obika cibersecurity	**CERTIFICACIÓN COMERCIAL**	**Fecha de emisión:** 09/06/2023 **Versión:** 01

INFORMACIÓN DE LA EMPRESA			
NOMBRE DE LA EMPRESA:	OBIKA S.A.S	NIT:	901.399.442-3

INFORMACIÓN DE LA EMPRESA QUE CERTIFICA					
NOMBRE DE LA EMPRESA:	CONSORCIO OPERACIÓN SEGURIDAD 2022			NIT:	901.636.132-2
PAÍS/CIUDAD:	Colombia-Bogotá	DIRECCIÓN:		Calle 166 No. 20-45, barrio Toberín	
NOMBRE DEL CONTACTO:	Gabriel de Jesús mazo Mayorquín	CC	10.528.956	CARGO:	Representante Legal
E-MAIL:	info@gammaingenieros.com			TELÉFONO:	+ 57 (1) 4076000

INFORMACIÓN DEL SERVICIO PRESTADO POR OBIKA			
NUMERO DEL CONTRATO/ORDEN DE COMPRA	CTO-02-2022		
OBJETO DEL CONTRATO	Servicios en el Centro de Operaciones de Seguridad (SOC). incluye la totalidad de la FASE 4: Monitoreo y Correlación de eventos de Seguridad Mensuales, Gestión de incidentes de Seguridad Mensuales y Gestión de infraestructura de Seguridad Mensuales.		
FECHA DE CIERRE	31 de marzo de 2023	VALOR DEL CONTRATO	COP 784.859.795, 52 M/CTE incluido IVA
FECHA DE INICIO	03 de octubre de 2022	DURACION DEL CONTRATO	6 meses
OBJETO DE LA CERTIFICACIÓN O REFERENCIA COMERCIAL	Consorcio operación seguridad 2022 se permite referenciar a la compañía OBIKA S.A.S, como una empresa especializada en servicios de ciberseguridad, seguridad informática y seguridad de la información, de acuerdo con la realización de los siguientes servicios:		

DESCRIPCIÓN O ALCANCE DEL CONTRATO

1. **Monitoreo y correlación de eventos de seguridad**

Objetivo

Reducir los tiempos de respuesta ante amenazas, los falsos positivos y los eventos de seguridad que requieren investigación, que se pueden generar dentro de Azure, Microsoft Office 365, Centro de datos principal y sede, lo cual, define una infraestructura hibrida a ser monitoreada.

Actividades

Identificación y preparación del servicio
Realizar el levantamiento de información e identificación de las necesidades del servicio, que incluye la identificación de las tecnologías a utilizar, eventos a ser analizados y presentados, la arquitectura técnica de comunicaciones, ubicación de los sensores de recolección de datos (Logs) en el caso que se requieran, confirmación del inventario de dispositivos a evaluar, Identificación del modelo de red y modelo de categorías de activos.
Integración
Realizar la definición del modelo de gestión en donde se crearán los niveles de escalamiento, periodicidad de recolección y entrega de información, indicadores de riesgos, condiciones, reglas y filtros que

	serán aplicados a los eventos dentro de su ciclo de vida. **Plataforma de análisis** Realizar las siguientes actividades sobre el SIEM Microsoft Sentinel suministrado por la ADRES: • Configuración de la ingesta de datos de las diferentes fuentes de eventos de los sistemas de ADRES, las cuales incluyen soluciones de seguridad, sistemas operativos, aplicaciones, equipos de red, directorios de identidad, bases de datos y repositorios de datos. Si se hace necesario la ADRES dispondrá de las máquinas virtuales que sean requeridas para la implementación de los sensores del SIEM para la recolección de datos desde las fuentes de eventos. • Configuración de los conectores o mecanismos de recopilación de datos con y sin agente o través de servicios API REST • Configuración del periodo de almacenamiento de los eventos recolectados en línea y en reposo. La ADRES aprovisionará el almacenamiento necesario de acuerdo con las fuentes de datos a integrar y correlacionar. • Configuración de tipos de alertas de acuerdo con el nivel de criticidad de los eventos e incidentes de seguridad de la información y ciberseguridad. • Configuración de reglas y filtros de correlación • Creación de técnicas de detección basadas en la agregación y en umbrales **Ejecución** Realizar el monitoreo y análisis de los eventos e indicadores con base en la información recolectada y su presentación formal mediante la generación de informes y matrices según el alcance del servicio. Una vez un evento es confirmado como sospechoso o incidente, este se debe reportar según los niveles de escalamiento definidos en la etapa de integración. Entre las actividades a realizar se encuentran: • Identificación, análisis, escalamiento, reporte de los casos, acciones de tratamiento e indicadores de compromiso y seguimiento de las alarmas, eventos e incidentes detectados. • Clasificación y priorización de alarmas, eventos e incidentes detectados y analizarlos con el fin de poder determinar sus causas, origen e impacto. • Definición y afinación de las reglas de correlación con base en el análisis de la información, los falsos positivos identificados y sobre la evolución de la organización, la infraestructura y las amenazas tecnológicas • Adición de excepciones y personalización de normas para reducir los falsos positivos • Exploración y análisis geoespaciales de datos de red. • Monitorización de datos en tiempo real • Personalización, definición y programación de nuevos informes • Análisis de datos retrospectivo con visualización Supervisión de la geolocalización de usuarios • Detección avanzada de amenazas usando reglas de correlación para identificar un ataque dirigido o identificar comunicaciones y movimientos internos sospechosos como movimientos laterales, escalamiento de privilegios entre otros. • Actualización permanentemente y de manera especializada para estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad y por ende repórtalas de manera oportuna. <u>Características</u> El servicio de monitoreo de eventos de seguridad se debe prestar en la modalidad 7x24 hasta la fecha de finalización del contrato, el cual incluye correlación de eventos, detección, investigación y respuesta

	ante eventos e incidentes, amenazas y ataques contra la plataforma tecnológica y los sistemas de información de la ADRES. El servicio de monitoreo de eventos de seguridad debe utilizar la plataforma dispuesta por ADRES8 , la cual debe incluir el análisis de las siguientes fuentes de información: • Azure Active Directory • Azure Active Directory Identity Protection • Azure Activity • Azure DDoS Protection • Azure Firewall • Azure Information Protection • Azure Key Vault • Azure SQL databases • Azure Sorage Account • Azure Web Application Firewall • Microsoft 365 Defender • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Endpoint • Microsoft Defender for Identity • Microsoft Defender for Office 365 • Windows Firewall • Windows Security Events • Dominios relacionados en el servicio de análisis de vulnerabilidades • IMPERVA • Web Application Firewall – WAF • Firewall Fortinet sede y centro de datos • Antivirus Sophos Para la integración se utilizarán los conectores de datos de Microsoft Sentinel para SYSLOG, Registros de eventos de Windows, Formato de evento común (CEF), Trusted Automated eXchange of Indicator Information (TAXII) (para la inteligencia sobre amenazas), Azure y Servicios de AWS. Los sistemas de ADRES proceden de múltiples fabricantes como Microsoft, Fortinet, Sophos, IMPERVA, entre otros. La gestión de alertas, eventos e incidentes de seguridad deberá contemplar el escalamiento y seguimiento de los casos detectados de acuerdo con el protocolo que se establezca para tal fin. A través de las capacidades de CYBER THREAT HUNTING de Microsoft SENTINEL, el prestador del servicio deberá realizar la búsqueda periódica y proactiva para la detección y aislamiento de amenazas de ciberseguridad que hayan evadido los controles aplicados en la infraestructura. Se utilizará el modelo de ataque MITRE's ATT&CK el cual constituye una base de datos de las técnicas y tácticas de los ciber atacantes. Los procesos de gestión y operación deben estar basados en las mejores prácticas de acuerdo con uno o varios modelos como ITIL, CSIRT, ISO27001, NIST entre otros. Se debe generar alertas la entidad cuando se presenten amenazas de alta criticidad, ataques detectados, comportamientos sospechosos críticos. El prestador del servicio deberá contar con un grupo de personal calificado para el monitoreo de los activos de información y la atención de eventos de seguridad Suministrar información acerca de advertencias, anuncios, boletines, y documentación sobre las mejores prácticas actuales, listas de verificación, ataques de día cero, Información de desarrollo y distribución de parches, con el fin de generar boletines internos y mantener al día a los usuarios de la Entidad sobre nuevas amenazas. El proveedor debe contemplar dentro de sus actividades el monitoreo de disponibilidad y salud de las plataformas. NOTA: Se aclara que los licenciamientos y costos asociados al almacenamiento y retención de información producto de la correlación de eventos de seguridad son asumidos por la ADRES.

	Entregables **Informe Mensual:** Generar un informe mensual del análisis de eventos, alertas, incidentes y problemas de seguridad con estadísticas y tendencias actuales. El informe debe incluir los siguientes reportes: • Top de dispositivos con incidentes de seguridad. • Top de ataques detectados en la entidad • Top de usuarios con autenticaciones fallidas. • Reporte de riesgo e incidentes • Reporte de alertas e incidentes recurrentes o de alta criticidad **2. Gestión de incidentes de seguridad** Objetivo Gestionar los incidentes o hallazgos que sean relevantes dentro del proceso y de conformidad con el procedimiento de respuesta a incidentes de seguridad y los acuerdos de niveles de servicio aprobados, con soporte especializado para casos que requieran de un despliegue con atención de campo. Actividades Realizar las siguientes actividades: • Definición y elaboración de una matriz de escalamiento • Elaboración de una matriz de criticidad de los principales activos de información de propiedad de la ADRES, incluyendo los responsables de seguridad de la información, a los cuales se les notificarán los eventos, incidentes o problemas de seguridad detectados. Gestión de los incidentes de seguridad conforme a los procedimientos acordados. Esta gestión incluye acciones de contención por parte del proveedor o de manera compartida con la ADRES. • Comunicación de ocurrencia del incidente, indicando como mínimo fecha y hora de detección del evento, naturaleza del evento, prioridad, IP de origen, IP de destino y recomendaciones de contención del incidente. • Generación de filtros en la herramienta de correlación de eventos con el fin de disminuir los falsos positivos. Características El servicio de Gestión de Incidentes se debe prestar en la modalidad 7x24 hasta finalizar el contrato, que incluye los procedimientos que permitan reaccionar ante los incidentes de la mejor manera posible minimizando los daños de los sistemas de información, diagnósticos eficaces, recolectando las evidencias necesarias y mitigando las causas de los incidentes. Se debe detectar, reportar, evaluar y responder a incidentes de seguridad, incluida la activación de controles adecuados para la prevención y la reducción de impactos, y la recuperación de ellos. Para ello, el prestador del servicio deberá establecer un procedimiento apoyado con una metodología CSIRT para la detección, alertamiento, notificación, seguimiento y respuesta de incidentes de seguridad; también para informar puntos débiles de seguridad; definir responsabilidades que se deberían asignar para la gestión de incidentes y proponer mejoras de seguridad de la infraestructura tecnológica. El prestador del servicio debe contar con un equipo de respuestas a incidentes conformado por personal interdisciplinario y especializado

	para la atención a incidentes de seguridad conforme a las metodologías y procedimientos definidos. Cada caso o tiquete debe ser respondido y analizado durante todo su ciclo de vida por cada una de las partes con el fin de contribuir el resultado correcto de la gestión de incidentes. Se debe realizar configuraciones en la plataforma dispuesta por ADRES para el monitoreo y correlación de eventos, con el fin de implementar controles preventivos y hacer mejoras al enfoque global para la gestión de incidentes de seguridad. Prestar soporte especializado para casos que requieran de un despliegue con atención de campo y realizar el análisis forense ante un incidente de seguridad cuando sea requerido por la ADRES y realizar el levantamiento de la cadena de custodia como apoyo primer respondiente. Realizar análisis forense cuando al materializarse un incidente de seguridad de la Información se determine que es necesario la ejecución de este tipo de servicios <u>Entregables</u> Reporte de cada incidente de seguridad ocurrido, con su debida recomendación de contención de este. **3. Gestión de infraestructura de seguridad** <u>Objetivos</u> Gestionar la infraestructura de seguridad de la ADRES que no se encuentre tercerizada con el fin de mejorar la respuesta ante incidentes y amenazas de seguridad. <u>Actividades</u> Se deben realizarlas siguientes actividades: a. Levantamiento de información, que incluye la identificación de las tecnologías a utilizar y las actividades de administración a realizar. b. Creación y ajustes de reglas utilizando las herramientas dispuestas por la ADRES, con el fin de contener una amenaza u optimizar algún control de seguridad. c. Proponer los controles de cambio en los casos que se requieran. d. Monitoreo de cambios realizados para detectar posibles afectaciones en la operación <u>Características</u> El servicio de gestión de infraestructura se debe prestar en la modalidad 7x24 hasta finalizar el contrato, mediante la utilización de la plataforma dispuesta por ADRES que no se encuentren tercerizada, que incluye: i) las herramientas del centro de operaciones de seguridad como son Microsoft Sentinel, Microsoft Azure Monitor, Microsoft Security Center, Microsoft Endpoint (Intune), Microsoft Cloud Apps Security, Azure Defender y Microsoft 365 Defender y ii) las herramientas adicionales como son las consolas de administración de Microsoft 365, Azure Firewall, Azure DDoS, Microsoft Information Protection y Azure Active Directory. El proveedor del servicio utilizará las herramientas adicionales como son las consolas de administración de Microsoft 365, Azure Firewall, Azure DDoS, Microsoft Information

	Protection y Azure Active Directory, solamente para realizar configuraciones de emergencia para una pronta contención de un incidente o amenaza. La administración de estas soluciones seguirá a cargo de los líderes de servicios de la ADRES. Para las herramientas de seguridad que se encuentran tercerizadas como UTM, WAF, DAM el prestador del servicio tendrá el rol gestor que facilite las acciones de contención de amenazas por parte de estos terceros. <u>Entregables</u> Informe mensual de configuraciones realizadas utilizando las herramientas de seguridad Documentación de la arquitectura de seguridad. Se debe realizar la elaboración y actualización de la documentación de la arquitectura de seguridad de la entidad, donde se consignen cada una de las herramientas de seguridad dispuestas por la ADRES. **4. Acompañamiento para la ejecución el plan de remediación** Cien (100) horas de acompañamiento en la ejecución del plan de remediación definido por la Entidad y ejecución de RETESTING, a realizar dentro de los tres (3) meses siguientes a la entrega y recibo a satisfacción de los informes y plan de remediación del primer TESTING. Las nuevas pruebas de vulnerabilidad (RETESTING) se efectuarán respecto de los activos en los que se evidenciaron brechas de seguridad relevantes (Nivel de criticidad Alto) conforme con lo consignado en los entregables definidos. **5. Formación en Ethical Hacking** Diez (10) horas en formación en teoría y práctica en Ethical Hacking las cuales se deberán realizar en sesiones de trabajo de 2 horas, la cual será transmitida a mínimo 3 colaboradores de la ADRES, que serán comunicados a través de la supervisión contractual. **6. Material de sensibilización** Cinco (5) propuestas de infografías y cinco (5) propuestas de fondos de escritorio relacionadas a la concientización en temas de Ciberseguridad y Seguridad de la Información. **7. Monitoreo de marca** Prestación del servicio de monitoreo de marca para la entidad ADRES el cual incluye: • Un (1) dominio • Dos (2) marcas • Filtración de credenciales • Monitoreo de abuso de marca (Redes sociales, dominios similares, phising) • Cinco (5) Takedowns durante la duración del contrato • Monitoreo 7x24 por la duración del contrato. 8. **Capacitación en seguridad** Curso oficial de Microsoft de analista de operaciones de seguridad para dos (2) personas, en idioma español, que incluya examen de certificación.

CALIDAD DEL SERVICIO PRESTADO:	Excelente **X** Bueno Regular Deficiente

FIRMA DEL REPRESENTANTE LEGAL O PERSONA ENCARGADA



Firma:
Gabriel Mazo Mayorquin
Representante Legal

Fecha de expedición:	09/06/23