DATOS DEL SOLICITANTE:	
Supervisor	INGRID REGINA PETRO GONZÁLEZ / *Gerente de Prevención del Fraude.*
Vicepresidencia / Oficina, Gerencia y Dirección	*Vicepresidencia de Seguridad y Riesgos Empresariales*
TIPO DE SOLICITUD:	
Adición Valor	*SI*
Prórroga Plazo	*SI*
Adición y Prórroga	*SI*
Modificación contenido de alguna cláusula	*SI*
Suspensión	*NO*
CONTRATO No:	*048 de 2023*
OBJETO:	Prestar el servicio de gestión y monitoreo de los dispositivos informáticos de la infraestructura tecnológica de Colpensiones a través de un centro de operaciones de seguridad SOC.
CONTRATISTA:	PASSWORD CONSULTING SERVICES S.A
PLAZO DE EJECUCION:	El plazo para la ejecución del contrato es de quince (15) meses.
VALOR DEL CONTRATO:	$567.997.500

ESTADO DE EJECUCIÓN FINANCIERA DEL CONTRATO

Valor pagos realizados incluida la factura del periodo: $ 444.164.501,15 discriminados, así:

PAGOS	VALOR UNITARIO	VALOR TOTAL
Servicio de gestión y monitoreo de los dispositivos informáticos de la infraestructura tecnológica de Colpensiones a través de un **centro de operaciones de seguridad SOC.**	$ 444.164.501,15	$ 444.164.501,15
Servicio de análisis y/o copia forense por demanda, para este propósito se tienen 100 horas disponibles, que serán consumidas y facturadas de acuerdo con la necesidad.	N/A No se hizo uso de horas	N/A No se hizo uso de horas
Servicio de investigación y respuesta a incidentes. Incluye el acompañamiento en todas las fases de la gestión de los incidentes de seguridad desde la fase de preparación hasta su contención y erradicación, por demanda, para este propósito se tienen 25 horas disponibles que serán consumidas y facturadas de acuerdo con la necesidad.	N/A No se hizo uso de horas	N/A No se hizo uso de horas
	TOTAL PAGADO	$ 444.164.501,15

Saldo del contrato: $ 123.832.998,85

JUSTIFICACIÓN:

La Gerencia de Prevención de Fraude (GPF) y la Vicepresidencia de Seguridad y Riesgos Empresariales (VSRE), teniendo las premisas establecidas por PETI, desarrolló el proyecto de detección y prevención del fraude, el cual se materializó en el contrato 183 de 2019, el cual tuvo como objetivo "Implementar, configurar, administrar, monitorear y soportar una solución integral de recolección, almacenamiento, correlación, tratamiento y análisis de logs, y otras fuentes de información, para la detección de anomalías a través de modelos de analítica descriptiva y predictiva, con el objetivo de detectar hechos de fraude y corrupción,

de acuerdo con la arquitectura de referencia", y en el que se adquirió e implementó la herramienta de ELASTICSEARCH Enterprise para el datacenter principal de Colpensiones, en ambientes de pruebas y producción. Elasticsearch es un SIEM (Security Incident and Event Management) que permite hacer correlación de eventos y gestionar alertas relacionadas con desviaciones al cumplimiento de las políticas de seguridad de la información y de protección de datos personales, herramienta que es utilizada por el servicio de SOC (Security Operation Center), y que a su vez se integró al contrato 090 de 2021, y actualmente al contrato 048 de 2023, en donde se realiza la gestión y monitoreo de los dispositivos informáticos de la infraestructura tecnológica de Colpensiones a través de un centro de operaciones de seguridad SOC, servicio que se apoya en el uso de esta herramienta y que ha permitido fortalecer la detección de hechos de fraude y/o corrupción, y el esquema de monitoreo que se hace desde la Gerencia de Prevención del Fraude.

Esta integración entre la herramienta y el servicio de SOC, se da adicionalmente como respuesta a lo requerido por la Superintendencia Financiera de Colombia en su Circular Externa 007 de 2018 sobre ciberseguridad, en donde Colpensiones debe mitigar los riesgos que pudieran afectar la seguridad de sus sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos, con el fin de fortalecer la protección de la información de Colpensiones, y en la que se requiere adicionalmente lo siguiente:

> *"3.4. Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.*
> *4.1. Prevención Las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad. En esta etapa, las entidades deben cuando menos.*

	4.1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información. *4.1.5. Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación.* *4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad."* *De acuerdo con lo establecido por la circular, y con el alcance actual del Centro de Operaciones de Seguridad SOC, el cual fue contratado el 11 de agosto de 2023 y hasta el 19 de noviembre de 2024 mediante el contrato 048 de 2023 bajo la modalidad de servicio, y con el objetivo de fortalecer y desarrollar metodologías y estrategias para gestionar y prevenir el riesgo de fraude y corrupción, basadas en buenas prácticas, es necesario ajustar los requerimientos para conformar el SOC en las instalaciones de Colpensiones, para de esta forma realizar un proceso acorde a las necesidades actuales, y en el que se dé continuidad a los servicios de un centro de operaciones de seguridad SOC, que gestione y realice el monitoreo 7x24 de los dispositivos a través del SIEM de Colpensiones.* *Para esto se requiere la adición de un mes más de operación por valor de* $ 34.166.500 y que corresponden al "Servicio de gestión y monitoreo de los dispositivos informáticos de la infraestructura tecnológica de Colpensiones a través de un centro de operaciones de seguridad SOC.", tomando los recursos del saldo disponible del contrato. De acuerdo con los anterior se requiere una prórroga en el plazo.
DESCRIPCIÓN MODIFICACIÓN - OTROSI:	En virtud de lo anterior, se requiere modificar: **1.** Modificar la cláusula **TERCERA. PLAZO DE EJECUCIÓN**

	El plazo para la ejecución del contrato será de dieciséis (16) meses, contados a partir de la suscripción del acta de inicio, previa aprobación de la garantía de cumplimiento del contrato.
CERTIFICADO DE DISPONIBILIDAD:	N/A
ANEXOS:	*Se adjunta a la solicitud, los siguientes documentos:* o *Informe Parcial de Ejecución y Supervisión*

Firmado en Bogotá, el 30 de octubre de 2024.

DIEGO FERNANDO FLÓREZ CORSO
GERENTE - VICEPRESIDENTE (A)
GERENCIA DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN
VICEPRESIDENCIA DE SEGURIDAD Y RIESGOS EMPRESARIALES

INGRID REGINA PETRO GONZÁLEZ
GERENTE DE PREVENCIÓN DEL FRAUDE

Objeto: *Prestar el servicio de gestión y monitoreo de los dispositivos informáticos de la infraestructura tecnológica de Colpensiones a través de un centro de operaciones de seguridad SOC.*
Elaboró: Alejandro Alvarez Alonso, Profesional - GPF
Revisó: William Alirio Sandoval, Profesional - GPF