

 AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	FORMATO			
	FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL			
Principio de procedencia: 4000.092	Clave: GCON-1.0-12-046	Versión: 02	Fecha: 04/oct/2019	Página: 1 de 7

CONTENIDO DEL INFORME

- CONDICIONES DEL CONTRATO
- OBJETO DEL CONTRATO
- ACTIVIDADES EJECUTADAS, OBLIGACIONES CUMPLIDAS, PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS.
- OBSERVACIONES A LAS ACTIVIDADES EJECUTADAS, A LAS OBLIGACIONES CUMPLIDAS, Y A LOS PRODUCTOS Y/O BIENES ENTREGADOS.
- OBSERVACIONES ADICIONALES, SI A ELLO HUBIERE LUGAR.
- PORCENTAJES DE AVANCE PRESUPUESTAL Y EN EJECUCIÓN DEL CONTRATO.

1. CONDICIONES DEL CONTRATO

Número de Contrato:	Contrato No.24001295 H3 2024
Nombre del Contratista:	UT Gestión Ciber
Periodo informe:	1 de agosto al 31 de agosto de 2025
Nombre de Supervisor:	Alvaro Eduardo Varela Arenas Freddy Alejandro Reina Morales
Nombre del Interventor:	
Área perteneciente:	Dirección de Infraestructura y Soporte de TI

2. OBJETO DEL CONTRATO

“PRESTAR SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA GESTIÓN DE EVENTOS DE CIBERSEGURIDAD DE LA RED DE DATOS.”

3. ACTIVIDADES EJECUTADAS, OBLIGACIONES CUMPLIDAS, PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS.

3.1. ACTIVIDADES EJECUTADAS:



AERONÁUTICA CIVIL
UNIDAD ADMINISTRATIVA ESPECIAL

FORMATO

FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL

Principio de procedencia:
4000.092

Clave: GCON-1.0-12-046

Versión: 02

Fecha: 04/oct/2019

Página: 2 de 7

PERÍODO: 1 al 31 de agosto del año 2025

ACTIVIDAD	DESCRIPCIÓN	ENTREGA
SIEM	Parametrización de regla (Windows Brute Force Detected)	25 de agosto de 2025
SIEM	Implementación del SOAR contra el FW de Aerocivil para bloqueos de IoC	31 de agosto de 2025
SIEM	Creación plan de trabajo para Monitoreo de anomalías DNS	29 de agosto de 2025
SIEM	Envío de información relevante para alimentar reglas de correlación	27 de agosto de 2025
Protección de marca	Identificación de documentos sensibles alojados en plataformas de terceros (Scribd)	3, 5, 6, 9, 11, 12, 20, 24, 26, 27, 30 y 31 de agosto de 2025
Protección de marca	Ejecución de 19 solicitudes de Takedown exitosas sobre dichos documentos	3, 5, 6, 9, 11, 12, 20, 24, 26, 27, 30 y 31 de agosto de 2025
Protección de marca	Detección de una credencial activa perteneciente a un usuario interno en la Deep Web, asociada a una plataforma externa	3 de agosto de 2025
Protección de marca	Emisión de 4 reportes semanales relacionados con usuarios identificados en el ciberespacio	5, 12, 19 y 26 de agosto de 2025
Protección de marca	Desarrollo de 11 boletines Lite por parte del equipo, con foco en malware, CVEs, IoCs, campañas y otras amenazas relevantes	23, 24, 25, 26, 27, 29 y 30 de agosto de 2025
Threat Hunting	Ejecución de investigaciones basadas en hipótesis. Conexiones Externas.	15 de agosto de 2025
Threat Hunting	Ejecución de investigaciones basadas en hipótesis. Tráfico DNS Persistente con Duración Acumulada.	26 de agosto de 2025

 <p>AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL</p>	FORMATO			
	FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL			
Principio de procedencia: 4000.092	Clave: GCON-1.0-12-046	Versión: 02	Fecha: 04/oct/2019	Página: 3 de 7

Threat Hunting	Elaboración y envío de los informes con las recomendaciones para las respectivas acciones de contención. Conexiones Externas.	19 de agosto de 2025
Threat Hunting	Elaboración y envío de los informes con las recomendaciones para las respectivas acciones de contención. Tráfico DNS Persistente con Duración Acumulada.	27 de agosto de 2025
Vulnerabilidades	Entrega de manual para despliegue masivo de agentes en server Windows para escaneos autenticados	12 de agosto de 2025
Vulnerabilidades	Despliegue de agentes en 4 máquinas, se espera despliegue masivo	20 de agosto de 2025
Vulnerabilidades	Remediación de vulnerabilidades altamente explotables en dispositivos de comunicación Cisco	5 al 19 de agosto de 2025
Vulnerabilidades	Scan de Vulnerabilidades WEB a 5 URL	15 y 28 de agosto de 2025
Reportes	Reporte semanal del estado y salud de las plataformas existentes	5, 12, 19, 26 de agosto de 2025
Reportes	Informe detallado de causas y acciones de las incidencias de ciberseguridad	5 de septiembre de 2025
Reportes	Informe quincenal de eventos de seguridad	12 y 26 de agosto de 2025
Gestión de vulnerabilidades	Seguimiento semanal al servicio de gestión de vulnerabilidades	6, 21 y 28 de agosto de 2025
Gestión de SOC	Seguimiento semanal al servicio	7, 14, 21 y 28 de agosto de 2025

3.2 OBLIGACIONES CUMPLIDAS:



AERONÁUTICA CIVIL
UNIDAD ADMINISTRATIVA ESPECIAL

FORMATO

FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL

Principio de procedencia:
4000.092

Clave: GCON-1.0-12-046

Versión: 02

Fecha: 04/oct/2019

Página: 4 de 7

OBLIGACIONES	DESCRIPCIÓN DE AVANCE O CUMPLIMIENTO	UBICACIÓN DE SOPORTES
3.1.1 Obligaciones directas del servicio del SOC Numerales: 1-11, 13-15, 17-18	Capacidades y dimensionamiento del servicio acorde a la especificación funcional del Formato 8	N/A
3.1.1 Obligaciones directas del servicio del SOC Numerales: 12, 20-21	Modelo de operativo para el servicio incluyendo los procesos para la atención de incidentes	Correo electrónico
3.1.1 Obligaciones directas del servicio del SOC Numerales: 16	Seguimiento a riesgos de acuerdo con la periodicidad definida	Correo electrónico
3.1.1 Obligaciones directas del servicio del SOC Numerales: 26	Disponibilidad del servicio SOC del 99.5% 7X24X365	Correo electrónico
3.1.1 Obligaciones directas del servicio del SOC Numerales: 30-31	Cumplimiento del alcance de los ítems a integrar en el monitoreo realizado por el servicio	Correo electrónico
3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 32-38	Licenciamiento de herramientas, no OpenSource, Fortinet y Tenable para el funcionamiento del servicio SOC	Correo electrónico
3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 39-40	Gestión de ticket con Aranda para gestión de requerimientos e incidentes con sus respectivos procesos de escalamiento	Aranda ITSM
3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 41-42	Integración de herramientas: FortiSIEM, FortiSOAR, FortiRecon y Tenable.	Correo electrónico
3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 43-46	Disponibilidad y acceso a Dashboard elaborados en Microsoft PowerBI	N/A
3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 49-50	Cumplimiento a cabalidad con la normatividad vigente: ISO27001, ISO27032, NIST SP 800-39, CRF y Ley 1581 Protección de datos	N/A

 AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	FORMATO			
	FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL			
Principio de procedencia: 4000.092	Clave: GCON-1.0-12-046	Versión: 02	Fecha: 04/oct/2019	Página: 5 de 7

3.1.2 Obligaciones sobre las herramientas tecnológicas que conforman el SOC. Numerales 51	Presentación de perfiles con su respectivo estudio de seguridad previo al inicio del contrato	Correo electrónico
3.1.3 Plan de comunicaciones Numerales 53-55	Aprobación del plan de comunicaciones y la matriz de comunicaciones	Correo electrónico
3.1.4 Obligaciones sobre Informes y políticas Numerales: 56-57, 63, 65-67,	Presentación de informes semanales, quincenales, mensuales y semestrales sobre el servicio	Correo electrónico
3.1.4 Obligaciones sobre Informes y políticas Numerales: 60, 70, 71 y 73	Definición del Modelo de operativo para el servicio incluyendo los procesos para la atención de requerimientos y matrices de escalamiento	Correo electrónico
3.1.5 Obligaciones sobre el equipo de trabajo Numerales: 75-80	Presentación de hojas de vida de los integrantes del equipo de acuerdo con las indicaciones de experiencia y especialidad.	Correo electrónico

3.3 PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS:

DESCRIPCIÓN DEL BIEN	CANTIDAD	FECHA DE ENTREGA	A SATISFACCIÓN	
Equipos Colectores de eventos marca Lenovo	2	3 de junio de 2025	SI	NO (x)

4 OBSERVACIONES A LAS ACTIVIDADES EJECUTADAS, A LAS OBLIGACIONES CUMPLIDAS, Y A LOS PRODUCTOS Y/O BIENES ENTREGADOS.

Los (2) equipos colectores marca Lenovo destinados para la colección de eventos se entregan usados para dar inicio al servicio mientras los equipos nuevos definitivos llegan al país. Se encuentra contemplada la entrega a más tardar el 20 de septiembre de 2025, sin embargo, se están realizando esfuerzos con el proveedor para anticipar esta fecha.

5 OBSERVACIONES ADICIONALES, SI A ELLO HUBIERE LUGAR.

 AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	FORMATO			
	FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL			
Principio de procedencia: 4000.092	Clave: GCON-1.0-12-046	Versión: 02	Fecha: 04/oct/2019	Página: 6 de 7

6 PORCENTAJES DE AVANCE PRESUPUESTAL Y EN EJECUCIÓN DEL CONTRATO.

A continuación, se presenta el porcentaje de avance presupuestal del presente contrato.

 AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	FORMATO					 UT Gestión Ciber NIT. 901.928.424 -I
	FORMATO 7 PROPUESTA ECONOMICA					
	Clave: APOY-9.0-12-014	Versión: 4		Fecha de aprobación: 08/07/2022		
OBJETO: PRESTAR SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA GESTIÓN DE EVENTOS DE CIBERSEGURIDAD DE LA RED DE DATOS						UT GESTIÓN CIBER
ÍTEM	DESCRIPCIÓN	UNIDAD	CANTIDAD	VALOR UNITARIO	VALOR PARCIAL	VALOR EJECUTADO
1	Despliegue y puesta en funcionamiento del servicio contratado SOC acorde a las especificaciones técnicas en el formato 8	Unidad	1	\$ 1.002.590.634,63	\$ 1.002.590.634,63	\$ 1.002.590.634,63
2	Servicio Mensual de SOC: 2.1. Acceso y Utilización mensual de las herramientas de monitoreo del SOC	Mes	20	\$ 50.000.000,00	\$ 1.000.000.000,00	\$ 100.000.000,00
	Servicio Mensual de SOC: 2.2. Servicio mensual de Gestión de Incidentes	Mes	20	\$ 30.000.000,00	\$ 600.000.000,00	\$ 60.000.000,00
	Servicio Mensual de SOC: 2.3. Servicio mensual de Gestión de Requerimientos	Mes	20	\$ 33.000.000,00	\$ 660.000.000,00	\$ 66.000.000,00
3	Programas de OJT de ciberseguridad para la entidad acorde a las especificaciones técnicas en el formato 8	Unidad	5	\$ 585.366,99	\$ 2.926.834,95	\$ -
Nota: Las cantidades contenidas en el formato 7 serán ajustadas de acuerdo con los meses a ejecutar teniendo en cuenta el plazo máximo de ejecución, que será el 31 de julio de 2026						
COSTOS TOTALES					\$ 3.265.517.469,58	\$ 1.228.590.634,63
IVA 19%					\$ 620.448.319,22	\$ 233.432.220,58
TOTAL PROYECTO					\$ 3.885.965.788,80	\$ 1.462.022.855,21

Se encuentra en trámite la solicitud mediante correo electrónico el 31 de julio de 2025 renuncia al anticipo contemplado en el contrato incluyendo los ajustes indicados por el supervisor del contrato; en virtud de que UT Gestión Ciber dispone de los recursos para iniciar las actividades objeto del contrato sin requerir el desembolso del anticipo. La eliminación del anticipo no afectará el cronograma de ejecución, ya que los flujos de caja garantizan el cumplimiento de las obligaciones.

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

 <p>AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL</p>	FORMATO			
	FORMATO 62 INFORME DE SUPERVISIÓN Y EJECUCIÓN CONTRACTUAL			
Principio de procedencia: 4000.092	Clave: GCON-1.0-12-046	Versión: 02	Fecha: 04/oct/2019	Página: 7 de 7

NOTA: SI EL SUPERVISOR DEL CONTRATO REQUIERE AÑADIR CAMPOS PARA RENDIR SU INFORME PUEDE HACERLO.



 Digitally signed by ALVARO EDUARDO VARELA ARENAS
 DN: street=AV CL 26 103 15, 2.5.4.13=FP GSE CL 77 7
 44 OF 701, cn=ALVARO EDUARDO VARELA ARENAS,
 serialNumber=79981362, st=BOGOTA D.C., l=BOGOTA
 D.C., email=alvaro.varela@aerocivil.gov.co, c=CO,
 title=DIRECTOR AERONAUTICO DE AREA GRADO 29,
 o=UNIDAD ADMINISTRATIVA ESPECIAL DE
 AERONAUTICA CIVIL,
 1.3.6.1.4.1.4710.1.3.2=899999059, name=C.C.,
 ou=DIRECCION DE INFRAESTRUCTURA Y SOPORTE DE
 TI
 Date: 2025.09.09 12:26:54 -05'00'

ALVARO EDUARDO VARELA ARENAS
Supervisor del contrato



FREDDY ALEJANDRO REINA MORALES
Supervisor del contrato