Contrato No.	ADRES-CTO-868-2023		
Nombre del Contratista y/o Representante Legal	Unión Temporal SOC ADRES 2023		
Nombre del Supervisor y/o Interventor	Guillermo Manuel Benítez Rodriguez	**Teléfono / Extensión**	(57) (1) 4322760 ext. 1724
Dependencia	Dirección de Gestión de Tecnologías de Información y Comunicaciones		
Objeto del Contrato	Prestar el Servicio de Centro de Operaciones de Seguridad para la ADRES (SOC)		
Fecha de Inicio	13/07/2023	**Fecha de Terminación**	31/12/2025

Periodo del Informe de Actividades	**Desde**	1/05/2025	**Hasta**	31/05/2025
Adición y/o Prórroga	No aplica			
Suspensión	No aplica			
Cesión	No aplica			

INFORME PARCIAL DE EJECUCIÓN DE OBLIGACIONES CONTRACTUALES [i]

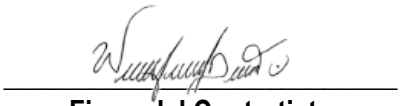
	Obligación contractual	Actividad desarrollada	Producto y/o Entregables	Alertas, inconvenientes o situaciones especiales que afectan el cumplimiento de la obligación
1	Prestar el servicio de análisis de vulnerabilidades descrito en el numeral 2.1 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye la evaluación de las debilidades o brechas, presentación de los respectivos informes y la construcción de la hoja de ruta con definición de las acciones a seguir para remediar los hallazgos encontrados sobre la infraestructura de TI	El servicio de análisis de vulnerabilidades es por demanda una vez al año: - Para el año 2023 se ejecutó en el mes de octubre. - Para el año 2024, se ejecutó en el mes de noviembre. - Para el año 2025, se tiene previsto ejecutar el ejercicio en el mes de Octubre.	N/A	N/A
2	Prestar el servicio de análisis de vulnerabilidades sobre las aplicaciones web descrito en el numeral 2.2 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye la evaluación de las debilidades o brechas, presentación de los respectivos informes y la construcción de la hoja de ruta con definición de las acciones a seguir para remediar los hallazgos encontrados sobre las aplicaciones.	El servicio de análisis de vulnerabilidades sobre las aplicaciones web es por demanda una vez al año: - Para el año 2023 se ejecutó en el mes de octubre. - Para el año 2024, se ejecutó en el mes de noviembre. - Para el año 2025, se ha realizado el análisis de vulnerabilidades a **seis (6)** aplicaciones web de un total de veinte (20). o normograma.adres.gov.co o adres-adres.epm.us-ashburn-1.ocs.oraclecloud.com/HyperionPlanning/ o gb6ddaf18fc114b-dbprdadrapex.adb.us-phoenix-1.oraclecloudapps.com/ords/r/adres/adres/login?tz=-5:00 o iatdqy.fa.ocs.oraclecloud.com/fscmUI/faces/FuseOverview o tramites-pru.adres.gov.co:443 o serviciostramites-pru.adres.gov.co:444	N/A	N/A
3	Prestar el servicio de Ethical Hacking descrito en el 2.3 del ANEXO – ESPECIFICACIONES TECNICAS, mediante la realización de ejercicios o pruebas específicas que busquen explotar de manera controlada uno o	El servicio de Ethical Hacking es por demanda una vez al año: - Para el año 2023, se ejecutó en el mes de noviembre. - Para el año 2024, se ejecutó en el mes de diciembre. - Para el año 2025, se tiene previsto ejecutar el ejercicio en el mes de noviembre.	N/A	N/A

	varios hallazgos encontrados en el análisis de vulnerabilidades.			
4	Prestar el servicio de Ingeniería Social descrito en el numeral 2.4 del ANEXO – ESPECIFICACIONES TECNICAS, mediante la realización de ejercicios controlados y dirigidos al personal de la entidad con el fin de obtener datos confidenciales o infectar los computadores con algún tipo de programa malicioso.	A continuación, se relacionan las actividades más relevantes del periodo: • Elaboración de las propuestas para el 2do ejercicio de ingeniería social para el 2025. • Definición y envió de la sensibilización a los usuarios de la ADRES, mediante el curso denominado "Ataque de navegador en el navegador" de Microsoft Defender. • Definir la propuesta y ajustar la simulación para el 2do ejercicio de ingeniería social del 2025.	N/A	N/A
5	Prestar el servicio de monitoreo y correlación de eventos de seguridad en la modalidad 7x24 según lo descrito en el numeral 2.5 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye correlación de eventos, detección, investigación y respuesta ante eventos, incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la ADRES.	A continuación, se relacionan las actividades más relevantes del periodo: • Identificación, análisis y atención de eventos de monitoreo el cual corresponde a **1.573** • Identificación, análisis y atención de alertas de monitoreo el cual corresponde a **8.371** • Durante el periodo, se bloquearon **404** indicadores de compromiso (IoC): o Hash – **232** IoCs o IP – **31** IoCs o URL/Dominio – **141** IoCs • Se identifica un Top cinco (5) de ataques detectados en la entidad. • Se identifica un Top cinco (5) de usuarios con autenticaciones fallidas. • Se identifica un Top cuatro (4) de dispositivos con eventos de seguridad.	• Monitoreo y Correlación de eventos de Seguridad_Mayo_2025.pdf • Anexos: o SecurityIncident_by_Events.csv o SecurityIncident_by_IncidentNumber.csv	N/A
6	Prestar el servicio de monitoreo y supervisión de la actividad de bases de datos en la modalidad 5x8 según lo descrito en el numeral 2.6 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye implementación de casos de uso, soporte técnico y mantenimiento de la infraestructura de la solución IMPERVA.	A continuación, se relacionan las actividades más relevante del periodo: • Bases de datos en monitoreo: o Nube Publica - Microsoft Azure: **98** bases de datos en Producción. o Nube Privada – On premise: **462** bases de datos en producción. o Nube Privada – On premise: **34** bases de datos en pruebas. • En la plataforma de IMPERVA DAM se configuran las políticas, quedando de la siguiente manera: - Políticas de seguridad: **91** - Políticas de auditoria: **7** • Se identifican un Top diez (10) de instancias de base de datos que más se alertan. • Monitoreo del estado de Salud del IMPERVA y validación de almacenamiento de la herramienta.	• Informe Monitoreo y supervisión de actividad de bases de datos_Mayo_2025.pdf	N/A
7	Prestar el servicio de Gestión de incidentes en la modalidad 7x24 según lo descrito en el numeral 2.7 del ANEXO – ESPECIFICACIONES TECNICAS, el cual incluye los procedimientos que permitan reaccionar ante los incidentes de la mejor manera posible, minimizando los daños de los sistemas de información, con diagnósticos eficaces, recolectando las evidencias necesarias y mitigando las causas de los incidentes.	A continuación, se relacionan las actividades más relevantes del periodo: • Durante el periodo en curso se registraron (**11**) **casos de Sentinel** documentados y/o escalados a la entidad. • Se documentaron (**41**) **requerimientos** por correo y se atendieron según creación de caso por mesa de servicio. • Se enviaron (**84**) **boletines de seguridad** de tipo lite y completos. • Se compartió el análisis de (**9**) casos de **monitoreo de marca**.	• Matriz de eventos o incidentes de seguridad - Mayo 2025.xlsx	N/A
8	Prestar el servicio de Gestión de infraestructura de seguridad en la modalidad 5x8 según lo descrito en el numeral 2.8 del ANEXO – ESPECIFICACIONES TECNICAS, con el fin de mejorar el tiempo de respuesta ante incidentes y amenazas de seguridad.	A continuación, se relacionan las actividades más relevantes del periodo: • Microsoft Sentinel, en el periodo se gestionó: o Libros: **23** o Conectores de datos: **26** o Reglas de analítica: **64** o Reglas de automatización: **38** o Cuadernos de Estrategia: **27** • Dentro del monitoreo al Azure Monitor, se identificó un total de 10 recursos pendientes por conexión al Azure ARC	• Gestión de infraestructura de seguridad_Mayo_2025.pdf	N/A

		• Para el Defender for cloud la postura de seguridad quedo en un **72%,** aumentando el porcentaje del periodo anterior en un **2 %**. • Para Microsoft Intune (Endpoint) se continuo con las depuraciones y validaciones para ajustar el inventario de dispositivos; se logró dejar en estado saludable a 5 dispositivos corporativos. • Para el Microsoft 365 Defender el puntaje de seguridad quedo en 990,25 puntos de 1.403 puntos, con un porcentaje del 70.58%. • Para el Azure Firewall, se llevaron acabo seguimientos y revisiones sobre la regla rc-anytoany. • Para el Azure DDoS, se llevaron acabo dos prueba de denegación de servicio sobre las IP del WAF y el Firewall. • Para el Microsoft Purview se identificó que el puntaje de cumplimiento está en 62% con 14.226 puntos de 22.605 puntos totales, adicional se cuenta con 37 acciones de mejora en cumplimiento y 500 por cumplir. • Para el Entra ID el puntaje de seguridad se encontró en **75,70%** el cual presento una disminución del 0.01% según el periodo anterior. • En el Azure Site Recovery se llevó a cabo: o El monitoreo del almacén ASR-VMVault-MOD, el cual no presento ninguna novedad.		
9	Prestar el servicio de revisión y análisis del plan de recuperación de desastres según lo descrito en el numeral 2.9 del ANEXO – ESPECIFICACIONES TECNICAS, con el fin de mejorar el plan de recuperación tiempo de respuesta ante incidentes y amenazas de seguridad.	El servicio de revisión y análisis del plan de recuperación de desastres es de forma global por año: • Para el mes, se realizó de forma exitosa la primera prueba del plan de recuperación de desastres, esto para la aplicación de reclamaciones ECAT.	Ejecución control de cambio DRP Reclamaciones.msg	N/A
10	Elaborar, entregar y socializar previa aprobación del supervisor, el plan de trabajo del contrato conforme a lo descrito en el numeral 3 del ANEXO – ESPECIFICACIONES TECNICAS.	El avance del proyecto general va en un 70% - Avance Real de la vigencia 2023: 100%. - Avance Real de la vigencia 2024: 100%. - En el 2025 se tiene un avance del 39%	Plan Global - ADRES-CTO_868_2023 - 03_06_2025.mpp	N/A
11	Presentar y disponer durante la ejecución del contrato de un equipo base de proyecto que contemple como mínimo los roles, perfiles y experiencia que se describen en el numeral 4 del ANEXO - ESPECIFICACIONES TECNICAS.	En el desarrollo la sesión de revisión de riesgos del proyecto que se realiza mensualmente en la obligación 11 se da cumplimiento a los roles mínimos solicitado por la ADRES.	GEDO-FR05_Acta de Reunion_20250523 – Riesgos.pdf	N/A
12	Aportar la respectiva certificación y mantener la interacción de centro de operaciones de seguridad con mínimo un (1) organismo de respuesta a incidentes de seguridad, conforme a los descrito en el numeral 5 del ANEXO - ESPECIFICACIONES TECNICAS.	Las certificaciones se encuentran vigentes a la fecha de la revisión del informe de cumplimiento para: • FIRST • ISO 27001.	• Certificado AENOR_SI-0052-2017 - ISO 27001_2017 • Carta de renovación: SIA CERT FIRST.pdf • Certificado IQNet_ES-SI-0052-2017 - ISO 27001_2013.pdf	N/A
13	Aprovisionar, asegurar y mantener durante la ejecución del contrato, sus instalaciones, equipos y los canales o enlaces de conectividad entre la ADRES y las instalaciones del contratista, con el fin de realizar de manera remota la operación del Centro de Operaciones de Seguridad.	Se continua con los canales de comunicación activos y no se han presentado ninguna eventualidad de estos.	N/A	N/A
14	Prestar el servicio adicional de un experto en seguridad bajo el esquema de trabajo hibrido y en la modalidad 5x8, con el fin de acompañar en la ejecución del plan de remediación o mitigación definido por la Entidad, identificar, optimizar y aplicar configuraciones de seguridad y elaborar procedimientos relacionados con la seguridad de la información.	A continuación, se relacionan las actividades más relevantes del periodo: • Gestión de las vulnerabilidades – Plan 2024: o Vulnerabilidades Web: ▪ Altas (**5**) y se mitigaron (**3**). o Vulnerabilidades de infraestructura: ▪ Críticas (**33**) y se mitigaron (**23**). ▪ Altas (**107**) y se mitigaron (**83**). ▪ Medias (**490**) y se mitigaron (**402**) • Gestión de dispositivos:	N/A	N/A

		○ Escalamiento de **6** casos en mesa de servicio de la ADRES, para remediación de las recomendaciones por Azure Defender for Cloud. • Registro de casos a la mesa de servicio. ○ Actualización de aplicaciones: **10** ○ Monitoreo y correlación de eventos: **33** ○ Vulnerabilidades: **6** • Revisión de **44** boletines de seguridad, de los cuales **33** fueron escalados para la gestión respectiva. • Validación y escalamiento de **4** incidentes en fuga de credenciales. • Revisión de vulnerabilidades relacionadas por el Defender 365. • Acompañamiento en él envió de curso de entrenamiento a funcionarios y contratistas ADRES. • Elaboración de la presentación de "Prevención Robo de credenciales" • Modificación de pieza curso de entrenamiento de Ciberseguridad. • Escalamiento de casos criticidad media , Matriz de vulnerabilidades 2024. • Validación de vulnerabilidades matriz del CSIRT y escalamiento de casos a MDS.		
15	Prestar el servicio de monitoreo de marca en la modalidad 7x24 por la duración del contrato que incluye: i) un dominio, ii) una (1) marca, iii) filtración de credenciales, iv) monitoreo de abuso de marca (Redes sociales, dominios similares, phising) y v) un (1) informe del servicio por mes.	A continuación, se relacionan las actividades más relevantes del periodo: • En el transcurso del periodo se identificaron **632 eventos**, los cuales están clasificados en 4 tipos: - Fuga de Datos: **427** - Fraudes Digitales: **167** - Piratería Online: **0** - Cybersquatting: **38** • Los tipos de fraude digital identificados son: ○ Phishing: **53** ○ Perfil falso en red social: **108** ○ Aplicación móvil falsa: **6** • Se identificaron **38 dominios** los cuales no alojan contenido que se categorice como malicioso según su criticidad.	• Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Mayo_2025.pdf	N/A
16	Prestar un servicio de inteligencia de amenazas con fuente de datos comercial e incorporación de indicadores de compromisos a Microsoft Sentinel.	Actualmente se encuentra en funcionamiento la herramienta (AXUR) como fuente de inteligencia de amenazas.	N/A	N/A

Hago constar que durante el periodo reportado se adelantaron las anteriores obligaciones y/o actividades.



Firma del Contratista
Williams Alexander Breto Martínez
Fecha: 9/06/2025

BALANCE ECONÓMICO

Valor Total Contrato (Inicial + Adición)		Valor Pagado	Valor a Pagar	Saldo Liberado	Saldo por Pagar
Vigencia 2023	$ 1,762,183,892.00	$ 1,451,749,187.00	$ 0.00	$ 310,434,705.00	$ 0.00
Vigencia 2024	$ 2,390,471,762.00	$ 2,390,471,762.00	$ 0.00	$ 0.00	$ 0.00
Vigencia 2025	$ 2,390,471,762.00	$ 585,123,119.00	$ 125,657,574.00	$ 0.00	$ 1,679,691,069.00
TOTAL	$ 6,543,127,416.00	$ 4,427,344,068.00	$ 125,657,574.00	$ 310,434,705.00	$ 1,679,691,069.00

La ADRES cancelará al CONTRATISTA, la suma de Ciento veinticinco millones seiscientos cincuenta y siete mil quinientos setenta y cuatro pesos ($125’657.574,00)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
INDRA Colombia
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	87040154	$ 889’089.200	01/06/2025	30/06/2025	05/06/2025
PENSION	87040154	$ 2.651’741.300	01/05/2025	31/05/2025	05/06/2025
ARL	87040154	$ 145’608.900	01/05/2025	31/05/2025	05/06/2025

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
DEXTERA
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	9486366832	$ 11’576.600	01/05/2025	31/05/2025	21/05/2025
PENSION	9486366832	$ 39’482.100	01/04/2025	30/04/2025	21/05/2025
ARL	9486366832	$ 7’839.600	01/04/2025	30/04/2025	21/05/2025

El Contratista tiene otros Contratos de Prestación de Servicios:

SI ☐ NO ☒

En la eventualidad que la Supervisión verifique que la información suministrada por el Contratista no es consistente o carece de validez, ésta deberá indicar las acciones tomadas: Realizar una breve descripción del hallazgo (Adjuntar soportes)

INFORME PARCIAL DE SUPERVISIÓN

De conformidad con el seguimiento a la ejecución del contrato, el (los) supervisor (es) certifica(n) que:

- El (la) Contratista durante el mes de Mayo del 2025, desarrolló y cumplió con el objeto contractual, las obligaciones generales y específicas, presentó y entregó los productos y/o informes establecidos en el Contrato o Convenio en mención.
- Apruebo los informes, productos y demás documentos presentados y entregados por el (la) Contratista durante el periodo mencionado en desarrollo de las obligaciones pactadas en el Contrato o Convenio en mención:
  - **Informe mensual del servicio de monitoreo y correlación de eventos de seguridad**: i) Monitoreo y Correlación de eventos de Seguridad_Mayo_2025.pdf; Anexos: i) SecurityIncident_by_Events.csv, ii) SecurityIncident_by_IncidentNumber.csv
  - **Informe mensual del servicio de gestión de incidentes**, el cual comprende el reporte **i)** Matriz de eventos o incidentes de seguridad - Mayo 2025.xlsx
  - **Informe mensual del servicio de gestión de infraestructura de seguridad**: i) Gestión de infraestructura de seguridad_Mayo_2025.pdf
  - **Informe del servicio Monitoreo y supervisión de actividad de bases de datos**: i) Informe Monitoreo y supervisión de actividad de bases de datos_Mayo_2025.pdf
  - **Informe mensual Monitoreo de Marca y Fuente de Inteligencia de Amenazas**: i) Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Mayo_2025.pdf
- A la fecha no existen causales de incumplimiento de las obligaciones contractuales que demanden actuaciones conminatorias o sancionatorias por parte de la Administración.
- Verifique la matriz de riesgos del contrato y se estableció, que no se ha materializado ninguno de los riesgos.
- Dejo constancia que el contratista entrego los documentos relacionados, pero por razones de confidencialidad de la información los archivos quedan almacenados en repositorio de Teams denominado Ciberseguridad en la carpeta \Contratos\ADRES-CTO-868-2023 - SOC\3. Ejecución\2. Obligaciones

OBSERVACIONES	
ANEXOS	1. Comprobante del pago de los Aportes respectivos al Sistema de Seguridad Social Integral en Salud y Pensiones y/o Aportes Parafiscales por parte del Contratista. 2. Soportes contractuales cargados en la sección 7 del contrato electrónico (Formato comprimido). 3. Cuenta de cobro o factura, según el Régimen sea Simplificado o Común. 4. Certificados de antecedentes disciplinarios de la Junta Central de Contadores de los revisores fiscales por parte del contratista. 5. Copia de la tarjeta profesional de los revisores fiscales por parte del contratista.

En constancia, firma:

BENITEZ RODRIGUEZ GUILLERMO MANUEL

Firmado digitalmente por BENITEZ RODRIGUEZ GUILLERMO MANUEL
Fecha: 2025.06.09 15:16:37 -05'00'

Supervisor(es) / Interventor(es):
Guillermo Manuel Benítez

En constancia, el presente documento se entiende aprobado por las partes una vez el usuario supervisor del contrato efectué la aprobación respectiva en la plataforma de SECOP II.

Lugar y Fecha: Bogotá, D. C., 9/06/2025

[i] Incluir las obligaciones específicas pactadas en el Contrato y/o Convenio.