# Apo.4.1.Fr.002 Cumplido para Pago

| Codigo: | Apo.4.1.Fr002 | Fecha | 31/01/2023 | Versiòn | 6 |
|---|---|---|---|---|---|

CONS **17**

PARA: SUBDIRECCION FINANCIERA Y GRUPO DE CONTRATOS RADICADO No.: CP -

**DATOS GENERALES DEL CONTRATO**

CONTRATO, ORDEN O CONVENIO No. **3** . **471** - **2023**

NIT O DOCUMENTO DE IDENTIFICACION DEL CONTRATISTA 901778397

OBJETO DEL CONTRATO, ORDEN O CONVENIO: CONTRATAR LOS SERVICIOS DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA EL MONITOREO, ALERTAMIENTO Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA PLATAFORMA TECNOLÓGICA DEL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

**No.Compromiso** 179823

FECHA DE SUSCRIPCION DEL CONTRATO, ORDEN O CONVENIO 11/12/2023

NOMBRE CONTRATISTA: CONSORCIO MNEMO SOC-MHCP

SALDO 1,117,646,160.00

VALOR DEL CONTRATO 2,313,205,920.00

VALOR ADICIONES .00

FECHA DE INICIO: 19/12/2023

FECHA DE TERMINACION: 31/10/2025

**VALOR PAGADO:** 1,195,559,760.00 **VALOR PENDIENTE POR EJECUTAR:** 1,117,646,160.00 **% EJECUCIÒN:** 52

**DATOS ESPECIFICOS DEL PAGO**

| Tipo de Pago | No. | Condicion de Pago | Aclaracion del | Valor.Pago | Iva Aplicado | Valor Iva | Amortizacion Anticipada | Total a Pagar |
|---|---|---|---|---|---|---|---|---|
| FACTURA NO. | FE 18 | CONDICION DE PAGO | MONITOREO,DIAGNÓSTICO,GENERACIÓN DE ALERTAS Y RECOMENDACIONES. MARZO 2025 | 74,749,495.80 | 19 % | 14,202,404.20 | | 88,951,900.00 |
| FACTURA NO. | FE 18 | CONDICION DE PAGO | SERVICIOS DE GESTIÓN Y ANÁLISIS DE VULNERABILIDADES. MARZO 2025 | 2,508,067.23 | 19 % | 476,532.77 | | 2,984,600.00 |
| | | | TOTALES | 77,257,563.03 | | 14,678,936.97 | | |

TOTAL A PAGAR 91,936,500.00

**Anexos y No. de Folios**

| | | | | | |
|---|---|---|---|---|---|
| Factura | 1 | Cuenta de Cobro | | Declaracion juramentada Seguridad Social | |
| Otros Anexos o Folios | 4 | Entrada a Almacen | | Constancias de pago de la seguridad social | 2 |
| | | | | Total de Folios Anexos | 7 |

En calidad de Supervisor/Interventor del contrato enunciado, certifico que he verificado el cumplimiento a satisfaccion de las obligaciones que emanan del contrato, la acreditacion del pago de obligaciones con el sistema de seguridad social integral y las cifras y valores corresondientes al periodo certificado para el reconocimiento del pago que por este instrumento se acredita

SUPERVISORES Y/O INTERVENTORES

Firmado digitalmente por Luis Orlando Arenas Ruiz

FIRMA:
NOMBRE: LUIS ORLANDO ARENAS RUIZ
CARGO: ASESOR
CEDULA: 79398357

**CONSORCIO MNEMO SOC-MHCP**
NIT 901.778.397-6
CALLE 99 10 19
Tel: (601) 5527210
Bogotá - Colombia
contadorjunior@mnemo.com

Factura electrónica de venta
**No. FE 18**

| | | | |
|---|---|---|---|
| **Señores** | MINISTERIO DE HACIENDA Y CREDITO PUBLICO | | |
| **NIT** | 899.999.090-2 | **Teléfono** | (601) 3811700 - Ext. 000 |
| **Dirección** | Cra 8 6C 38 | **Ciudad** | Bogotá - Colombia |

| **Fecha y hora Factura** | |
|---|---|
| **Generación** | 24/04/2025, 16:18 |
| **Expedición** | 24/04/2025, 16:25 |
| **Vencimiento** | 24/05/2025 |

| Ítem | Descripción | Cantidad | Vr. Total |
|---|---|---|---|
| 1 | Monitoreo,Diagnóstico,Generación de Alertas y recomendaciones.<br>Contrato: 3.471-2023<br>Periodo de facturación:01/3/2025 al 31/03/2025 | 1.00 | 88,951,900.00 |
| 2 | Servicios de gestión y análisis de vulnerabilidades.<br>Contrato: 3.471-2023<br>Periodo de facturación:01/03/2025 al 31/03/2025 | 1.00 | 2,984,600.00 |

**Total items:** 2

| | |
|---|---|
| **Total Bruto** | 77,257,563.03 |
| IVA 19% | 14,678,936.97 |
| **Total a Pagar** | **91,936,500.00** |

**Valor en Letras:**
Noventa y un millones novecientos treinta y seis mil quinientos pesos m/cte

**Forma de pago:**
Crédito

**Medio de pago:**
Otro - Crédito - Cuota No. 001 vence el 2025-05-24 por $ 91,936,500.00

**Observaciones:**
#$13-01-01-000;13.471-2023;Luis.Arenas@minhacienda.gov.co#$
Distribución del ingreso:
Mnemo Colombia S.A.S. 99% NIT 900.396.176-1 Contribuyente
Mnemo Evolution & integration Service SA 1% NIT:901.306.687-2 Contribuyente

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764084941503 aprobado en 20241209 prefijo FE desde el número 14 al 5000 Vigencia: 12 Meses**
Responsable de IVA - Actividad Económica 6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Tarifa 9.66
**CUFE:** bdac59d1b525c417947c56f5a2d00baaa9f8f98bb00eb0e0b1f9c41f7539ba2fc554cc2d93d2529aa44d4c6e221a9b0a

## CONTENIDO DEL INFORME

1. Condiciones del Contrato ..... 1
2. Objeto del Contrato ..... 1
3. Obligaciones del Contrato, Actividades Ejecutadas y Productos Entregados ..... 1

## 1. CONDICIONES DEL CONTRATO

| | |
|---|---|
| Número de Contrato: | 3.471 - 2023 |
| Nombre del Contratista: | **CONSORCIO MNEMO SOC-MHCP** |
| Periodo informe: | marzo 01 al 31 de marzo de 2025 |
| Supervisor: | Luis Orlando Arenas Ruiz |
| Área perteneciente: | Dirección de Tecnología |

## 2. OBJETO DEL CONTRATO

Contratar los servicios de un Centro de Operaciones de Seguridad (SOC) para el monitoreo, alertamiento y gestión de la seguridad de la información de la plataforma tecnológica del Ministerio de Hacienda y Crédito Público.

## 3. OBLIGACIONES DEL CONTRATO, ACTIVIDADES EJECUTADAS Y PRODUCTOS ENTREGADOS

Las obligaciones adquiridas son las siguientes:

| |
|---|
| **1. Debe prestarse 7x24x365 (Siete días a la semana, veinticuatro horas al día trescientos sesenta y cinco días al año), incluye días festivos, y fines de semana, con analistas de seguridad y un líder de servicios SOC, con un esquema de escalamiento de incidentes**<br>• Para el mes de marzo del 2025 se ejecutó monitoreo sobre los 24 activos de información integrados en el SIEM Qradar de IBM y la configuración de los 82 casos de uso para el proceso de alertamiento. Se realiza el envío de alertas tempranas y preventivas para el servicio de CTI, vigilancia digital y SOC. |
| **2. Debe monitorear, identificar y notificar alertas de vulnerabilidades que puedan derivar en incidentes de seguridad que afecten a la infraestructura de sistemas, redes o servicios del Ministerio de Hacienda. Lo anterior de acuerdo con esquema de escalamiento definido por el Ministerio**<br>• Para el mes de marzo del 2025 se realizó el envío de 80 alertas de seguridad a los funcionarios y colabores del MHCP incluidos en la matriz de escalamiento versión 11, sobre los 24 activos integrados con el dispositivo SIEM, descritos en el informe mensual de SOC de marzo. |

**3. Debe soportar la toma de decisiones en caso de identificarse que la infraestructura del Ministerio de Hacienda pueda estar sujeta a una amenaza, vulnerabilidad o ataque.**

- Para el mes de marzo se realiza recomendaciones y acompañamiento de remediaciones sobre el alertamiento de los activos incorporados para el monitoreo, para cada uno de los servicios prestados:
  -SOC: Mediante las sesiones de afinamiento técnico con periodicidad semanal los martes.
  -Vigilancia digital: Monitoreo en tiempo real de la exposición de dominios, filtración de credenciales, exposición y reputación de la marca entre otras.
  -CTI: De acuerdo con la infraestructura de MHCP se relacionan las alertas preventivas y tempranas para dar cierre a las vulnerabilidades, brechas de los fabricantes e información sobre potenciales amenazas de seguridad.
  -Forense: Actividad de extracción de forense de acuerdo con solicitud de investigación realizada por el área de tecnología y control interno de MHCP.

**4. Debe soportar la toma de decisiones en caso de identificarse que la infraestructura del Ministerio de Hacienda pueda estar sujeta a una amenaza, vulnerabilidad o ataque.**

- Se enviaron las alertas tempranas asociada a nuevas vulnerabilidades que afectan a proveedores y equipos que se manejan y se tienen en la infraestructura de MHCP.
- Se enviaron las alertas preventivas asociadas a IOC para la gestión interna de MHCP.
- Envió de alertas de vigilancia digital para dar gestión de baja a dominios y sitios no oficiales usando el nombre de la entidad, se enviaron alertas referentes a menciones de marca, ataque a la reputación, filtración de documentos y credenciales de terceros y empleados.
- Atención a requerimiento para análisis forense Numero 5 de acuerdo con el escenario y expediente indicado por MHCP.
- Socialización de informe de análisis de riesgo y nivel de madurez en la postura de ciberseguridad desde diferentes frentes: Gestión de riesgos de seguridad de la información Nivel de riesgo y ciberseguridad, Riesgo de implementación y seguimiento y riesgo técnico.

**5. Gestión avanzada de incidentes, medición de impacto, generación de planes de acción que debe ser utilizada por el personal interno del SOC para establecer un sistema experto de tratamiento de los incidentes, donde se realiza la caracterización, se cataloga por taxonomía interna y se diseña el plan de acción adecuado.**

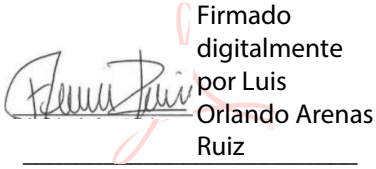
- Proceso de alertamiento desde el servicio de soc, cti y vigilancia digital, en cuyos entregables mensuales y socializaciones de estos se destacan las recomendaciones y acciones principales a tener en cuenta para la mitigación de riesgo de acuerdo con los hallazgos y vulnerabilidades.
- Socialización del análisis de riesgo realizado a entidad desde diferentes frentes y el estado de madurez a nivel de seguridad de la información y ciberseguridad de la entidad.
- Se realiza el estudio e investigaciones de vulnerabilidades e IOC que pueden afectar a la infraestructura de la entidad, de las cuales se generan unas recomendaciones descritas en las alertas tempranas y preventivas.

| |
|---|
| **6. Entregar informes periódicos (por lo menos mensual) con los reportes históricos de monitoreo y gestión de alarmas realizadas.**<br><br>• Se realiza él envió de los informes de alertas tempranas y preventivas para el servicio de CTI, informe de servicio de SOC y servicio de vigilancia digital correspondiente a marzo del 2025. |
| **7. Se debe realizar periódicamente (por lo menos cada tres meses), sobre una cantidad de 1000 IP´s correspondientes a componentes de la infraestructura computacional del Ministerio. Sobre los activos que el Ministerio considere críticos o que soporten servicios esenciales de la entidad, el análisis debe realizarse de forma permanente y persistente.**<br><br>• Se encuentra en gestión culminación de levantamiento información, pruebas de alcance, validación de permisos de red e inicio de análisis de vulnerabilidades de los activos con conectividad para analizar en el 1 trimestre del 2025. |
| **8. Se debe realizar periódicamente (dos veces al año), sobre una cantidad de 10 aplicaciones y/o IP correspondientes a componentes de la infraestructura del Ministerio. Sobre los activos que el Ministerio considere críticos o que soporten servicios esenciales de la entidad**<br>.<br><br>• Levantamiento de información de los 10 activos para el ejercicio de ethical hacking del 1 semestre del 2025. |
| **Productos del contrato**<br><br>Los productos y entregables del contrato se relacionan en el siguiente Link: |

**FIRMA DEL CONTRATISTA**
Humberto de Jesús Vélez

En mi calidad de supervisor del contrato me permito avalar el contenido del informe y el avance en la ejecución del mismo de acuerdo a lo descrito.

El contrato no presenta a la fecha dificultades en su ejecución, ni situaciones exógenas que afecten el normal desarrollo del mismo.




**FIRMA SUPERVISOR**
Luis Orlando Arenas