



EMPRESA PARA LA SEGURIDAD URBANA - ESU

NIT 890.984.761-8

CONTRATO No.

201700333

CONTRATISTA		NIT	TELÉFONO	FECHA DE SUSCRIPCIÓN	
COLOMBIA TECNOLÓGICA SAS - COLTECNO SAS		900.488.849-5	(1)7037812	27/11/2017	
REPRESENTANTE LEGAL		CÉDULA	DIRECCIÓN DE CONTACTO		TEL./CEL. CONTACTO
LILIAN-ALEXANDRA GRISALES JUNCA		52.388.684	AVENIDA CARRERA 15 # 119 - 43 OFICINA 510		(1)7037812
CORREO ELECTRÓNICO		CIUDAD DE EJECUCIÓN	RADICADO REQUERIMIENTO	BIENES O SERVICIOS	DISPONIBILIDAD PRESUPUESTAL
info@coltecno.com.co		Medellín	2017006492	Bienes	2017000841
CONVENIO	CENTRO DE COSTOS	RÚBRO PRESUPUESTAL	DESCRIPCIÓN RÚBRO	VALOR CONTRATO	COMPROMISO PRESUPUESTAL
4600069558 de 2017	31512	33000218-1	Sostenimiento sistema 123	\$13.511.252	2017001978

Entre los suscritos, **GABRIEL IGNACIO NANCLARES QUINTERO**, identificado con cédula de ciudadanía No. 8.431.074, actuando en su calidad de Secretario General de la **EMPRESA PARA LA SEGURIDAD URBANA - ESU**, con NIT. 890.984.761-8, empresa industrial y comercial del Estado del orden municipal, dotada de personería jurídica, autonomía administrativa y financiera y patrimonio propio e independiente creada por el Decreto Ley 178 del 20 de febrero de 2002, modificado por el Acuerdo 33 de 2010, nombrado mediante Resolución 094 de enero 25 de 2016, facultado por el Reglamento de Contratación de la **EMPRESA PARA LA SEGURIDAD URBANA - ESU**, adoptado mediante Acuerdo 055 de 2014, modificado por el Acuerdo 077 de 2017, quien en adelante se denominará la **ESU**, de una parte y de la otra parte **LILIAN ALEXANDRA GRISALES JUNCA**, identificada con cédula de ciudadanía 52.388.684, actuando en nombre y representación legal de **COLOMBIA TECNOLÓGICA S.A.S. - COLTECNO S.A.S** con NIT 900.488.849-5, en calidad de **CONTRATISTA**, con el objeto de celebrar el presente contrato, previas las siguientes:

#### CONSIDERACIONES

1. Que la Empresa para la Seguridad Urbana - ESU, que hace parte de la estructura orgánica de la Alcaldía de Medellín, suscribió el contrato interadministrativo No. 4600069558 de 2017, con el objeto de realizar administración delegada de recursos para el sostenimiento y mantenimiento del Sistema Integrado de Emergencia y Seguridad Metropolitano -SIES - M.

2. Que en el marco del contrato interadministrativo de mandato de administración delegada de recursos, se requirió a la ESU adquirir cuatro (4) Access point para dar acceso de conectividad a las salas de crisis, sala auxiliar, sala de despacho, auditorio y salas de reuniones del SIES – y la Secretaría de Seguridad y Convivencia del Municipio de Medellín.
3. Que de conformidad con lo establecido en el contrato interadministrativo y en aplicación de las disposiciones del Reglamento Interno de Contratación de la ESU, se convocó la Solicitud Privada de Ofertas – SPVA 2017-101.
4. Que se recibió propuesta por parte de COLOMBIA TECNOLÓGICA SAS – COLTECNO SAS, COLOMBIA TELECOMUNICACIONES S.A. E.S.P. UNE EPM TELECOMUNICACIONES S.A y SMART INGENIERÍA DE COLOMBIA SAS. Las cuales fueron verificadas por el comité de contratación, encontrándose ajustada la propuesta de COLOMBIA TECNOLÓGICA SAS – COLTECNO SAS
5. Que mediante Comité de contratación del 22 de Noviembre de 2017, se recomendó la selección de la propuesta presentada por COLOMBIA TECNOLÓGICA S.A.S. – COLTECNO SAS, por lo que a través del presente instrumento se formaliza la contratación, que se registrá por las siguientes cláusulas:

**OBJETO:** El contratista se obliga con la ESU a suministrar cuatro (4) access point para la Secretaría de Seguridad y Convivencia del Municipio de Medellín; de conformidad con las cantidades y especificaciones mínimas establecidas en los términos y condiciones de contratación y la propuesta presentada por el contratista y aceptada por la ESU, documentos que hacen parte integrante del contrato.

1. **ALCANCE DEL OBJETO:** El objeto de la presente solicitud privada de oferta de mínima cuantía, comprende el suministro cuatro (4) Access point, los cuales deben cumplir con al menos los siguientes requerimientos técnicos:

REQUERIMIENTOS TECNICOS MÍNIMOS
<p>Estándares de red:</p> <ul style="list-style-type: none"> <li>• IEEE 802.11b</li> <li>• IEEE 802.11g</li> <li>• IEEE 802.11n</li> <li>• IEEE 802.11ac</li> </ul> <p>Bandas de radio frecuencia:</p> <ul style="list-style-type: none"> <li>• 2,4 y 5 GHz</li> </ul> <p>Puertos:</p> <ul style="list-style-type: none"> <li>• 1 Gigabit WAN (10/100/1000)</li> </ul> <p>Temperatura de funcionamiento: Entre 0 y 40 °C</p> <p>Humedad de funcionamiento: Entre 10 y 80 % sin condensación</p> <p>Garantía limitada de 1 año para hardware</p> <p>Tasa de enlace máxima: 1300 Mbps</p> <p>Compatibilidad con plataformas:</p> <p>Windows XP, Vista, 7, 8, 10 (32/64 Bits), Sistemas Operativos MAC</p> <p>Interfaz de Radio Frecuencia: Un radio a 2.4GHz 802.11b/g/n y uno a 5GHz 802.11a/n</p>



- Un radio a 2.4GHz 802.11b/g/n y uno a 5GHz 802.11a/n/ac
  - Un radio dedicado para funciones de Prevención de Intrusos Inalámbricos (WIPS) y análisis de espectro en ambas bandas
  - Banda de operación en 2.412-2.484GHz y 5.150-5.250GHz (UNII-1), 5.250-5.350 GRZ (UNII-2), 5.470-5.600, 5.660-5.725 GHz (UNII-2e) y 5.725-5.825GHz (UNII-3)
  - Antena integrada al chasis del tipo omnidireccional con ganancia de 5dBi@2.4GHz y 5.5dBi@5GHz
  - Arreglo MIMO 3x3 con tres tramas espaciales (spatial streams)
  - La solución deberá contar con la funcionalidad de selección de la banda de operación por cada SSID:
    - Modo dual, publicando el SSID en ambas bandas, 2.4 y 5GHz
    - 5GHz únicamente
    - Ambas bandas pero con la capacidad de detectar dispositivos que soporten ambas bandas, direccionándolos a la de 5GHz por estar menos congestionada
  - Ancho de banda de canales de 20 y 40MHz y 80MHz
  - Tasa de datos combinada de 1.9Gbps
  - Soporte de especificación 802.11ac Wave 2 MU-MIMO
  - Soporte de Maximal Ratio Combining (MRC)
  - Formación de haz (beamforming)
  - Agregación de paquetes
  - Soporte a Cyclic Shift Diversity (CSD)
- Interfaz alámbrica de red:
- Una interfaz 100/1000Base-T (RJ-45) con soporte a 48V DC 802.3af para PoE
  - VLAN tagging basado en IEEE802.1q
  - Cada Access Point deberá soportar los siguientes esquemas de direccionamiento IP:
    - Modo NAT, donde los usuarios pueden recibir una dirección directamente desde el Access Point, a fin de ahorrar direcciones IP privadas de la red local, o prescindir de un servidor DHCP
    - Modo Bridge, donde el Access Point releven los mensajes de DHCP desde un servidor superior, haciendo a los usuarios móviles parte de la LAN
    - Roaming de capa 3 (L3), que permita al usuario mantener la misma dirección IP en caso de cambio de segmento de red (por ejemplo al desplazarse entre pisos distintos), manteniendo la sesión activa todo el tiempo

**Gestión:**

- Gestión centralizada desde una consola basada en web, accesible desde cualquier dispositivo con acceso a Internet
- Firewall para bloqueo de tráfico a nivel del punto de acceso
- Modelado de tráfico para asignación diferenciada de límites de ancho de banda por aplicación y/o servicio por dispositivo conectado, y/o por red inalámbrica en servicio.
- Prevención de intrusos en el canal inalámbrico y detección de interferencia en las bandas de operación mediante un tercer radio de monitoreo dedicado para funciones de monitoreo, permitiendo así que no se sacrifique desempeño para los clientes inalámbricos
- Gestión centralizada desde una consola de administración basada en Web fuera de banda, desde la cual se deberá poder acceder, configurar y monitorear, todos los equipos WLAN considerados en este proceso.
- De igual manera, desde la misma consola de administración basada en Web, se deberán poder generar los reportes de operación correspondientes a todos los equipos WLAN
- La consola deberá ser accesible desde cualquier equipo que cuente con conexión a Internet tanto al interior como al exterior de las instalaciones de la ESU, soportando cualquier navegador de Internet disponible en el mercado

- El acceso a la consola de administración se deberá realizar mediante un método de autenticación de dos factores (two-factor), incluyendo, mas no limitando, a nombre de usuario, contraseña y soft-token en dispositivos móviles y/o computadoras personales, validando además que el acceso se realice mediante equipos de cómputo autorizados, mediante el envío de un correo electrónico o SMS con un código de validación
- El acceso a la consola de gestión deberá ser por HTTPS (puertos 8080 y 443) y sus certificados de seguridad deberán ser emitidos por entidades reconocidas en Internet
- La consola de administración deberá soportar la definición de cuentas de administrador basadas en roles; reportando cambios a las mismas en una bitácora de eventos (logs) y alertas, que se podrán consultar por medio de la misma consola

**Calidad de Servicio:**

- Calidad de Servicio en el canal inalámbrico basado en WMM/802.11e
- Soporte de DSCP 802.1p
- Modelado de tráfico a nivel de capa 7 (L7)
  - Mediante la consola de administración y sin necesidad de agregar un equipo externo adicional, se debe soportar la capacidad de restringir o abrir el ancho de banda por usuario y por SSID de manera simétrica (mismo ancho de banda de bajada y de subida) o asimétricamente (diferente ancho de banda a la bajada respecto a la subida), dentro de las capacidades de la salida a Internet del sistema.
  - La asignación de ancho de banda mediante el modelado de tráfico, deberá poderse definir mediante dos mecanismos:
    - Manual
      - Rangos CIDR/IP
      - hostname (URL)
      - Puertos UDP/TCP
      - Combinación de Red, Subnet y puerto
      - Red local (subredes y redes de clase completa en la LAN)
    - Mediante categorías de tráfico
      - Blogging
      - Email
      - Compartición de archivos
      - Juegos
      - Noticias
      - Respaldo en línea
      - Peer-to-peer
      - Redes sociales y compartición de fotos
      - Actualizaciones de programas y antivirus
      - Deportes
      - VoIP y videoconferencia
      - Compartición de archivos vía web
  - La política de modelado de tráfico deberá permitir la asignación simétrica o asimétrica de los límites de ancho de banda por aplicación a nivel global, por usuarios y por grupo de usuarios
  - Igual manera, mediante la política de modelado de tráfico deberá poder priorizarse cierto tipo de tráfico y asociarse a una etiqueta de QoS mediante DSCP con al menos 4 clases de servicio (Best Effort, Background, Video y Voz)

### Servicios de seguridad

La solución de Red Inalámbrica debe de incluir las siguientes funcionalidades de seguridad:

#### Firewall

- a) La solución inalámbrica de red deberá soportar la definición de reglas de firewall de capa 3 y capa 7 independientes por cada SSID habilitado en la red.
- b) Mediante las reglas de capa 3, se definirán políticas de acceso por:
  1. Protocolo (UDP o TCP)
  2. Host, subred o red origen
  3. Puerto TCP o UDP origen
  4. Host, subred o red destino
  5. Puerto TCP o UDP destino
- c) Mediante las reglas de capa 7, se deberá soportar la restricción de tráfico a partir de categorías definidas, entre ellas:
  1. Blogging
  2. Email
  3. Compartición de archivos
  4. Juegos
  5. Noticias
  6. Respaldo en línea
  7. Peer-to-peer
  8. Redes sociales y compartición de fotos
  9. Actualizaciones de programas y antivirus
  10. Deportes
  11. VoIP y videoconferencia
  12. Compartición de archivos vía web
- d) Políticas basadas en identidad

La solución propuesta deberá permitir la asignación de políticas individuales de acuerdo a la identidad de los usuarios conectados a la red interna, a partir de su dirección MAC, dirección IP, nombre de la computadora, así como nombre del usuario en el Active Directory, LDAP o credenciales de RADIUS.

- e) Políticas basadas en grupos
  - Políticas de firewall específicas para grupos deberá esta soportada por la solución propuesta.
  - Los políticas podrán ser aplicadas directamente a un usuario para indicar su pertenencia a ese grupo, o bien podrán descargarse la información de grupos declarados en el controlador de dominio de la red interna
- f) Control de acceso a la red inalámbrica: La solución deberá soportar la creación de 15 SSIDs

como máximo, permitiendo para cada uno los siguientes métodos de acceso:

- Abierta y sin encriptación para eventos abiertos al público en general, Cualquier persona puede asociarse con su dispositivo
- Llave compartida con anterioridad (Pre-Shared key) con WPA2
- Control de acceso basado en dirección MAC mediante autenticación Radius
- WPA2-Enterprise, donde las credenciales de los usuarios se validan con 802.1x, con las siguientes opciones de autenticación:
  1. Un servidor RADIUS incluido en la misma solución
  2. Un servidor RADIUS externo, contra una base de datos genérica de usuarios o bien integrada con Active Directory y/o LDAP
- Acceso vía portal captivo (splash page), que permita habilitar los siguientes métodos de autenticación, conforme lo requiera la ESU
  1. Portal captivo directo, donde no se requieren credenciales de usuario, pero que permite desplegar un mensaje de bienvenida previo al acceso a Internet del usuario
  2. Portal "Click-through", donde el usuario debe ver un portal de bienvenida y dar "click" a un botón para continuar su acceso
  3. Portal captivo tipo "sign-on", donde se le requiera al usuario sus credenciales de usuario y contraseña para su autenticación por cualquiera de los siguientes métodos:
    - a. Un servidor RADIUS interno a la solución propuesta
    - b. Un servidor RADIUS externo hospedado en alguna localidad de la entidad
    - c. Autenticación hacia una base de datos de Directorio Activo de la entidad
    - d. Autenticación mediante credenciales de Facebook para eventos especiales, donde el portal captivo habilitado, será la página de fan de la entidad en dicha red social
- Con excepción de la autenticación portal captivo deberá ser personalizable en formato, permitiendo la adición de logos corporativos, mensajes customizados, etc.
- De igual manera, se deberá contar con la funcionalidad de Walled Garden, que permita el acceso a direcciones públicas y/o dominios de Internet específicos, previos a la autenticación del cliente
- De acuerdo a lo que requiera la ESU, la solución deberá permitir o bloquear el tráfico no-HTTP

g) Control de acceso a la red (Network Access Control)

La solución deberá contar con la opción de verificación de la presencia de un software para la detección de antivirus actualizado en el dispositivo de usuario, previo a su autenticación a la red

h) Asignación de políticas de acceso por tipo de dispositivo

De acuerdo con el tipo de dispositivo y/o sistema operativo (Android, Blackberry, Chrome OS, iPad, iPhone, iPod, , MacOS X, Windows, Windows phone o cualquier otro sistema operativo), se podrá colocar en una lista blanca o una lista negra para permitir o bloquear el acceso

i) Filtrado de Contenido

La solución deberá incluir en los mismos dispositivos, la funcionalidad de filtrado parcial de contenido para la categoría de Sitios de Adultos como mínimo, sin requerir para tal efecto añadir una solución de seguridad externa

**j) Detección y Prevención de Intrusos en el Canal Inalámbrico**

- La solución de red inalámbrica, deberá contar con un sistema de defensa y análisis de interferencia que tenga por funcionalidades las siguientes:
  - i. Escaneo en tiempo real de interferencia en los canales de las bandas de 2.4 y 5GHz
  - ii. Deberá descargar desde la consola central las últimas actualizaciones en firmas de ataques
  - iii. Deberá habilitar políticas de detección y remediación granulares sobre la misma consola de gestión de la solución
  - iv. El WIPS deberá estar basado en un motor heurístico que permita detectar los ataques más sofisticados; mediante el monitoreo de las tramas de administración y mediante la inspección del tráfico inalámbrico de clientes, incluyendo los probe requests y paquetes de desasociación e identificar las variantes a partir del comportamiento normal
  - v. Deberá identificar y organizar las siguientes categorías de ataques como mínimo:
    1. SSIDs no autorizados
    2. Intentos de robo de identidad (spoofs) del AP
    3. Inundación de paquetes que tengan como finalidad generar eventos de negación de servicio (DoS)
  - vi. Para efectos de remediar los ataques, la solución deberá permitir la configuración de la contención de ataques basados en políticas, así como en patrones como el nombre exacto o similar del SSID
  - vii. Deberá notificar de eventos de seguridad a los administradores de la red por medio de correo electrónico

**Reportes y monitoreo**

- Con la finalidad de mantener visibilidad sobre la infraestructura instalada, la solución deberá incluir dentro de la misma consola de gestión, un inventario de equipo: tanto operativo como desconectado, accesible para los administradores de la red
- La solución deberá generar sobre demanda, un reporte ejecutivo por la última hora, la última semana, el último mes y sobre un período específico de monitoreo, incluyendo los siguientes parámetros:
  - Utilización agregada de ancho de banda durante el período de monitoreo, cuantificando los Bytes de bajada y de subida transferidos durante el tiempo especificado
  - Los Top 50 Access Points del sistema por utilización
  - Los SSID's con mayor consumo
  - Conteo individual de clientes durante el período seleccionado y por día
  - Los Top 50 usuarios por utilización
  - Las Top 50 aplicaciones con mayor presencia en la red
  - Los Top 50 dispositivos por fabricante
  - Los Top 50 sistemas operativos de dispositivos móviles que se conectaron a la red

- Deberá proporcionar a los administradores con una lista de logs de eventos y de cambios en la configuración.
- Deberá contarse de igual manera con un reporte de utilización por aplicación, identificando el servicio consultado, la categoría a la que pertenece (Deportes, música, video, e-mail, tiempo real, etc) y su utilización en bits por segundo durante el tiempo. De igual manera se requiere que se identifique el usuario y grupo de usuarios que hicieron uso de dicha aplicación.
- Finalmente, la solución deberá contabilizar y presentar a los administradores, reportes de Presencia de los dispositivos de usuarios, incluyendo:
  - Dispositivos que pasaron dentro del área de cobertura pero permanecieron un intervalo de tiempo pequeño
  - Dispositivos que aunque no se conectaron, permanecieron al menos 5 minutos en la zona de cobertura
  - Dispositivos que finalmente se conectaron a la red
  - Duración de las visitas a la zona de cobertura de los dispositivos conectados e identificados previamente
  - Medición de la lealtad de los visitantes, cuantificando primeras visitas, visitas diarias, semanales y mensuales

- El contratista deberá garantizar la calidad de los ítems requeridos, y deberá reponerlos en caso de encontrarse defectuosos, sin costo adicional bajo ningún concepto para el contratante.

El tiempo de respuesta para la solicitud de reposición de los equipos será de máximo 3 días hábiles, y la reposición de los equipos deberá darse en un plazo máximo de un (1) mes.

La ciudad de recepción y entrega de los equipos que requieran gestión de garantías será la ciudad de Medellín.

- **Garantía comercial:** El contratista se obliga a entregar los elementos contratados con su respectiva certificación de garantía comercial de al menos doce (12) meses, las cuales deben ser expedidas por el fabricante o el oferente suscrita por el Representante Legal.

La atención de reclamaciones por concepto de Garantías deberá darse en máximo 3 días hábiles, y la solución a los requerimientos que por este concepto sean emitidos, el Contratista, deberá resolverlos en máximo un (1) mes.

**PLAZO:** El plazo para la ejecución del contrato objeto de la presente Solicitud Privada de Oferta de mínima cuantía es hasta el 29 de diciembre de 2017, contados a partir de la aprobación de las garantías por parte de la Secretaría General de la ESU. El plazo del contrato podrá adicionarse, antes de su vencimiento mediante documento suscrito por las partes, previa verificación por parte del supervisor del cumplimiento del objeto contractual, los precios y las condiciones de ejecución del contrato, siempre y cuando sea conveniente y favorable para la ESU.

En desarrollo del contrato que surja en virtud de esta Solicitud Privada de Oferta se admitirán entregas parciales de los elementos a contratar, optimizando los tiempos de entregas por ítems o por cantidades. En todo caso el proponente seleccionado deberá entregar la totalidad de los elementos adjudicados, de conformidad con el plazo establecido en estos pliegos.





**VALOR: TRECE MILLONES QUINIENTOS ONCE MIL DOSCIENTOS CINCUENTA Y DOS PESOS M/L (\$13.511.252) IVA incluido.**

**FORMA DE PAGO:** La ESU cancelará el valor del contrato mediante pago único, previa presentación de la Garantía Comercial exigida, la aprobación de la póliza exigida y el recibo de cumplimiento de la prestación del servicio por parte del supervisor del contrato. La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario, y deberá quedar causada en el mes de diciembre de 2017, en la fecha máxima estipulada para tal fin por parte de la ESU. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando. Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte de sus empleados al Sistema de Seguridad Social Integral y a las entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.

La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando.

- El contratista deberá acreditar la efectiva prestación del servicio y/o producto por medio de una constancia de recibo firmada por el beneficiario. Una vez aprobada la constancia de recibo por parte del supervisor del contrato, éste emitirá el recibo a entera satisfacción del producto y/o servicio contratado.

- Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause por razón de la celebración, ejecución y pago de este Contrato serán a cargo exclusivo del contratista.

- En virtud del Contrato Interadministrativo No. 4600069558, suscrito con la Secretaría de Seguridad y Convivencia del Municipio de Medellín, entre los impuestos, tasas y contribuciones que estarán a cargo del contratista, están los siguientes: Estampilla Pro Cultura-Municipio de Medellín 0.5% y Estampilla Pro Universidad de Antioquia 1%. En todo caso, corresponde al contratista sufragar todos los impuestos, tasas y contribuciones entre otros, que le correspondan de conformidad con la normatividad vigente.

- Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá treinta (30) días calendario para proceder a su pago. En caso de incurrir en mora en los pagos, la ESU reconocerá al CONTRATISTA un interés equivalente al DTF anual de manera proporcional al tiempo de retraso.

- Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte de sus empleados al Sistema de Seguridad Social Integral y a las entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.

- La ESU realizará la transferencia electrónica a la cuenta informada por el contratista, siempre y cuando éste no se encuentre en mora en la gestión comercial facturada por la ESU. La ESU, en su condición de entidad contratante, podrá realizar los cruces de cuenta y compensaciones legales que

sean necesarias a efectos de garantizar el cumplimiento oportuno de las obligaciones dinerarias a cargo de los proveedores. El Contratista solo podrá realizar cruce de cuentas o compensación legal de obligaciones dinerarias siempre que medie autorización expresa y escrita por parte de la Gerencia de la ESU.

**CRUCE DE CUENTAS:** Con la firma del presente documento EL CONTRATISTA autoriza a la Empresa para la Seguridad Urbana -ESU-, para que al momento de efectuar cualquier pago a su nombre, de manera automática y sin previo aviso, la ESU realice cruce de cuentas para compensar los dineros que EL CONTRATISTA adeuda a la Entidad por cualquier concepto, salvo que sobre los mismos se tenga suscrito un acuerdo de pago entre las partes.

**GARANTÍAS:** EL CONTRATISTA se obliga a constituir a favor de "LA EMPRESA PARA LA SEGURIDAD URBANA - ESU Y/O MUNICIPIO DE MEDELLÍN", una garantía única a favor de entidades estatales que ampare el cumplimiento de las obligaciones contractuales, otorgada por una compañía de seguros autorizada para operar en Colombia por la Superintendencia Financiera y preferiblemente con poderes decisorios en la Ciudad de Medellín.

✓ **Cumplimiento:** Por el diez por ciento (10%) del valor del mismo, con una vigencia igual a la duración del contrato y seis (6) meses más.

**OBLIGACIONES DEL CONTRATANTE:** La ESU en desarrollo del presente contrato tendrá los siguientes derechos y deberes: 1) Exigir al contratista la ejecución idónea y oportuna del objeto contratado. 2) Actualizar y adoptar las medidas necesarias cuando se produzcan fenómenos que alteren en su contra el equilibrio económico o financiero del contrato, previo informe del supervisor, sobre la ocurrencia de tales hechos. 3) Adelantar las acciones conducentes a obtener la indemnización de los daños que sufran en desarrollo o con ocasión del contrato. 4) Ejercer las acciones a que haya lugar, por las situaciones administrativas de la Entidad, como consecuencia del presente contrato. 5) Pagar oportunamente al contratista el valor del contrato, de conformidad con lo establecido en la cláusula correspondiente a forma de pago. 6) Prestar al contratista todo lo necesario para la adecuada ejecución del objeto contractual.

**OBLIGACIONES DEL CONTRATISTA:** El contratista en desarrollo del presente contrato tendrá los siguientes derechos y obligaciones: 1) Recibir oportunamente el pago estipulado en la cláusula correspondiente a forma de pago de este contrato. 2) Cumplir de buena fe con el objeto del presente contrato, de conformidad con la propuesta adjunta, la cual hace parte integral del contrato. 3) Designar un representante para efectos de facilitar y agilizar el manejo de la información entre las partes. 4) Presentar los informes requeridos sobre la ejecución del contrato. 5) Presentar las observaciones y recomendaciones para el buen desarrollo del contrato. 6) Cumplir con el objeto contractual acordado en la forma, cantidad, lugar, fechas y especificaciones requeridas por la ESU. 7) Constituir las garantías que le sean exigidas en el presente contrato y mantenerlas vigentes por el tiempo estipulado por la ESU. 8) Acreditar el pago de aportes parafiscales y seguridad social para cada uno de los pagos. 9) Acatar los requerimientos y observaciones que con ocasión de la ejecución del contrato le hagan el supervisor y/o la contratante. 10) Las demás que tengan relación directa con la naturaleza y objeto del presente contrato.

**SUPERVISIÓN:** El seguimiento técnico, administrativo, financiero, contable y jurídico del cumplimiento a satisfacción del presente objeto contractual se realizará por MARTHA LUZ SÁNCHEZ, o quien sea designado por el Subgerente de Servicios Logísticos de la ESU.



**INDEMNIDAD:** De conformidad con el Artículo 55 del Acuerdo 055 de 2014 modificado por el Acuerdo 077 de 2017, el CONTRATISTA se obliga a mantener libre a la ESU de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes en la ejecución del presente Contrato.

**CLÁUSULA PENAL PECUNIARIA:** De conformidad con el artículo 1592 del Código Civil Colombiano, las partes convienen que en caso de incumplimiento del CONTRATISTA en las obligaciones del contrato, o de la terminación del mismo por hechos imputables a él, éste pagará a la ESU en calidad de cláusula penal pecuniaria una suma equivalente al diez por ciento (10%) del valor total del contrato, la cual será considerada como pago parcial pero no definitivo de los perjuicios causados a la ESU. El valor de la cláusula penal pecuniaria se tomará directamente de cualquier suma que se adeude al CONTRATISTA, si la hay, y/o se hará efectiva la garantía de cumplimiento del contrato. Si lo anterior no fuere posible, se cobrará por la vía judicial.

**EXCLUSIÓN DE RELACIÓN LABORAL:** El contratista ejecutará el objeto de este contrato con plena autonomía técnica y administrativa, sin relación de subordinación o dependencia, por lo cual no se generará ningún tipo de vínculo laboral.

**CESIÓN DEL CONTRATO:** El presente contrato no podrá ser cedido total o parcialmente por el contratista, salvo autorización expresa y escrita de la ESU.

**DOMICILIO:** El domicilio contractual es el Municipio de Medellín.

**NATURALEZA JURÍDICA DEL PRESENTE CONTRATO:** Este Contrato se rige por las normas comerciales y civiles, y especialmente, por el Acuerdo 055 de 2014 modificado por el Acuerdo 077 de 2017, expedido por la Junta Directiva de la ESU.

**UTILIZACIÓN DE MECANISMOS DE SOLUCIÓN DIRECTA EN LAS CONTROVERSIAS CONTRACTUALES:** La ESU y el contratista buscarán solucionar en forma ágil, rápida y directa las diferencias y discrepancias surgidas de la actividad contractual. Para tal efecto, al surgir las diferencias acudirán al empleo de los mecanismos de solución de controversias contractuales, a la conciliación, a la amigable composición o a la transacción.

**CONFIDENCIALIDAD:** LAS PARTES se comprometen a guardar la reserva sobre toda la información confidencial y estratégica de la otra parte, a la que tengan acceso con ocasión de las negociaciones mencionadas en este documento. El término Información confidencial hace referencia a los documentos o datos no accesibles al público, que hayan sido mantenidos por cada titular bajo su control, cuyo contenido represente un valor actual o potencial dentro de los activos de la empresa u ostente un carácter estratégico para ésta; Incluye, sin limitarse a ella, información financiera, comercial, tecnológica, de mercado o cualquiera otra suministrada o a la que se tenga acceso en razón del desarrollo de las negociaciones mencionadas. La información confidencial puede estar soportada en medio escrito, digital o cualquiera otro, conocido o por conocer, o ser revelada en forma verbal, siempre y cuando advierta de su carácter reservado ante la parte receptora o esté señalada como tal en el momento mismo de la entrega. Se entenderá por parte reveladora la propietaria de la información, y por parte receptora quien la recibe o tiene acceso a ella con ocasión de las negociaciones señaladas en el objeto del presente documento.

Para el cumplimiento de lo anterior LAS PARTES deben: a) garantizar que los empleados a su servicio y demás personas autorizadas, respeten la obligación de secreto sobre cualquier información confidencial, b) la Parte Receptora utilizará la Información Confidencial exclusivamente en relación con el propósito que se han señalado las partes, c) la Parte Receptora mantendrá dicha Información de manera confidencial y privada, d) la Parte Receptora se abstendrá de reproducir la Información Confidencial o darla a conocer, e) la Parte Receptora tratará la Información Confidencial con el mismo cuidado que ella acostumbra para proteger la información confidencial de su propiedad. Se conviene que toda la Información Confidencial será guardada por la Parte Receptora en un lugar con acceso restringido al cual sólo podrán acceder los Representantes de la Parte Receptora que razonablemente requieran conocer la Información Confidencial en razón de las negociaciones que se lleven a cabo, f) ni la ejecución de este contrato, ni el suministro de cualquier información en virtud del mismo, se interpretará, directa o indirectamente, como otorgamiento a las partes o a sus Representantes, de licencia alguna o derecho para utilizar Información Confidencial para su propio beneficio o beneficio de cualquier otra persona natural o jurídica, g) la Parte Reveladora garantiza a la Parte Receptora que está debidamente autorizada para revelar Información Confidencial a la Parte Receptora y acuerda indemnizar y proteger contra todo daño a la Parte Receptora de cualquier responsabilidad relacionada con el suministro de dicha Información Confidencial o el uso establecido y permitido mediante este contrato.

**TERMINACIÓN:** El presente Contrato se podrá dar por terminado por las siguientes causas: 1) Cuando se alcance y se cumpla totalmente el objeto del contrato. 2) Por Mutuo acuerdo de las Partes, siempre que la terminación no implique renuncia a derechos causados o adquiridos a favor de las partes. 3) Cuando por razones de fuerza mayor o caso fortuito se haga imposible el cumplimiento de los objetivos propuestos. 4) Por el incumplimiento de cualquiera de las obligaciones establecidas para cada una de las Partes. 5) Por vencimiento del término fijado para la ejecución del mismo. 5) Por las demás causales señaladas en la ley.

**LIQUIDACIÓN:** La liquidación del Contrato procederá de conformidad con lo establecido en el artículo 46 del Acuerdo 055 de 2014 modificado por el Acuerdo 077 de 2017 - Reglamento de Contratación de la ESU. Para ella, las partes de común acuerdo celebrarán un acta en la que se dé cuenta del estado del contrato dentro de los cuatro (4) meses siguientes a la fecha de terminación del mismo. Dentro de este plazo, las partes acordarán los ajustes, revisiones y reconocimientos a que haya lugar, de los cuales quedará constancia en el acta de liquidación. Si es del caso, para la liquidación se exigirá al CONTRATISTA la ampliación de la vigencia de los amparos y garantías para avalar las obligaciones que deba cumplir con posterioridad a la extinción del contrato. Si durante el término de liquidación bilateral del contrato no es posible obtener la suscripción del acta correspondiente por parte del contratista, se procederá a la liquidación unilateral, notificando de manera escrita al contratista y se dejará soporte documental de la gestión para la suscripción. En los contratos que tengan saldos inferiores a 0,09 UVT, se podrán liberar saldos sin acta de liquidación, con la solicitud escrita del supervisor y aprobación del Directivo del área correspondiente.

**INHABILIDADES E INCOMPATIBILIDADES:** El CONTRATISTA con la firma del presente contrato, declara bajo la gravedad de juramento que no se encuentra incurso en ninguna de las inhabilidades e incompatibilidades consagradas en la Constitución y la Ley. La contravención a lo anterior, dará lugar a las sanciones de ley.

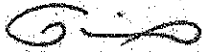
**TRATAMIENTO DE DATOS PERSONALES:** Con observancia de la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 886 de 2014 y las decisiones judiciales adoptadas en materia de tratamiento de datos

personales, las partes entienden y aceptan que a través de la gestión de las actividades contenidas en este contrato, podrán ser responsables y/o encargadas del tratamiento de datos personales. En virtud de lo anterior, las partes manifiestan que cuentan con las autorizaciones previas y expresas de los titulares para hacer uso de sus datos personales, así como con los soportes o mecanismos en los que constan éstas, para los fines consagrados en sus avisos o políticas de privacidad y que les permitirán a los titulares acceder, conocer, rectificar, corregir y suprimir sus datos de cualquiera de las bases que sean administradas por las partes durante la ejecución del contrato, para lo cual éstas mantendrán habilitados los mecanismos permitidos por la Ley para tales efectos.

**IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SG - SST).** El contratista deberá encontrarse en las adaptaciones que den lugar para la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), de conformidad con el Decreto 1072 de 2015, así como sus modificaciones y los documentos que los complementen. En todo caso previo al inicio de la ejecución del contrato, el contratista deberá presentar las evidencias de las acciones realizadas en la implementación del mencionado, y el cumplimiento del anexo técnico de la Resolución 1111 de 2017 del Ministerio del Trabajo.

**DOCUMENTOS DEL CONTRATO:** 1- Disponibilidad y compromiso presupuestal. 2- Cedula de Ciudadanía. 3- Propuesta presentada por el contratista. 4- RUT. 5- Certificado de Existencia y Representación. 6- Certificado de paz y salvo aportes al sistema de seguridad social y parafiscal. 7- Certificado de antecedentes disciplinarios. 8- Certificado de antecedentes fiscales. 9- Certificado de antecedentes judiciales. 10- SPVA 2017-101. 11- Demás documentos que se deriven del presente contrato.

**POR LA ESU**



**GABRIEL IGNACIO NANCLARES QUINTERO**  
Secretario General

**POR EL CONTRATISTA**



**LILIAN ALEXANDRA GRISALES JUNCA**  
Representante Legal

Revisó: Alejandra Muñoz Jiménez - Profesional Universitario, Unidad de Gestión Jurídica  
Proyectó: Catalina Molina Betancur - Profesional Universitario de la Unidad Estratégica de Servicios de Logística 