CONTENIDO DEL INFORME

1. CONDICIONES DEL CONTRATO
2. OBJETO DEL CONTRATO
3. ACTIVIDADES EJECUTADAS, OBLIGACIONES CUMPLIDAS, PRODUCTOS ENTREGADOS Y/O BIENES ENTREGADOS.
4. OBSERVACIONES A LAS ACTIVIDADES EJECUTADAS, A LAS OBLIGACIONES CUMPLIDAS, Y A LOS PRODUCTOS Y/O BIENES ENTREGADOS.
5. OBSERVACIONES ADICIONALES, SI A ELLO HUBIERE LUGAR.
6. 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 julio al 31 de julio 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.

ENTREGABLE No. 1 – *"Despliegue y puesta en funcionamiento del servicio contratado SOC acorde a las especificaciones técnicas en el formato 8".*

3.1. ACTIVIDADES EJECUTADAS:

PERÍODO: 1 al 31 de julio del año 2025

ACTIVIDAD	DESCRIPCIÓN	ENTREGA
Modelo operativo para el servicio	Presentación del modelo operativo para el servicio: 1. Estructura organizacional 2. Procesos operativos SOC 3. Grupos de atención y matriz de escalamientos 4. Definición de servicios SOC 5. Acuerdos de niveles de servicios	1 de julio de 2025 Presentación presencial del modelo
Integración de activos	Finalización de la integración de activos FortiEDR, FortiWAF, FortiAnalyzer y Office365 al FortiSIEM	1 de julio de 2025 Correo electrónico
Inicio de operación SOC	Formalización del inicio de la prestación del servicio con la creación de tickets de Aranda ITSM	7 de julio de 2025 Correo electrónico
Hallazgos protección de marca	Se reportan 5 credenciales expuestas y 5 presuntas suplantaciones de dominio	9 de julio de 2025 Correo electrónico
Hallazgos protección de marca	Se reportan 3 credenciales expuestas	14 de julio de 2025 Correo electrónico
Visita a instalaciones del servicio SOC	Visita al SOC Presentación de Modelo de Servicio Presentación de los perfiles contractuales Presentación de los líderes de los servicios SOC	15 de julio de 2025 Presencial
Mesa de trabajo Aranda ITSM	Charla sobre uso de Aranda para la creación de requerimientos para atención del servicio SOC	17 de julio de 2025 Virtual
Escaneo de vulnerabilidades	Ejecución de proceso para descubrimiento de activos con escaneos desde Tenable	17 de julio de 2025 Correo electrónico

Integración de activos	Finalización de integración de activos Windows y switches a FortiSIEM	22 de julio de 2025 Correo electrónico
Reportes	Reporte semanal del estado y salud de las plataformas existentes	22 de julio de 2025 Correo electrónico
Gestión de vulnerabilidades	Mesa de trabajo para definición y alcance del servicio de vulnerabilidades	23 de julio de 2025 Virtual
Integración de activos	Finalización de integración de activos Linux a FortiSIEM	29 de julio de 2025 Correo electrónico
Reportes	Informe detallado de causas y acciones de las incidencias de ciberseguridad	29 de julio de 2025 Correo electrónico
Reportes	Reporte semanal del estado y salud de las plataformas existentes	29 de julio de 2025 Correo electrónico
Reportes	Informe quincenal de eventos de seguridad	29 de julio de 2025 Correo electrónico
Gestión de vulnerabilidades	Seguimiento semanal al servicio de gestión de vulnerabilidades	29 de julio de 2025 Virtual

3.2 OBLIGACIONES CUMPLIDAS:

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
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.

6 PORCENTAJES DE AVANCE PRESUPUESTAL Y EN EJECUCIÓN DEL CONTRATO.

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

Ítem	Descripción	Presupuesto	Ejecución	(%) Ejecución Estimada	(%) Ejecución Real	Frecuencia
1	Implementación	$1.002.590.634	$1.002.590.634	100%	100%	Única vez
2	Utilización de herramientas	$650.000.000	$50.000.000	8%	8%	1/13*
	Gestión de incidentes	$390.000.000	$30.000.000	8%	8%	1/13*
	Gestión de requerimientos	$429.000.000	$33.000.000	8%	8%	1/13*
3	Programa OJT	$2.926.834	$ -	0%	0%	Por demanda

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.

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: 2025.08.22 11:09:04 -05'00'

ALVARO EDUARDO VARELA ARENAS
Supervisor del contrato

FREDDY ALEJANDRO REINA MORALES
Supervisor del contrato