos del host
- Protección Móvil

Detección y Respuesta de endpoints

- Investigación impulsada por IA
- Integración con plataformas del mismo fabricante y de terceros
- Marco de remediación y respuesta a incidentes automatizado
- Shell remoto seguro
- Registro y análisis continuos
- Habilitación de la cacería de amenazas
- Etiquetado de comportamiento basado en IA
- Ingesta y búsqueda de IoC

2. SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

La solución DLP avanzada deberá incluir:

Prevención de perdida de datos

- Control de dispositivos
- Inventario de aplicaciones GenAI y SaaS con análisis de riesgos de datos.
- DLP integrado para web, correo electrónico, impresoras, portapapeles y medios extraíbles.
- Inspección de contenido en tiempo real (dentro y fuera de la red).
- Flujo de datos seguro: Prevención de pérdida de datos basada en el origen de los datos.
- Seguimiento del linaje de datos con detección de manipulación de archivos.
- Coaching personalizado para empleados con telemetría de respuesta.
- Biblioteca global de políticas sobre privacidad de datos y cumplimiento normativo
- Soporte para etiquetas de confidencialidad de Microsoft Purview
- Soporte de Evidence Store para el análisis forense de archivos y portapapeles.
- Cronograma de actividades de gestión de incidentes y DLP.
- Políticas de adaptación dinámica al riesgo.

Gestión de riesgos internos

- Visibilidad de la actividad del usuario en todos los dispositivos y unidades de almacenamiento en la nube empresarial.
- Análisis de comportamiento impulsado por aprendizaje automático.
- Biblioteca de detección de amenazas internas mapeada con MITRE ATT&CK.
- Detección de secuencias de exfiltración de datos por amenazas internas.
- Acciones de aislamiento y bloqueo de puntos finales.
- Soporte de Evidence Store para análisis forense de captura de pantalla.
- Gestión de casos

Integración de software como servicio (SaaS) empresarial

- Microsoft Office 365 Connector
- Capacitación a empleados en tiempo real a través de mensajería de Teams.
- Compatibilidad con M365 (Purview)
- Controles para compartir archivos

3. SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN, PRUEBAS, PUESTA EN MARCHA, ESTABILIZACIÓN Y SOPORTE.

El contratista deberá disponer del personal técnico especializado necesario para la implementación, configuración, puesta en operación, administración y soporte de la plataforma de seguridad objeto del contrato.

El personal requerido será responsable directo de la ejecución técnica, operación y soporte especializado de las soluciones contratadas, de conformidad con los requerimientos definidos por la Entidad.

El plazo para la instalación, configuración, pruebas, puesta en marcha de las soluciones de EDR y DLP será de dos (2) meses y el tiempo de la suscripción del licenciamiento y del soporte de dichas plataformas será de doce (12) meses.

El plazo de ejecución del contrato es de DOS (2) MESES, a partir de la suscripción de acta de inicio previo el cumplimiento de los requisitos de perfeccionamiento y ejecución (Registro presupuestal y aprobación de la garantía única), previo cumplimiento de los requisitos de perfeccionamiento y ejecución establecidos en el artículo 41 de la Ley 80 de 1993.

Nota Aclaratoria: El termino de cobertura de las suscripciones y soporte de la misma debe ser por DOCE (12) meses, a partir de la firma del acta de inicio, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista.

4. PERSONAL MINIMO REQUERIDO

El contratista deberá garantizar como mínimo los siguientes perfiles:

Rol	Actividades	Perfil Profesional	Certificaciones Requeridas	Experiencia	Cantidad personal
COORDINADOR DE EJECUCIÓN DEL CONTRATO	Responsable de la planeación, coordinación, seguimiento y control de la ejecución técnica del contrato, asegurando el cumplimiento del alcance, cronograma, niveles de servicio y entregables definidos por la Entidad.	Pregrado: Ingeniero de Sistemas y/o Electrónico y/o Telecomunicaciones y/o Telemática o afines. Posgrado: Especialización y/o Maestría en Gerencia de Proyectos y/o áreas afines a Tecnologías de la Información.	• Project Management Professional (PMP) • ITIL versión 3 o superior	• Mínimo seis (6) años de experiencia general contados a partir de la expedición de la tarjeta profesional • Mínimo cuatro (4) años y/o cuatro (4) proyectos de experiencia específica en la coordinación y gestión de proyectos de implementación de soluciones tecnológicas y/o de seguridad, acreditada mediante certificaciones laborales y/o contratos.	1
INGENIERO DE IMPLEMENTACIÓN – EDR	Responsable de la instalación, configuración, pruebas y puesta en operación de las funcionalidades de protección de endpoints, garantizando su correcto funcionamiento, alineación con las políticas de la Entidad y mínima afectación al rendimiento de los equipos.	Pregrado: Ingeniero de Sistemas y/o Electrónico y/o Telecomunicaciones y/o Telemática o afines.	• Certificación en nivel profesional o especialista en administración de EDR del fabricante de la oferta	• Mínimo dos (2) años y/o dos (2) proyectos de experiencia específica en implementación de soluciones de seguridad en EDR del fabricante ofertado.	1
INGENIERO DE IMPLEMENTACIÓN – DLP	Responsable de la instalación, configuración, pruebas y puesta en operación de las funcionalidades de protección de datos, garantizando su correcto funcionamiento, alineación con las políticas de la Entidad y mínima afectación al rendimiento de los equipos.	Pregrado: Ingeniero de Sistemas y/o Electrónico y/o Telecomunicaciones y/o Telemática o afines.	• Certificación en nivel profesional o especialista en administración de DLP del fabricante de la oferta.	• Mínimo dos (2) años y/o dos (2) proyectos de experiencia específica en implementación de soluciones de seguridad en DLP del fabricante ofertado.	1

Nota 1: Los perfiles anteriores deben ser aportados por el contratista para la aprobación por parte del supervisor para el inicio del contrato.

Nota 2: El contratista deberá incluir la hoja de vida, copia de la cédula de ciudadanía y los soportes de la experiencia profesional y de la formación académica correspondientes a los tres profesionales descritos anteriormente.

Nota 3: El contratista podrá presentar un único perfil para cada uno de los roles para el caso de ingeniero de implementación – edr e ingeniero de implementación – dlp, siempre que dicho perfil cumpla integralmente con los requisitos exigidos para cada rol.

Nota 4: Las actividades desarrolladas por el personal requerido se limitarán exclusivamente a la ejecución técnica, administración, operación y soporte de las plataformas de seguridad contratadas, sin que en ningún caso se entiendan como servicios de consultoría, asesoría estratégica o conceptual.

5. CONDICIONES DE GARANTÍA Y SOPORTE TÉCNICO ADICIONALES DEL SERVICIO

- El contratista deberá prestar el servicio de acompañamiento técnico y resolución de incidentes que no sean gestionados automáticamente por la consola de administración, así como brindar asesoría y orientación en mejores prácticas para la adecuada administración y operación de la solución de protección implementada por la Entidad.
- El contratista deberá atender los requerimientos de soporte técnico, ya sea de forma presencial o virtual, según las solicitudes emitidas por la entidad, durante la vigencia del servicio de soporte contratado.
- El contratista deberá proveer soporte especializado durante un (1) año, garantizando la disponibilidad de múltiples canales de atención, tales como línea telefónica, correo electrónico, chat en línea y plataforma de gestión de incidentes, a través de los cuales la Entidad podrá registrar, consultar y dar seguimiento a sus requerimientos y/o incidentes técnicos.
- El contratista deberá disponer de personal técnico debidamente certificado en las soluciones ofertadas EDR y DLP, encargado de la atención, análisis y resolución de los requerimientos e incidentes reportados por la Entidad, asegurando la calidad, oportunidad y trazabilidad de las acciones ejecutadas.
- El contratista para el servicio de soporte deberá garantizar calidad, oportunidad y trazabilidad de las acciones ejecutadas, incluyendo el registro detallado de incidentes, actividades realizadas, recomendaciones técnicas, aplicación de cambios y evidencias de solución, como insumo para auditoría, control interno y mejora continua.
- El contratista deberá garantizar la vigencia de las suscripciones, licencias, actualizaciones, parches de seguridad y soporte de fábrica de todos los componentes incluidos, durante el período contratado, asegurando la continuidad operativa y la protección efectiva de la infraestructura tecnológica de la Entidad.

6. SOPORTE Y ACUERDOS DE NIVELES DE SERVICIO

- Junto con la implementación, puesta en marcha, el proveedor deberá entregar documento que certifique que la UAERMV a partir del Acta de Inicio contará con el servicio de asistencia con esquema de soporte 7x24x365 con fabricante y soporte local por parte del Contratista.

- El contratista deberá suministrar e implementar, durante la vigencia del servicio de soporte, todas las actualizaciones estables de software, firmware y parches correspondientes a la solución de protección, de manera integral y conforme a las versiones oficialmente liberadas por el fabricante.

- El contratista se obliga a atender y resolver los requerimientos e incidentes reportados por la Entidad relacionados con la solución, a través de los canales de atención dispuestos para tal fin (plataforma web, línea telefónica o correo electrónico), garantizando una disponibilidad continua del servicio bajo el esquema 7x24x365.

- El contratista deberá iniciar la atención de los requerimientos e incidentes dentro de las dos (2) horas siguientes a su reporte por parte de la Entidad y garantizar su gestión para la lograr una solución adecuada y ágil. En los casos en que sea necesario el soporte de tercer nivel por parte del fabricante, el contratista deberá realizar el escalamiento correspondiente, gestionar el caso y ejecutar todas las acciones requeridas conforme a los lineamientos establecidos por el fabricante.

- El servicio de soporte deberá contemplar la gestión de incidentes, cambios controlados, ajustes de configuración, validación de funcionamiento, análisis de eventos y recomendaciones técnicas, en concordancia con las buenas prácticas de operación de infraestructura crítica y seguridad de la información.

7. HABILITANTES TECNICOS

FICHA TECNICA

Para tal efecto, el proponente deberá presentar, junto con su oferta, la ficha técnica detallada del bien o servicio ofertado, en la que se evidencie el cumplimiento de la totalidad de los requerimientos y especificaciones mínimas exigidas por la Entidad. Esta ficha técnica

deberá:

- Contener documentación oficial del fabricante (fichas de producto, catálogos técnicos, manuales u hojas de datos).

CERTIFICACIONES DE PARTNER AUTORIZADO EMITIDA POR EL FABRICANTE

- El proponente debe adjuntar junto con su propuesta carta emitida por el fabricante y dirigida a la entidad donde certifique que el proponente es Partner, canal o socio con el nivel más alto de membresía en la marca ofrecida en Colombia. La misma no debe ser con fecha superior a 30 días anteriores a la fecha de cierre de este proceso.

Nota: En caso de tratarse de un proponente plural (consorcio o unión temporal), el presente requisito podrá ser acreditado por cualquiera de sus integrantes, siempre que dicho integrante participe directamente en la ejecución del objeto contractual relacionado con la solución ofertada.

GARANTÍAS QUE APLIQUEN O SE REQUIERAN DE ACUERDO CON EL OBJETO CONTRACTUAL

Con fundamento en lo establecido en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, y dada la naturaleza, valor y complejidad del contrato objeto de este proceso de selección, se hace necesario exigir garantías que permitan amparar eventuales perjuicios de carácter contractual o extracontractual durante la ejecución del contrato.

En este sentido, se justifica la exigencia de las siguientes garantías:

ETAPA	AMPAROS	%	VIGENCIA	JUSTIFICACIÓN
CONTRACTUAL	CUMPLIMENTO de las obligaciones surgidas del contrato estatal, incluyendo en ellas el pago de multas y cláusula penal pecuniaria, cuando se hayan pactado en el contrato	20% DEL TOTAL DEL CONTRATO	A partir de la suscripción del contrato comprende el plazo del soporte de las plataformas (Un año) y seis (6) meses más y/o hasta su liquidación	Cubre a la entidad de los perjuicios directos derivados del incumplimiento total o parcial de las obligaciones nacidas del contrato, así como su cumplimiento tardío o defectuoso, cuando ellos son imputables al contratista.
CONTRACTUAL	CALIDAD DEL SERVICIO	20% DEL TOTAL DEL CONTRATO	A partir de la suscripción del contrato comprende el plazo del soporte de las plataformas (Un año) y un (1) año más contado a partir de la fecha de entrega final y recibo a satisfacción de la UAERMV y hasta su liquidación.	Cubre a la entidad de los perjuicios, derivados de la mala calidad de los servicios prestados de acuerdo con las especificaciones técnicas establecidas en el contrato, o por incumplimiento de los parámetros o normas establecidos para el respectivo servicio
CONTRACTUAL	PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES	5% DEL TOTAL DEL CONTRATO	Duración del contrato contando el tiempo de vigencia de las suscripciones y tres (3) años más.	Protege a las entidades contratantes contra el incumplimiento de las obligaciones laborales que tiene el contratista con el personal utilizado para la ejecución del contrato.

NOTA 1. El vendedor debe cargar las garantías a través del módulo previsto para el efecto en el SECOP II.

Las vigencias de los amparos de la presente cláusula deberán ajustarse a la fecha del acta de inicio del contrato, igualmente deberán ajustarse al suscribir las actas de suspensión, reinicio, mayores cantidades, terminación, prórrogas, adiciones, modificaciones contractuales y liquidación.

El hecho de la constitución de estos amparos no exonera al CONTRATISTA de las responsabilidades legales en relación con los riesgos

asegurados.

Dentro de los términos estipulados en este Contrato, ninguno de los amparos otorgados podrá ser cancelado o modificado sin la autorización expresa de la UAERMV. El CONTRATISTA deberá mantener vigente las garantías, amparos y pólizas a que se refiere esta cláusula, y serán de su cargo el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan. Si el CONTRATISTA se demora en modificar las garantías, éstas podrán variarse por la aseguradora o banco a petición de la UAERMV y a cuenta del CONTRATISTA, quien por la firma del Contrato autoriza expresamente a la UAERMV para descontar los valores respectivos de los saldos que hubiere a su favor, previa facturación de los servicios prestados y una vez realizadas las deducciones y/o retenciones por tributos a que haya lugar, sin perjuicio de las acciones legales que la UAERMV pueda ejercer en su contra.

Las garantías requieren aprobación de la oficina de contratos de la UAERMV o la dependencia que tenga dicha función.

Las únicas exclusiones aceptables para las pólizas que se constituyan en relación con el presente Contrato serán las señaladas en el Decreto 1082 de 2015, las demás exclusiones se entenderán por no escritas.

Lo dispuesto en este numeral en cuanto a la aprobación de la garantía, no basta para que en cualquier momento de la ejecución y/o liquidación del Contrato que la UAERMV advierta que la Garantía Única de Cumplimiento no cumple con alguno de los requisitos exigidos en este Contrato o las normas que regulen la materia, pueda exigir al Contratista la corrección, ampliación o adecuación de dicha Garantía, en un plazo máximo de quince (15) Días Hábiles contados desde el requerimiento escrito que para el efecto deberá formularle la UAERMV, so pena de hacerse acreedor a las multas establecidas en la cláusula correspondiente del Contrato.

REQUERIMIENTOS AMBIENTALES:

Dar cumplimiento a lo señalado en el Plan Institucional de Gestión Ambiental- PIGA-, Interno de la UAERMV, observando las normas sobre protección y conservación del medio ambiente, uso eficiente de los recursos adecuada segregación de los residuos, participación activa en las actividades de sensibilización para el cuidado y la protección del medio ambiente y demás disposiciones que regulen la materia.

NORMATIVIDAD APLICABLE Y REQUERIMIENTOS LEGALES:

La presente contratación se fundamenta en el siguiente marco normativo:

- Ley 80 de 1993 “Por la cual se expide el Estatuto General de Contratación de la Administración Pública”.
- Ley 1150 de 2007 “Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.”
- Ley 1474 de 2011 “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”.
- Ley 2069 de 2020 “Por medio del cual se impulsa el emprendimiento en Colombia”
- Ley 1882 de 2018 “Por la cual se adicionan, modifican y dictan disposiciones orientadas a fortalecer la contratación pública en Colombia, la Ley de Infraestructura y se dictan otras disposiciones”.
- Ley 2195 de 2022 “Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones”.
- Decreto Ley 019 de 2012 “Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública”.
- Decreto 1082 de 2015 “Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional”.
- En consideración a lo dispuesto en el Decreto 310 de 2021 "Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. y 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional".
- Manual de Contratación de la UAERMV que se encuentre vigente.
- Téngase en cuenta lo establecido en el Decreto 189 de 2020, “Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones”, y la Directiva 03 de 2021 implementación art. 14.
- Disposiciones del Decreto 1860 de 2021, "Por el cual se modifica y adiciona el Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin reglamentar los artículos 30, 31, 32, 34 y 35 de la Ley 2069 de 2020, en lo relativo al sistema de compras públicas y se dictan otras disposiciones".
- Circular 013 de 2021 expedida por la secretaría distrital de la mujer.

OTRA NORMATIVIDAD APLICABLE AL PROCESO

- Ley 1341 de 2009, modificada por la Ley 1978 de 2019, La Ley 1341 de 2009 consagra derechos y deberes de los prestadores y usuarios de los servicios de Tecnologías de la Información y las Comunicaciones, así como establece que el Fondo de Tecnologías de la Información y las Comunicaciones tendrá entre sus funciones "Cofinanciar planes, programas y proyectos para el fomento de la industria de software y de computación en la nube" De acuerdo con la forma de entregar los servicios por parte de los proveedores, los tipos de contrato que se ajustan de mejor forma a la adquisición de software son: (i) el contrato de compraventa, cuando se trata de la adquisición de una solución lista, y (ii) en el caso de servicios por demanda, el contrato de suministro, pues ocurren prestaciones económicas que serán suministradas según las necesidades del usuario, cumpliendo con el principio de pagar efectivamente el software utilizado, permitiendo la elasticidad del consumo7. Por otra parte, frente a la responsabilidad de proveedores (fabricantes) y distribuidores de Software, el artículo 60 de la Ley 1480 de 2011 (estatuto del consumidor) dispuso que "todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca o ponga en el mercado, así como la calidad ofrecida. En ningún caso estas podrán ser inferiores o contravenir lo previsto en reglamentos técnicos y medidas sanitarias o fitosanitarias." El incumplimiento de esta obligación dará lugar a: (i) responsabilidad solidaria del productor y proveedor por garantía ante los consumidores. (ii) responsabilidad administrativa individual ante las autoridades de supervisión y control en los términos de esta ley y (iii) responsabilidad por daños por producto defectuoso, en los términos de esta ley."

- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" buscando preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Esta ley protege a los sistemas de Información de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

NORMATIVIDAD COMPLEMENTARIA

- DECRETO 332 DE 2020 MODIFICADO POR EL DECRETO DISTRITAL 634 DE 2023

Se encuentran exceptuados de la aplicación de las medidas afirmativas previstas en este decreto, los procesos adelantados por acuerdo marco de precios, bolsa de productos, tienda virtual del Estado y las tipologías contractuales para la adquisición de bienes y servicios que por su naturaleza no requieran de personal para la ejecución del contrato y/o convenio, entre ellos arrendamiento de bienes inmuebles, compraventa, adquisición de bienes a través de la bolsa de productos, subastas a través de martillo, suministros, enajenación de bienes, comodatos, prestación de servicios profesionales y de apoyo a la gestión.

Atendiendo las disposiciones incluidas en la Ley 2069 de 2020 y en su Decreto Reglamentario 1860 de 2021 y una vez efectuado el análisis de oportunidad para la aplicación de lo establecido en el artículo 2.2.1.2.4.2.16 del Decreto 1082 de 2015, se concluye que, conforme a la naturaleza del proceso y sus componentes, la entidad no considera viable incluir la población vulnerable y/o sujetos de especial protección constitucional, teniendo en cuenta las siguientes consideraciones:

El proceso contractual tiene como objeto "SUSCRIPCIÓN, IMPLEMENTACIÓN Y SOPORTE DE UNA PLATAFORMA DE CIBERSEGURIDAD DE NUEVA GENERACIÓN PARA LA PROTECCIÓN INTEGRAL DE LOS ACTIVOS DIGITALES DE LA UAERMV, ORIENTADA A LA PREVENCIÓN, DETECCIÓN Y RESPUESTA AVANZADA ANTE AMENAZAS EN ENDPOINTS Y PREVENCIÓN DE PÉRDIDAS DE DATOS."

Teniendo en cuenta las características del contrato a celebrar COMPRAVENTA, el objeto contractual y el alcance de las obligaciones del contratista adjudicatario, se concluye que es improcedente exigir para la ejecución del contrato, la participación de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional.

- DECRETO 0142 DE 1 DE FEBRERO DE 2023, MODIFICATORIO DEL DECRETO 1082 DE 2015

Según lo estipulado en el decreto 0142 de 2023 por el cual se modifica y adiciona el Decreto número 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional para promover el acceso al sistema de Compras Públicas de las MiPymes, las Cooperativas y demás entidades de la economía solidaria, se incorporan criterios sociales y ambientales en los Procesos de Contratación de las Entidades Estatales, se incluye el Título de emprendimiento comunal y se dictan otras disposiciones, se hace el siguiente análisis:

Artículo 4. Modificación del artículo 2.2.1.1.2.2.2 de la Subsección 2 de la Sección 2 del Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015. Modifíquese el artículo 2.2.1.1.2.2.2. de la Subsección 2 de la Sección 2 del Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015. es pertinente indicar que NO le es aplicable al presente proceso de selección, por cuanto, su aplicación está supeditada para los procesos de licitación pública y selección abreviada de menor cuantía.

Ahora bien, frente a los criterios sociales, la entidad determinó que no es viable por la naturaleza, objeto y obligaciones contempladas en el presente estudio.

Artículo 6. del Decreto 142 de 2023 que adiciona el artículo 2.2.1.2.4.2.19 a la Subsección 2 de la Sección 4 del Capítulo 2 del Título 1 de la Parte 2 del libro 2 de la sección 4 del Capítulo 2 del Título 1 de la Parte 2 del Libro 2 del Decreto 1082 de 2015, teniendo en cuenta el resultado del análisis de mercado y el análisis de la información financiera de los posibles proveedores numeral 3. Análisis de la Oferta, literal c.; se observa que existen en el mercado un gran número de empresas MiPymes que pueden participar en el presente proceso de selección, de acuerdo con el valor estimado del proceso, y los requisitos habilitantes técnicos diferenciales de acuerdo a lo establecido en el Decreto 1860 de 2021, que promuevan y faciliten la participación en los procedimientos de selección competitivos de las MiPymes domiciliadas en Colombia.

Aspectos de tipo ambiental

De acuerdo con el concepto emitido por la Oficina de Servicios y Control Ambiental – OSCS de la UAERMV, no se requieren licencias ambientales para la ejecución de este contrato, dado que el objeto contractual corresponde a la adquisición, optimización, modernización y soporte de una plataforma tecnológica y no implica obras, intervenciones físicas ni actividades con impacto ambiental directo.
No obstante, el contratista deberá cumplir la cláusula ambiental institucional, dando cumplimiento a lo dispuesto en el Plan Institucional de Gestión Ambiental (PIGA), observando las normas sobre protección y conservación del medio ambiente, uso eficiente de los recursos, adecuada segregación de residuos y participación en actividades de sensibilización y cuidado ambiental
Las demás normas que deroguen y/o sustituyan a las descritas al momento de la firma del acta de inicio.

REQUERIMIENTOS MÍNIMOS PARA LA ENTREGA DEL BIEN, OBRA O SERVICIO OBJETO DEL CONTRATO:

Generales

El contratista deberá suministrar, implementar y poner en operación las soluciones EDR y DLP, bajo modelo de suscripción, que cumpla como mínimo con los siguientes requisitos:

1. La solución deberá ser nativa en la nube, sin requerir infraestructura local adicional para su operación, administración o almacenamiento de telemetría.
2. La solución deberá incluir capacidades integradas de protección según lo estipulado en la ficha técnica.
3. El contratista deberá garantizar la provisión de licencias activas para la totalidad de los endpoints y/o datos cubiertos durante toda la vigencia de la suscripción.
4. La solución deberá ser compatible, como mínimo, con sistemas operativos Windows, Linux y macOS, así como integrarse con servicios de identidad basados en Directorio Activo local y servicios de identidad en la nube, garantizando las funcionalidades solicitadas según el fabricante.
5. La administración de la solución deberá realizarse mediante una consola centralizada, con acceso seguro, control de roles y autenticación multifactor (MFA) en caso de que aplique.
6. La solución deberá contar con administración centralizada desde la nube mediante una o más consolas, módulos, agentes, servicios o componentes técnicamente integrados. Se permitirá el uso de componentes complementarios cuando sean necesarios para cumplir las capacidades solicitadas, siempre que estén incluidos en el licenciamiento ofertado y no generen costos adicionales para la Entidad durante la vigencia de la suscripción. El proponente deberá identificar claramente los componentes, agentes, consolas e integraciones que conforman su solución
6. El contratista deberá garantizar la instalación de agentes, su correcta comunicación con la consola central y la integración con las plataformas definidas por la entidad.
7. La suscripción deberá incluir soporte de fábrica, actualizaciones, parches y mejoras durante toda la vigencia contractual.
8. El contratista deberá entregar documentación técnica y operativa, así como evidencias de la correcta implementación y funcionamiento de la solución.

Requerimientos mínimos específicos – Solución EDR avanzada

Higiene de TI

- Descubrimiento de activos
- Evaluación de activos
- Reducción de la superficie de ataque
- Control de aplicaciones
- Control de dispositivos USB

Protección de endpoints

- NGAV (pre-ejecución)
- Protección posterior a la ejecución
- Análisis de sandbox
- Inteligencia de amenazas en la nube

- Visualización de la cadena de ataque
- Análisis forense avanzado de incidentes
- Etiquetado MITRE
- Navegador seguro
- Cortafuegos del host
- Protección Móvil

Detección y Respuesta de endpoints

- Investigación impulsada por IA
- Integración con plataformas del mismo fabricante y de terceros
- Marco de remediación y respuesta a incidentes automatizado
- Shell remoto seguro
- Registro y análisis continuos
- Habilitación de la cacería de amenazas
- Etiquetado de comportamiento basado en IA
- Ingesta y búsqueda de IoC

Requerimientos mínimos específicos – Solución DLP avanzada

Prevención de perdida de datos

- Control de dispositivos
- Inventario de aplicaciones GenAI y SaaS con análisis de riesgos de datos.
- DLP integrado para web, correo electrónico, impresoras, portapapeles y medios extraíbles.
- Inspección de contenido en tiempo real (dentro y fuera de la red).
- Flujo de datos seguro: Prevención de pérdida de datos basada en el origen de los datos.
- Seguimiento del linaje de datos con detección de manipulación de archivos.
- Coaching personalizado para empleados con telemetría de respuesta.
- Biblioteca global de políticas sobre privacidad de datos y cumplimiento normativo
- Soporte para etiquetas de confidencialidad de Microsoft Purview
- Soporte de Evidence Store para el análisis forense de archivos y portapapeles.
- Cronograma de actividades de gestión de incidentes y DLP.
- Políticas de adaptación dinámica al riesgo.

Gestión de riesgos internos

- Visibilidad de la actividad del usuario en todos los dispositivos y unidades de almacenamiento en la nube empresarial.
- Análisis de comportamiento impulsado por aprendizaje automático.
- Biblioteca de detección de amenazas internas mapeada con MITRE ATT&CK.
- Detección de secuencias de exfiltración de datos por amenazas internas.
- Acciones de aislamiento y bloqueo de puntos finales.
- Soporte de Evidence Store para análisis forense de captura de pantalla.
- Gestión de casos

Integración de software como servicio (SaaS) empresarial

- Microsoft Office 365 Connector
- Capacitación a empleados en tiempo real a través de mensajería de Teams.
- Compatibilidad con M365 (Purview)
- Controles para compartir archivos

Entregables mínimos del contratista, aplica para las soluciones EDR y DLP

El contratista deberá entregar como mínimo:

- Licencias activas de la plataforma durante toda la vigencia del contrato.
- Implementación e integración inicial de la solución.
- Evidencias de funcionamiento de la plataforma y sus funcionalidades.
- Manuales técnicos y operativos.
- Soporte de fábrica y acompañamiento durante la puesta en operación.

- Acta de entrega y aceptación del servicio por parte de la entidad.

Criterio de aceptación

La entrega del servicio se considerará satisfactoria cuando:

- La solución se encuentre operativa en la infraestructura definida.
- Se verifique la correcta aplicación de políticas de detección, prevención y respuesta.
- Se cuente con acceso funcional a la consola de administración centralizada.
- Se evidencie el cumplimiento de los requerimientos técnicos mínimos aquí definidos.

REQUISITOS TÉCNICOS GENERALES POR ETAPA:

Se deberán tener en cuenta los siguientes aspectos para la ejecución del contrato:

Durante la presentación de las propuestas:	**1. SOLUCIÓN DE ENDPOINT DETECTION AND RESPONSE O DETECCIÓN Y RESPUESTA DE ENDPOINTS AVANZADA (EDR).** El oferente deberá demostrar que la solución dispone, como mínimo, de: **Higiene de TI** • Descubrimiento de activos • Evaluación de activos • Reducción de la superficie de ataque • Control de aplicaciones • Control de dispositivos USB **Protección de endpoints** • NGAV (pre-ejecución) • Protección posterior a la ejecución • Análisis de sandbox • Inteligencia de amenazas en la nube • Visualización de la cadena de ataque • Análisis forense avanzado de incidentes • Etiquetado MITRE • Navegador seguro • Cortafuegos del host • Protección Móvil **Detección y Respuesta de endpoints** • Investigación impulsada por IA • Integración con plataformas del mismo fabricante y de terceros • Marco de remediación y respuesta a incidentes automatizado • Shell remoto seguro • Registro y análisis continuos • Habilitación de la cacería de amenazas • Etiquetado de comportamiento basado en IA • Ingesta y búsqueda de IoC **2. SOLUCIÓN DE DATA LOSS PREVENTION O PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)** El oferente deberá demostrar que la solución dispone, como mínimo, de: **Prevención de perdida de datos** • Control de dispositivos • Inventario de aplicaciones GenAI y SaaS con análisis de riesgos de datos. • DLP integrado para web, correo electrónico, impresoras, portapapeles y medios extraíbles. • Inspección de contenido en tiempo real (dentro y fuera de la red). • Flujo de datos seguro: Prevención de pérdida de datos basada en el origen de los datos.

	• Seguimiento del linaje de datos con detección de manipulación de archivos. • Coaching personalizado para empleados con telemetría de respuesta. • Biblioteca global de políticas sobre privacidad de datos y cumplimiento normativo • Soporte para etiquetas de confidencialidad de Microsoft Purview • Soporte de Evidence Store para el análisis forense de archivos y portapapeles. • Cronograma de actividades de gestión de incidentes y DLP. • Políticas de adaptación dinámica al riesgo. **Gestión de riesgos internos** • Visibilidad de la actividad del usuario en todos los dispositivos y unidades de almacenamiento en la nube empresarial. • Análisis de comportamiento impulsado por aprendizaje automático. • Biblioteca de detección de amenazas internas mapeada con MITRE ATT&CK. • Detección de secuencias de exfiltración de datos por amenazas internas. • Acciones de aislamiento y bloqueo de puntos finales. • Soporte de Evidence Store para análisis forense de captura de pantalla. • Gestión de casos **Integración de software como servicio (SaaS) empresarial** • Microsoft Office 365 Connector • Capacitación a empleados en tiempo real a través de mensajería de Teams. • Compatibilidad con M365 (Purview) • Controles para compartir archivos
Antes de la entrega del bien, obra o servicio:	Antes de iniciar la puesta en operación, el contratista deberá: • Entregar el plan de implementación. • Presentar el cronograma detallado. • Definir juntamente con la supervisión el plan de despliegue. • Plan de transferencia de conocimiento • Definir la estrategia de instalación de agentes. • Validar los mecanismos de integración con: o Directorio Activo o Plataformas definidas por la entidad • Presentar el procedimiento de reversa (rollback) en caso de ser requerido. • Presentar la matriz de riesgos de implementación. • Validar el acceso a las consolas.
Durante la ejecución del contrato:	Durante la ejecución, el contratista deberá garantizar: Operación • suministro de licencias activas • funcionamiento continuo de las plataformas • disponibilidad del servicio Implementación • instalación de agentes • integración con la consola • integración con plataformas institucionales Soporte • soporte de fábrica • actualizaciones • parches • mejoras • escalamiento Operación técnica Mantener operativas las funcionalidades correspondientes a las plataformas contratadas: EDR • Higiene de TI • Protección de endpoints • Detección y Respuesta de endpoints

	• Alertas, notificaciones y reportes DLP • Prevención de perdida de datos • Gestión de riesgos internos • Integración de software como servicio (SaaS) empresarial • Alertas, notificaciones y reportes
Después de la entrega del bien, obra o servicio:	Como condición para el recibo a satisfacción, el contratista deberá entregar: Documentación • manuales técnicos • manuales operativos • arquitectura implementada • documentación de configuración Evidencias • funcionamiento de la consola • funcionamiento de agentes • funcionamiento de políticas • funcionamiento de notificaciones • funcionamiento de reportes • evidencias de integración Capacitación • transferencia de conocimiento • capacitación a administradores Entregables • licencias activas • acta de implementación • acta de puesta en operación • acta de recibo • soporte de fábrica vigente
OBSERVACIONES Y/O RECOMENDACIONES:	

QUIEN LO ELABORA:	QUIEN LO APRUEBA:
NOMBRE: DANIELA ALEJANDRA AVILA MONTENEGRO	NOMBRE: YENNY HASLEY YAZO LOZADA
CARGO: Contratista OTI	CARGO: Jefe (E) Oficina De Tecnología De La Información

Documento 20261140350573 firmado electrónicamente por:	
YENNY HASLEY YAZO LOZADA	Jefe de Oficina - Oficina de Tecnologías de la Información OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN yenny.yazo@umv.gov.co Fecha firma: 18-11-2026 14:37:36
DANIELA ALEJANDRA AVILA MONTENEGRO	Contratista OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN daniela.montenegro@umv.gov.co Fecha firma: 18-11-2026 14:38:34
Revisó:	CARLOS ABEL BASTIDAS CUBILLOS - Contratista – Líder de Infraestructura y Servicios - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - carlos.bastidas@umv.gov.co
	MARINO MIGUEL MORENO RHENALS - Contratista - OFICINA DE TECNOLOGÍAS DE

	LA INFORMACIÓN - marino.moreno@umv.gov.co
Proyectó:	BERNARDO ALFONSO DUQUE FORERO - Contratista - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - bernardo.duque@umv.gov.co

cc7ce452654fc8dacba0e3a46786581d73d5ed7a9c3d9352b7128a744a25e466
Codigo de Verificación CV: cd121 Comprobar desde: https://www.umv.gov.co/portal/verificar/