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**	1/08/2023	**Hasta**	31/08/2023
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	A continuación, se relacionan las actividades más relevantes del periodo: • Entendimiento de la prestación del servicio • Revisión de prerrequisitos del servicio. • Identificación de IPs objeto de la auditoría. • Definición del escaneo de vulnerabilidades. • Identificación y levantamiento de carta de aceptación de riesgo por posibles vulnerabilidades que no se puedan cerrar.	• ADRES - Vulnerabilidades TI y WEB - Informe de asistencia 8-02-23.csv • ADRES - Aclaración Carta aceptación de riesgo - Informe de asistencia 8-28-23.csv • Aceptacion de riesgo Vulnerabilidades.docx	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.	A continuación, se relacionan las actividades más relevantes del periodo: • Entendimiento de la prestación del servicio • Revisión de prerrequisitos del servicio. • Identificación de las URL's objeto de la auditoría. • Definición del escaneo de vulnerabilidades sobre aplicaciones WEB. • Identificación y levantamiento de carta de aceptación de riesgo por posibles vulnerabilidades que no se puedan cerrar.	• ADRES - Vulnerabilidades TI y WEB - Informe de asistencia 8-02-23.csv • ADRES - Aclaración Carta aceptación de riesgo - Informe de asistencia 8-28-23.csv • Aceptacion de riesgo Vulnerabilidades.docx	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.	Según el plan de trabajo la ejecución del servicio está sujeto a la ejecución y obtención de los resultados de los Análisis de Vulnerabilidades TI y Análisis de Vulnerabilidades sobre Componentes de aplicaciones Web.	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	A continuación, se relacionan las actividades más relevantes del periodo: • Entendimiento de la prestación del servicio de Ingeniería social.	• ADRES - Ingeniería Social - Informe de asistencia 8-24-23.csv	N/A

	dirigidos al personal de la entidad con el fin de obtener datos confidenciales o infectar los computadores con algún tipo de programa malicioso.	• Revisión de prerrequisitos del servicio. • Identificación de los posibles casos que se podrían realizar en el primer ejercicio.		
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: • Entendimiento de la prestación del servicio del servicio de monitoreo y correlación de eventos de seguridad • Verificación del acceso a la plataforma. • Identificación y atención de eventos de monitoreo. • Informe mensual.	• Monitoreo y Correlación de eventos de Seguridad 20230831.pdf • query_data_Incident_Clousd.csv • Grafica_Consolidado_Gestión_Eventos_Sentinel_AGO_2023.pdf • query_data_Login_Failure_AGO_2023.csv • ADRES - Validación de SIEM - Informe de asistencia 8-02-23.csv • ADRES - Eventos de Seguridad - Informe de asistencia 8-11-23.csv • ADRES - Prerrequisitos Monitoreo y correlación de eventos de seguridad - Informe de asistencia 8-03-23.csv • ADRES - Prerrequisitos Monitoreo y correlación de eventos de seguridad (cont.) - Informe de asistencia 8-04-23.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 la actividad más relevante del periodo: • Reuniones de trabajo para realizar configuraciones de VPN y tener acceso a los servidores	• ADRES - Validación de VPN - Informe de asistencia 8-02-23.csv • ADRES - Acceso aplicaciones - Informe de asistencia 8-09-23.csv	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: • Se establecen canales de comunicación para escalamientos de la ADRES hacia Indra y viceversa. • Elaboración de los informes por escalamientos realizados pro al ADRES y detectados por la plataforma. • Atención de casos sobre la plataforma Sentinel.	• ADRES - Acceso aplicaciones - Informe de asistencia 8-09-23.csv • query_data_Incident_Cloused.csv • Grafica_Consolidado_Gestión_Eventos_Sentinel_AGO_2023.pdf • Gestión de incidentes de seguridad 20230831.pdf	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: • Entendimiento de la prestación del servicio de Gestión de Infraestructura. • Se establecen canales de comunicación para escalamientos de la ADRES hacia Indra y viceversa. • Se realizan sesiones para la creación de cuentas de usuarios • Elaboración del informe mensual.	• ADRES - Acceso aplicaciones - Informe de asistencia 8-09-23.csv • Gestión de infraestructura de seguridad 20230831.pdf • Grafica_Consolidado_Gestión_Eventos_Sentinel_AGO_2023.pdf	N/A
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 la actividad más relevante del periodo: • Entendimiento de la prestación del servicio del plan de recuperación de desastres.	• ADRES - DRP - Informe de asistencia 8-15-23.csv	N/A
10	Elaborar, entregar y socializar previa aprobación del supervisor, el plan de trabajo	A continuación, se relacionan las actividades más relevantes del periodo:	• Kick Off Ciberseguridad ADRES.pdf	N/A

	del contrato conforme a lo descrito en el numeral 3 del ANEXO – ESPECIFICACIONES TECNICAS.	• Se realizo KickOff donde se da el alcance de la prestación del servicio. • Se elaboró y socializo el plan de trabajo. • Desarrollo de los procedimientos de requerimientos e incidentes y gestión de vulnerabilidades.	• MPC-ID-23SA36-001-Plan de trabajo.pdf • PPC-ID-23SA36-001-Gestion Inc Req Seguridad.pdf • PPC-ID-23SA36-002-Gestion Vuln Seguridad.pdf	
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.	Se presenta el equipo base con cumplimiento de los ROLES.	• Verificacion Equipo de Trabajo.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.	A continuación, se relacionan las actividades más relevantes del periodo: • FIRST • ISO 27001	• Certificate-sia-cert-2023 • ISO 27001 Indra Colombia - NR88B-.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.	• Configuraciones de VPN y tener acceso a los servidores. • Indra cuenta con plataformas perimetrales en alta disponibilidad donde están configurados las plataformas perimetrales de manera activo activos y por donde se encuentran publicados el canal de Internet	• ADRES - Validación de VPN - Informe de asistencia 8-02-23.csv	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.	El profesional definido como "un experto en seguridad" se tiene previsto presentarlo para aprobación a la ADRES para el mes de noviembre de 2023.	N/A	N/A
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: • Se tuvo reunión de inicio del servicio de Monitoreo de Marca, donde se definió: - Un (1) dominio - Una (1) marca - Filtración de credenciales - Monitoreo de abuso de marca (Redes sociales, dominios similares, phising) - Monitoreo 7x24 por la duración del contrato. - Un (1) informe del servicio por mes	• ADRES - Monitoreo de marca y Fuente de inteligencia - Informe de asistencia 8-24-23.csv • Monitoreo de Marca y Fuente de Inteligencia de Amenazas AGOSTO 20230907.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.	A continuación, se relacionan las actividades más relevantes del periodo: • Se tuvo reunión de inicio del servicio de Inteligencia de amenazas, donde se definió: - Se presento información de cuentas de correo electrónico con credenciales comprometidas en Internet	• ADRES - Monitoreo de marca y Fuente de inteligencia - Informe de asistencia 8-24-23.csv • Monitoreo de Marca y Fuente de Inteligencia de Amenazas AGOSTO 20230907.pdf	N/A

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

WILLIAMS ALEXANDER BRETO MARTINEZ

Firmado digitalmente por WILLIAMS ALEXANDER BRETO MARTINEZ
Nombre de reconocimiento (DN): street=Calle 93 # 16 - 25, 2.5.4.13=RE GSE CL 77 7 44 OF 701, cn=WILLIAMS ALEXANDER BRETO MARTINEZ, serialNumber=683018, st=BOGOTA D.C., l=BOGOTA D.C., email=wbreto@indracompany.com, c=CO, title=SEGUNDO REPRESENTANTE LEGAL GRUPO 1, o=INDRA COLOMBIA SAS, 1.3.6.1.4.1.47103.3.2=830013774, name=C.E, ou=GERENCIA AREA ADMINISTRATIVA Y FINANCIERA
Fecha: 2023.10.26 19:43:46 -05'00'

Firma del Contratista

Fecha: 10/10/2023

BALANCE ECONÓMICO

Valor Total Contrato (Inicial + Adición)		Valor Pagado	Valor a Pagar	Saldo Liberado	Saldo por Pagar
Vigencia 2023	$1762.183.892,00	$0,00	$105.951055,00	$0,00	$1656.232.837,00
Vigencia 2024	$2.390.471762,00	$0,00	$0,00	$0,00	$2.390.471762,00
Vigencia 2025	$2.390.471762,00	$0,00	$0,00	$0,00	$2.390.471762,00
TOTAL	$6.543.127.416,00	$0,00	$105.951055,00	$0,00	$6.437.176.361,00

La ADRES cancelará al CONTRATISTA, la suma de ciento cinco millones novecientos cincuenta y un mil cincuenta y cinco pesos ($105.951.055,00)

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

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	70526596	817.423.400	01/09/2023	30/09/2023	04/09/2023
PENSION	70526596	2.359.103.800	01/08/2023	31/08/2023	04/09/2023
ARL	70526596	133.672.400	01/08/2023	31/08/2023	04/09/2023

PAGO DE SEGURIDAD SOCIAL PERSONAS NATURALES
DEXTERA
Mes de ejecución contractual

CONCEPTO	PLANILLA No.	VALOR	PERIODO		FECHA DE PAGO
			DESDE	HASTA	
SALUD	9455368138	14.580.100	01/08/2023	01/08/2023	24/08/2023
PENSION	9455368138	50.023.800	01/08/2023	01/08/2023	24/08/2023
ARL	9455368138	14.518.700	01/08/2023	01/08/2023	24/08/2023

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. Se deja constancia que durante el mes de julio de 2023 se adelantaron actividades de presentación, revisión y aprobación tanto del equipo de trabajo como del plan de trabajo, por lo cual no se prestó ni facturó ningún servicio.
2. El (la) Contratista durante el mes de agosto de 2023, desarrolló y cumplió con objeto contractual, las obligaciones generales y específicas, presentó y entregó los productos y/o informes establecidos en el Contrato o Convenio en mención.
3. 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
- Informe mensual del servicio de gestión de incidentes, el cual comprende los reportes i) SUSPICIOUS CLIENT COMMUNICATION, ii) ADAPTIVE APPLICATION CONTROL POLICY VIOLATION WAS AUDITED y iii) THREAT MANAGEMENT.
- Informe mensual del servicio de gestión de infraestructura de seguridad

4. A la fecha no existen causales de incumplimiento de las obligaciones contractuales que demanden actuaciones conminatorias o sancionatorias por parte de la Administración.
5. Verifique la matriz de riesgos del contrato y se estableció, que no se ha materializado ninguno de los riesgos.
6. 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.

En constancia, firmo:

BENITEZ RODRIGUEZ GUILLERMO MANUEL

Firmado digitalmente por BENITEZ RODRIGUEZ GUILLERMO MANUEL
Fecha: 2023.10.27 14:50:42 -05'00'

Supervisor(es) / Interventor(es)

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., 10/10/2023

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