ESTUDIOS PREVIOS
CONTRATACIÓN DIRECTA PERSONA JURÍDICA
Artículo 2.2.1.1.2.1.1. del Decreto 1082 de 2015

Fecha de elaboración:	21/08/2026
Dependencia solicitante:	Dirección de Tecnología
Nombre e identificación del responsable	Jessica Andrea Agudelo Vélez

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER:

La Institución Universitaria Digital de Antioquia – IU Digital es un Establecimiento Público de Educación Superior del orden departamental, cuyo objeto principal es la educación en la modalidad digital en ambientes virtuales de aprendizaje. Bajo este escenario, la infraestructura tecnológica y los esquemas de ciberseguridad se consolidan como el pilar fundamental y el canal primario a través del cual la Institución garantiza la prestación del servicio público de educación superior y el acceso al conocimiento en su ecosistema 100% digital.

La Dirección de Tecnología, como área misional responsable de liderar, planear, administrar y soportar la arquitectura tecnológica y los esquemas de ciberseguridad institucionales, tiene el deber imperativo de asegurar la alta disponibilidad, seguridad, integridad y resiliencia de las redes y plataformas que sustentan la operación académica y administrativa de nuestro ecosistema. Bajo esta premisa, surge la necesidad ineludible de garantizar la detección temprana, visibilidad, monitoreo centralizado y correlación de eventos de seguridad en tiempo real. Para ello, es indispensable mantener plenamente operativa, actualizada, soportada e integrada la solución de ciberseguridad basada en la plataforma **FortiSIEM** respaldada por los servicios administrados de monitoreo del Centro de Operaciones de Seguridad Regional (**R-SOC 24/7/365**). Esta solución permite recolectar, normalizar y correlacionar logs de eventos, aplicando análisis avanzado para la detección y atención proactiva de incidentes en el ecosistema tecnológico de la IU Digital.

En el contexto actual de la IU Digital, la necesidad trasciende la adquisición abstracta de software; se requiere con urgencia asegurar por un periodo de doce (12) meses la renovación de las licencias de **FortiSIEM All-In-One Subscription** (para mínimo 50 dispositivos y 10 EPS/dispositivo), **FortiSIEM Subscription para Agentes Avanzados** (50 agentes Log & FIM) y soporte **FortiCare Premium**; la continuidad de la infraestructura dedicada en el Data Center de Tigo (VDC con VDOM dedicada, Firewall Cloud, IDS/IPS Cloud, VPN Client-to-Site/Site-to-Site e Internet dedicado de 30 Mbps); la prestación del servicio administrado de monitoreo R-SOC; y la contratación de servicios profesionales especializados para la configuración e integración de tres (3) fuentes de datos clave al FortiSIEM:

1. **FortiNAC** (1.000 agentes),
2. **FortiEDR** (1.000 agentes), y
3. **FortiMail Workspace Security** (700 buzones).

Esta integración técnica contempla el despliegue de nueve (9) casos de uso de correlación (tres por cada tecnología), tres (3) reportes analíticos personalizados, un (1) dashboard personalizado con 9 widgets y una política automatizada de notificación de alertas de seguridad por correo electrónico.

Para tal efecto, resulta imperativo adelantar un proceso de selección bajo la modalidad de **Contratación Directa**, en la tipología de contrato de **Prestación de Servicios de Apoyo a la Gestión** relacionado con actividades operativas, logísticas o asistenciales con persona jurídica (conforme al literal h del numeral 4 del artículo 2 de la Ley 1150 de 2007, el artículo 2.2.1.2.1.4.9 del Decreto 1082 de 2015 y la Sentencia SU 41.719 de 2013 del Consejo de Estado), específicamente con la empresa **UNE EPM TELECOMUNICACIONES S.A.** (NIT 900.092.385-9).

Esta determinación se fundamenta en un análisis técnico, operativo y de indisolubilidad jurídica que se resume en los siguientes tres factores de ponderación misional:

- **A. Imposibilidad legal de Convenio Interadministrativo por cambio de naturaleza jurídica:** Históricamente, el licenciamiento, soporte y operación de la ciberseguridad institucional se venía ejecutando bajo el amparo del Convenio Marco No. IUD2019051 con la empresa UNE EPM. Ante la transición de la naturaleza jurídica de dicha empresa (que opera actualmente bajo el régimen de derecho privado como Sociedad Anónima Cerrada), la IU Digital se encuentra imposibilitada jurídicamente para utilizar la figura del Convenio Interadministrativo para este objeto. No obstante, dado que esta modificación corporativa de la entidad aliada no extingue la necesidad de protección de la universidad ni altera la infraestructura técnica existente, resulta imperativo migrar a la modalidad de **Contratación Directa para la Prestación de Servicios de Apoyo a la Gestión**, coadyuvando a las funciones tecnológicas internas para asegurar la continuidad del monitoreo y evitar la parálisis o vulneración del ecosistema digital perimetral.
- **B. Interdependencia técnica indisoluble con la infraestructura perimetral e institucional preexistente:** Desde la perspectiva de ingeniería de telecomunicaciones y ciberseguridad, el sistema FortiSIEM y los servicios del R-SOC no operan como componentes de software aislados. La plataforma centralizadora de logs se alimenta e integra en tiempo real con el clúster de Firewall físico de la IU Digital en configuración de alta disponibilidad (HA), compuesto por dos (2) dispositivos perimetrales FortiGate 600E (seriales unívocos **FG6H0ETB20904804** y **FG6H0ETB20904880**), de propiedad de la universidad. Asimismo, recopila logs de los servidores de la universidad (15 nodos On-premises y 2 máquinas virtuales en AWS), así como de las consolas de FortiNAC, FortiEDR y FortiMail. Toda esta telemetría transita de forma segura hacia la VDOM dedicada del Data Center de Tigo a

través de túneles VPN Site-to-Site preestablecidos, configurados y soportados de manera directa por la red de UNE EPM. Intentar introducir un tercero para operar la consola FortiSIEM o para desplegar las fases de integración (Kick-off, ingesta, parsing en CMDB, Rule Engine y tuning) de los 2.700 agentes totales de la IU Digital rompería el ecosistema unificado de seguridad de la marca (*Security Fabric*), generando un gravísimo riesgo de desconfiguración en las reglas de correlación del colector virtual, alteración en el direccionamiento IP de la universidad, reprocesos técnicos de enrutamiento y una inaceptable ventana de desprotección y exposición a ciberamenazas (como ransomware o exfiltración).

- **C. Salvaguarda de los Principios de Economía, Eficiencia y Continuidad del Servicio Público:** Al ser **UNE EPM** el integrador tecnológico histórico de la IU Digital que diseñó e implementó la arquitectura perimetral actual (canales de internet dedicados, VDC de seguridad y enrutamientos IPSec), la empresa ostenta un conocimiento especializado y unívoco sobre la dinámica de red institucional. Contratar con un proveedor diferente exigiría asumir una costosa curva de aprendizaje técnico y administrativo, generando reprocesos de ingeniería, mayores tiempos de despliegue (que excederían el límite de inicio requerido del 5 de septiembre de 2026) y sobrecostos presupuestales innecesarios para la universidad. A la luz de los principios de Economía y Eficiencia (Art. 25 de la Ley 80 de 1993), la forma óptima de proteger las inversiones de capital anteriores hechas por la IU Digital y garantizar que el servicio de monitoreo SOC 24/7/365 se mantenga ininterrumpido y sin degradaciones del servicio de seguridad es adjudicar el contrato a la empresa que ya opera y mantiene estable dicha infraestructura.

Finalmente, se justifica la celebración de este contrato de apoyo a la gestión con una persona jurídica externa, por cuanto la Dirección de Tecnología de la IU Digital carece material y técnicamente del personal de ingeniería de redes con certificaciones de fabricante en régimen de turnos continuos para operar de forma autónoma una consola SIEM las 24 horas del día, los 365 días del año, o para desplegar los servicios en nube perimetral requeridos. Así, la contratación de este servicio especializado se enmarca plenamente dentro de las actividades operativas y de soporte material idóneo permitidas por el artículo 2.2.1.2.1.4.9 del Decreto 1082 de 2015 y la jurisprudencia unificada de contratación estatal colombiana.

1.1. LA FORMA DE SATISFACER LA NECESIDAD:

Para efectos de dar cumplimiento a los objetivos misionales de la Institución Universitaria Digital de Antioquia – IU Digital, la solución técnica, económica y jurídicamente viable para satisfacer la necesidad planteada de manera ininterrumpida y con los más altos estándares de seguridad es la suscripción de un contrato bajo la modalidad de **Contratación Directa**, en la causal de **Prestación de Servicios Profesionales y de Apoyo a la Gestión** (conforme al **artículo 2.2.1.2.1.4.9 del Decreto 1082 de 2015** y el **literal h del numeral 4 del artículo 2 de la Ley 1150 de 2007**), con la empresa **UNE EPM TELECOMUNICACIONES S.A. (NIT 900.092.385-9)**.

Esta tipología contractual se justifica plenamente bajo los parámetros de la **Sentencia SU 41.719 de 2013 del Consejo de Estado**, que define los servicios de apoyo a la gestión como esfuerzos de soporte operativo, logístico o asistencial destinados a coadyuvar al funcionamiento de la administración, requiriendo en este caso el respaldo especializado y continuo de una estructura tecnológica externa para mitigar amenazas.

A continuación, se detalla la forma precisa en que se estructurará la satisfacción de esta necesidad técnica e institucional, corrigiendo y blindando los Estudios Previos originales:

A. Configuración Técnica de la Solución (Malla de Ingeniería)

La satisfacción de la necesidad se ejecutará durante un **plazo de doce (12) meses** a través de cuatro componentes indisolubles:

1. **Renovación y Soporte de Licenciamiento (SKU de Fábrica):** Se garantizará la suscripción anual de la plataforma **FortiSIEM All-In-One** (mínimo 50 dispositivos, 10 EPS por dispositivo, SKU FC1-10-FSM98-180-02-12), **cincuenta (50) licencias de Agentes Avanzados FortiSIEM** (Log & FIM, SKU FC1-10-FSM98-182-02-12), y el soporte técnico especializado del fabricante **FortiCare Premium** (SKU FC2-10-FSM97-248-02-12). Esto proveerá a la IU Digital del derecho de uso legal de la herramienta de correlación de eventos.
2. **Infraestructura de Nube y Conectividad Dedicada:** Se mantendrá alojado el servidor virtual colector FortiSIEM all-in-one dentro de la nube privada de seguridad (**Virtual Data Center - VDC**) en el **Data Center físico de Tigo**. Esta capa de seguridad estará protegida mediante una **VDOM dedicada** con Firewall e IDS/IPS Cloud habilitados, interconectada en tiempo real con la universidad mediante **túneles VPN Site-to-Site (S2S)** y amparada por un canal de **Internet dedicado de 30 Mbps** para la recepción segura de telemetría.
3. **Monitoreo Administrado 24/7/365 (R-SOC):** Se asegura la delegación operativa del monitoreo proactivo del ecosistema al **Regional Security Operations Center (R-SOC) de Tigo Business**, certificado bajo las normas internacionales **ISO 27001** (Seguridad de la Información) e **ISO 20000-1** (Gestión de Servicios de TI). Este servicio garantiza un Acuerdo de Nivel de Servicio (**SLA**) con un **tiempo de notificación menor a treinta (30) minutos** para incidentes o alertas de alto riesgo.
4. **Servicios Profesionales Especializados de Integración:** Comprende la planeación, configuración, normalización, mapeo en la CMDB e ingesta de logs en el colector de **2.700 agentes/buzones** provenientes de tres plataformas clave entregadas por la universidad:
    - **FortiNAC** (1.000 agentes).
    - **FortiEDR** (1.000 agentes).
    - **FortiMail Workspace Security** (700 cuentas/buzones). Esta integración se materializará en un **plazo de noventa (90) días calendario** mediante el despliegue de **nueve (9) casos de uso** (3 por tecnología), **tres (3) reportes analíticos**, un

dashboard con 9 widgets y políticas automatizadas de notificación de alertas por correo electrónico.

B. Justificación de la Idoneidad, Experiencia y Exclusividad Técnica del Proveedor

La selección directa de **UNE EPM TELECOMUNICACIONES S.A.** no es discrecional; obedece a un imperativo técnico de **indisolubilidad de infraestructura** y minimización del riesgo fiscal de la IU Digital:

- **Conocimiento Preexistente y Protección del Capital de Red:** UNE EPM es el integrador tecnológico histórico de la universidad que diseñó, configuró e implementó la arquitectura perimetral actual. Esto incluye el soporte directo sobre el clúster perimetral físico HA, conformado por dos (2) dispositivos **FortiGate 600E (seriales unívocos FG6H0ETB20904804 y FG6H0ETB20904880)** propiedad de la universidad. Asimismo, la telemetría se alimenta de **15 servidores on-premises** y **2 máquinas virtuales en AWS**.
- **Inviabilidad de Migración (Costos y Desprotección):** Si la IU Digital intentara contratar a un tercero para la prestación de estos servicios o la adquisición del SIEM, se vería obligada a desmantelar la configuración actual de enrutamientos de red, reconfigurar de forma manual los colectores de agentes en los 2.700 endpoints, reconstruir los túneles VPN Site-to-Site hacia otro Data Center y reescribir desde cero las reglas de análisis y parsing del Rule Engine del SIEM. Lo anterior traería consigo:
    1. **Sobrecostos significativos** de ingeniería externa que violarían el Principio de Economía.
    2. Un **tiempo de implementación y reprocesos técnicos** que dejaría a la universidad sin monitoreo SOC por semanas.
    3. Una inaceptable **ventana de vulnerabilidad crítica perimetral** frente a ciberamenazas (como malware o ransomware) que podría paralizar el servicio público de educación virtual en ambientes institucionales de aprendizaje.
- UNE EPM es la única persona jurídica del mercado que ostenta simultáneamente la propiedad física del Data Center Tigo donde está alojado el VDC de seguridad y el control operativo directo de las reglas perimetrales configuradas en los túneles VPN preexistentes, garantizando compatibilidad absoluta de extremo a extremo (*Security Fabric*).

C. Transición Legal: Del Convenio Interadministrativo al Contrato Directo

A causa de la evolución societaria de **UNE EPM Telecomunicaciones S.A.** (que actualmente se encuentra constituida como una sociedad anónima cerrada de carácter eminentemente privado), la figura jurídica del **Convenio Interadministrativo** no resulta procedente para amparar el nuevo vínculo, aun cuando existan antecedentes de cooperación mutua como el Convenio Marco No. IUD2019051 y el Contrato No. IUD2019034.

No obstante, esta transformación societaria no extingue la necesidad de seguridad informática de la IU Digital. Por consiguiente, la vía idónea y blindada es la **Contratación Directa de Apoyo a la Gestión** con persona jurídica, amparada presupuestalmente por el **CDP No. 20260468** por valor de **$184.274.640** y perfeccionada técnica y financieramente bajo el amparo de la entrega del licenciamiento unificado, aprovisionamiento cloud y actas de recibo antes del 31 de diciembre de 2026, respetando el principio de anualidad presupuestal y asegurando la estabilidad y continuidad de la infraestructura que soporta la operación académica.

1.2. UBICACIÓN DEL PROCESO EN LA ESTRUCTURA DEL PLAN DE DESARROLLO INSTITUCIONAL:

PLAN DE DESARROLLO:	Plan de Desarrollo Institucional 2023 – 2026 'Digitalidad Próxima'.
EJE ESTRATÉGICO:	1. Consolidación del modelo educativo de la Institución Universitaria Digital.
ASUNTO ESTRATÉGICO:	1.2. Desarrollo de oferta académica pertinente, situada y multimodal.
PROYECTO:	1.2.2. Consolidación del Plan Estratégico de Tecnologías de la Información – PETI.

1.3. COMPETENCIA DEL ORGANISMO PARA ADELANTAR EL PROCESO:

El Ordenador del gasto se encuentra facultado para contratar mediante el literal i) del artículo 43 y el artículo 81 del Acuerdo Directivo No. 20260218 del 20 de abril de 2026, la Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, sus decretos reglamentarios y demás normas concordantes, y como tal actuando en calidad de rector y representante legal de **LA INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA – IU. DIGITAL,** Establecimiento Público del Orden Departamental, creado por la Asamblea Departamental de Antioquia mediante la Ordenanza No 74 de 2017, con **NIT. 901.168.222-9**.

2. MODALIDAD:

La modalidad de selección es:

CONTRATACIÓN DIRECTA	**X**

2.1. CAUSAL DE CONTRATACIÓN DIRECTA:

CONVENIOS O CONTRATOS INTERADMINISTRATIVOS.	
CONTRATOS PARA EL DESARROLLO DE ACTIVIDADES CIENTÍFICAS Y TECNOLÓGICAS.	
CUANDO NO EXISTA PLURALIDAD DE OFERENTES EN EL MERCADO.	

PARA LA PRESTACIÓN DE SERVICIOS PROFESIONALES Y DE APOYO A LA GESTIÓN	**X**
EL ARRENDAMIENTO O ADQUISICIÓN DE INMUEBLES.	
SELECCIÓN DE PERITOS EXPERTOS O ASESORES TÉCNICOS PARA PRESENTAR O CONTRADECIR EL DICTAMEN PERICIAL EN PROCESOS JUDICIALES.	
CONTRATOS CON LOS CABILDOS INDÍGENAS Y LAS ASOCIACIONES DE AUTORIDADES TRADICIONALES INDÍGENAS.	
CONTRATOS CON LOS CONSEJOS COMUNITARIOS DE LAS COMUNIDADES NEGRAS, REGULADOS POR LA LEY 70 DE 1993.	
CONTRATOS CON ORGANIZACIONES DE BASE DE PERTENECIENTES A POBLACIONES AFROCOLOMBIANAS, RAIZALES Y PALENQUERAS O CON LAS DEMÁS FORMAS Y EXPRESIONES ORGANIZATIVAS.	

2.2. EL TIPO DE CONTRATO:

El tipo de contrato corresponde a:

PRESTACIÓN DE SERVICIOS	**X**
PRESTACIÓN DE SERVICIOS APOYO A LA GESTIÓN TECNOLÓGICA	
COMPRAVENTA	
ARRENDAMIENTO	
SUMINISTRO	
OBRA PÚBLICA	
OTROS (CUAL)	

3. OBJETO Y ESPECIFICACIONES:

3.1. OBJETO: Prestar servicios de apoyo a la gestión relacionados con actividades operativas, logísticas o asistenciales para la configuración e integración de las plataformas FortiNAC, FortiEDR y FortiMail Workspace Security a la solución FortiSIEM de la Institución Universitaria Digital de Antioquia, aunado a la renovación del licenciamiento FortiSIEM, la provisión de infraestructura dedicada en Data Center y la prestación del servicio administrado de monitoreo de ciberseguridad R-SOC 24/7, incluyendo soporte técnico especializado.

3.2. ALCANCE DEL OBJETO:

El alcance del presente contrato de prestación de servicios de apoyo a la gestión relacionados con actividades operativas, logísticas y asistenciales comprende la ejecución de todas las actividades necesarias para la renovación de licenciamiento de ciberseguridad, provisión de infraestructura tecnológica dedicada en nube, monitoreo administrado bajo esquema 24/7/365 a través del Centro de Operaciones de Seguridad Regional (R-SOC) e integración técnica avanzada

de las plataformas de seguridad institucionales hacia la solución centralizadora FortiSIEM. Lo anterior está destinado a garantizar la visibilidad unificada de la red, la correlación inteligente de eventos en tiempo real, la detección proactiva y contención de amenazas, y la absoluta continuidad del ecosistema digital que soporta la operación académica y administrativa de la IU Digital.

Para garantizar la correcta ejecución del objeto y la satisfacción integral de la necesidad de la Dirección de Tecnología, el alcance se detalla a través de los siguientes cinco (5) componentes de ingeniería y licenciamiento especializado:

COMPONENTE 1: Renovación y Soporte de Licenciamiento Especializado FortiSIEM

Consiste en la provisión, renovación y soporte de los derechos de uso anual de la plataforma de correlación de eventos de seguridad (SIEM) de la marca Fortinet, debidamente registrados y activados a nombre de la Institución Universitaria Digital de Antioquia:

- **Suscripción FortiSIEM All-In-One (Cantidad: 50):** Suscripción anual para la consola centralizada con capacidad de administrar un mínimo de 50 dispositivos y hasta 10 Eventos por Segundo (EPS) por dispositivo (SKU FC1-10-FSM98-180-02-12).
- **Licencias para Agentes Avanzados FortiSIEM (Cantidad: 50):** Suscripción anual para cincuenta (50) agentes avanzados con capacidades de captura de Logs y Monitoreo de Integridad de Archivos (FIM) (SKU FC1-10-FSM98-182-02-12).
- **Soporte de Fábrica FortiCare Premium (Cantidad: 1):** Soporte técnico especializado del fabricante por un período de doce (12) meses para despliegues de software FortiSIEM (SKU FC2-10-FSM97-248-02-12).

COMPONENTE 2: Provisión y Operación de Infraestructura Dedicada en Data Center Tigo

El contratista garantizará la disponibilidad, conectividad, seguridad perimetral y soporte operativo de la nube privada de seguridad (**Virtual Data Center - VDC**) alojada físicamente en el Data Center de Tigo, donde reside el colector e inteligencia del FortiSIEM de la universidad:

- **Servidor VM Colector (Cantidad: 1):** Aprovisionamiento y soporte técnico del cómputo y almacenamiento virtual dedicado para hospedar la plataforma FortiSIEM All-In-One.
- **Malla de Seguridad (Virtual Domain - VDOM Dedicada):** Operación de un entorno de red lógicamente aislado, protegido por reglas de alta disponibilidad (HA) con capacidades activas de Firewall Cloud (hasta 30 Mbps, 6.000 sesiones concurrentes, 10 reglas iniciales) e IDS/IPS Cloud (módulos perimetrales habilitados con 2 perfiles de inspección profunda).
- **Conectividad y Transporte Seguro de Logs (VPN & Internet):** Configuración y mantenimiento de dos (2) túneles seguros VPN Site-to-Site (IPSec) dedicados para transportar de manera encriptada la telemetría desde la universidad hacia el colector

virtual, respaldados por un canal de Internet Dedicado de 30 Mbps para la recepción continua de flujos Syslog/API.

COMPONENTE 3: Servicio Administrado de Monitoreo de Ciberseguridad R-SOC (24/7/365)

Consiste en la delegación de la operación y vigilancia proactiva de la red de la IU Digital a través del equipo de analistas de seguridad certificados del **Centro de Operaciones de Seguridad Regional (R-SOC)** de Tigo Business:

- **Monitoreo Continuo:** Vigilancia 24/7/365 orientada a identificar actividades anómalas, vectores de ataque o malware en las fuentes configuradas.
- **Cumplimiento de SLA e Incidentes Críticos:** Envío de notificaciones formales y alertas de seguridad ante incidentes categorizados como de riesgo Significativo en un **tiempo máximo de treinta (30) minutos**, aportando recomendaciones técnicas inmediatas de remediación basadas en estándares internacionales (ISO 27001, ISO 20000-1, NIST).
- **Consola de Acceso Operativo:** Entrega de un (1) usuario con rol de lectura en la consola central FortiSIEM para que la universidad pueda realizar monitoreo y consultas autogestionadas en tiempo real.

COMPONENTE 4: Servicios Profesionales de Integración Técnica a FortiSIEM

Comprende el despliegue del proyecto de ingeniería especializada para integrar, normalizar, parsear e ingresar logs de **dos mil setecientos (2,700) agentes/buzones** distribuidos en tres plataformas críticas preexistentes de la universidad hacia el colector FortiSIEM virtualizado:

1. **FortiNAC (1.000 agentes concurrentes):** Integración de las consolas virtuales de control y aplicación (FNC-CAX-VM) que gestionan la capa de acceso y postura de la red institucional.
2. **FortiEDR (1.000 endpoints):** Ingesta de eventos de telemetría de seguridad avanzada (pre y post-infección) de los endpoints universitarios.
3. **FortiMail Workspace Security (700 buzones de correo):** Integración API/SaaS de la protección corporativa para las cuentas institucionales de Google Workspace (SKU FC2-10-PVMCL-1214-02-DD).

COMPONENTE 5: Despliegue de Lógica de Correlación, Analítica y Cierre Operativo

La integración técnica de las fuentes de datos (FortiNAC, FortiEDR y FortiMail) se materializará de manera obligatoria a través de los siguientes entregables configurados en la plataforma SIEM:

- **Configuración de Nueve (9) Casos de Uso unificados en el Rule Engine (3 por tecnología):**
  - **FortiNAC:**

1. *UC-NAC-01:* Detección de Dispositivo Desconocido o No Permitido en Red (Rogue/Unregistered intentando asociarse a VLAN).
2. *UC-NAC-02:* Alerta de Aislamiento/Quarantine de Host por Incumplimiento de Postura (*Compliance Fail*).
3. *UC-NAC-03:* Detección de anomalías de autenticación masiva en acceso (umbral de fallos 802.1X).

- **FortiMail:** 4. *UC-MAIL-01:* Campaña Dirigida de Phishing / Spear Phishing (mismo asunto o IP externa atacando masivamente en un lapso corto). 5. *UC-MAIL-02:* Detección de adjunto malicioso con carga útil (Malware/Virus encontrado correlacionado con remitente y receptor). 6. *UC-MAIL-03:* Incremento inusual de fallos de alineación SPF/DKIM/DMARC (detección de intentos de suplantación de identidad).
- **FortiEDR:** 7. *UC-EDR-01:* Ejecución de Malware Bloqueada/Prevenida en Endpoint (asignación automática de incremento de criticidad de riesgo del host). 8. *UC-EDR-02:* Detección temprana de intento de Ransomware / Cifrado Inusual en volumen y tiempo corto. 9. *UC-EDR-03:* Endpoint Infectado / Amenaza Detectada fuera de la red corporativa (visibilidad de teletrabajadores y hosts *Off-net*).

- **Tres (3) Reportes Analíticos Personalizados:** Un reporte automatizado tipo *Analytics Query* de entrega mensual por cada una de las tecnologías integradas.
- **Un (1) Dashboard Personalizado:** Consola visual centralizada en tiempo real que contendrá un máximo de **nueve (9) widgets** unificados que muestren la telemetría, eventos e incidentes consolidados de las 3 fuentes.
- **Una (1) Política de Automatización y Notificación:** Parametrización en el SIEM para el envío inmediato de alertas por correo electrónico hacia las cuentas del equipo técnico de la universidad y del SOC ante eventos catalogados de alta criticidad.
- **Dos (2) Sesiones de Tuning (Ajuste Fino):** Dedicación de hasta 4 horas totales dentro de los primeros 15 días tras la salida a producción para la mitigación de falsos positivos y balanceo del Rule Engine.
- **Transferencia de Conocimiento:** Sesión de capacitación técnica (duración mínima de 2 horas) dirigida al personal de la Dirección de Tecnología sobre navegación de eventos, visualización de dashboards y triaje básico de alertas.
- **Documentación Técnica LLD (Low Level Design):** Entrega de memorias técnicas detalladas que contengan el diagrama de integraciones, las reglas de correlación parametrizadas, las configuraciones de API/Syslog y las guías de los tableros de control entregados.

3.3. AUTORIZACIONES PERMISOS Y LICENCIAS:

N/A

4. PLAZO:

El plazo de ejecución del contrato será de doce (12) meses, previo cumplimiento de la totalidad de los requisitos de perfeccionamiento y ejecución, específicamente con la firma del contrato por

ambas partes y la aprobación formal de las garantías (pólizas) exigidas por parte de la Institución Universitaria Digital de Antioquia.

Para efectos de garantizar la continuidad ininterrumpida del monitoreo de ciberseguridad y evitar ventanas de vulnerabilidad en la red, el término de ejecución y la vigencia de este servicio tecnológico se proyecta para iniciar el 05 de septiembre de 2026 (día siguiente a la fecha de terminación del licenciamiento actual), siempre y cuando para dicha fecha se haya surtido satisfactoriamente la firma del contrato, la expedición del Registro Presupuestal (RP) y la correspondiente aprobación de la Garantía Única de Cumplimiento por parte de la universidad.

5. LUGAR DE EJECUCIÓN:

La presente contratación se ejecutará en el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín o donde la Institución Universitaria Digital de Antioquia lo requiera.

6. ANÁLISIS ECONÓMICO DE SECTOR:

De conformidad con lo dispuesto en el **artículo 2.2.1.1.1.6.1 del Decreto 1082 de 2015** y en concordancia con los lineamientos de la *Guía para la Elaboración de Estudios de Sector* expedida por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, la Institución Universitaria Digital de Antioquia – IU Digital procede a efectuar el análisis del sector relacionado con el objeto contractual desde las perspectivas legal, comercial, financiera y técnica.

Se deja expresa constancia de que, según las directrices de Colombia Compra Eficiente para la causal de contratación directa de prestación de servicios profesionales y de apoyo a la gestión, **no es obligatorio que la Entidad Estatal realice un estudio exhaustivo de la oferta y la demanda del sector para comparar precios y calidades en un proceso competitivo abierto**. En consecuencia, el presente análisis se enfoca de manera rigurosa en la debida planeación, la trazabilidad del histórico institucional de red, la razonabilidad de los precios ofertados frente al mercado corporativo cerrado del fabricante y la justificación técnico-económica de las condiciones acordadas con el proveedor idóneo.

6.1. Perspectiva Legal del Sector

El mercado de la ciberseguridad corporativa, el licenciamiento de plataformas analíticas de correlación de eventos (SIEM) y la delegación de servicios de monitoreo a Centros de Operaciones de Seguridad (SOC) en Colombia se rige por estrictas normativas de propiedad intelectual (Ley 23 de 1982 y Decisión Andina 486), de protección de datos personales (Ley 1581 de 2012) y de gestión de servicios de tecnología de la información bajo estándares internacionales.

La empresa a contratar, **UNE EPM TELECOMUNICACIONES S.A. (NIT 900.092.385-9)**:

- Cuenta con plena capacidad jurídica y habilitación estatutaria para la provisión de servicios de tecnologías de la información, conectividad, hosting y ciberseguridad, de conformidad con su Certificado de Existencia y Representación Legal de la Cámara de Comercio de Medellín para Antioquia (Matrícula No. 21-365172-04).
- Acredita un régimen comercial de carácter cerrado, habiendo transformado su naturaleza jurídica hacia el derecho privado (Sociedad Anónima Cerrada, catalogada como Gran Contribuyente por la DIAN en su Registro Único Tributario - RUT).
- Cumple formalmente con sus obligaciones laborales, parafiscales y del sistema de seguridad social integral (Salud, Pensión, ARL, SENA, ICBF y Cajas de Compensación) correspondiente a la vigencia actual, debidamente certificado por su Revisor Fiscal (firma delegada KPMG S.A.S.).
- El contratista y sus representantes legales declararon bajo la gravedad de juramento no encontrarse incursos en ninguna de las causales de inhabilidad, incompatibilidad o prohibiciones de rango constitucional o legal para contratar con entidades estatales, conforme al artículo 8 de la Ley 80 de 1993.

6.2. Perspectiva Comercial y Condiciones de Ejecución

La dinámica comercial del sector de ciberseguridad perimetral y soluciones SIEM está fuertemente supeditada a las políticas comerciales del fabricante exclusivo de la tecnología (**Fortinet Inc.**). El software propietario bajo la modalidad de suscripción anual, la infraestructura cloud dedicada para su alojamiento y el servicio analítico de monitoreo 24/7/365 **constituyen una solución integrada indivisible**. Fragmentar comercialmente estos componentes (adquiriendo el software con un distribuidor y pretendiendo contratar el hosting o el SOC con un tercero ajeno a la red de UNE) anularía las garantías de soporte técnico directo del fabricante (FortiCare Premium) e impediría el cumplimiento de los estrictos niveles de servicio de seguridad requeridos por la IU Digital.

- **Sincronización del Esquema Transicional de Pago:** El presente proceso cuenta con el amparo del **CDP No. 20260468 por valor de $184.274.640** con cargo exclusivo al presupuesto de la vigencia fiscal 2026. Para dar estricto cumplimiento al **Principio de Anualidad Presupuestal** (Decreto 111 de 1996), la dinámica comercial se estructurará bajo el esquema de **Único Pago (100%)**. Este pago se causará y ejecutará en la vigencia actual una vez que el contratista entregue a satisfacción de la supervisión el licenciamiento anual debidamente registrado y activado a nombre de la universidad en el portal del fabricante, aprovisione de forma definitiva la nube dedicada en el Data Center físico Tigo y entregue el informe técnico de inicio de operación e integración de agentes. Con esto, el hecho generador del gasto (la entrega y puesta en marcha del activo tecnológico) se perfecciona en el año 2026, quedando la posterior cobertura de monitoreo R-SOC durante el resto del plazo de 12 meses como la garantía técnica de

calidad, soporte de ingeniería y mantenimiento continuo de la infraestructura tecnológica adquirida.

6.3. Perspectiva Financiera: Análisis y Razonabilidad del Presupuesto

Para verificar la razonabilidad de los costos y la eficiencia en la destinación de los recursos públicos de la IU Digital, la Dirección de Tecnología evaluó de manera pormenorizada la propuesta comercial formalizada por **UNE EPM** el 20 de agosto de 2026 (Oferta Técnico Comercial No. V1). La estructura de precios consolidada para un período de ejecución de doce (12) meses es la siguiente:

Componente del Servicio Técnico	**Cant.**	**Meses**	**Tarifa Mensual (Sin IVA)**	**IVA Mensual (19%)**	**Tarifa Mensual (Con IVA)**	**Valor Total 12 Meses (Con IVA)**
Servicios avanzados de monitoreo de seguridad R-SOC (Incluye suscripción anual FortiSIEM All-In-One [50 dispositivos], licencias de 50 agentes avanzados Log & FIM, soporte técnico FortiCare Premium de fábrica y servicios profesionales de integración)	1	12	$11.500.000	$2.185.000	$13.685.000	**$164.220.000**
Servidor VM (Collector) (Arrendamiento de cómputo y almacenamiento virtual dedicado dentro del Virtual Data Center - VDC en el Data Center Tigo)	1	12	$1.150.000	$0 *(Exento)*	$1.150.000	**$13.800.000**

VPN Site-to-Site (S2S) (Aprovisionamiento y soporte de túnel cifrado IPsec IPS perimetral dedicado para transporte seguro de telemetría)	1	12	$220.000	$41.800	$261.800	**$3.141.600**
Internet DataCenter 30 MB (Canal de internet dedicado para terminación segura de túneles e ingesta masiva de logs en el colector)	1	12	$218.000	$41.420	$259.420	**$3.113.040**
TOTALES CONSOLIDADOS DEL PROCESO	**1**	**12**	**$13.088.000**	**$2.268.220**	**$15.356.220**	**$184.274.640**

Justificación Técnico-Económica y Eficiencia Financiera:

1. **Eficiencia por Renta de Servicios Administrados (Mitigación de OPEX y CAPEX):** Si la IU Digital pretendiera estructurar esta solución de forma independiente, se vería obligada a incurrir en costos masivos de capital (CAPEX) para la compra de servidores físicos de alta gama, licenciamiento perpetuo de consolas SIEM y, críticamente, la contratación directa de mínimo cuatro (3) ingenieros de ciberseguridad certificados para cubrir turnos rotativos en un SOC 24/7/365. La tarifa mensual de $13.088.000 (Sin IVA) provista por UNE unifica de manera eficiente el derecho de uso legal del software, el hardware cloud del VDC Tigo, los enlaces dedicados y la ingeniería especializada de ciberseguridad del R-SOC de Tigo Business.
2. **Optimización por Servicios Profesionales de Integración Incluidos:** El análisis financiero resalta que la propuesta comercial **no imputa sobrecostos ni valores adicionales de ingeniería por la fase de integración especializada de fuentes**. El soporte de ingeniería para planeación, registro en CMDB, normalización y puesta en marcha de **2.700 agentes/buzones** (integrando FortiNAC con 1.000 agentes, FortiEDR con 1.000 endpoints y FortiMail con 700 cuentas de Google Workspace) se encuentra plenamente cubierto dentro de la tarifa unificada del monitoreo, lo que representa un ahorro sustancial para el presupuesto institucional.
3. **Tratamiento Tributario Optimizado:** En estricto cumplimiento de la normativa tributaria colombiana (Estatuto Tributario), se destaca la correcta exención de IVA en el rubro de

Servidor VM (Collector) por concepto de hosting y servicios de nube, aplicando de forma precisa el beneficio fiscal sobre el presupuesto general de la universidad.

6.4. Perspectiva Técnica del Sector

Desde la perspectiva puramente de ingeniería de redes y telecomunicaciones, el sector de ciberseguridad corporativa exige un enfoque unificado bajo el concepto de **Security Fabric (Malla de Seguridad Integrada de Fortinet)**. En el ecosistema 100% virtual de la IU Digital, la solución FortiSIEM actúa como el cerebro central que recibe, normaliza y correlaciona telemetría en tiempo real. Este colector se conecta de forma directa con el clúster perimetral físico HA de firewalls de propiedad de la universidad, conformado por dos (2) dispositivos de seguridad **FortiGate 600E (seriales unívocos FG6H0ETB20904804 y FG6H0ETB20904880)**.

- **Idoneidad Técnica Unívoca de UNE EPM:** Al ser UNE EPM Telecomunicaciones S.A. el propietario y operador de la red física de enrutamiento y transporte (túneles VPN Site-to-Site) que conecta perimetralmente la universidad con su Virtual Data Center (VDC), es el **único proveedor del sector con capacidad técnica de garantizar que la telemetría transite sin interrupciones y sin latencia crítica** hacia la consola SIEM. El personal de ingeniería de UNE cuenta con el conocimiento técnico de la topología institucional y de la ingesta de logs de 15 servidores on-premises, 2 máquinas virtuales en AWS y las consolas FortiNAC, FortiEDR y FortiMail preexistentes. Intentar contratar con un proveedor diferente obligaría a la universidad a asumir sobrecostos de reingeniería, cambios de direccionamiento IP de red perimetral, la desconexión temporal de los túneles VPN y una **gravísima e inaceptable ventana de vulnerabilidad perimetral** que dejaría expuesta la base de datos de estudiantes y docentes a ataques cibernéticos de alta severidad (como ransomware o secuestro de datos).

7. VALOR DEL CONTRATO:

El valor del presente contrato es por la suma de **CIENTO OCHENTA Y CUATRO MILLONES DOSCIENTOS SETENTA Y CUATRO MIL SEISCIENTOS CUARENTA PESOS M/CTE. ($184.274.640**), incluidos todos los impuestos y la totalidad de costos directos e indirectos a que haya lugar.

El presente contrato se imputará con cargo al presupuesto de la Institución Universitaria Digital de Antioquia así:

GASTOS DE FUNCIONAMIENTO	**X**
GASTOS DE INVERSIÓN	**N/A**
CDP No.	**20260468**
CÓDIGO BPIN (SOLO APLICA PARA GASTOS DE INVERSIÓN).	**N/A**
NÚMERO DE LA NECESIDAD DEL PLAN ANUAL DE ADQUISICIONES.	**01FDT**

8. FORMA DE PAGO:

La Institución Universitaria Digital de Antioquia – IU. Digital-, pagará al contratista la suma de **CIENTO OCHENTA Y CUATRO MILLONES DOSCIENTOS SETENTA Y CUATRO MIL SEISCIENTOS CUARENTA PESOS M/CTE. ($184.274.640)** IVA incluido, los cuales se cancelarán de la siguiente forma:

Se realizará un único pago correspondiente al 100% a la entrega final de las licencias renovadas. Dicho pago no podrá sobrepasar el 31 de diciembre del 2026.

El pago estará sujeto al cumplimiento de los trámites administrativos a que haya lugar, para lo cual se deben presentar y entregar previamente los siguientes documentos:

a) Certificado o constancia de estar a paz y salvo con el pago de parafiscales y/o seguridad social integral de conformidad con lo establecido en las normas vigentes sobre la materia.
b) Informe de actividades adelantadas por EL CONTRATISTA, en el respectivo período (cuando aplique).
c) La evidencia de documentos que soporten el informe de actividades.
d) Productos requeridos en el contrato.

No obstante, los pagos serán cancelados en pesos colombianos mediante transferencias en la cuenta bancaria informada por el CONTRATISTA, previos los descuentos de ley.

9. CODIFICACIÓN DEL BIEN, OBRA O SERVICIO SEGÚN LAS NACIONES UNIDAS – UNSPSC:

El servicio está codificado en el clasificador de bienes y servicios UNSPSC como se indica a continuación:

NOMBRE DE CLASIFICACIÓN UNSPSC	CLASE
Servicio de licencias del software del computador	81112501
Servicios de personal temporal	80111600

10. OBLIGACIONES DE LAS PARTES:

10.1. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

El **CONTRATISTA** se obliga para con la Institución Universitaria Digital de Antioquia – IU Digital, en su condición de ejecutor material y soporte operativo especializado de la Dirección de Tecnología, a coadyuvar a la gestión misional de ciberseguridad mediante el cumplimiento estricto de las siguientes obligaciones específicas:

A. OBLIGACIONES DE GESTIÓN DE LICENCIAMIENTO Y SOPORTE DE FÁBRICA

1. **Suministro y Registro de Licenciamiento Especializado:** Realizar el aprovisionamiento, registro, activación y sincronización a nombre de la Institución Universitaria Digital de Antioquia, en el portal oficial del fabricante **Fortinet Inc.**, del siguiente licenciamiento unificado por un periodo de doce (12) meses:
    - **Consola Central SIEM:** Cincuenta (50) suscripciones anuales **FortiSIEM All-In-One Subscription** (SKU FC1-10-FSM98-180-02-12), que gestionen un mínimo de 50 dispositivos con capacidad de procesar hasta 10 Eventos por Segundo (EPS) por dispositivo.
    - **Agentes de Seguridad Avanzados:** Cincuenta (50) licencias **FortiSIEM Subscription para Agentes Avanzados** (Log & FIM, SKU FC1-10-FSM98-182-02-12).
    - **Soporte de Fábrica:** Un (1) soporte técnico corporativo del fabricante **FortiCare Premium** (SKU FC2-10-FSM97-248-02-12) para despliegues de software FortiSIEM.
2. **Garantía de Actualización e Integridad:** Asegurar el acceso ininterrumpido durante toda la vigencia del contrato a actualizaciones de software, parches de seguridad, nuevas firmas de reglas de correlación, corrección de bugs y bases de conocimiento global de amenazas del fabricante Fortinet.
3. **Soporte Técnico de Tercer Nivel:** Actuar como canal de escalamiento directo ante el soporte de fábrica de Fortinet (Nivel 3) para la resolución de incidentes técnicos o fallas complejas inherentes al software FortiSIEM que no puedan ser resueltas por el R-SOC.

B. OBLIGACIONES DE INFRAESTRUCTURA CLOUD Y CONECTIVIDAD DEDICADA

4. **Operación del Virtual Data Center (VDC):** Mantener aprovisionada, configurada y disponible la infraestructura de computación y almacenamiento virtual dedicada (**Virtual Data Center - VDC**) en el **Data Center físico de Tigo**, destinada al hospedaje y procesamiento de la máquina virtual del colector central FortiSIEM (*Servidor VM Collector*).
5. **Configuración de Malla de Seguridad (VDOM):** Operar y soportar técnicamente la red del VDC mediante una **VDOM dedicada** que cuente con alta disponibilidad (HA) y tenga habilitados y parametrizados los perfiles perimetrales de Firewall Cloud (hasta 30 Mbps, 6.000 sesiones concurrentes y 10 reglas de control de acceso iniciales) e IDS/IPS Cloud (módulos perimetrales habilitados con 2 perfiles de inspección profunda de paquetes).
6. **Transporte Seguro de Logs (Enlaces y VPN):** Soportar técnicamente y de forma ininterrumpida la transmisión segura de la telemetría institucional a través de la configuración y mantenimiento de dos (2) túneles seguros **VPN Site-to-Site (IPSec) dedicados** y de un canal de **Internet Dedicado de 30 Mbps** para la finalización de los túneles e ingesta continua de flujos Syslog/API en el colector.

C. OBLIGACIONES DEL SERVICIO ADMINISTRADO DE MONITOREO R-SOC (24/7/365)

7. **Monitoreo Proactivo Continuo:** Prestar de manera ininterrumpida, las **veinticuatro (24) horas del día, los siete (7) días de la semana y los trescientos sesenta y cinco (365) días del año (24/7/365)**, el servicio administrado de vigilancia, análisis y detección de incidentes sobre las fuentes de datos configuradas de la universidad, utilizando el capital humano especializado del **Centro de Operaciones de Seguridad Regional (R-SOC)** de Tigo Business, certificado bajo las normas **ISO 27001** e **ISO 20000-1**.
8. **Cumplimiento Estricto de Tiempos de Notificación (SLA):** Clasificar y notificar formalmente a los contactos técnicos de la universidad las alertas e incidentes de ciberseguridad identificados, cumpliendo estrictamente con la siguiente escala de Acuerdos de Nivel de Servicio:
    - **Impacto Significativo (Riesgo Alto/Caída del Servicio):** Notificación inmediata en un tiempo **máximo de treinta (30) minutos**, aportando de manera obligatoria recomendaciones técnicas de contención y buenas prácticas basadas en procedimientos ISO/NIST.
    - **Impacto Moderado (Riesgo Medio):** Notificación en un tiempo máximo de **cuatro (4) horas**.
    - **Impacto Menor (Riesgo Bajo/Cambios):** Notificación en un tiempo máximo de **ocho (8) horas** o en los informes mensuales.
9. **Atención de Fallas y Soporte Técnico Remoto:** Iniciar la solución remota de incidentes y fallas sobre la infraestructura o servicios de seguridad contratados, cumpliendo con un **tiempo de resolución menor a cuatro (4) horas** para incidentes de impacto Significativo, menor a **diez (10) horas** para Moderados y menor a **veinticuatro (24) horas** para Menores, operando en modalidad 24/7/365.
10. **Aprovisionamiento de Cuenta de Lectura:** Habilitar y entregar a la Dirección de Tecnología de la IU Digital un (1) usuario con privilegios de **solo lectura** (*Read-Only Access*) en la consola FortiSIEM, permitiendo la visualización autogestionada de tableros, telemetría e incidentes en tiempo real.

D. OBLIGACIONES DE SERVICIOS PROFESIONALES E INTEGRACIÓN TÉCNICA AVANZADA

11. **Kick-Off e Ingeniería de Prerrequisitos:** Liderar la sesión inicial de kick-off del proyecto para definir la matriz de contactos técnicos, levantar prerrequisitos de red (apertura de puertos Syslog/API) y registrar las consolas directivas de las fuentes de origen en el módulo CMDB del FortiSIEM.
12. **Integración Técnica de Fuentes Preexistentes:** Ejecutar las actividades profesionales de ingeniería especializada para configurar la ingesta, transmisión, parsing y normalización de logs de **dos mil setecientos (2.700) agentes/buzones** distribuidos en las siguientes tres plataformas institucionales preexistentes:

- **FortiNAC (1.000 agentes concurrentes):** Integración de dos (2) consolas virtuales de control y aplicación FNC-CAX-VM.

- **FortiEDR (1.000 endpoints):** Integración API/SaaS para la ingesta de telemetría de endpoints.
- **FortiMail Workspace Security (700 cuentas de correo):** Integración mediante API/Syslog para el análisis de logs de protección de correo corporativo.

13. **Mapeo de Telemetría Externa Adicional:** Sincronizar el colector FortiSIEM con la infraestructura preexistente de la universidad para asegurar el monitoreo y recepción de logs de los equipos perimetrales físicos **FortiGate 600E (seriales unívocos FG6H0ETB20904804 y FG6H0ETB20904880)** de la universidad, así como de **quince (15) servidores on-premises** (físicos/virtuales) y **dos (2) máquinas virtuales alojadas en AWS**.
14. **Parametrización del Motor de Correlación (9 Casos de Uso):** Diseñar, configurar y validar en el *Rule Engine* de FortiSIEM un total de **nueve (9) reglas de correlación personalizadas** (3 por tecnología), alineadas unívocamente con las métricas de valor acordadas para FortiNAC, FortiMail y FortiEDR:
    - *FortiNAC:* Detección de Dispositivos Desconocidos (Rogue/Unregistered), Aislamiento de Hosts por falla de postura (*Compliance Fail*) y Anomalías de Autenticación Masiva en switches (802.1X).
    - *FortiMail:* Detección de Campañas Dirigidas de Phishing/Spear Phishing, Detección de Sandbox de adjuntos maliciosos y Picos Inusuales de fallos SPF/DKIM/DMARC (Spoofing).
    - *FortiEDR:* Bloqueo de Malware correlacionado con incremento de riesgo de host, Detección de intentos de Ransomware (Modificación de archivos inusual) y Detección de endpoints infectados fuera de la red corporativa (*Off-net Hosts*).
15. **Configuración de Analítica y Tableros:** Desarrollar y entregar en la plataforma tres (3) Reportes Analíticos mensuales personalizados (uno por tecnología integrada) y un (1) Dashboard personalizado que contenga **nueve (9) widgets analíticos** consolidados para la visualización en tiempo real de incidentes por parte de la universidad.
16. **Automatización de Alertas:** Parametrizar en la consola una (1) Política de Notificación Automatizada para el envío inmediato de alertas por correo electrónico hacia las cuentas técnicas y buzones de distribución designados por el supervisor del contrato.

E. OBLIGACIONES DE CIERRE TÉCNICO, DOCUMENTACIÓN Y TRANSFERENCIA

17. **Afinamiento y Tuning de Consola:** Ejecutar un mínimo de dos (2) sesiones de tuning (con una dedicación de hasta 4 horas totales dentro de los primeros 15 días posteriores a la salida a producción de las integraciones), orientadas a calibrar umbrales, depurar el motor de correlación y mitigar falsos positivos.
18. **Acompañamiento Posimplementación:** Brindar un periodo de soporte técnico y acompañamiento remoto especializado de **quince (15) días calendario** posteriores a la firma de las actas de integración, con el fin de estabilizar el flujo de eventos Syslog/API.

19. **Entrega de Documentación Técnica:** Elaborar y entregar al supervisor del contrato el documento de diseño técnico de bajo nivel (**Low Level Design - LLD**), el cual debe detallar de manera minuciosa la topología de la integración, los flujos de comunicación habilitados, la lógica interna de los 9 casos de uso configurados y la guía de navegación de los dashboards entregados.
20. **Transferencia de Conocimiento Operativo:** Dictar una sesión de capacitación y transferencia de conocimiento técnica y operativa, con una **duración mínima de dos (2) horas**, dirigida al personal de la Dirección de Tecnología, cubriendo temas de navegación de eventos en FortiSIEM, triaje de alertas de las nuevas fuentes, generación de reportes y administración básica del sistema.

F. OBLIGACIONES DE SEGURIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

21. **Acuerdo de Confidencialidad y NDA:** Suscribir el Acuerdo de Confidencialidad institucional comprometiéndose a mantener bajo la más estricta reserva toda la información, datos personales, topologías de red, logs, credenciales o vulnerabilidades que conozca de la universidad con ocasión del contrato, acatando con rigurosidad las disposiciones de la **Ley 1581 de 2012** de Protección de Datos Personales.
22. **Aislamiento de Telemetría (VDOM Aislada):** Garantizar que toda la telemetría, logs de eventos e información sensible de la universidad permanezca estrictamente almacenada en la VDOM dedicada del Data Center Tigo asignada de manera exclusiva a la IU Digital, sin que pueda ser consolidada, transferida o explotada para fines ajenos al contrato.

10.2. OBLIGACIONES GENERALES DEL CONTRATISTA:

El **CONTRATISTA**, en el marco del contrato de prestación de servicios de apoyo a la gestión que suscriba con la Institución Universitaria Digital de Antioquia – IU Digital, se compromete a cumplir con las siguientes obligaciones generales de carácter administrativo, legal, financiero y de seguridad:

1. **Cumplimiento del Objeto Contractual:** Ejecutar de manera oportuna, eficiente y con los más altos estándares de calidad técnica e idoneidad profesional, el objeto y alcance del contrato, de conformidad con las especificaciones de su propuesta técnica del 20 de agosto de 2026, los estudios previos y las directrices impartidas por el supervisor designado por la IU Digital.
2. **Cumplimiento de Aportes al Sistema de Seguridad Social y Parafiscales:** Acreditar durante toda la ejecución y vigencia del contrato, así como para la viabilidad de los pagos correspondientes, encontrarse al día con el pago de sus aportes al Sistema de Seguridad Social Integral (Salud, Pensión, ARL) y aportes Parafiscales (SENA, ICBF, Cajas de Compensación Familiar), de conformidad con el artículo 50 de la Ley 789 de 2002 y la Ley 1150 de 2007. Para tal efecto, presentará la certificación de cumplimiento

correspondiente emitida por su Revisor Fiscal o Representante Legal, en concordancia con el soporte de revisoría expedido por la firma delegada KPMG S.A.S.

3. **Mantenimiento del Registro en SECOP II:** Mantener plenamente activo, actualizado y sin inconsistencias su perfil de registro como proveedor en la plataforma de contratación pública **SECOP II (Colombia Compra Eficiente)**, garantizando que su información jurídica, financiera y de representación legal coincida estrictamente con los documentos contractuales y tributarios vigentes.
4. **Cumplimiento de Obligaciones Tributarias:** Estar al día en el cumplimiento de sus obligaciones fiscales y tributarias del orden nacional, departamental y municipal, manteniendo actualizado su **Registro Único Tributario (RUT)** bajo su condición de persona jurídica privada y catalogada como Gran Contribuyente ante la Dirección de Impuestos y Aduanas Nacionales (DIAN).
5. **Prevención de Lavado de Activos y Financiación del Terrorismo (SARLAFT):** Garantizar que sus recursos, accionistas, directivos y representantes legales no se encuentren vinculados de ninguna forma con actividades ilícitas, lavado de activos, financiación del terrorismo o incluidos en listas restrictivas de carácter nacional o internacional (como la Lista OFAC / Clinton). Asimismo, autoriza a la IU Digital para realizar las consultas periódicas de antecedentes penales, fiscales, disciplinarios y contractuales en las bases de datos de los organismos de control y el Ministerio de Tecnologías de la Información y las Comunicaciones (incluyendo la base de datos de deudores de alimentos REDAM).
6. **Cláusula de Indemnidad:** Mantener a la Institución Universitaria Digital de Antioquia – IU Digital libre y a salvo de cualquier reclamación, demanda, pleito, acción legal o cobro judicial o extrajudicial interpuesto por terceros (incluyendo trabajadores del contratista, subcontratistas o fabricantes de software) con ocasión de la ejecución del contrato, asumiendo de forma exclusiva los costos de defensa técnica, indemnizaciones o condenas que pudiesen derivarse de su actividad operativa.
7. **Autonomía Técnica y Administrativa:** Ejecutar el contrato con absoluta autonomía técnica, administrativa, financiera y directiva sobre su personal y recursos. Queda expresamente establecido que el contrato no genera vínculo laboral, relación de subordinación, ni intermediación laboral de ningún tipo entre la IU Digital y el personal especializado o de ingeniería que el contratista asigne para la prestación del servicio de R-SOC o las fases de integración tecnológica.
8. **Seguridad y Salud en el Trabajo (SST):** Garantizar que todo el personal técnico e ingenieros asignados para la ejecución material de las actividades del contrato cumplan rigurosamente con el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), contando con las afiliaciones y coberturas de riesgos laborales (ARL) vigentes y los elementos de protección personal necesarios para su labor.
9. **Régimen de Inhabilidades e Incompatibilidades:** Declarar bajo la gravedad de juramento que no se encuentra incurso en ninguna de las causales de inhabilidad, incompatibilidad o

prohibición legal para contratar con el Estado establecidas en la Constitución Política, la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011 y demás normas concordantes.

10. **Suministro de Información y Trazabilidad:** Atender con diligencia, oportunidad y de forma escrita todos los requerimientos de información, aclaraciones, informes técnicos de incidentes de ciberseguridad o reportes de la consola FortiSIEM que sean solicitados por el supervisor del contrato o por los entes de control fiscal y disciplinario del Estado.
11. **Garantía Única de Cumplimiento:** Constituir a su costa, a favor de la IU Digital, la Garantía Única de Cumplimiento (Póliza de Seguros) que ampare los riesgos del contrato de acuerdo con los términos, porcentajes y vigencias exigidas en el pliego de condiciones y los estudios previos, procediendo a su correspondiente actualización o ampliación ante modificaciones en plazo o valor si a ello hubiere lugar.
12. **Confidencialidad y Reserva de la Información:** Guardar estricta reserva y confidencialidad sobre la información sensible de la universidad a la que tenga acceso por razón del servicio, incluyendo la arquitectura de red, direccionamiento IP, vulnerabilidades identificadas, contraseñas de acceso y bases de datos institucionales, obligándose a no divulgar, copiar, reproducir ni transferir dichos datos a terceros sin autorización expresa de la universidad.
13. **Uso de Canales y Herramientas Autorizadas:** Utilizar únicamente los canales formales de comunicación técnica establecidos en el protocolo de Kick-Off y reportar de manera oportuna a la Dirección de Tecnología cualquier anomalía o posible falla que pueda comprometer la estabilidad, rendimiento o seguridad del ecosistema digital de la universidad.

10.3. OBLIGACIONES DEL CONTRATANTE:

La Institución Universitaria Digital de Antioquia – IU Digital, en su calidad de entidad contratante, se compromete a cumplir rigurosamente con las siguientes obligaciones de carácter administrativo, financiero y técnico para garantizar el equilibrio contractual y la correcta ejecución del servicio tecnológico:

A. OBLIGACIONES DE GESTIÓN ADMINISTRATIVA Y FINANCIERA

1. **Gestión Presupuestal y del Gasto:** Realizar de manera oportuna todas las gestiones administrativas, presupuestales y financieras de su competencia para asegurar la debida apropiación, reserva y destinación de los recursos amparados en el **CDP No. 20260468**, garantizando el respaldo presupuestal del contrato.
2. **Trámite de Pago Único:** Cancelar al contratista el valor total del contrato correspondiente a **CIENTO OCHENTA Y CUATRO MILLONES DOSCIENTOS SETENTA Y CUATRO MIL SEISCIENTOS CUARENTA PESOS M/CTE ($184.274.640) IVA incluido**, bajo la modalidad de **Pago Único (100%)** con cargo a la vigencia fiscal actual, una vez el supervisor verifique y

apruebe las actas de entrega, los informes técnicos de inicio de operación y las certificaciones de activación del licenciamiento anual en la plataforma del fabricante.

3. **Designación de Supervisión Especializada:** Designar formalmente a un Profesional Especializado adscrito a la Dirección de Tecnología para que ejerza la supervisión del contrato, liderando las funciones de acompañamiento, vigilancia, control técnico y verificación de los hitos de integración y prestación del servicio del R-SOC.
4. **Verificación de Cumplimiento y Recibo a Satisfacción:** Comprobar la efectiva prestación del servicio tecnológico, el cumplimiento de los Niveles de Servicio (SLA) de notificación del SOC, y certificar mediante acta suscrita de forma conjunta el recibo a satisfacción de cada componente contratado.
5. **Exigibilidad Contractual:** Exigir al contratista la ejecución idónea, oportuna e ininterrumpida de todas y cada una de las obligaciones específicas asociadas a la renovación de FortiSIEM y soporte R-SOC 24/7/365.
6. **Notificación de Irregularidades:** Informar por escrito de manera inmediata y oportuna al contratista cualquier inconsistencia, anomalía, falla técnica o irregularidad detectada en el desarrollo de la ejecución o en el reporte mensual de incidentes.

B. OBLIGACIONES DE COOPERACIÓN TÉCNICA E INGENIERÍA

7. **Suministro Oportuno de Información e Infraestructura:** Facilitar al contratista el acceso seguro, oportuno y completo a la información técnica, topología de red, direccionamiento IP y plataformas preexistentes de la universidad que sean estrictamente necesarias para el despliegue físico de las integraciones de FortiNAC, FortiEDR y FortiMail Workspace Security.
8. **Establecimiento de Matrices de Comunicación:** Definir, entregar en la fase de Kick-Off y mantener actualizada una matriz de comunicaciones institucional en tres (3) niveles jerárquicos: **técnico-operativo, seguridad de la información y responsable administrativo del servicio**, especificando contactos de emergencia 24/7/365.
9. **Transferencia de Accesos Administrativos Temporales:** Proporcionar los accesos, privilegios y credenciales administrativas temporales sobre las consolas de la universidad en la medida en que sea estrictamente necesario para que el equipo de servicios profesionales del R-SOC configure los llamados API o Syslog del colector FortiSIEM. La universidad conservará en todo momento su autonomía y el control operativo global de red.
10. **Alineación y Cooperación en Incidentes:** Colaborar activamente con los ingenieros de ciberseguridad de la consola R-SOC en el análisis de alertas y triaje de incidentes de seguridad digital, proveyendo detalles oportunos de la red ante la detección de anomalías o vectores de ataque activos.
11. **Notificación de Pruebas de Red y Falsos Positivos:** Informar de manera anticipada y por escrito al contratista sobre la realización de pruebas de vulnerabilidad controladas,

auditorías éticas de hacking, escaneos internos o verificaciones de red planificadas por la universidad, con el propósito de que el SOC parametrice de forma transitoria las excepciones en el motor de correlación y evite la generación masiva de alertas o falsos positivos.

12. **Custodia de Copias de Seguridad (Backup):** Mantener un esquema robusto y autónomo de realización de copias de seguridad de sus bases de datos, sistemas de información y configuraciones de red en los medios de almacenamiento físico o nube que la universidad considere idóneos. El cliente es el directo responsable de la información que ingresa y procesa en sus sistemas.

C. DELIMITACIÓN Y RESPONSABILIDAD DE REMEDIACIÓN

13. **Mantenimiento y Ciclo de Vida de Plataformas Propias:** Garantizar que la infraestructura física y tecnológica propia de la IU Digital (incluyendo servidores on-premises, clúster de Firewalls físicos perimetrales **FortiGate 600E seriales FG6H0ETB20904804 y FG6H0ETB20904880**, y plataformas de AWS) se mantengan con alimentación eléctrica estable, ambiente adecuado de centro de datos, licenciamiento legítimo del fabricante y soporte técnico vigente. El contratista (UNE EPM) no será responsable de indisponibilidades ocasionadas por fallas de hardware perimetral o de energía de la universidad.
14. **Ejecución Autónoma de Remedias y Parches:** Asumir de forma exclusiva la responsabilidad material de aplicar y ejecutar las configuraciones, remediaciones de parches, hardening y recomendaciones operativas que el equipo de SOC/NOC de UNE EPM reporte para mitigar las vulnerabilidades identificadas. La no implementación de dichas recomendaciones exime de responsabilidad al proveedor frente a la materialización de un ataque derivado de dicha vulnerabilidad.
15. **Autorización Expresa de Acciones de Contención:** Evaluar y autorizar de forma inmediata al R-SOC la ejecución de tareas de contención remota de riesgos críticos que sean notificadas por el SOC. En caso de que la Dirección de Tecnología de la universidad no autorice las acciones preventivas sugeridas, el contratista queda exento de cualquier perjuicio o incidente de seguridad que se materialice de manera subsecuente.

11. PRODUCTOS:

Para efectos de control técnico, supervisión contractual, debida ejecución de los recursos públicos y viabilización del trámite de **Pago Único (100% de la vigencia fiscal actual)** amparado en el **CDP No. 20260468**, el **CONTRATISTA** se compromete a entregar a la Institución Universitaria Digital de Antioquia – IU Digital los siguientes productos formales como condición indispensable para la expedición de la certificación de recibo a satisfacción por parte de la supervisión:

PRODUCTO 1: Certificado de Licenciamiento Unificado y Reporte Oficial de Fábrica (Fortinet)

Documento o reporte original expedido de manera oficial directamente por el portal de licenciamiento del fabricante (**Fortinet Inc.**) a nombre de la **Institución Universitaria Digital de Antioquia** (NIT 901.168.222-9), que certifique fehacientemente la renovación, registro, activación y vigencia por doce (12) meses de las suscripciones y soportes especializados contratados. Este producto deberá acreditar documentalmente:

- **Activación de la Suscripción Central SIEM (Cantidad: 50):** Registro de las cincuenta (50) licencias anuales de **FortiSIEM All-In-One Subscription** (SKU FC1-10-FSM98-180-02-12) con capacidad de administrar un mínimo de 50 dispositivos y procesar hasta 10 Eventos por Segundo (EPS) por dispositivo.
- **Activación de Licencias de Agentes Avanzados (Cantidad: 50):** Registro de cincuenta (50) licencias de suscripción **FortiSIEM Subscription para Agentes Avanzados** (Log & FIM, SKU FC1-10-FSM98-182-02-12).
- **Vigencia del Soporte Corporativo (Cantidad: 1):** Soporte técnico de fábrica por doce (12) meses de **FortiCare Premium** para despliegues de software FortiSIEM (SKU FC2-10-FSM97-248-02-12).
- La asignación formal y exclusiva de los derechos de uso del software a nombre de la universidad en el centro de soporte del fabricante.

PRODUCTO 2: Informe Técnico de Aprovisionamiento de Infraestructura Cloud de Ciberseguridad

Informe de ingeniería especializada detallado que documente el aprovisionamiento, conectividad y estado inicial de los servicios de nube dedicada y telecomunicaciones en el **Data Center físico de Tigo**. El informe deberá contener como mínimo:

- **Aprovisionamiento de Cómputo Cloud (Collector VM):** Detalle técnico de la arquitectura aprovisionada en el Virtual Data Center (VDC), con especificaciones de los recursos virtuales que hospedan la consola centralizada de seguridad FortiSIEM All-In-One.
- **Malla de Seguridad perimetral (VDOM Dedicada):** Configuración y políticas aplicadas sobre el entorno de red virtual, detallando los módulos de alta disponibilidad (HA), Firewall Cloud (30 Mbps, 6.000 sesiones concurrentes, 10 reglas de control de acceso) e IDS/IPS Cloud (módulos perimetrales con 2 perfiles de inspección profunda).

- **Transporte Seguro de Logs (Enlaces y VPN):** Documentación técnica del enrutamiento de red perimetral que soporte la interconexión de dos (2) túneles seguros **VPN Site-to-Site (IPSec) dedicados** y de un canal de **Internet Dedicado de 30 Mbps** para la recepción continua de logs de eventos en el colector.

PRODUCTO 3: Informe Técnico de Integración e Ingesta de Telemetría (2.700 Agentes/Buzones)

Documento de ingeniería detallado que contenga la memoria técnica de integración y la evidencia de recepción, parsing y normalización en la base de datos de CMDB del SIEM de las tres plataformas de origen preexistentes de la universidad:

- **FortiNAC (1.000 agentes concurrentes):** Configuración e integración de las dos (2) consolas virtuales de control y aplicación FNC-CAX-VM.
- **FortiEDR (1.000 endpoints):** Integración API/SaaS para la ingesta de telemetría de 1.000 agentes de endpoints corporativos.
- **FortiMail Workspace Security (700 cuentas de correo):** Integración Syslog/API de la consola SaaS para 700 buzones de correo en Google Workspace.
- **Mapeo de Telemetría Externa Adicional:** Evidencia de la ingesta de logs del clúster físico de Firewalls **FortiGate 600E (seriales unívocos FG6H0ETB20904804 y FG6H0ETB20904880)** de propiedad de la universidad, así como de los **quince (15) servidores on-premises** y **dos (2) máquinas virtuales en AWS**.

PRODUCTO 4: Documento de Diseño de Bajo Nivel (LLD) de Ciberseguridad, Reglas y Analítica

Documento técnico de diseño de bajo nivel (**Low Level Design - LLD**) que registre la lógica analítica configurada de manera exclusiva en el FortiSIEM de la IU Digital:

- **Configuración de Nueve (9) Casos de Uso Personalizados en el Rule Engine (3 por tecnología):**
  - *FortiNAC:* Rogue/Unregistered Device en VLAN (UC-NAC-01), Quarantine/Compliance Fail de host (UC-NAC-02), Masive 802.1X Auth anomalies (UC-NAC-03).
  - *FortiMail:* Spear Phishing campaigns (UC-MAIL-01), Malicious attachment sandbox detection (UC-MAIL-02), SPF/DKIM/DMARC anomalies (UC-MAIL-03).
  - *FortiEDR:* Blocked Malware con Device/User Risk Score (UC-EDR-01), Ransomware/File System spikes (UC-EDR-02), Off-net Infected Host (UC-EDR-03).

- **Tres (3) Reportes Analíticos Personalizados:** Estructura técnica de un reporte analítico mensual unificado tipo *Analytics Query* por cada una de las tecnologías integradas.
- **Un (1) Dashboard Personalizado:** Diseño de la consola visual unificada en tiempo real con **nueve (9) widgets** consolidados.
- **Una (1) Política de Automatización y Alerta:** Configuración técnica de la política de notificación inmediata por correo electrónico para alertas catalogadas como críticas.

PRODUCTO 5: Informe de Inicio de Operación R-SOC, Protocolos de Escalado y Niveles de Servicio (SLA)

Documento formal expedido por el área de operaciones del contratista que certifique la activación del monitoreo administrado en el Centro Regional de Operaciones de Seguridad (R-SOC). Deberá contener:

- **Esquema Operativo R-SOC:** Definición de los canales de atención remota, telefónica y de correo (24/7/365), y la matriz de contactos técnicos y de escalamiento en tres niveles de ingeniería (Niveles 1, 2 y 3).
- **Acuerdos de Nivel de Servicio (SLA):** Certificación formal de los tiempos objetivos para la atención de fallas (atención inmediata con resolución en 4 horas para criticidad Significativa) y el compromiso de notificación de incidentes de riesgo significativo en un tiempo **máximo de treinta (30) minutos**.
- **Certificados de Calidad del SOC:** Copias de los certificados vigentes del R-SOC bajo estándares internacionales **ISO 27001** (Sistemas de Gestión de Seguridad de la Información) e **ISO 20000-1** (Gestión de Servicios de TI).

PRODUCTO 6: Certificación de Transferencia de Conocimiento y Bitácora de Estabilización

Informe que acredite la fase final de transferencia y afinamiento técnico del servicio:

- **Acta de Transferencia de Conocimiento:** Constancia de la sesión técnica de capacitación y transferencia (duración mínima de **dos (2) horas**) dirigida al personal técnico de la Dirección de Tecnología, cubriendo la navegación de eventos en FortiSIEM, visualización de tableros, generación de reportes e interpretación analítica de alertas.
- **Bitácora de Afinamiento y Acompañamiento Remoto:** Registro de la ejecución de las dos (2) sesiones de tuning (un total de 4 horas dentro de los primeros 15 días posteriores a la salida a producción) orientadas a mitigar falsos positivos, junto con la evidencia del

soporte técnico de acompañamiento por **quince (15) días calendario** posteriores a la implementación.

PRODUCTO 7: Notificación Oficial de Entrega de Solución y Acta de Recibo a Satisfacción

Documentos formales que legalizan la terminación de la fase de despliegue e inicio de la operación continua:

- **Notificación de Entrega:** Comunicación formal y detallada del contratista informando la entrega funcional y estabilidad técnica de la infraestructura cloud, licenciamiento e integraciones realizadas.
- **Acta de Recibo a Satisfacción:** Documento oficial del proceso debidamente suscrito de forma conjunta por el contratista (UNE EPM) y el supervisor de la IU Digital (adscrito a la Dirección de Tecnología). En esta acta se dejará constancia unívoca de que las licencias se activaron, la infraestructura opera de forma óptima en el Data Center de Tigo, las integraciones se completaron a cabalidad, el R-SOC se encuentra monitoreando activamente 24/7/365 y el flujo de telemetría hacia FortiSIEM opera con absoluta estabilidad sin generar reprocesos técnicos en la red perimetral e institucional preexistente.

12. SUPERVISIÓN:

La supervisión del contrato será ejercida por un **Profesional Especializado** o quien haga sus veces, adscrito a la **Dirección de Tecnología**, o en su defecto la persona que mediante comunicación interna designe el ordenador del gasto, quien deberá dar cumplimiento a lo establecido en el artículo 83º y siguientes de la Ley 1474 de 2011 y las demás que la modifiquen, adicionen o complementen, expedida por la Institución.

13. CARGAS ADMINISTRATIVAS:

El contratista asumirá el valor de las pólizas, garantías y demás gastos administrativos relacionados con la ejecución del contrato.

14. CARGAS TRIBUTARIAS:

En razón a la ejecución del contrato a celebrar, el contratista deberá asumir todas las cargas tributarias que se generen con ocasión de la celebración del contrato tales como retención en la fuente, RETEICA, RETEIVA y demás a que haya lugar y esté obligado según las disposiciones legales vigentes.

15. ESTIMACIÓN, TIPIFICACIÓN Y ASIGNACIÓN DE RIESGOS:

De conformidad con lo establecido en el artículo 4 de la Ley 1150 de 2007 y lo establecido en el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015, se presenta el análisis del riesgo y la forma de mitigarlo en el presente proceso de contratación.

El análisis de la identificación, clasificación, evaluación, calificación, asignación, tratamiento y monitoreo de los riesgos se elaboró con base en el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación, expedido por Colombia Compra Eficiente.

Ver anexo 1 Matriz de riesgo.

16. ANÁLISIS DE MECANISMOS DE COBERTURA DEL RIESGO:

Buscando minimizar cualquier perjuicio que pudiera sufrir la Institución Universitaria Digital de Antioquia, derivado de las obligaciones surgidas en la ejecución del presente contrato, en la etapa de planeación del proceso se realizó un análisis del objeto, valor, obligaciones y de los riesgos previsibles contemplados en la matriz del contrato.

En virtud de lo anterior, se estima necesario la exigencia de garantías que aseguren el cumplimiento del contrato de conformidad con lo establecido en el Decreto Reglamentario 1082 de 2015, así:

Descripción Amparo	%	Duración Adicional	Período
De Cumplimiento del Contrato y Cláusula Penal	10,00	6	MESES
De Calidad del Servicio	10,00	6	MESES

Estas pólizas deben allegarse dentro de los tres (3) días calendario siguientes a la suscripción del contrato.

Las pólizas exigidas deberán tener como beneficiarios y asegurados a la Institución Universitaria Digital de Antioquia – IU. Digital.

17. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN O FORMA DE CONTRATACIÓN:

Teniendo en cuenta la naturaleza jurídica del contrato a celebrar y el análisis de las necesidades operativas de la Dirección de Tecnología, la modalidad de selección que corresponde adelantar es la de **Contratación Directa**, fundamentada en la causal de **"Prestación de Servicios Profesionales y de Apoyo a la Gestión"**, de conformidad con lo establecido en el **literal h) del numeral 4 del artículo 2 de la Ley 1150 de 2007**, siguiendo las reglas señaladas en el **artículo 2.2.1.2.1.4.9. del Decreto Reglamentario 1082 de 2015**.

A continuación, se exponen de manera rigurosa los pilares normativos, doctrinarios y fácticos que amparan la legalidad de esta selección directa con una persona jurídica de derecho privado:

17.1. Habilitación Normativa de la Causal de Apoyo a la Gestión

El **artículo 2.2.1.2.1.4.9 del Decreto 1082 de 2015** faculta expresamente a las Entidades Estatales para hacer uso de esta modalidad bajo los siguientes parámetros sustanciales:

> *"Las Entidades Estatales pueden contratar bajo modalidad de contratación directa la prestación de servicios profesionales y de apoyo a la gestión con la **persona natural o jurídica** que esté en capacidad de ejecutar el objeto del contrato, siempre y cuando la Entidad Estatal verifique la **idoneidad o experiencia requerida y relacionada** con el área de que se trate. En este caso, no es necesario que la Entidad Estatal haya obtenido previamente varias ofertas, de lo cual el ordenador del gasto debe dejar constancia escrita. Los servicios profesionales y de apoyo a la gestión corresponden a aquellos de naturaleza intelectual diferentes a los de consultoría que se derivan del cumplimiento de las funciones de la Entidad Estatal; así como los relacionados con **actividades operativas, logísticas o asistenciales**…".*

De la norma citada se desprenden tres reglas de oro aplicables a este proceso:

1. **Habilitación Subjetiva Amplia:** Permite contratar de manera directa tanto a personas naturales como a **personas jurídicas** (como lo es **UNE EPM Telecomunicaciones S.A.**).
2. **Exención de Pluralidad de Ofertas:** Se exceptúa la obligación de tramitar y comparar múltiples cotizaciones o propuestas competitivas, bastando con la constancia escrita del ordenador del gasto sobre la idoneidad y conveniencia del contratista seleccionado.
3. **Inclusión de Labores Asistenciales:** Clasifica de forma inequívoca el soporte operativo y logístico de la administración dentro del concepto de apoyo a la gestión.

17.2. Delimitación Jurisprudencial del Apoyo a la Gestión (El "Hacer Material")

Para definir el alcance y alcance material del apoyo a la gestión, la jurisprudencia de unificación del **H. Consejo de Estado**, mediante la **Sentencia SU 41.719 de 2013**, determinó que este tipo de contratos:

> *"(…) conforme se deduce del análisis a la ley de contratación pública, son todos los demás contratos de prestación de servicios permitidos por el artículo 32 No. 3 de la Ley 80 de 1993 que no correspondan a los profesionales, esto es, que involucren cualesquiera otras actividades también identificables e intangibles que evidentemente sean requeridas por la entidad estatal y que impliquen el desempeño de un esfuerzo o actividad (de) **apoyo, acompañamiento, o soporte**, de lo cual se puede deducir que caben actividades no propiamente intelectuales sino más bien*

*caracterizadas por la **acción material del contratista**, en donde no es que el contratista no piense, sino que lo **predominante de su actividad es el actuar como ejecutor**, con el propósito y finalidad de satisfacer necesidades de las entidades estatales en lo relacionado con la **gestión administrativa o funcionamiento** de la misma.”*.

17.3. Subsunción Técnica y Operativa del Objeto Contractual

A la luz de la norma y la jurisprudencia de unificación, el objeto del presente proceso (que integra la renovación de licenciamiento FortiSIEM, soporte FortiCare Premium, Virtual Data Center dedicado en Tigo, monitoreo SOC 24/7/365 e integración especializada de las fuentes FortiNAC, FortiEDR y FortiMail) **no se configura como una adquisición abstracta de activos de software (suministro) ni como un arrendamiento civil independiente**, sino como un **servicio integrado de apoyo a la gestión tecnológica**.

Lo predominante en la ejecución de este contrato es la **acción material y asistencial de ingeniería continua** que prestará el contratista. El contratista actuará como el **brazo operativo ejecutor** de la Dirección de Tecnología, coadyuvando de forma directa a la vigilancia y defensa perimetral del ecosistema 100% virtual a través del cual la IU Digital garantiza el servicio público de educación superior. Carecer de la infraestructura del R-SOC o de las actividades logísticas de integración de los 2.700 agentes colocaría a la universidad en una situación de parálisis administrativa y desprotección perimetral absoluta, lo que justifica catalogar el objeto bajo esta tipología asistencial.

17.4. Verificación de Capacidad Jurídica, Duración, Idoneidad y Experiencia del Contratista

De acuerdo con el **artículo 6 de la Ley 80 de 1993** (modificado por el **artículo 1 de la Ley 2160 de 2021**), las personas jurídicas que contraten con el Estado deben acreditar que su duración institucional no será inferior a la del plazo del contrato y un año más. Al revisar los soportes del expediente, se verifica el cumplimiento pleno de este y otros requisitos habilitantes en cabeza de **UNE EPM TELECOMUNICACIONES S.A.**:

- **Capacidad y Duración:** De acuerdo con su Certificado de Existencia y Representación Legal de la Cámara de Comercio de Medellín, la compañía cuenta con una duración ilimitada y su objeto social principal se encuentra directamente relacionado con la provisión de telecomunicaciones, hosting y tecnologías de la ciberseguridad.
- **Naturaleza Societaria:** Está registrada ante el SECOP II como una **Sociedad Anónima Cerrada Colombiana** de carácter comercial privado, con RUT activo bajo la calidad de **Gran Contribuyente** con domicilio principal en Medellín.
- **Paz y Salvo Parafiscal:** Se acredita que se encuentra al día con la totalidad de sus obligaciones parafiscales y del Sistema de Seguridad Social Integral (SENA, ICBF, Salud,

Pensión y Riesgos), debidamente certificado por su Revisor Fiscal delegado de la firma **KPMG S.A.S.** con corte a la vigencia actual.

- **Idoneidad y Experiencia Relacionada Unívoca:** El contratista demuestra una idoneidad técnica única e insustituible para esta gestión. Actúa como el **integrador tecnológico histórico de la universidad**, habiendo diseñado e implementado el clúster perimetral físico HA compuesto por los dos (2) firewalls **FortiGate 600E (seriales unívocos FG6H0ETB20904804 y FG6H0ETB20904880)** propiedad de la IU Digital, así como el Virtual Data Center (VDC) donde reside el FortiSIEM.
- **Trazabilidad Convencional Histórica:** Esta relación contractual se ha perfeccionado históricamente a través del **Convenio Marco de Cooperación No. IUD2019051**, el cual fue objeto de una **Prórroga No. 02** aprobada de forma bilateral para extender su vigencia general por el término de **tres (3) años, contados a partir del 13 de febrero de 2025**. Si bien el cambio en la naturaleza jurídica de UNE EPM (sociedad cerrada de derecho privado) impide jurídicamente recurrir a la figura del Convenio Interadministrativo directo para esta ejecución de recursos de la vigencia 2026 amparados en el **CDP No. 20260468**, la idoneidad y el conocimiento técnico de la red institucional permanecen inalterados, validando plenamente la contratación directa de apoyo a la gestión con esta persona jurídica para proteger las inversiones del Estado y asegurar la continuidad operativa.

18. CLÁUSULA DE CONFIDENCIALIDAD

Quien suscriba el contrato deberá manifestar que es jurídicamente capaz de salvaguardar la información recolectada y suministrada a la Entidad, obligando a: 1. Guardar confidencialidad sobre los mecanismos, y sistemas de información que le brinda la Entidad; 2. Reconocer y dar manejo adecuado a la información recolectada en desarrollo del objeto contractual; 3. Responsabilizarse por la información suministrada; 4. Suministrar información veraz, completa y correcta, lo cual lo responsabiliza ante el Institución y ante terceros por inexactitudes, errores o falsedad en desarrollo de las diferentes actuaciones.

19. PROPIEDAD INTELECTUAL

El presente contrato comporta actuaciones meramente mecánicas sin dar lugar a la generación de creaciones intelectuales por parte de EL CONTRATISTA. EL CONTRATISTA reconoce que esta actividad no le hace partícipe de ningún derecho de propiedad intelectual reconocido o que pudiera ser reconocido sobre los derechos de la IU DIGITAL. EL CONTRATISTA sólo podrá utilizar las marcas y demás signos distintivos de la IU DIGITAL con el fin de cumplir el objeto de este contrato conforme las normas del Manual de Identidad Visual de estas. Finalizado el plazo contractual o terminado el Contrato por cualquiera de las causas previstas en este, se extingue la autorización de uso de los signos distintivos de la IU DIGITAL. EL CONTRATISTA queda obligado a realizar las actividades objeto de este contrato sin que ello implique un menoscabo en la

reputación de las marcas y signos distintivos de LA IU. DIGITAL, así como los valores que ésta propugna.

En virtud del presente contrato no tiene lugar ningún tipo cesión o transferencia de derechos de propiedad intelectual generados con ocasión de este contrato a favor de ninguna de Las Partes, ni de terceros. Las Partes acuerdan que cada una conservará la plena propiedad y titularidad sobre su Propiedad Intelectual y ninguna de Las Partes estará autorizada o facultada para obstaculizar el ejercicio de los derechos que cada una tiene sobre aquélla.



Jessica Andre Agudelo Vélez
Directora de Tecnología (E)

Acción	Nombre	Fecha
Proyectó y Elaboró:	Juan Pablo Montoya	20/08/2026
Revisó:	Cesar Alexander Zapata Jimenez	21/08/2026
Revisó:	Manuela Villa Morales	21/08/2026
Revisó y Aprobó:	Jessica Andre Agudelo Vélez	21/08/2026
Los anteriores, declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por lo tanto, bajo nuestra responsabilidad presentamos para firma.		