



CLÁUSULA ADICIONAL

Código: FT-M3-COM-3

Versión: 01

Página 1 de 6

CLÁUSULA ADICIONAL No. 1 AL CONTRATO NO 202400167

CONTRATO INTERADMINISTRATIVO:	4600102500 de 2024
PLAZO DEL INTERADMINISTRATIVO:	Vigencia de CIENTO TREINTA Y UN DÍAS (131) sin superar la presente vigencia
CONTRATO No:	202400167
CONTRATISTA:	BMIND S.A.S. BIC
NIT:	900.105.979-1
OBJETO DEL CONTRATO:	Implementación de soluciones tecnológicas para mejorar el control fiscal del Distrito Especial De Ciencia, Tecnología e Innovación de Medellín
PLAZO DEL CONTRATO:	Hasta el 31 de diciembre de 2024 a partir de la aprobación de la póliza única de cumplimiento (20 de septiembre de 2024)
VALOR DEL CONTRATO:	\$665.581.053 Impuestos incluidos
CLÁUSULA ADICIONAL No 1:	Modificar ítem de Forma de pago

La presente constituye la Cláusula adicional No. 1 al contrato No 202400167 de 2024, cuyo objeto es *“Implementación de soluciones tecnológicas para mejorar el control fiscal del Distrito Especial De Ciencia, Tecnología e Innovación de Medellín”*, por la cual es necesario modificar la forma de pago establecida en el contrato 202400167, suscrito entre la Empresa para la Seguridad y Soluciones Urbanas (ESU) y el proveedor BMIND S.A.S BIC. La modificación consistirá en implementar pagos parciales durante la vigencia del contrato”, previas las siguientes:

CONSIDERACIONES

- A. El 28 de agosto de 2024 , entre la Empresa para la Seguridad y Soluciones Urbanas - ESU y el Distrito Especial de Ciencia Tecnología e Innovación de Medellín - Secretaría de Suministros y Servicios, se suscribió el Contrato Interadministrativo No. 4600102500 de 2024 cuyo objeto es **“CONTRATO INTERADMINISTRATIVO DE MANDATO SIN REPRESENTACIÓN PARA LA IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS PARA MEJORAR EL CONTROL FISCAL EN EL MARCO DE LOS CONVENIOS 4600094992 DE 2022 Y 4600100888 DE 2024.”**, con un plazo de ejecución de 131 días calendario sin superar la presente vigencia y por un valor inicial de **SETECIENTOS CUARENTA Y CINCO MILLONES DOSCIENTOS CUARENTA Y CUATRO MIL TRESCIENTOS TRECE PESOS M/L. (\$745.244.313) Impuesto incluido.**
- B. El 20 de septiembre de 2024, se suscribió, entre la Empresa para la Seguridad y Soluciones Urbanas -ESU y el proveedor BMIND S.A.S BIC, el Contrato No. 202400167, cuyo objeto es *“Implementación de soluciones tecnológicas para mejorar el control fiscal del Distrito Especial de Ciencia, Tecnología e innovación de Medellín”*, con un valor inicial de **SEISCIENTOS SESENTA Y CINCO MILLONES QUINIENTOS OCHENTA Y UN MIL CINCUENTA Y TRES PESOS (\$665.581.053)** impuestos incluidos y con un plazo de ejecución hasta el 31 de diciembre de 2024 a partir de la aprobación de la póliza única de cumplimiento por parte de la Unidad de Gestión Jurídica de la ESU.

- C. Las garantías que amparan el contrato No. 202400167 se encuentran vigentes, fueron aprobadas por la entidad, así:

Nombre Aseguradora	N° Póliza	Tipo de Amparo	Cobertura de la Póliza		Fecha de Aprobación de la Garantía	Valor Amparado
			Desde	Hasta		
Seguros Mundial	BCH-100037870	Cumplimiento	20/09/2024	30/06/2025	20/09/2024	\$66.558.105,30
		Prestaciones sociales	20/09/2024	31/12/2027	20/09/2024	\$33.279.052,65
		Calidad del servicio	20/09/2024	30/06/2025	20/09/2024	\$66.558.105,30

- D. En cumplimiento del Reglamento de Contratación de la ESU, el 21 de octubre de 2024, mediante escrito radicado No. 20240006017, la Supervisión del contrato No. 202400167 presentó la justificación para modificar la forma de pago del mencionado contrato teniendo en cuenta:

El contrato No. 202400167 tiene como alcance adquirir licencias de office 365, servicio infraestructura OCI (Oracle Cloud Infraestructure) y administración y soporte de acuerdo con lo indicado a continuación:

Para la ejecución del contrato se requiere:

- a) Administrar la plataforma de nube pública, consiste en tomar medidas para optimizar y gestionar de manera efectiva los recursos y servicios de la infraestructura en la nube. Lo anterior implica:
- Gestión de recursos: Esto implica administrar y controlar los recursos de la nube, como instancias de servidores virtuales, almacenamiento, bases de datos y redes. Incluye actividades como la creación, configuración, escalado y eliminación de recursos según sea necesario para satisfacer las demandas de la empresa.
 - Monitoreo y rendimiento: Es esencial supervisar de cerca la infraestructura en la nube para garantizar un rendimiento óptimo y prevenir problemas. Esto implica la recopilación de métricas y registros, el análisis del rendimiento de los recursos y la detección temprana de posibles cuellos de botella o problemas de seguridad.
 - Seguridad y cumplimiento: La seguridad es un aspecto crítico de la administración de la plataforma de nube pública. Implica implementar medidas de seguridad como el control de acceso, la autenticación, el cifrado de datos, la detección de intrusiones y la protección contra amenazas. Además, se deben cumplir las regulaciones y políticas de seguridad aplicables a la industria y a la empresa.
 - Optimización de costos: La administración efectiva de la plataforma de nube pública implica optimizar los costos asociados con los servicios en la nube. Esto incluye el seguimiento de los gastos, la identificación de oportunidades de



ahorro, la selección adecuada de tipos de instancias y servicios que se ajusten a las necesidades de la empresa, y la implementación de estrategias de ahorro, como el apagado de recursos no utilizados.

- Automatización y orquestación: La automatización de tareas repetitivas y la orquestación de los procesos son componentes clave de la administración de la plataforma de nube pública. Esto implica el uso de herramientas y scripts para automatizar despliegues, configuraciones y tareas de administración, lo que ahorra tiempo y reduce errores manuales.
- Respaldo y recuperación de datos: Es fundamental establecer políticas de respaldo y recuperación de datos para proteger la información crítica de la empresa. Esto implica realizar copias de seguridad periódicas de los datos almacenados en la nube y establecer planes de recuperación ante desastres para garantizar la continuidad del negocio en caso de interrupciones.
- Actualizaciones y parches: Mantener la plataforma de nube pública actualizada con las últimas actualizaciones y parches de seguridad es esencial para proteger contra vulnerabilidades conocidas. La administración de la plataforma implica aplicar de manera regular las actualizaciones recomendadas por el proveedor de servicios en la nube y llevar a cabo pruebas adecuadas para garantizar que las actualizaciones no afecten la funcionalidad de las aplicaciones.

b) Monitorear y gestionar los eventos en nube, consiste en la administración de la infraestructura en la nube. Esto implica supervisar y analizar los eventos que ocurren en la plataforma de nube pública para garantizar el rendimiento, la seguridad y la disponibilidad de los servicios. Lo anterior implica:

- Supervisión de recursos: Se realiza un seguimiento constante de los recursos de la nube, como instancias de servidores virtuales, bases de datos, almacenamiento y redes. Esto implica recopilar métricas relevantes, como el uso de CPU, memoria, ancho de banda y almacenamiento, para evaluar el rendimiento y la utilización de los recursos. La supervisión se puede realizar utilizando herramientas de monitoreo proporcionadas por el proveedor de servicios en la nube o mediante soluciones de terceros.
- Registro de eventos: Se capturan y almacenan los eventos y registros generados por los servicios y aplicaciones en la nube. Los eventos pueden incluir acciones realizadas en la infraestructura, como el inicio o detención de instancias, cambios en la configuración de seguridad o acceso a los recursos. El registro de eventos proporciona una visibilidad completa de las actividades y permite el análisis posterior, la solución de problemas y la auditoría de seguridad.
- Alertas y notificaciones: Se establecen alertas y notificaciones para recibir notificaciones en tiempo real sobre eventos importantes o anomalías en la nube. Estas alertas pueden configurarse para diversos eventos, como superar umbrales de rendimiento, errores de aplicaciones, cambios no autorizados en la configuración o intentos de acceso no autorizados. Las alertas permiten a los administradores y equipos de operaciones tomar medidas inmediatas cuando surgen problemas o violaciones de seguridad.
- Análisis y solución de problemas: El monitoreo continuo de eventos en la nube permite realizar análisis y diagnóstico de problemas en tiempo real. Cuando se

detecta un evento inusual o un problema de rendimiento, los equipos de operaciones pueden investigar rápidamente la causa raíz y tomar medidas correctivas. El análisis de eventos también puede ayudar a identificar patrones de uso, tendencias o posibles mejoras en la infraestructura o aplicaciones.

- Automatización de respuestas: La gestión de eventos en la nube puede aprovechar la automatización para responder rápidamente a ciertos eventos. Por ejemplo, se pueden configurar acciones automáticas para escalar la capacidad de recursos cuando se superen ciertos umbrales de uso, o para desencadenar respuestas automáticas a eventos de seguridad, como el bloqueo de direcciones IP sospechosas. La automatización agiliza la respuesta y reduce la intervención manual.
 - Integración con herramientas de gestión: El monitoreo y gestión de eventos en la nube se puede integrar con herramientas de gestión más amplias, como sistemas de gestión de servicios (ITSM) o plataformas de operaciones en la nube. Esto permite una visión más holística de la infraestructura y facilita la colaboración y la gestión eficiente de incidentes y problemas. Monitorear y gestionar los eventos en la nube implica supervisar y analizar el rendimiento y la seguridad de los recursos en la nube, capturar registros.
- c) Administrar y gestionar los servicios de seguridad en la plataforma nube pública, consiste en implementar y mantener medidas de seguridad para proteger los recursos y los datos alojados en la nube. Lo anterior implica:
- Configuración de seguridad: Esto implica establecer políticas de seguridad y configurar adecuadamente los controles de seguridad proporcionados por el proveedor de servicios en la nube. Se deben aplicar medidas como el control de acceso, la autenticación de usuarios, el cifrado de datos, la segmentación de redes y la protección contra amenazas.
 - Gestión de identidades y accesos: Es esencial administrar usuarios, roles y permisos dentro de la plataforma de la nube para garantizar el acceso a los recursos y la seguridad de la información y los accesos a los recursos en la nube. Esto incluye la gestión de identidades, la autenticación de usuarios, la implementación de políticas de contraseñas seguras, el control de privilegios y el monitoreo de actividades de acceso para detectar comportamientos sospechosos.
 - Protección contra amenazas: Se deben implementar medidas de seguridad para proteger los recursos en la nube contra amenazas como ataques de malware, hacking, denegación de servicio y fugas de datos. Esto puede incluir la implementación de firewalls, sistemas de prevención de intrusiones (IPS), detección de malware, filtrado de contenido y sistemas de monitoreo de seguridad.
 - Auditoría y cumplimiento: La administración de servicios de seguridad en la nube también implica llevar a cabo auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y las regulaciones aplicables. Esto puede incluir la revisión de registros de eventos, análisis de vulnerabilidades y asegurarse de que se sigan las mejores prácticas de seguridad.

- Respuesta a incidentes: Se deben establecer procesos y planes de respuesta a incidentes para abordar y mitigar posibles brechas de seguridad o eventos adversos. Esto incluye la identificación temprana de incidentes, la contención de la situación, la investigación forense, la notificación a las partes afectadas y la implementación de medidas correctivas.
- Actualizaciones y parches de seguridad: Mantener la plataforma de nube pública actualizada con las últimas actualizaciones y parches de seguridad es crucial para protegerla contra vulnerabilidades conocidas. Esto implica aplicar de manera regular las actualizaciones recomendadas por el proveedor de servicios en la nube y realizar pruebas adecuadas para garantizar que las actualizaciones no afecten la funcionalidad de las aplicaciones.
- Educación y concientización sobre seguridad: La gestión de servicios de seguridad en la nube también implica fomentar una cultura de seguridad y brindar capacitación y concientización a los usuarios y al personal de la empresa. Esto ayuda a promover buenas prácticas de seguridad, como el uso de contraseñas seguras, la protección de datos confidenciales y la identificación de posibles amenazas y ataques.

La necesidad de modificar el contrato surge debido a la forma de pago establecida con el proveedor del servicio, ya que está definido de la siguiente forma: “La ESU cancelará el valor del contrato **mediante único pago** contra suscripción de las licencias y con el recibo de cumplimiento de la prestación del servicio objeto de la contratación y la emisión del recibo a satisfacción por parte del supervisor del contrato”

El ítem que cumple con el pago inmediato corresponde a la Infraestructura Oracle Cloud (OCI) durante un año, la cual se soporta con la entrega de la suscripción del servicio.

En cuanto a la administración y soporte (Bolsa de créditos) es importante tener en cuenta que el mantenimiento y soporte va ligado a la vigencia de las licencias de la Infraestructura de Oracle Cloud (OCI), la cual está establecida para un año y el contrato interadministrativo del cual se derivó se encuentra vigente hasta 31 de diciembre, por lo cual la forma de pago debe estar definida sobre el plazo contractual.

Las licencias de Office relacionadas no pueden pagarse en el pago inicial, ya que éstas vencen el 11 de diciembre del año en curso.

Con base en lo expuesto, es necesario modificar la forma de pago establecida en el contrato 202400167, suscrito entre la Empresa para la Seguridad y Soluciones Urbanas (ESU) y el proveedor BMIND S.A.S BIC. La modificación consistirá en implementar pagos parciales durante la vigencia del contrato, en función del plazo del contrato interadministrativo del cual se deriva.

E. La información presupuestal es la siguiente:

Contrato Interadministrativo	4600102500 de 2024
Centro de costos	33277
Rubro al presupuesto	23202020080382-1





CLÁUSULA ADICIONAL

Código: FT-M3-COM-3

Versión: 01

Página 6 de 6

Descripción al Rubro	IMPLEMENTACION DE SOLUCIONES TECNOLOGICAS
Disponibilidad presupuestal	2024000652
Registro presupuestal	2024000889
Requerimiento N°	20241005000

Por lo anterior, las partes acuerdan:

PRIMERO: Modificar la forma de pago, quedando de la siguiente manera:

“La ESU cancelará el valor del contrato mediante pagos parciales de acuerdo con las actividades ejecutadas dentro del mes y la emisión del recibo a satisfacción por parte del supervisor del contrato o de acuerdo con la necesidad del servicio objeto de la contratación”.

SEGUNDO: Esta cláusula adicional está cubierta por las garantías expedidas para el contrato No. 202400167, sin embargo, de ser necesario, el Contratista deberá reponer el monto de la garantía cada vez que, debido a los requerimientos o sanciones impuestas, el mismo se disminuyere o agotare. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

TERCERO: Al recibo del presente documento, el CONTRATISTA contará con máximo dos (2) días hábiles para la suscripción y legalización.

CUARTO: Las modificaciones que se estipulan en el presente documento, no constituyen novación al contrato, el cual continua vigente en todo aquello que no ha sido modificado por el presente documento, y sus cláusulas permanecerán indemnes.

Para constancia se firma en la ciudad de Medellín, el 24 de octubre de 2024


CAMILO ZAPATA WILLS
Gerente ESU


CAROLINA GARCIA SANCHEZ
Representante Legal

Aprobó: Laura Alexandra Sepúlveda Marín - Secretaria general

Aprobó: Angelica María López Garces-Subgerente de Servicios

Aprobó: Nathalia Restrepo Caro- Subgerente Administrativo y Financiero

Aprobó: Diego Alejandro Londoño Montoya- Supervisor del contrato N°202400167

Revisó: Carlos Valencia Osorio-Contratista- Subgerencia administrativa y financiera

Revisó: Luis Miguel García Rendon-Profesional Universitario-Unidad Gestión Jurídica

Proyectó: Juliana Isabel Aguilar Duque-Profesional Universitario-Unidad compras y contratación

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.