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**	31/05/2026

Periodo del Informe de Actividades	**Desde**	1/02/2026	**Hasta**	28/02/2026
Fecha de Suscripción Adición	24/12/2025			
RP Adición	No. 27 del 11 de enero de 2026			
Valor RP Adición	$ 1’370.500.199,60			
Fecha suscripción Prórroga	24/12/2025			
Fecha inicio Prórroga	01/01/2026			
Fecha final Prórroga	31/05/2026			
Fecha Suscripción Suspensión	No aplica			
Fecha inicio Suspensión	No aplica			
Fecha final Suspensión	No aplica			
Fecha suscripción Cesión	No aplica			
Rp 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 ejecutó en el mes de Octubre. - Para el año 2026, se planea ejecutar en el mes de Mayo	- No aplica	No aplica
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	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 ejecutó en el mes de octubre.	- No aplica	No aplica

	remediar los hallazgos encontrados sobre las aplicaciones.	- Para el año 2026, se planea ejecutar en el mes de Mayo		
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 varios hallazgos encontrados en el análisis de vulnerabilidades.	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 ejecutó en el mes de noviembre. - Para el año 2026, este servicio no está incluido.	- No aplica	No aplica
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: •Se elabora y se define la propuesta para el 1er ejercicio de ingeniería social 2026. •Se configuran y ejecutan los 4 señuelos para la primera prueba de ingeniería social de la vigencia 2026. •Se recopilan los datos de las pruebas realizadas. •Se elaboran los entregables de los resultados.	• Informe especifico de Ejercicio de Ingeniería Social - Febrero 2026.pdf • Memorias de sensibilización - Febrero 2026.pptx • Entrenamiento 1 Ingeniería Social Febrero 2026.xlsx • Prueba Phishing Febrero Contratistas-Servidores ADRES.xlsx	No aplica
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 **1.870** • Identificación, análisis y atención de alertas de monitoreo el cual corresponde a **20.487** • Durante el periodo, se bloquearon **691** indicadores de compromiso (IoC): o Hash – **163** IoCs o IP – **278** IoCs o URL/Dominio – **250** 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_Febrero_2026.pdf • Anexos: o SecurityIncident_by_Events.csv o SecurityIncident_by_IncidentNumber.csv	No aplica
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 relevantes del periodo: • Bases de datos en monitoreo: o Nube Publica - Microsoft Azure: **59** bases de datos en Producción. o Nube Privada – On premise: **467** bases de datos en producción. o Nube Privada – On premise: **34** bases de datos en pruebas. • En la plataforma de IMPERVA DAM actualmente se encuentran las politicas: - Políticas de seguridad: **11** - Políticas de auditoria: **7** • Se identifican un Top diez (10) de instancias de base de datos que más se alertan. • Se finalizo la configuración e integración, a nivel de Imperva DAM, de 3 instancias de base de datos. • Se gestionó la solicitud para la ejecución del escaneo de vulnerabilidades sobre 2 instancias de base de datos. • Monitoreo del estado de Salud del IMPERVA y validación de almacenamiento de la herramienta.	• Informe Monitoreo y supervisión de actividad de bases de datos_Febrero_2026.pdf	No aplica
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 (**63**) **casos de Sentinel** documentados y/o escalados a la entidad. • Se documentaron (**39**) **requerimientos** por correo y se atendieron según creación de caso por mesa de servicio. • Se enviaron (**66**) **boletines de seguridad**	Matriz de eventos o incidentes de seguridad - Febrero 2026.xlsx	No aplica

		• Se compartió el análisis de (**2**) casos de **monitoreo de marca**.		

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:
		  ○ Libros: **27**
		  ○ Conectores de datos: **32**
		  ○ Reglas de analítica: **94**
		  ○ Reglas de automatización: **16**
		  ○ Cuadernos de Estrategia: **29**
		• Dentro del Azure Monitor se identificó el aumento de unidades pasando de 70 a 75 respecto a dispositivos con el agente AMA instalado.
		• Para el Defender for cloud la postura de seguridad quedo en un **58%,** disminuyendo en 4% el porcentaje del periodo anterior.
		• Para Microsoft Intune (Endpoint) se gestionó la solicitud para el enrolamiento de equipos que no han sido enrolados pertenecientes al piso 8.
		• Para el Microsoft 365 Defender el puntaje de seguridad quedo en 1113,98 puntos de 1.560 puntos, con un porcentaje del 71.41%.
		• Para el Azure Firewall, se realizó la configuración de dos reglas de red tipo (Deny) hacia dominios desconocidos (Aquary y Corix999).
		• Para el Azure DDoS, se realizó el monitoreo a los activos incluidos en la herramienta.
		• Para el Microsoft Purview se identificó que el puntaje de cumplimiento está en 61% con 14.309 puntos de 23.393 puntos totales, adicional se cuenta con 43 acciones de mejora en cumplimiento y 553 por cumplir.
		• Para el Entra ID se identificó un puntaje de seguridad del 91.75%, presentando un aumento aproximado del 0.20% a comparación del periodo anterior.
		• En el Azure Site Recovery se llevó a cabo:
		  ○ El monitoreo de replicación de información en los dispositivos incluidos en la herramienta.
		  ○ Se revisaron y ajustaron 3 servidores que estaban presentando demoras en la replicación de datos.
			Gestión de infraestructura de seguridad_Febrero_2026.pdf	No aplica

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 año 2023, se entregó la documentación en el mes de diciembre. -Para el año 2024, se entregó la documentación en el mes de noviembre. -Para el año 2025, se entregó la documentación en el mes de noviembre. - Para el año 2026, el servicio no se encuentra incluido.	No aplica	No aplica
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 en el periodo 2023 a 2025 está en el 100% de ejecución. -El avance del proyecto en el periodo 2026 está en el 21% de ejecución.	Plan Global - ADRES-CTO_868_2023 - 02_03_2026.mpp	No aplica
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_V02 20260226 - Riesgos.pdf	No aplica
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	No aplica

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.	No aplica	No aplica
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 de remediación de vulnerabilidades 2026: ○ Criticas (**39**) y se mitigaron (**6**) ○ Altas (**70**) y se mitigaron (**11**). ○ Medias (**348**) y se mitigaron (**74**) ○ Bajas (**247**) y se mitigaron (**65**) • Se escalan **53** de casos a la mesa de servicio. ○ Vulnerabilidades (21) ○ Eventos de seguridad (32) • Apoyar la planeación y seguimiento del primer ejercicio de ingeniería social 2026 • Gestionar la necesidad de publicar en SENDA el link del repositorio "La base de conocimiento de ciberseguridad"	No aplica	No aplica
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 **213 eventos**, los cuales están clasificados en 3 tipos: - Fuga de Datos: **179** - Fraudes Digitales: **10** - Cybersquatting: **24** • Los tipos de fraude digital identificados son: ○ Phishing: **3** ○ Perfil falso en red social: **2** ○ Aplicación móvil falsa: **5** • Se identificaron **24 dominios** los cuales no alojan contenido que se categorice como malicioso según su criticidad.	Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Febrero_2026.pdf	No aplica
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. A la fecha se cuenta con el licenciamiento vigente hasta el 17 de agosto del 2026.	Licencia Axur.pdf	No aplica

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



Firma del Contratista
Williams Alexander Breto Martínez
Fecha: 26/03/2026

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	$ 2,390,471,762.00	$ 0.00	$ 0.00	$ 0.00
Vigencia 2026	$ 1,370,500,199.60	$ 135,710,179.92	$ 227,447,279.92	$ 0.00	$ 1,007,342,739.76
TOTAL	$ 7,913,627,615.60	$ 6,368,402,890.92	$ 227,447,279.92	$ 310,434,705.00	$ 1,007,342,739.76

La ADRES cancelará al CONTRATISTA, la suma de Doscientos veintisiete millones cuatrocientos cuarenta y siete mil doscientos setenta y nueve pesos con noventa y dos centavos ($227’447.279,92)

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES: INDRA Colombia

CONCEPTO	PLANILLA No.	ENTIDAD	VALOR	PERIODO	
				DESDE	HASTA
Salud	61066501	Varias	$ 812’017.900	1/03/2026	31/03/2026
Pensión	61066501	Varias	$ 2.604’370.800	1/02/2026	28/02/2026
ARL	61066501	Cia. de Seguros Bolivar S.A.	$ 147’255.500	1/02/2026	28/02/2026

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES: DEXTERA

CONCEPTO	PLANILLA No.	ENTIDAD	VALOR	PERIODO	
				DESDE	HASTA
Salud	9500020571	Varias	$ 17’907.600	1/02/2026	28/02/2026
Pensión	9500020571	Varias	$ 51’814.200	1/01/2026	31/01/2026
ARL	9500020571	ARL Sura	$ 8’974.600	1/01/2026	31/01/2026

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:

1. El (la) Contratista durante el mes de Febrero del 2026, 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.
2. 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:
   - I. **Informe mensual del servicio de monitoreo y correlación de eventos de seguridad**: i) Monitoreo y Correlación de eventos de Seguridad_Febrero_2026.pdf; Anexos: i) SecurityIncident_by_Events.csv, ii) SecurityIncident_by_IncidentNumber.csv
   - II. **Informe mensual del servicio de gestión de incidentes**, el cual comprende el reporte **i)** Matriz de eventos o incidentes de seguridad - Febrero 2026.xlsx
   - III. **Informe mensual del servicio de gestión de infraestructura de seguridad**: i) Gestión de infraestructura de seguridad_Febrero_2026.pdf
   - IV. **Informe del servicio Monitoreo y supervisión de actividad de bases de datos**: i) Informe Monitoreo y supervisión de actividad de bases de datos_Febrero_2026.pdf, Anexos: i) Inventario de DB Febrero 2026.xlsx
   - V. **Informe mensual Monitoreo de Marca y Fuente de Inteligencia de Amenazas**: i) Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Febrero_2026.pdf
   - VI. **Informe Ingenieria Social:** i) Informe especifico de Ejercicio de Ingeniería Social - Febrero 2026.pdf, ii) Memorias de sensibilización - Febrero 2026.pptx, iii) Entrenamiento 1 Ingeniería Social Febrero 2026.xlsx y iv) Prueba Phishing Febrero Contratistas-Servidores ADRES.xlsx
3. A la fecha no existen causales de incumplimiento de las obligaciones contractuales que demanden actuaciones conminatorias o sancionatorias por parte de la Administración.
4. Verifique la matriz de riesgos del contrato y se estableció, que no se ha materializado ninguno de los riesgos.
5. 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	No aplica
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, firmo:

BENITEZ RODRIGUEZ GUILLERMO MANUEL

Digitally signed by BENITEZ RODRIGUEZ GUILLERMO MANUEL
Date: 2026.03.27 08:28:47 -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 efectúe la aprobación respectiva en la plataforma de SECOP II.

Lugar y Fecha: Bogotá, D. C., 27/03/2026

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