

	EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU			CONTRATO	
	NIT 890.984.761-8			202300217	
				FT-M6-GC-01 Versión: 10	
CONTRATISTA	NIT	TELÉFONO	FECHA DE SUSCRIPCIÓN		
EVOLUTION TECHNOLOGIES GROUP S A S.	830147784-9	317-427-25-81	28/07/2023		
REPRESENTANTE LEGAL	CÉDULA	DIRECCIÓN DE CONTACTO		TEL./CEL. CONTACTO	
DIEGO FERNANDO RIVERA JIMENEZ	16.369.548	CARRERA 7 #127-48 Oficina. 607- BOGOTÁ		317-427-25-81	
CORREO ELECTRÓNICO	CIUDAD DE EJECUCIÓN	RADICADO REQUERIMIENTO	BIENES O SERVICIOS	DISPONIBILIDAD PRESUPUESTAL	
<a href="mailto:drivera@evolution-it.com.co">drivera@evolution-it.com.co</a> <a href="mailto:jmedina@evolution-it.com.co">jmedina@evolution-it.com.co</a>	MEDELLIN	20231003970	Servicios	2023000507	
CONVENIO	CENTRO DE COSTOS	RUBRO PRESUPUESTAL	DESCRIPCIÓN RUBRO	VALOR CONTRATO	COMPROMISO PRESUPUESTAL
4600098681 DE 2023	21362	23202020080334 -1 /83152 23202020080333 -1/83131	LICENCIAS - SECRETARÍA DE INNOVACION DIGITAL  SERVICIOS - SECRETARÍA DE INNOVACION DIGITAL	NUEVE MIL SETENTA Y NUEVE MILLONES DOSCIENTOS TREINTA Y CUATRO MIL DOSCIENTOS VEINTISÉIS PESOS M/L (\$9.079.234.226)  DICRIMINADOS ASI:  SIETE MIL CIENTO CINCUENTA Y NUEVE MILLONES QUINIENTOS CINCUENTA Y CUATRO MIL TRESCIENTOS OCHENTA Y NUEVE PESOS (\$7.159.554.389) Incluyen IVA  MIL NOVECIENTOS DIECINUEVE MILLONES SEISCIENTOS SETENTA Y NUEVE	2023000687

				MIL OCHOCIENTOS TREINTA Y SIETE PESOS (\$1.919.679.837) Exento de IVA de conformidad con el Artículo 476 estatuto tributario	
--	--	--	--	---	--

**OBJETO**

El contratista se obliga con la ESU a "Servicios profesionales y adquisición de licencias para el fortalecimiento de la seguridad informática para la Secretaría de Innovación Digital, del Distrito Especial de Ciencia Tecnología e Innovación 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 Servicios profesionales para el fortalecimiento de la seguridad informática para la Secretaría de Innovación Digital, del Distrito Especial de Ciencia Tecnología e Innovación de Medellín, el cual que incluye cinco componentes y de acuerdo con las siguientes especificaciones.

Servicio	Detalle	Precio	IVA	Costo final pesos (COP)
Fortalecimiento en la Operación	Revisión SOC	\$ 269.324.434	\$ 51.171.642	\$ 320.496.076
	Revisión SIEM+ Ciberinteligencia	\$ 490.335.189	\$ 93.163.686	\$ 583.498.875
	Licencia	\$ 1.153.262.466	N/A	\$ 1.153.262.466
Gestión continua de Vulnerabilidades	Servicios	\$ 255.320.778	\$ 48.510.948	\$ 303.831.726
	Licencia	\$ 766.417.371	N/A	\$ 766.417.371
CyberArk (PAM)	Servicios	\$ 233.371.172	\$ 44.340.523	\$ 277.711.695
	Licencia	\$ 634.127.593	\$ 120.484.243	\$ 754.611.836
Firewall Base de Datos	Servicios	\$ 288.684.000	\$ 54.849.960	\$ 343.533.960
	Licencia	\$ 2.710.467.729	\$ 514.988.869	\$ 3.225.456.598
Solución CISCO NAC	Servicios	\$ 307.929.600	\$ 58.506.624	\$ 366.436.224
	Licencia	\$ 826.871.765	\$ 157.105.635	\$ 983.977.400
<b>TOTAL</b>		<b>\$ 7.936.112.097</b>	<b>\$ 1.143.122.129</b>	<b>\$ 9.079.234.226</b>

## **Especificaciones esenciales:**

### **Componente 1: Fortalecimiento en la Operación.**

- Revisión Centro de Operaciones de Seguridad SOC
- Revisión del SOC para dar cumplimiento a lo dispuesto en el artículo 17 de la resolución 0500 de 2021 capacidades y servicios de SOC institucionales
- Propuesta de estructura, proceso, procedimiento, formatos, manuales, perfiles, recomendación de herramientas.
- Propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.
- Fortalecimiento de seguridad FIRST
- Plan de acción.

### **Revisión de solución SIEM**

- Evaluación de fuentes y Eventos de Seguridad
- Revisión de documentación asociada a políticas, procedimientos, manuales, instructivos o prácticas asociadas a gestión de usuarios, gestión de logs, gestión de eventos, gestión de accesos, gestión de la actualización de las plataformas tecnológicas.
- Generación de Catálogo descriptivo para el fortalecimiento de actividades de detección y caracterización de eventos de seguridad.

### **Ciberinteligencia y apoyo.**

- Implementación de SIEM.
- Suministro de la solución Splunk Enterprise Security suscripción por 2 años, capacidad de ingesta 50GB/d con almacenamiento en la nube 3 meses. Enterprise Support. (1 contact)
- Implementación de cinco (5) conectores.
- Documento de configuración e implementación
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.

### **Integración Splunk con MISP**

- Documento de configuración e implementación MISP.
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.

### **Parametrizaciones Splunk**

- Configuración de 5 alertas base y creación de 1 acción para la notificación de incidentes.
- Configuración de 5 Dashboards & reports
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
- Recomendaciones de seguridad basadas en hallazgos encontrados durante el servicio.

### **Componente 2: Gestión continua de Vulnerabilidades**

- Revisión del proceso de gestión de vulnerabilidades de la entidad.
- Revisión de Procesos, procedimientos, formatos, instructivos, documentos que soportan el proceso de gestión de vulnerabilidades.
- Revisión de capacidades asociadas al proceso. (Personas, herramientas)



- Revisión de la estructura actual para la gestión continua de vulnerabilidades.

#### **Pruebas de Seguridad:**

- Pruebas de vulnerabilidad para cien (100) direcciones internas.
- Informe ejecutivo, informe técnico.

#### **Suministro de licenciamiento SaaS:**

- Suministro de una suscripción de Tenable por 24 meses. a continuación, se detalle los componentes a entregar:
- Tenable.sc Security Center Suscripción, IP Bands: 1650
- Tenable.io Web Application Scanning, Web Apps: 30
- Transferencia de conocimiento
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual

#### **Capacitación: Pruebas de seguridad en plataformas críticas.**

- Grupo máximo: diez (10) funcionarios
- Diez (10) horas
- Modalidad: Virtual.

#### **Componente 3: Solución de Gestión de Accesos Privilegiados-PAM**

- Suministro de la solución de Gestión de Accesos Privilegiados-PAM CyberArk para la Para 30 usuarios privilegiados. Con los siguientes components a entregar:
- Credential Protection, Session Isolation, Recording, Detection, Remote Access, and Strong Authentication. Price per user permonth Cantidad: 30
- Para implementar la solución PAM en la Entidad con sus módulos base, se ofrecen los servicios profesionales de diseño, implementación, configuración de la solución con el siguiente alcance:
  - Integración con el dominio
  - Parametrización de los módulos PSM, CPM y PVWA
  - Configuración de 16 accesos a servidores
  - Transferencia de conocimiento
  - Documento de configuración
  - Documento de operación.
  - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
  - Capacitación: Privileged Access Management
  - Grupo máximo: diez (10) funcionarios
  - Diez (10) horas
  - Modalidad: Virtual.
  - Suscripción por 24 meses

#### **Componente 4: Solución de seguridad para bases de datos Database Activity Monitoring (DAM)**

- Suministro de la solución Database Activity Monitoring (DAM) por 24 meses Imperva-DAM para la Entidad, Con los siguientes components a entregar:



- Imperva \*SF-SUB-DBF-X452-GWCL-GWCL-TBL  
\*Suscripción de software X4520 para Firewall de base de datos (cantidad 3).
- Imperva \*SS-REPUESTO-X452-H1 \*X4520 Gateway Appliance (cantidad 3)
- Imperva \*SS-REPUESTO-X452-SL3 \*X4520, repuesto in situ para Gateway Appliance. ( cantidad 3)
- Imperva - \*SF-SUB-M17-TBL \*Suscripción de software M170 para el software Management Server, suscripción mejorada. (cantidad 1)
- Imperva - \*SS-REPUESTO-M17-H1 \*Servidor de gestión M170, Appliance. (cantidad 1)
- Imperva - \*SS-REPUESTO-M17-SL3 \*M170 Management Server, repuesto in situ para Appliance. (cantidad 1)
- Imperva - SKU: \*U-DBURM-SUB-100-R-TBL \*Actualización: licencia de administración de derechos de usuario para 100DBis, suscripción mejorada. (cantidad 1)

#### **Implementación de Imperva-DAM con sus módulos base, Para un máximo de 10 bases de datos**

- Transferencia de conocimiento.
- Transferencia de conocimiento
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Capacitación: Seguridad en base de datos y aplicaciones.
- Grupo máximo: Diez (10) funcionarios
- Diez (10) horas
- Modalidad: Virtual.

#### **Componente 5: Solución de Control de Acceso a la red (Next Generation NAC)**

- Suministro de la solución CISCO ISE por 24 meses así:
  - Cisco ISE Virtual Machine Common PID Cantidad 3.
  - SOLN SUPP SWSS Cisco ISE Virtual Machine Common PID Cantidad 3.
  - Cisco Identity Service Engine Essentials Subscription Cantidad: 5100
  - Cisco Identity Service Engine Premier Subscription Cantidad: 7400
  - Cisco ISE Device Admin Node License Cantidad: 3
  - Cisco AnyConnect Apex License, Users: Cantidad: 400
- Implementación de CISCO-ISE con sus módulos base, Para un máximo de 50 dispositivos.
  - Transferencia de conocimiento
  - Documento de configuración
  - Documento de operación.
  - Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
  - Capacitación: 10 horas- Seguridad en redes bajo la filosofía Zero Trust. Control de Acceso a la red.
  - Grupo máximo: 10 personas
  - Modalidad: Virtual.

Las fases propuestas son:

- **FASE I** - Inicio del Proyecto – Entendimiento de la Situación – Construcción del Plan de Gestión del Proyecto

- **FASE II** - Revisión y Fortalecimiento de seguridad Informática.
- **FASE III** – Cierre del proyecto

### **Horario de los servicios**

El horario de ejecución de los servicios será jornada laboral, de lunes a viernes, 8 horas diarias y se establecerá un punto de contacto entre la **ESU** y la **SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN** con el fin de hacer un seguimiento a las actividades. De esta forma se podrá tener una visibilidad completa de lo que está ocurriendo en el proyecto, y de esta manera por vía telefónica o por medio de correo tendrán la posibilidad de direccionar su ejecución. En caso de requerir la ejecución de actividades fuera de este horario la **ESU** y la **SECRETARIA DE INNOVACION DIGITAL DE MEDELLIN** coordinarán las actividades a ejecutar en ventanas programadas y mediante procedimientos de control de cambios del proyecto.

### **FASES DEL PROYECTO**

**FASE I** - Inicio del Proyecto – Entendimiento de la Situación – Construcción Plan Gestión Proyecto En esta etapa se define con exactitud el alcance del proyecto, se ajusta el cronograma de trabajo y responsables; de manera adicional, se define y firma del plan de calidad del proyecto que se convierte su carta de navegación.

Para cumplir con el objetivo de esta etapa, se recopila toda la información necesaria para la ejecución del proyecto. Esta información es la siguiente:

- Pliegos, ofertas y demás documentos de definición y formalización del proyecto
- Requerimientos y necesidades iniciales, vs. implementación actual
- 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
- Contratos
- Clientes de la solución
- Requerimientos normativos, legales que aplican al objeto del Proyecto
- Identificación y formalización de expectativas del cliente.

### **Entregables**

- ✓ Alcance y Objetivos del Proyecto (Según contrato y lo acordado con las partes)
- ✓ 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 base de definitivos.

### **FASE II – Revisión y Fortalecimiento de la seguridad Informática.**

#### **Descripción del servicio**

En esta fase se evaluará el estado de seguridad informática de la **SECRETARIA DE INNOVACION DIGITAL** **siguiendo** las buenas prácticas de seguridad y estándar de la industria. Se desarrollarán cada uno de los componentes definidos en el alcance.

Para cumplir con este objetivo, se utilizará la siguiente estructura de referencia:

- Contexto de la Organización
- Gestión de incidentes de seguridad de la información.
- Controles de seguridad informática base.
- Mejora Continua

#### **Entregables**

- ✓ Requisitos de técnicos para la ejecución del servicio.
- ✓ Cronograma detallado de actividades del proyecto por componente conforme al alcance.

#### **Características de la prestación del servicio:**

Los componentes del servicio son los siguientes

#### **Fortalecimiento de la Operación (Componente 1)**

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

- Revisión de la documentación existente.
- Entrevistas con personal de la Entidad responsable de los procesos y controles de seguridad informática asociados.
- Diagnóstico y análisis del proceso.
- Criterios de valor para identificar las actividades relevantes:
- Tamaño de la entidad, estructura organizacional de seguridad de la información y de seguridad informática, referencias a estándares de seguridad para la gestión de incidentes y cumplimiento legal.

Específicamente se desarrollará:

#### **A. Revisión Centro de Operaciones de Seguridad SOC**

- Revisión de estructura actual del proceso
- Revisión del SOC para dar cumplimiento a lo dispuesto en el artículo 17 de la resolución 0500 de 2021 capacidades y servicios de SOC institucionales
- Propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.
- Fortalecimiento de seguridad FIRST

#### **Entregables:**

- Documento de Informe de madurez de la operación SOC bajo el framework de SOC-GAP
- Documento de estructura del proceso, procedimiento, formatos, manuales, especificación de capacidades requeridas para soportar la operación del SOC (perfiles), recomendación de herramientas.
- Documento de propuesta de especificaciones técnicas para la tercerización del servicio de acuerdo con la oferta disponible en el mercado actual.



- Documento de actividades requeridas y recomendaciones para postular equipo de respuesta de incidentes ante el FIRST

#### **B. Revisión de solución SIEM**

- Evaluación de fuentes y Eventos de Seguridad
- Revisión de documentación asociada a políticas, procedimientos, manuales, instructivos o prácticas asociadas a:
  - ✓ Gestión de usuarios
  - ✓ Gestión de logs
  - ✓ Gestión de eventos,
  - ✓ Gestión de accesos,
  - ✓ Gestión de la actualización de las plataformas tecnológicas

#### **Entregables:**

- Documento que entrega el Catálogo descriptivo para el fortalecimiento de actividades de detección y caracterización de eventos de seguridad que contiene:
- Dispositivos críticos conforme al contexto de Arquitectura tecnológica de la entidad.
- Recomendación de eventos de seguridad a monitorear por tecnología conforme al contexto tecnológico de la entidad.
- Recomendaciones de reglas de filtrado y detección de eventos de seguridad que se deben de configurar en el SIEM.

#### **C. Ciberinteligencia y apoyo.**

- Implementación de SIEM.
- Splunk Enterprise Security suscripción por 2 años, capacidad de ingesta 50GB/d con almacenamiento en la nube 3 meses. Enterprise Support. (1 contact)
  - Implementación de cinco (5) conectores
  - Documento de configuración e implementación
  - Documento de operación.
  - Capacitación por cuatro horas para diez (10) funcionarios

#### **Integración Splunk con MISP**

- Documento de configuración e implementación.
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual

#### **Parametrizaciones Splunk**

- Configuración de 5 alertas base y creación de 1 acción para la notificación de incidentes.
- Configuración de 5 Dashboards & Reports
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.

#### **Entregables:**

- Documento de implementación de herramienta de los siguientes componentes
- Splunk Enterprise Security (Habilitación de Servicio nube)
- Integración MISP
- Parametrización Splunk.
- Documento de configuración e implementación de:
- Splunk y cinco (5) conectores

- ✓ Integración MISP
- ✓ Parametrización Splunk
- ✓ Documento de operación.
- ✓ Splunk Enterprise Security
- ✓ MISP
- ✓ Acta de Capacitación para diez (10) funcionarios

4 horas en administración por cada solución para un total de doce (12) horas:

- Enterprise Security
- MISP
- Parametrización Splunk

\*Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

**Nota:** LA SECRETARÍA DE INNOVACIÓN DIGITAL proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.O, permisos, puertos, protocolos, etc.

### **Gestión continua de Vulnerabilidades (Componente 2)**

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

- Revisión de la documentación existente.
- Entrevistas con personal de la Entidad responsable de los procesos y controles de seguridad informática asociados.
- Diagnóstico y análisis del proceso.

Criterios de valor para identificar las actividades relevantes:

Tamaño de la Entidad, estructura organizacional de seguridad de la información y de seguridad informática, referencias a estándares de seguridad para la gestión de incidentes y cumplimiento legal.

Específicamente se desarrollará:

#### **Revisión de Proceso de Gestión de Vulnerabilidades.**

Análisis, diseño, capacitación e implementación del proceso operativo de Gestión de Vulnerabilidades para la Entidad.

La revisión, diseño y ajustes (optimización) del proceso de Gestión de Vulnerabilidades iniciará con talleres de trabajo y/o entrevistas donde se recolectará toda la información asociada con los procesos, procedimientos, puntos de control, herramientas, responsables y documentación asociada con la gestión actual de la Entidad frente a las vulnerabilidades, de manera que sea posible identificar la situación actual (GAP) frente aspectos operativos de seguridad, requisitos normativos y negocio.

A continuación, se detallan las actividades que se van a realizar para este componente:

- Realización de talleres de trabajo que incluyen entrevistas y evaluación del estado actual (Actividades, Personas, Políticas y Herramientas) de la Gestión de Vulnerabilidades.

El propósito fundamental es conocer detalladamente cómo funciona la operación de la Entidad, los roles y participantes, la interacción con las áreas usuarias y la articulación actual de estos elementos en todo el proceso.

- Se procederá a evaluar lo encontrado para incluir mejoras operativas respecto al cumplimiento de normas, buenas prácticas, estándares internacionales, y políticas-normas-estándares propios que apliquen a la operación de la Entidad.
- Diseño y definición del proceso de Gestión de Vulnerabilidades para la Entidad, donde se incluye descripción del proceso, KPIs, Tableros de Control, Roles y Responsabilidades

**Realización de talleres de trabajo que incluyen entrevistas y descripción de la situación propuesta donde se detalle lo siguiente:**

- Actividades del nuevo proceso
- Roles, responsabilidades y aptitudes
- Niveles de seguridad
- Riesgos
- Modelos de Amenazas
- Cronogramas esperados de solución

#### **Entregables**

- Informe de la situación actual (Gap inicial) del proceso de Gestión de Vulnerabilidades
- Plan de Mejora del Proceso de Gestión de Vulnerabilidades
- Acta de entrega del Proceso de Gestión de Vulnerabilidades
- Acta de divulgación y socialización del Proceso de Gestión de Vulnerabilidades

#### **Pruebas de Seguridad:**

- Identificación de IPs objeto de la auditoría.
- Pruebas de vulnerabilidad para cien (100) direcciones internas.

#### **Entregables:**

- Plan de pruebas de seguridad
- Resumen Ejecutivo donde se centralizan los resultados de las pruebas de seguridad realizadas
- Informe técnico con el detalle de las pruebas en el cual se describen las vulnerabilidades y los resultados obtenidos, recomendaciones de mitigación.
- Acta de socialización de resultados.

#### **Suministro de licenciamiento:**

- Licenciamiento durante 24 meses de:
  - Tenable.sc Security Center Suscripción, IP Bands: 1650
  - Tenable.io Web Application Scanning , Web Apps: 30
  - Transferencia de conocimiento



- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Capacitación: Pruebas de seguridad en plataformas críticas.

**Entregables:**

- Acta de implementación de herramienta (Habilitación de Servicio en la nube) y Arquitectura:
- Tenable.sc y Tenable.io
- Documento de configuración de:
- Tenable.sc y Tenable.io
- Documento de operación.
- Tenable.sc y Tenable.io
- Acta de Capacitación de Tenable.sc y Tenable.io para diez (10) funcionarios, cuatro (4) horas por cada solución para un total de ocho (8) horas. Modalidad Virtual.
- Acta de Capacitación Pruebas de seguridad en plataformas críticas para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

**Solución de Gestión de Accesos Privilegiados PAM (Componente 3)**

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

- Entendimiento de requisitos de la entidad frente a la Gestión de Accesos Privilegiados.
- Entrevistas con personal de la entidad responsable de los procesos y controles de seguridad informática asociados.
- Entendimiento de los activos y Sistemas más Críticos.
- Estrategia de despliegue de la solución de Gestión de Accesos Privilegiados PAM.

**Específicamente se desarrollará:**

**Suministro de la solución de Gestión de Accesos Privilegiados-PAM CyberArk por 24 meses para la Entidad.**

- Para 30 usuarios privilegiados por 24 meses. a continuación, se detalle los componentes a entregar:
- Credential Protection, Session Isolation, Recording, Detection, Remote Access, and Strong Authentication. Cantidad: 30

**Implementación de la solución PAM en la Entidad con sus módulos base, se ofrecen los servicios profesionales de diseño, implementación, configuración de la solución con el siguiente alcance:**

- Ejecución de CyberArk Discovery & Audit (CyberArk DNA®) para escanear los sistemas basados en Active Directory.
  - Revisión de informe.
  - Análisis de resultados.
  - Priorización de Cuentas privilegiadas a proteger.
- Integración con el dominio
- Parametrización de los módulos PSM, CPM y PVWA
- Configuración de 16 accesos a servidores

### **Transferencia de conocimiento**

- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual

### **Capacitación: Seguridad en base de datos y aplicaciones.**

- Grupo máximo: diez (10) funcionarios
- Diez (10) horas
- Modalidad: Virtual.
- Suscripción por 24 meses

### **Entregables:**

- Reporte de CyberArk Discovery & Audit
- Documento de implementación de herramienta CyberArk y Arquitectura:
- CyberArk (PSM, CPM y PVWA)
- Documento de configuración:
- CyberArk (PSM, CPM y PVWA)
- Documento de operación.
- CyberArk (PSM, CPM y PVWA)
- Acta de Capacitación para diez (10) funcionarios, 4 horas en administración por cada solución. Modalidad Virtual. para un total de doce (12) horas:
  - PSM
  - CPM
  - PVWA
- Acta de Capacitación Privileged Access Management para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

\*Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

**Nota: LA SECRETARÍA DE INNOVACIÓN DIGITAL** proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.O, permisos, puertos, protocolos, etc.

### **Solución de seguridad para bases de datos Database Activity Monitoring (DAM) (Componente 4)**

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

- Entendimiento de requisitos de la entidad frente a la protección de bases de datos.
- Entrevistas con personal de la entidad responsable de los procesos y controles de seguridad informática asociados.
- Entendimiento de las bases de datos más Críticas para la Entidad.
- Estrategia de despliegue de la solución de seguridad para bases de datos Database Activity Monitoring (DAM)

### **Específicamente se desarrollará:**

**Suministro de la solución Database Activity Monitoring (DAM) por 24 meses Imperva-DAM para la Entidad, a continuación, se detalle los componentes a entregar:**

- Imperva - \*SF-SUB-DBF-X452-GWCL-GWCL-TBL\* Suscripción de software X4520 para Firewall de base de datos (cantidad 3).
- Imperva - \*SS-REPUESTO-X452-H1 \*X4520 Gateway Appliance (cantidad 3)
- Imperva - \*SS-REPUESTO-X452-SL3 \*X4520, repuesto in situ para Gateway Appliance. (cantidad 3)
- Imperva - \*SF-SUB-M17-TBL \*Suscripción de software M170 para el software Management Server, suscripción mejorada. (cantidad 1)
- Imperva - \*SS-REPUESTO-M17-H1 \*Servidor de gestión M170, Appliance. (cantidad 1)
- Imperva - \*SS-REPUESTO-M17-SL3 \*M170 Management Server, repuesto in situ para Appliance. (cantidad 1)
- Imperva - \*U-DBURM-SUB-100-R-TBL \*Actualización: licencia de administración de derechos de usuario para 100DBis, suscripción mejorada. (cantidad 1)

**Implementación de Imperva-DAM en la Entidad con sus módulos base. Para un máximo de 10 bases de datos. Transferencia de conocimiento.**

- Transferencia de conocimiento
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Capacitación: Seguridad en base de datos y aplicaciones.
- Grupo máximo: Diez (10) funcionarios
- Diez (10) horas
- Modalidad: Virtual.

**Entregables:**

- Documento de implementación de herramienta y Arquitectura:
- Imperva Database Activity Monitoring (DAM)
- Documento de configuración:
- Imperva Database Activity Monitoring (DAM)
- Documento de operación.
- Imperva Database Activity Monitoring (DAM)
- Acta de Capacitación Administración de Imperva Database Activity Monitoring (DAM) para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
- Acta de Capacitación Seguridad en base de datos y aplicaciones para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

\*Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

**Solución de Control de Acceso a la red (Next Generation NAC) (Componente 5)**

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

- Entendimiento de requisitos de la entidad frente al control de acceso a la red.
- Entrevistas con personal de la entidad responsable de los procesos y controles de seguridad informática asociados.
- Entendimiento de Arquitectura de red de la entidad.
- Estrategia de despliegue de Control de Acceso a la red (Next Generation NAC)

**Específicamente se desarrollará:**



#### **Suministro de la solución CISCO ISE 24 meses así:**

- Cisco ISE Virtual Machine Common PID Cantidad 3.
- SOLN SUPP SWSS Cisco ISE Virtual Machine Common PID Cantidad 3.
- Cisco Identity Service Engine Essentials Subscription Cantidad: 5100
- Cisco Identity Service Engine Premier Subscription Cantidad: 7400
- Cisco ISE Device Admin Node License Cantidad: 3
- Cisco AnyConnect Apex License, Users: Cantidad: 400
- Implementación de CISCO-ISE en la Entidad con sus módulos base. Para un máximo de 50 dispositivos. Transferencia de conocimiento.
- Transferencia de conocimiento
- Documento de configuración
- Documento de operación.
- Capacitación para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual
- Capacitación: Seguridad en redes bajo la filosofía Zero Trust.
- Grupo máximo: Diez (10) funcionarios
- Diez (10) horas
- Modalidad: Virtual.

#### **Entregables:**

- Documento de implementación de herramienta y Arquitectura:
- CISCO-ISE
- Documento de configuración:
- CISCO-ISE
- Documento de operación.
- CISCO-ISE
- Acta de Capacitación Administración de CISCO-ISE para diez (10) funcionarios, cuatro (4) horas. Modalidad Virtual.
- Acta de Capacitación Seguridad en redes bajo la filosofía Zero Trust. para diez (10) funcionarios, diez (10) horas. Modalidad Virtual.

\*Se entregará acta de asistencia, diapositivas y evaluación de la capacitación.

**Nota:** LA SECRETARÍA DE INNOVACIÓN DIGITAL proporcionará los recursos de Hardware y software base necesarios para la implementación de las soluciones ofertadas en el presente componente. En la primera fase del proyecto se entregará el documento de requerimientos técnicos requeridos por cada solución: Características de hardware, S.O, permisos, puertos, protocolos, etc.

#### **FASE III – Cierre del Proyecto**

Una vez finalizado el proyecto, se realizará una presentación con sus resultados. De manera adicional, se realiza una entrega formal de toda la documentación del proyecto que se encuentre dentro de su alcance. Esta presentación va acompañada de la carta de aceptación de implementación de la solución y visto bueno de parte del cliente.

#### **Entregables**

- Medio Magnético con Documentación definitiva
- Presentación de cierre
- Acta de Finalización del Proyecto

**PLAZO**

El Plazo de ejecución del presente contrato será hasta el 31 de diciembre de 2023, una vez aprobada la garantía única de cumplimiento por la Unidad de Gestión Jurídica de la ESU.

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 **NUEVE MIL SETENTA Y NUEVE MILLONES DOSCIENTOS TREINTA Y CUATRO MIL DOSCIENTOS VEINTISÉIS PESOS M/L (\$ 9.079.234.226)** DICRIMINADOS ASI: **SIETE MIL CIENTO CINCUENTA Y NUEVE MILLONES QUINIENTOS CINCUENTA Y CUATRO MIL TRESCIENTOS OCHENTA Y NUEVE PESOS (\$7.159.554.389)** Incluyen IVA Y MIL NOVECIENTOS DIECINUEVE MILLONES SEISCIENTOS SETENTA Y NUEVE MIL OCHOCIENTOS TREINTA Y SIETE PESOS (\$1.919.679.837) Exento de IVA de conformidad con el Artículo 476 estatuto tributario.

**TITULAR DESTINATARIO**

Los bienes y/o servicios antes descritos son con destino a la secretaría de innovación Digital en virtud Contrato Interadministrativo 4600098681 DE 2023.

**FORMA DE PAGO**

La ESU cancelará el valor del contrato mediante pagos parciales, con el recibo de cumplimiento a satisfacción por parte del supervisor del contrato y los pagos correspondiente al licenciamiento o suscripciones se facturarán previa orden de compra.

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 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.
- Se debe realizar la factura para cada uno de los servicios soporte o suministro.
- Para el caso de proveedores que se encuentren obligados a facturar electrónicamente, la facturación deberá ser remitida al correo electrónico [facturacion@esu.com.co](mailto:facturacion@esu.com.co) y la fecha límite para la recepción de las mismas estará sujeta a las fechas definidas en la Circular 001 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 prestación de los servicios objeto del presente contrato, se harán en el Distrito Especial de Ciencia y Tecnología 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, bodegaje, transporte, pruebas en caso de que aplique, en el Municipio de Medellín y/o en el sitio que le defina la ESU.

### GARANTÍA CONTRACTUAL

El Contratista se obliga a constituir a favor de "LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS Y/O SECRETARÍA DE INNOVACION DIGITAL DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN 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 y los pliegos de condiciones, los cuales hacen 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 Profesional Universitario de la Unidad Estratégica de Servicios de la Subgerencia de Servicio de la ESU, 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 el 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**

En caso de que exista información sujeta a alguna reserva legal, las partes deben mantener la confidencialidad de esta información, la cual deberá estar previamente marcada como tal, para ello, debe comunicar a la otra parte que la información suministrada tiene el carácter de confidencial. Cada una de las partes acuerda mantener la confidencialidad de la información Confidencial de la otra parte durante un periodo de tres años contados a partir de la fecha de revelación.

#### **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 administrativamente declarado por parte de 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 de propuesta comercial y anexos técnicos del mismo. 12- Consulta de



Inhabilidades de la Ley 1918 de 2018 y Decreto 753 de 2019 - 12- Demás documentos que se deriven del presente contrato, SPVA 2023-65.

**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 en el Distrito Especial de Ciencia Tecnología e Innovación de Medellín.

**POR LA ESU,**



**EDWIN MUÑOZ ARISTIZABAL.**  
Gerente ESU.

**POR EL CONTRATISTA,**



**DIEGO FERNANDO RIVERA JIMENEZ**  
Representante Legal contratista.

Aprobó: Jacqueline Ocampo Arboleda - Subgerente de Servicios   
Aprobó y Revisó: Juan Felipe Hernández Giraldo- secretario general   
Aprobó: Marelbi Verbel Peña - Subgerente Administrativo y Financiero   
Revisó: Sandra Auxilio Arias Chavarría - Profesional Universitaria - Unidad Gestión Jurídica   
Revisó: Erika Natalia Ramírez- Contratista Asesora Gerencial   
Proyectó: Héctor Cifuentes Herron - Profesional Universitario - Subgerencia de Servicios 

**Nota:**

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.