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**	1/09/2024	**Hasta**	30/09/2024
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, según el control de cambios en el cronograma del plan, el ejercicio está planeado para realizarse en el mes de noviembre.	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, según el control de cambios en el cronograma del plan, el ejercicio está planeado para realizarse en el mes de noviembre.	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 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, según el control de cambios en el cronograma del plan, el ejercicio está planeado para realizarse en el mes de diciembre.	N/A	N/A

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: • Sensibilización a los usuarios de la ADRES, mediante el curso denominado "Phishing masivo" de Microsoft Defender • Definir el alcance del ejercicio y la población objeto para la tercera simulación de ingeniería social para el año 2024. • Programación, configuración y ejecución del tercer ejercicio de ingeniería social para el año 2024. • Elaboración del informe especifico del Ejercicio de Ingeniería Social y memoria de sensibilización los cuales contienen los resultados y estadísticas de la simulación.	• Informe especifico de Ejercicio de Ingeniería Social - Septiembre 2024.pdf • Memorias de sensibilización - Septiembre 2024.pptx • Anexos: o Prueba Phishing Septiembre 2024 Contratistas.xlsx o Prueba Phishing Septiembre 2024 Servidores Públicos.xlsx o Informe de simulación de ataques - Microsoft Defender.xlsx	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 **3.185** • Identificación, análisis y atención de alertas de monitoreo el cual corresponde a **15.322** • Durante el periodo, se bloquearon **404** indicadores de compromiso (IoC): o Hash – **206** IoCs o IP – **84** IoCs o URL/Dominio – **106** IoCs o Correo/Malware-Phishing – **8** IoCs • Se identifica un Top cinco (5) de ataques detectados en la entidad. • Se identifica un Top cuatro (4) de usuarios con autenticaciones fallidas. • Se identifica un Top Cuatro (4) de dispositivos con eventos de seguridad.	• Monitoreo y Correlación de eventos de Seguridad_Septiembre_2024.pdf • Anexos: o SecurityIncident_by_Events.csv o SecurityIncident_by_Incident Number.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: **391** bases de datos en producción. o Nube Privada – On premise: **30** bases de datos en pruebas. • En la plataforma de IMPERVA DAM se configuran las políticas, quedando de la siguiente manera: - Políticas de seguridad: 71 - Políticas de auditoria: 7 • Se identifican un Top diez (10) de instancias de base de datos que más se alertan. • Investigación de las alertas Unauthorized Database and Schema y Unauthorized Source Application • Ejecución de un análisis de vulnerabilidades a la instancia de base de datos: BDPWEB01 • Monitoreo del estado de Salud del IMPERVA y validación de almacenamiento de la herramienta.	Informe Monitoreo y supervisión de actividad de bases de datos_Septiembre_2024.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 (**27**) **casos de Sentinel documentados** y/o escalados a la entidad. • Se documentaron (**19**) **requerimientos** por correo y se atendieron según creación de caso por mesa de servicio. • Se enviaron (**103**) **boletines de seguridad** de tipo lite y completos. • Se compartió el análisis de (**6**) **posibles casos de suplantación de marca**.	Matriz de eventos o incidentes de seguridad - Septiembre 2024.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 –	A continuación, se relacionan las actividades más relevantes del periodo: • Microsoft Sentinel, en el periodo se gestionó: o Libros: **17**	Gestión de infraestructura de seguridad_Septiembre_2024.pdf	N/A

	ESPECIFICACIONES TECNICAS, con el fin de mejorar el tiempo de respuesta ante incidentes y amenazas de seguridad.	○ Conectores de datos: **23** ○ Reglas de analítica: **47** ○ Reglas de automatización: **40** ○ Cuadernos de Estrategia: **23** • Dentro del monitoreo al Azure Monitor se evidencio lo siguiente: ○ Servidores habilitados para ARC: **83** migrados con éxito. ○ Máquinas virtuales Azure: **64** migrados con éxito. • Para el Defender for cloud la postura de seguridad quedo en un **68%,** disminuyendo en un 6% a comparación del periodo anterior. • Los grupos que integran la protección de dispositivos por plataforma, en Microsoft Intune (Endpoint) son los siguientes: - ADD_Dispositivos_472: **54** - ADD_Dispositivos_AdministracionCentral: **722** - AAD_Dispositivos_Personales: **1.597** • Para el Microsoft 365 Defender el puntaje de seguridad quedo en 827,03 puntos de 1.449 puntos, con un porcentaje del 57.08%. • Para el Microsoft Purview se identificó que el puntaje de cumplimiento está en 56% con 11.486 puntos de 20.292 puntos totales, adicional se cuenta con 45 acciones de mejora en cumplimiento y 554 por cumplir. • Para el Entra ID el puntaje de seguridad se encontró en **72,83%** el cual presento una disminución aproximada del 3% según el periodo anterior. • En el Azure Site Recovery se llevó a cabo: ○ Sesiones de trabajo para aplicar recomendaciones de Microsoft para la configuración de novedades en el Azure Site modernizado.		
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.	A continuación, se relacionan las actividades más relevantes del periodo: • Ajuste y aprobación del RFC para la segunda simulación del año 2024. • Ejecución de la segunda simulación del año 2024	N/A	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.	Se elaboro el cronograma de actividades para el año 2024 y una proyección para el 2025. El avance del proyecto general va en un 39% - Avance Real de la vigencia 2023: 100%. - En el 2024 se tiene un avance del 73%	Plan Global - ADRES-CTO_868_2023 - 02_10_2024.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_20240926 - 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 Indra/Minsait realizo proceso de recertificación de ISO 27001.	• Certificate-sia-cert-2023 • IQNetES-SI-0052-2017_2023-11-07.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	A continuación, se relacionan las actividades más relevantes del periodo:	N/A	N/A

	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.	• Gestión de las vulnerabilidades acumuladas.
		  ○ Vulnerabilidades Web: Identificadas con nivel de riesgo Alto tres (**3**) y se mitigaron tres (**3**).
		  ○ Vulnerabilidades de infraestructura:
		  ▪ Identificadas con nivel de riesgo: Crítico treinta y tres (**33**) y se mitigaron veintiséis (**26**).
		  ▪ Como altas: ciento ochenta y dos (**182**) y se mitigaron ciento treinta y nueve (**139**).
		• Gestión de dispositivos:
		  ○ Depuración de **9** dispositivos duplicados.
		  ○ Validación de compatibilidad en **173** dispositivos.
		  ○ Escalamiento de **5** casos en mesa de servicio de la ADRES, para remediación de las recomendaciones por Azure Defender for Cloud.
		• Asignación de casos a la mesa de servicio.
		  ○ Actualización de aplicaciones: **3**
		  ○ Monitoreo y correlación de eventos: **6**
		  ○ Vulnerabilidades: **6**
		  ○ Incidente de seguridad: **1**
		• Revisión y escalamiento de **67** boletines de seguridad.
		• Validación y escalamiento de **4** incidentes en fuga de credenciales.
		• Apoyo y acompañamiento al tercer ejercicio de ingeniería social del año 2024.
		• Desarrollo y ajuste del repositorio Sway
		• Análisis de dominios catalogados inseguros (gov.co)
		• Validación del cambio de nombre de la URL Senda.		

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 **439 eventos**, los cuales están clasificados en 4 tipos:
		  - Fuga de Datos: **60**
		  - Fraudes Digitales: **355**
		  - Piratería Online: **0**
		  - Cybersquatting: **24**
		• Los tipos de fraude digital identificados son:
		  ○ Phishing: **302**
		  ○ Perfil falso en red social: **49**
		  ○ Aplicación móvil falsa: **4**
		• 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 _ Septiembre _ 2024.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
Jose Fernando Quintero

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	$ 1,170,246,238.00	$ 208,150,397.00	$ 0.00	$ 1,012,075,127.00
Vigencia 2025	$ 2,390,471,762.00	$ 0.00	$ 0.00	$ 0.00	$ 2,390,471,762.00
TOTAL	$ 6,543,127,416.00	$ 2,621,995,425.00	$ 208,150,397.00	$ 310,434,705.00	$ 3,402,546,889.00

La ADRES cancelará al CONTRATISTA, la suma de Doscientos ocho millones ciento cincuenta mil trecientos noventa y siete pesos ($208’150.397,00)

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

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	80630305	$ 859’985.200	01/10/2024	31/10/2024	02/10/2024
PENSION	80630305	$ 2.510’208.000	01/09/2024	30/09/2024	02/10/2024
ARL	80630305	$ 144’415.700	01/09/2024	30/09/2024	02/10/2024

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
DEXTERA
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	9473528913	$ 12’177.600	01/09/2024	30/09/2024	19/09/2024
PENSION	9473528913	$ 40’961.400	01/08/2024	31/08/2024	19/09/2024
ARL	9473528913	$ 9’396.300	01/08/2024	31/08/2024	19/09/2024

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 Septiembre del 2024, 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_Septiembre_2024.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 - Septiembre 2024.xlsx
  - Informe mensual del servicio de gestión de infraestructura de seguridad: i) Gestión de infraestructura de seguridad Septiembre 2024.pdf
  - Informe del servicio Monitoreo y supervisión de actividad de bases de datos: se entrega el siguiente documento: i) Informe Monitoreo y supervisión de actividad de bases de datos Septiembre 2024.pdf
  - Informe mensual Monitoreo de Marca y Fuente de Inteligencia de Amenazas: i) Monitoreo de Marca y Fuente de Inteligencia de Amenazas_Septiembre_2024.pdf
  - Entregables del servicio de Ingeniería Social: i) Informe especifico de Ejercicio de Ingeniería Social - Septiembre 2024.pdf, ii) Memorias de sensibilización - Septiembre 2024.pptx; Anexos: i) Prueba Phishing Septiembre 2024 Contratistas.xlsx, ii) Prueba Phishing Septiembre 2024 Servidores Públicos.xlsx, iii) Informe de simulación de ataques - Microsoft Defender.xlsx
- 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: 2024.10.15 08:57:02 -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: Bogotá, D. C.

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