CONTRATISTA		NIT	TELÉFONO	FECHA DE SUSCRIPCIÓN	
EVOLUTION TECHNOLOGIES GROUP S A S		830.147.784-9	317 4272581	30/09/2021	
REPRESENTANTE LEGAL		**CÉDULA**	**DIRECCIÓN DE CONTACTO**		**TEL./CEL. CONTACTO**
DIEGO FERNANDO RIVERA JIMENEZ		16.369.548	CRA 7 127-48 OFICINA 607		6017441985
CORREO ELECTRÓNICO		**CIUDAD DE EJECUCIÓN**	**RADICADO REQUERIMIENTO**	**BIENES O SERVICIOS**	**DISPONIBILIDAD PRESUPUESTAL**
jmedina@evolution-it.com.co		MEDELLÍN	2021105974	SERVICIOS	2021001207
CONVENIO	**CENTRO DE COSTOS**	**RUBRO PRESUPUESTAL**	**DESCRIPCIÓN RUBRO**	**VALOR CONTRATO**	**COMPROMISO PRESUPUESTAL**
4600091467 de 2021	32059	23202020080229-1/83131	FORTALECIMIENTO DE SEGURIDAD INFORMATICA	$568.016.988	2021001577

OBJETO
El contratista se obliga con la ESU a Consultoría especializada en seguridad informática para el diagnóstico de vulnerabilidades y nivel de criticidad de las diferentes plataformas tecnológicas del SIES-M de la secretaría de Seguridad y Convivencia del Municipio de Medellín; de conformidad con 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.

ALCANCE DEL OBJETO
El alcance del objeto del presente contrato comprende: Consultoría especializada en seguridad informática para el diagnóstico de vulnerabilidades y nivel de criticidad de las diferentes plataformas tecnológicas del SIES-M de la Secretaría de Seguridad y Convivencia del Municipio de Medellín; de acuerdo con las siguientes especificaciones.

FASE I: CONSISTE EN LA RECOPILACIÓN DE TODA LA INFORMACIÓN PARA LA EJECUCIÓNDEL CONTRATO.

- Requerimientos y necesidades iniciales, vs. Implementación actual.
- Modelos de seguridad y privacidad de la información previos.

- Metodologías utilizadas.
- Nivel de apoyo de la alta dirección.
- Cultura de la Organización.
- Metodología existente para gestión de activos de información.
- Metodología existente para gestión de riesgos.
- Responsables y demás involucrados (Stakeholders).
- Terceros involucrados.
- Clientes de la solución.
- Requerimientos normativos, legales que aplican al objeto del Proyecto.
- Identificación y formalización de expectativas del cliente.

Entregables por parte del aliado proveedor:

- ✓ Acuerdo de criterios de aceptación y niveles de servicio acordados.
- ✓ Plan de Gestión del Proyecto y entregables asociados (PMI) como:
  - Plan de Riesgos del Proyecto.
  - Plan de Calidad del Proyecto.
  - Plan de Comunicaciones del Proyecto.
- ✓ Cronograma detallado de actividades actualizado del proyecto y línea basede definitivos

FASE II – CONSISTE EN EL DIAGNÓSTICO Y VALORACIÓN DE LA SEGURIDAD INFORMÁTICA, LOS CUALES SE DEBEN VALORAR EN CONCORDANCIA CON EL MODELO DESEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR EL MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y DE LAS COMUNICACIONES-TIC, REFERENTES LEGALES Y LA NORMA ISO/IEC 27001:2013.

- Contexto de la Organización.
- Liderazgo y Compromiso (de la Alta Dirección).
- Planeación – Gestión del Riesgo.
- Soporte – Asignación de los Recursos Necesarios, documentación, entre otros.
- Operaciones.
- Evaluación de Desempeño.
- Mejora Continua.

En cada uno de los puntos por revisar, se evaluará el estado de cumplimiento, la brecha que tiene la Secretaría de Seguridad y Convivencia del municipio de Medellín y las acciones a implementar para cerrar los hallazgos.

Características de la prestación del servicio:

A través de entrevistas y revisión de la documentación existente se identificarán las necesidades de la organización, en detalle se ejecutarán las siguientes actividades:

- Revisión de la documentación existente.
- Entrevistas con personal de la organización responsable de los controles de seguridad informática.
- Diagnóstico y análisis de brecha, el diagnóstico se hará con el alcance definido, y usando como referencia los controles establecidos por la norma ISO 27001:2013 relacionados con seguridad

informática.
- Valoración Técnica (Pruebas de Vulnerabilidades Técnicas).

El aliado deberá tener en cuenta los siguientes criterios de valor para identificar las actividades relevantes: Tamaño de la organización, estructura organizacional de seguridad de la información y de seguridad informática y el modelo de privacidad de la información.

Entregables por parte del aliado proveedor:

- ✓ Informe de Brecha con recomendaciones de cierre de hallazgos.
- ✓ Reporte de Hallazgos de Valoración técnica.
- ✓ Presentaciones e informes del avance de la ejecución.
- ✓ Plan de Proyecto Actualizado.

El aliado deberá tener en cuenta el Marco Normativo para este proceso.

Se identificará el Marco Normativo al cual está sujeta la entidad con relación a la Seguridad Informática:

- Guías del Modelo de Seguridad y Privacidad de la Información (MSPI), emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones-TIC, especialmente las Guías:

  Guía 5 - Gestión Clasificación de Activos.
  Guía 7 - Gestión de Riesgos.
  Guía 8 - Controles de Seguridad de la Información.
  Guía 21 - Gestión de Incidentes.

- CONPES 3795 de 2019.
- CONPES 3995 de 2020.
- Ley 1712 de 2014, ley de transparencia y del derecho de acceso a la información pública.

Adicionalmente se deberán tomar como guía las siguientes normas y guías técnicas:

- ISO/IEC 27001:2013 Information technology— Security techniques — Information security management systems — Requirements.
- ISO/IEC 27002:2013 — Code of practice for information security management.
- ISO 31000:2018 - Principles and Guidelines on Implementation.
- IEC 31010:2019 - Risk management -- Risk assessment techniques.
- ISO/IEC 27005:2018 Information technology — Security techniques —Information security risk anagement.
- ISO/IEC 27035:2011 - Security Incident Management.

Se deberá realizar el Análisis del Contexto de la organización.

A partir de la información recolectada, el aliado deberá generar un informe del estado actual yde brecha, así como las recomendaciones y matriz DOFA pertinentes para que laSecretaría de Seguridad y

Convivencia del municipio de Medellín de cumplimiento a los requerimientos establecidos por la normativa aplicable y las buenas prácticas.

Se deberá realizar el Análisis de Políticas Existentes

El aliado deberá verificar las políticas, procesos, instructivos y cualquier documento (formal o no formal) con el que cuente la entidad y sus partes involucradas con el fin de consolidar en lasrecomendaciones para las áreas de la Secretaría de Seguridad y Convivencia del municipio de Medellín relacionados con la seguridad informática, la seguridad de la información, la continuidad de negocio, la recuperación ante desastres, la atención de incidentes y el manejo de crisis.

Se deberá realizar el Análisis de Infraestructura Tecnológica

Al aliado deberá identificar los elementos tecnológicos críticos involucrados en los procesos denegocio de la Secretaría de Seguridad y Convivencia del municipio de Medellín identificando las vulnerabilidades presentes mediante la realización de pruebas de vulnerabilidad. Este análisis se realizará con una muestra de hasta cincuenta (50) dispositivos tecnológicos.

A continuación, se describe la metodología que se debe llevar a cabo para la realización de lasactividades:

- ✓ Recolección de Información: Entender los activos más importantes de la Entidad y su localización.
- ✓ Las pruebas deben incluir un escaneo de puertos para cada uno de los objetivos definidos.
- ✓ Se debe realizar una identificación completa de cada uno de los elementos a nivel de sistema operativo.
- ✓ Se debe realizar un análisis de cada uno de los servicios identificados y como se puede realizaruna interacción con cada uno de ellos en búsqueda de posibles vulnerabilidades o puntos de acceso a los sistemas analizados.
- ✓ Se revisarán las bases de datos disponibles para los elementos analizados, en búsqueda de código que permita generar un compromiso a los elementos que están siendo evaluados dentro del análisis de vulnerabilidades.
- ✓ Se debe realizar una revisión de permisos a nivel de autorización y esquemas de autenticación que se encuentren establecidos en los elementos objeto de las pruebas.
- ✓ Se debe realizar una revisión completa de los controles de seguridad a nivel de red establecidos para la infraestructura, con el fin de determinar posibles vulnerabilidades en lamisma.
- ✓ Se debe realizar una valoración de impacto de las vulnerabilidades encontradas.
- ✓ Se debe realizar un mapeo de la aplicación en búsqueda de puntos de interacción con el usuario que permitan realizar una revisión manual de los principales riegos existentes en una aplicación basados en el OWASP Top.
- ✓ Esta revisión se hará a las direcciones que contengan aplicaciones que se encuentren dentrodel alcance definido para la ejecución del análisis.
- ✓ Las vulnerabilidades en los objetivos están clasificadas con base en los estándares OWASP, PTES y OSSTMM por tanto las pruebas propuestas toman como referencia las recomendaciones definidas en estos tres estándares en cuanto a pruebas de seguridad se refiere.

- ✓ Las vulnerabilidades en los servidores (sistema operativo y aplicaciones instaladas) también son evaluadas bajo los estándares OSSTMM, PTES y NIST SP 800-115, el desarrollo de las pruebas permite tomar algunos elementos que pueden ser relevantes dentro de las pruebasde cada uno de los estándares.

La ejecución de las pruebas se hará de manera acordada, programada y con el mecanismo de conexión establecido por la Secretaría de Seguridad y Convivencia. En cuanto al tratamiento de la información compartida resultado de esta guía, se aplicará el acuerdo deconfidencialidad definido en este anexo técnico.

Análisis de vulnerabilidades.

Dentro de este análisis el aliado proveedor buscará descubrir fallas en los sistemas y aplicaciones, las cuales puedan ser aprovechadas por un atacante. Las fallas pueden encontrarse enmarcadas desde de una mala configuración del equipo o servicio, hasta problemas de seguridad en la aplicación. El proceso de análisis puede variar dependiendo de los componentes que serán probados. Las pruebas desarrolladas en esta fase deben incluir lossiguientes procedimientos.

- Pruebas Activas.
  - Automatizadas.
- Escáneres de Vulnerabilidades en Red.
- Escáner de Vulnerabilidades Web.
- Específicas de protocolos.
  - Conexiones Manuales directas.
  - Conexiones ofuscadas.
- Pruebas Pasivas.
  - Análisis de Metadatos.
  - Monitoreo de Tráfico.
- Investigación.
  - Investigación Pública.
  - Bases de Datos de Vulnerabilidades o Boletines de Fabricantes.
  - Bases de Datos.
  - Contraseñas por Defecto.
  - Guías de Aseguramiento.
  - Errores Comunes de configuración o Fuzzers.
  - Desensamblado de código.

•Se verificará y sin limitarse a los siguientes aspectos:

- Control de acceso. Acceso a funciones/recursos no autorizadas.
- Autenticación. Fallas para determinar la identidad de un individuo/entidad, y en el proceso de autenticación.
- Gestión de sesiones. Problemas en la emisión, uso, protección, cambio y finalización de las sesiones.

- Gestión de configuración. Problemas relacionados con la gestión administrativa o confalta de buenas prácticas de fortalecimiento de los sistemas de información (Aplicaciones, Servidor web, SO, BD, otros).
- Manejo de errores. Errores que puedan afectar la operación del sistema o revelen información crítica del mismo.
- Protección de datos en el almacenamiento. Cookies, atributos, otros.
- Protección de datos en el transporte de datos. Criptografía, uso de algoritmos débiles,mala gestión de claves/certificados digitales, otros similares.
- Validaciones de entrada. Inyección de: scripts, peticiones SQL, comandos SO, HTML, otros.
- Desborde de buffer. Capacidades para alterar los datos, alterar los programas o llevarestos últimos a que fallen.
- Denegación de servicio (DoS). Agotamiento de recursos, fallas en el acceso a los recursos por parte de usuarios válidos.
- Otros relevantes para el objeto del servicio a contratar.

Entregables por parte del aliado proveedor

- ✓ El aliado proveedor deberá elaborar un Resumen Ejecutivo donde se centralizarán los resultados de todas las pruebas realizadas y presentará la postura general de la organización frente a la seguridad de la infraestructura objeto de las pruebas.

- ✓ Deberá desarrollar un Informe Técnico detallando las actividades ejecutadas para encontrar las vulnerabilidades y los resultados obtenidos cuando no fue posible hallarlas. Toda la información recolectada que se considere relevante será entregada como anexos, con el fin de transferir conocimientos al cliente dentro del valor de la contratación realizada.

- ✓ El aliado proveedor deberá realizar una presentación de los resultados y transferencia de conocimientos a la Secretaría de Seguridad y Convivencia del municipio de Medellín de loshallazgos encontrados y la forma de remediarlos.

Análisis de Brecha ISO27001:2013.

El aliado proveedor deberá realizar un análisis de brecha (GAP Analysis) para determinar el estado actual de la Secretaría de Seguridad y Convivencia del municipio de Medellín frente a lanorma ISO 27001:2013, lo cual permitirá identificar la situación base de la Seguridad Informática de la entidad.

Existen tres (3) componentes clave en el éxito del control de la Seguridad, ya que son considerados críticos dentro de un Sistema de Gestión de Seguridad de la Información.

Estos componentes son:

- Gestión de Activos de Información.
- Gestión de Riesgos asociados a la Seguridad de la Información.
- Gestión de Incidentes de Seguridad de la Información.

Estos objetivos de control serán diagnosticados y valorados para obtener una postura de la entidad frente a estos ítems. A continuación, se detallan los componentes:

Gestión de Activos de Información

Consiste en la definición, validación y documentación del Proceso de Gestión de Activos de Información, teniendo en cuenta elementos normativos y de buenas prácticas, tales como:

- Numeral A.8 del anexo de controles de la norma ISO 27001:2013, que establece los siguientes elementos a definir e implementar:

    - Gestión de Activos.
    - Responsabilidad por los Activos.
    - Inventario.
    - Propiedad.
    - Uso Aceptable.
    - Devolución o Clasificación de la Información.
    - Clasificación/Categorización.
    - Rotulación.
    - Manejo de los Medios de Información.
    - Gestión Medios Removibles.
    - Destrucción.
    - Transporte de Medios.

- Normas ISO 55001 e ISO 55002, en donde se define el ciclo de vida de los activos, teniendo en cuenta como mínimo las siguientes fases del ciclo de vida:
    - Creación o Procesamiento.
    - Operación y Mantenimiento.
    - Almacenamiento.
    - Transmisión.
    - Eliminación.
    - Destrucción y desincorporación del Activo.

- Ley 1712 de 2014, ley de transparencia y del derecho de acceso a la información pública.

Nota: *Si la entidad cuenta con un proceso de gestión de activos de información, se revisará y valorará de acuerdo con sus necesidades actuales y se recomendarán los marcos normativos de gestión de incidentes que la entidad requiera. De manera adicional, como base fundamental para la Gestión de activos de información se verificará el inventario inicial, que se convierte en la línea base de gestión e implementación*

de controles y la priorización de la implementación, lo anterior, basado en la sensibilidad, en términos de seguridad informática de cada activo identificado. El alcance es la infraestructura del SIES-M.

Gestión de Riesgos

Esta fase verifica la forma en que el riesgo está siendo identificado, valorado y tratado. También se revisan los criterios de aceptación del riesgo. A partir de la información recolectada, el aliado proveedor debe generar las recomendaciones pertinentes para cerrar la brecha identificada.

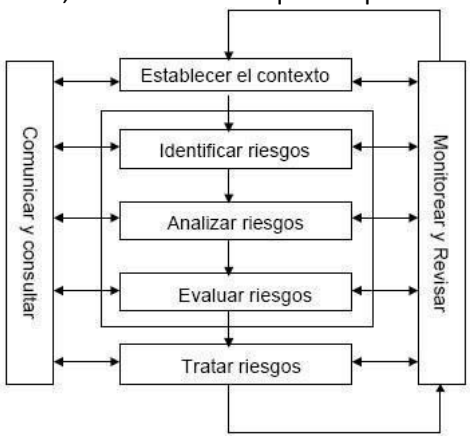
Para la valoración del proceso de gestión de riesgos, se utilizan referencias normativas como los lineamientos para la Administración del Riesgo del Departamento Administrativo la FunciónPública – DAFP, ISO 27005:2018 y la ISO 31000:2018.

El resultado de las revisiones es un diagnóstico de cumplimiento de la metodología de gestión deriesgo de acuerdo con lo establecido en la norma ISO 27001:2013 y usando como referencia los estándares y lineamientos para la Administración del Riesgo del Departamento Administrativo la Función Pública – DAFP, ISO 27005:2018 y la ISO 31000:2018 y recomendaciones para el cumplimiento de acuerdo con el resultado del diagnóstico. El aliado proveedor identificará los riesgos de seguridad informática para el alcance del proyecto (SIES-M).

Típicamente las etapas del proceso de gestión de riesgos son:

- Definición de la Metodología de Gestión del Riesgo.
- Valoración del Riesgo.
    - Identificación del Riesgo
    - Valoración del Riesgo.
    - Análisis del Riesgo.
- Planes de Tratamiento del Riesgo.
- Monitoreo del Riesgo.

A continuación, se muestra el esquema que se debe seguir para la gestión del riesgo



Esquema de la metodología ISO 27005 e ISO 31000 para la gestión del riesgo.

Gestión de Incidentes de Seguridad Informática

El propósito de esta fase es verificar las políticas y procedimientos de gestión de incidentes de seguridad informática con un enfoque estructurado y planificado que permita manejar adecuadamente los eventos que se presentan en la Secretaría de Seguridad y Convivencia del municipio de Medellín y que puedan afectar la seguridad de la información de la Entidad; esto con base en la normatividad vigente. El aliado proveedor revisará la documentación existente que tenga la Secretaría en cuanto a gestión de incidentes de seguridad informática que apliquen a la gestión del SIES-M y se usará como guía la norma ISO 27001:2013.

Se verificará que el proceso contemple como mínimo:

- Planificación y preparación o Detección y reporte.
- Evaluación y decisión.
- Respuesta.
- Lecciones aprendidas.

Análisis de Brecha ISO27002:2013.

En esta fase se verifican los controles definidos en el **Anexo A** de la norma ISO/IEC 27001:2013 que se encuentran detallados en la ISO27002:2013 estos dominios son:

- A.8 Gestión de Activos.
- A.9 Control de Acceso.
- A.10 Criptografía
- A.11 Seguridad Física y del Entorno.
- A.12 Seguridad de las Operaciones
- A.13 Seguridad de las Comunicaciones
- A.14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
- A.15 Relaciones con Proveedores.
- A.16 Gestión de Incidentes de Seguridad de la Información.
- A.17 Aspectos de Seguridad de la Información de Gestión de Continuidad del Negocio.

Por cada dominio el aliado proveedor diagnosticará y valorará los controles implementadosy se generarán las recomendaciones de acuerdo con los hallazgos, teniendo en cuenta las necesidades de la Secretaría de Seguridad y Convivencia del municipio de Medellín y tomando como referencia los controles sugeridos en la ISO/IEC 27002:2013 y los estándaresespecíficos existentes.

FASE III – CONSISTE EN EL CIERRE DE LA EJECUCIÓN CONTRATO.

Una vez finalizado todo el diagnostico, el aliado proveedor deberá realizar una presentación con sus resultados y una entrega formal de toda la documentación de ejecución del contratoque se encuentre dentro

de su alcance.

Esta presentación deberá ir acompañada de la carta de aceptación de los entregables y de la propuesta de la estrategia de seguridad informática recomendada para el SIES-M como cliente final.

Entregables por parte del aliado proveedor

- ✓ Medio Magnético con Documentación definitiva.
- ✓ Presentación de cierre.
- ✓ Acta de entrega toda la ejecución del contrato

Especificaciones del Servicio
Para toda la ejecución del contrato se debe tener presente:

- El enfoque de la consultoría es dirigido a la seguridad informática del SIES-M, de igual manera el aliado proveedor debe ofrecer un entregable de recomendaciones generales sobre seguridad de la información incluyendo pautas para sensibilización del personal.

- También es necesario que la consultoría complemente las buenas prácticas de seguridad informática y de la información de acuerdo con la normatividad vigente, así como con los lineamientos definidos dentro de las políticas de seguridad informática de la Secretaría deInnovación digital del Municipio de Medellín.

- El alcance del contrato permitirá identificar las posibles vulnerabilidades existentes opotenciales y con base a esto el consultor recomendara cuales son los controles más eficientes para eliminar o mitigar el riesgo. El aliado proveedor no implementará ningún control en esta primera etapa del proyecto. El servicio profesional de consultoría especializada tiene como objetivo principal diagnosticar el estado actual de la entidad frentea la seguridad informática y el Modelo de Seguridad y Privacidad de la Información de acuerdo con la Estrategia de Gobierno Digital y basado en la norma ISO 27001:2013 para elSIES-M.

- La consultoría, solo informa con base en el escenario de estudio. El aliado proveedor solo tiene el alcance de diagnosticar el estado de seguridad informática, en caso de encontrar alguna situación de riesgo muy alto y de atención inmediata, debe apoyar con la formulación de las posibles soluciones para mitigar o resolver la situación presentada, las cuales serán evaluadas e implementadas por el equipo interno de tecnología del SIES-M. En general la consultoría no tiene responsabilidades operativas de acción sobre el tratamientode incidentes.

- Todas las actividades de diagnóstico que el aliado proveedor realice a los diferentes dispositivos del SIES-M, deberá tener aprobación de la Secretaría de Seguridad y Convivencia en coordinación con el supervisor del contrato de la ESU.

- El aliado proveedor deberá cumplir con todos los entregables solicitados por el cliente, los cuales deberán ser entregados al supervisor del contrato.

- El aliado no podrá realizar ninguna actividad sin la aprobación y conocimiento del supervisor del contrato y que no esté contemplada en el mismo.

PLAZO
Hasta el treinta uno (31) de diciembre de 2021, a partir de la aprobación de la póliza única de cumplimiento por parte de la Unidad de Gestión Jurídica. El plazo del contrato podrá ser modificado antes de su vencimiento mediante documento suscrito por las partes, previa verificación de la necesidad o conveniencia por parte del supervisor, teniendo en cuenta el cumplimiento del contrato, los precios y las condiciones de ejecución del contrato.

VALOR
El valor del presente contrato asciende a la suma de QUINIENTOS SESENTA Y OCHO MILLONES DIECISEIS MIL NOVECIENTOS OCHENTA Y OCHO PESOS M.L**.** (**$**568.016.988**)** IVA incluido.

TITULAR DESTINATARIO
Los bienes antes descritos son con destino a la Secretaria de Seguridad y Convivencia del Municipio de Medellín, en virtud del Contrato Interadministrativo de administración delegada de recursos N°4600091467 de 2021.

FORMA DE PAGO
La ESU cancelará el valor del contrato mediante pagos parciales con el recibo de cumplimiento de la entrega de los servicios objeto de la contratación y la emisión del recibo a satisfacción por parte del supervisor del contrato.

- ✓ Se debe tener presente el siguiente detalle de los pagos parciales:

Entregable por Fase	**Porcentaje para pago**
Entregable Fase I	33.3%
Entregable Fase II	33.3%
Entregable Fase III	33.3%

- ✓ 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.
- ✓ Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa, estampilla o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause con ocasión del contrato serán a cargo exclusivo del contratista.
- ✓ 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.
- ✓ Para el caso de proveedores que se encuentren obligados a facturar electrónicamente, la facturación deberá ser remitida al correo electrónico facturacion@esu.com.co y la fecha límite para la recepción de las mismas estará sujeta a las fechas definidas en la circular 001 del 5 de enero de 2021, documento donde adicionalmente se define la elaboración del recibo a satisfacción por parte del supervisor designado y el proceso de cierre contable en calidad de empresa industrial y comercial del estado.

CRUCE DE CUENTAS

Con la firma del presente contrato el contratista autoriza a la 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.

LUGAR DE EJECUCIÓN

La entrega de todos los servicios se harán en la Secretaría de Seguridad de Municipio de Medellín o en el sitio que le defina la ESU, previa coordinación con el supervisor del contrato.

PARÁGRAFO: Estarán a cargo del contratista todos los costos, trámites y documentos que se deriven del cumplimiento del objeto contractual, inclusive la entrega, transporte.

ENTREGABLES DEL CONTRATO

El contratista deberá cumplir con los siguientes entregables por fase en ejecución del presente

Fase	Entregable
Fase I	✓ Acuerdo de criterios de aceptación y niveles de servicio acordados. de Gestión del Proyecto y entregables asociados (PMI) como: - Plan de Riesgos del Proyecto. - Plan de Calidad del Proyecto. - Plan de Comunicaciones del Proyecto. ✓ Cronograma detallado de actividades actualizado del proyecto y línea base de definitivos

Fase II	✓ Informe de Brecha con recomendaciones de cierre de hallazgos. ✓ Reporte de Hallazgos de Valoración técnica. ✓ Presentaciones e informes del avance de la ejecución. ✓ Plan de Proyecto Actualizado ✓ Resumen Ejecutivo donde se centralizarán los resultados de todas las pruebas realizadas ✓ Informe Técnico detallando las actividades ejecutadas para encontrar las vulnerabilidades y los resultados obtenidos ✓ Presentación de los resultados y transferencia de conocimientos a la Secretaría de Seguridad y Convivencia del municipio de Medellín de los hallazgos encontrados y la forma de remediarlos.
Fase III	✓ Medio Magnético con Documentación definitiva. ✓ Presentación de cierre. ✓ Acta de entrega toda la ejecución del contrato

CONOGRAMA

El contratista deberá cumplir con los plazos pactados en el cronograma presentado en la propuesta y adjunto a este contrato como ***Anexo 1. Cronograma***. Este cronograma podrá ser ajustado si es necesario, en coordinación con el supervisor del contrato.

PERSONAL ASIGANDO

El contratista deberá disponer para la ejecución del contrato del personal profesional solicitado en el numeral 7.2.4 del pliego de condiciones y aportado en la oferta presentada y aceptada por la ESU.

- ✓ Ingeniero director del proyecto – Dedicación 100%
- ✓ Ingeniero Técnico. – Dedicación 100%
- ✓ Tecnólogo Coordinador – Dedicación 100%
- ✓ Personal técnico - Dedicación 100%:

GARANTÍA CONTRACTUAL

El Contratista se obliga a constituir a favor de "La Empresa para la Seguridad y Soluciones Urbanas - ESU Y/O MUNICIPIO DE MEDELLIN – SECRETARIA DE SEGURIDAD Y CONVIVENCIA", una garantía única de las expedidas para 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:

Garantías y Mecanismos de cobertura del riesgo: El Contratista se obliga a garantizar el cumplimiento de las obligaciones surgidas a favor de la ESU, con ocasión de la ejecución del contrato, de acuerdo con la siguiente tabla:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento	20%	con una vigencia igual a la duración del contrato y seis (6) meses más
Calidad del servicio	20%	con una vigencia igual a la duración del contrato y seis (6) meses más
Salarios, prestaciones sociales e indemnizaciones al personal	10%	con vigencia igual al plazo del contrato y tres (3) años más

PARÁGRAFO 1: El contratista deberá modificar el monto de la garantía cada vez que sea necesario, en razón del incremento del contrato o la afectación por reclamaciones. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU directamente solicitará a la Compañía de Seguros la modificación de la misma, además podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

PARÁGRAFO 2: Al recibo del contrato, el contratista contará con máximo dos (2) días hábiles para la constitución de la póliza única de cumplimiento y entrega de la documentación respectiva.

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 el contrato. **6)** Facilitar al contratista 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 el 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 y en los términos del Código Civil. **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**) Considerar que las relaciones contractuales están basadas en el reconocimiento, seguimiento de las reglas, principios de la ética y la buena fe contractual; en un ambiente de respeto y de confianza que genere valor para las partes y para la sociedad en general. **11)** Rechazar las prácticas corruptas y delictivas en general; se prevendrá y combatirá el fraude, el soborno, la extorsión y otras formas de corrupción. **12)** Tanto en el desarrollo de los proyectos y procesos, como en su área de

influencia, el contratista promoverá prácticas que reflejen la protección y conservación del medio ambiente, el respeto al pluralismo democrático, a las minorías étnicas, a la equidad de género y a los derechos humanos en general. **13)** Velar por el respeto de la dignidad en las condiciones de trabajo por parte de sus contratistas y subcontratistas, por lo que no se avalarán prácticas discriminatorias, trabajo forzado o de menores. **14)** Cumplir con las políticas de prevención que eviten la utilización y explotación sexual de niños, niñas y adolescentes en el desarrollo de sus actividades comerciales, así como a no contratar menores de edad en cumplimiento de los pactos, convenios y convenciones internacionales ratificados por Colombia, según lo establece la Constitución Política de 1991 y demás normas vigentes sobre la materia, en particular aquellas que consagran los derechos de los niños. **15)** Las demás que tengan relación directa con la naturaleza y objeto del presente contrato.

SUPERVISIÓN

La supervisión del Contrato será realizada por el profesional universitario de la Subgerencia de Servicios o quien sea designado por el funcionario competente. Al Supervisor le corresponderá realizar el seguimiento administrativo, técnico, financiero, contable, jurídico del contrato. En todo caso la designación podrá hacerse directamente por el Gerente.

INDEMNIDAD

De conformidad con el reglamento de contratación de la ESU **e**l Contratista se obliga a indemnizar a la Entidad con ocasión de la violación o el incumplimiento de las obligaciones previstas en el presente Contrato. El Contratista se obliga a mantener indemne a la ESU de cualquier daño o perjuicio originado en reclamaciones de terceros que tengan como causa sus actuaciones hasta por el monto del daño o perjuicio causado y hasta por el valor del presente Contrato. Igualmente, el Contratista mantendrá indemne a la Entidad por cualquier obligación de carácter laboral, o relacionadas que se originen en el incumplimiento de las obligaciones laborales que el Contratista asume frente al personal, subordinados o terceros que se vinculen a la ejecución de las obligaciones derivadas 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, pagará a la ESU en calidad de cláusula penal pecuniaria una suma equivalente al diez por ciento (10%) del valor total del contrato. El valor pactado de la presente cláusula penal es el de la estimación anticipada de perjuicios, no obstante, la presente cláusula no impide el cobro de todos los perjuicios adicionales que se causen sobre el citado valor. Si lo anterior no fuere posible, se cobrará por la vía judicial. Las partes convienen, conforme lo establece el artículo 1600 del código civil, que podrá pedirse a la vez la pena y la indemnización de perjuicios a que hubiere lugar.

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 contratista no podrá ceder total o parcialmente su posición contractual sin la autorización previa, expresa y escrita de la ESU. EL contratista tampoco podrá ceder total o parcialmente derechos u obligación contractual alguna sin la autorización previa, expresa y escrita 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. En todo caso, la implementación de los anteriores mecanismos estará supeditada a la necesidad del servicio por parte de la ESU o de sus clientes.

CONFIDENCIALIDAD

El contratista se compromete a guardar la reserva sobre toda la información confidencial, estratégica o sensible por la naturaleza de la misma que pueda obtener de la Secretaría de seguridad y Convivencia del Municipio de Medellín y de la ESU, a la que tengan acceso con ocasión del objeto del presente contrato. 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, sensible, de inteligencia o cualquiera otra suministrada o a la que se tenga acceso en razón del desarrollo de la ejecución del contrato. 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.

El incumplimiento por parte del contratista de sus obligaciones, contenidas en los pliegos de condiciones, con sus documentos anexos, la propuesta comercial presentada y demás documentos integrantes, así como los postulados de la diligencia y buena fe contractual, dará lugar a que la ESU inicie un procedimiento sancionatorio de carácter contractual.

Para el cumplimiento de lo anterior el contratista debe: 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 el objeto del contrato**. 2)** Por mutuo acuerdo de las partes. **3**) Cuando por razones de fuerza mayor o caso fortuito se haga imposible el cumplimiento del objeto contractual. **4)** Por el incumplimiento del contrato

administrativamente declarado por la ESU de cualquiera de las obligaciones establecidas en el contrato**. 5)** Por vencimiento del plazo pactado. **6)** Por las demás causales señaladas en la Ley.

LIQUIDACIÓN

El contrato será objeto de liquidación dentro de los cuatro (4) meses siguientes a su terminación.

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.

En todo caso la liquidación del contrato estará sujeta a las disposiciones del reglamento de contratación de la ESU.

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

El contratista asume la obligación de proteger los datos personales a los que acceda con ocasión del contrato, así como las obligaciones que como responsable o encargado le correspondan acorde con la Ley 1581 de 2012 y sus decretos reglamentarios en cuanto le sean aplicables. Por tanto, deberá adoptar las medidas de seguridad, confidencialidad, acceso restringido y de no cesión en relación con los datos personales a los cuales accede, cualquiera que sea la forma de tratamiento. Las medidas de seguridad que deberán adoptarse son de tipo lógico, administrativo y físico acorde a la criticidad de la información personal a la que accede y/o recolecta, para garantizar que este tipo de información no será usada, comercializada, cedida, transferida y no será sometida a tratamiento contrario a la finalidad comprendida en lo dispuesto en el objeto contractual. En caso de tratarse de datos sensibles, de niños, niñas y adolescentes, tales como origen racial, organizaciones sociales, datos socioeconómicos, datos de salud, entre otros, las medidas de seguridad a adoptar serán de nivel alto. El contratista aportará, para la formalización del contrato, copia de su Política de Protección de Datos Personales y de Seguridad de la Información a la ESU, la cual deberá dar cumplimiento a lo establecido en las disposiciones referente a protección de datos personales. El contratista, con la presentación de la oferta manifiesta que conoce la Política de Protección de Datos de la ESU y que, de ser aceptada la oferta en el proceso del asunto, acepta y se compromete a dar cumplimiento a lo establecido en ella y demás protocolos establecidos por la ESU para el tratamiento de datos personales. Igualmente, El contratista se compromete a informar y hacer cumplir a sus trabajadores las obligaciones contenidas en esta cláusula y las demás que contenga la normativa referente a la protección de datos personales, asimismo los trabajadores de El contratista deben conocer y aceptar la Política de Protección de Datos Personales de la ESU. El contratista indemnizará los perjuicios que llegue a causar a El contratante como resultado del incumplimiento de las leyes 1266 de 2008 y 1581 de 2012, aplicables al tratamiento de la información personal, así como por las sanciones que llegaren a imponerse por violación de la misma. El incumplimiento de las obligaciones derivadas de esta cláusula se considera como un incumplimiento grave por los riesgos legales que conlleva el indebido tratamiento de datos personales, y en consecuencia será considerada justa causa para la terminación del contrato, y dará lugar al cobro de la cláusula penal pactada, sin necesidad de ningún requerimiento, a los cuales renuncia desde ahora

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 el inicio de la ejecución del contrato, el contratista deberá presentar las evidencias de las acciones realizadas en la implementación del mencionado, y el cumplimiento de la tabla de valores de la Resolución 0312 de 2019 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 legal. 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- Registro Nacional de Medidas Correctivas - RNMC. 11- Solicitud privada de oferta SPVA 2021-38. 12-Acuerdo marco 202100183. 13- Consulta de Inhabilidades de la Ley 1918 de 2018 y Decreto 753 de 2019. 14- Demás documentos que se deriven del presente contrato.

NATURALEZA JURÍDICA DEL CONTRATO

Este Contrato se rige por las normas comerciales y civiles, y especialmente, por el Reglamento de Contratación de la Entidad, expedido por la Junta Directiva de la ESU.

DOMICILIO

El domicilio contractual es el Municipio de Medellín.

POR LA ESU,

EDWIN MUÑOZ ARISTIZABAL
Gerente ESU

POR EL CONTRATISTA,

DIEGO FERNANDO RIVERA JIMENEZ
Representante Legal
EVOLUTION TECHNOLOGIES GROUP S A S

Aprobó: Mauricio Alejandro Patiño Restrepo - Subgerente de Servicios
Aprobó: Marelbi Verbel Peña - Subgerente Administrativo y Financiero
Aprobó: Juan Felipe Hernández Giraldo - Secretario General
Revisó: Erika Natalia Ramírez – Asesora de Gerencia ENRM
Revisó: Andrés Felipe Delgado Osorio – Contratista - Unidad de Gestión Jurídica
Proyectó: Daladier Evelio Tangarife Berrio- Profesional Universitario – Unidad Estratégica de Servicios Logísticos

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, por tanto, bajo nuestra responsabilidad lo presentamos para firma.