FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

<table>
<tr><td>OBJETOPOR CONTRATAR:</td><td>Prestación de servicios de garantía, soporte, mantenimiento y actualización para los equipos de seguridad informática, con que cuenta la UAECD, así como el servicio de monitoreo y seguridad SOC.</td></tr>
<tr><td>DENOMINACIÓN DEL BIEN O SERVICIO:</td><td>
<table>
<tr><th>CÓDIGO UNSPSC</th><th>SEGMENTO</th><th>FAMILIA</th><th>CLASE</th></tr>
<tr><td>43222500</td><td>43- Difusión de Tecnologías de Información y Telecomunicaciones</td><td>22 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos</td><td>25 - Equipo de seguridad de red</td></tr>
<tr><td>43222600</td><td>43- Difusión de Tecnologías de Información y Telecomunicaciones</td><td>22 - Equipos o plataformas y accesorios de redes multimedia o de voz y datos</td><td>26 - Equipo de servicio de red</td></tr>
<tr><td>43233200</td><td>43 - Difusión de Tecnologías de Información y Telecomunicaciones</td><td>23 – Software</td><td>32-Software de seguridad y protección 18 – Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td>81111800</td><td>81 – Servicios basados en ingeniería, investigación y tecnología</td><td>11 - Servicios informáticos</td><td>18 – Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td>81112200</td><td>81 – Servicios basados en ingeniería, investigación y tecnología</td><td>11 – Servicios informáticos</td><td>22-Mantenimiento y soporte de software</td></tr>
</table>
</td></tr>
<tr><td>UNIDAD DE MEDIDA:</td><td>
<table>
<tr><th colspan="4">EQUIPOS PARA GARANTÍA, SOPORTE Y MANTENIMIENTO</th></tr>
<tr><th>N.°</th><th>Descripción</th><th>Cant.</th><th>Unidad de Medida</th></tr>
<tr><td>1</td><td>ADQUISICIÓN Y RENOVACIÓN TECNOLÓGICA: Adquisición de Hardware (FortiAnalyzer), renovación de licencias Nube (OCI/Azure) y On-Premise. Incluye soporte directo del fabricante.</td><td>1</td><td>Global</td></tr>
<tr><td>2</td><td>SERVICIO DE MONITOREO DE MARCA, SEGURIDAD SOC Y GESTIÓN MENSUAL DE VULNERABILIDADES: Vigilancia 24/7 de la infraestructura,</td><td>12</td><td>Mes</td></tr>
</table>
</td></tr>
</table>

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

		incluye la operación de licenciamiento del Ítem 3, análisis de hallazgos y entrega de informes mensuales de gestión de riesgos. (INCLUYE LA TOTALIDAD DE LOS COSTOS SALARIALES, PRESTACIONALES Y ADMINISTRATIVOS DE LOS CINCO (5) PERFILES PROFESIONALES EXIGIDOS EN LA FICHA TÉCNICA).		
	3	ADQUISICIÓN / RENOVACIÓN DE LICENCIAMIENTO PARA ANÁLISIS DE VULNERABILIDADES: Suscripción de licenciamiento (tipo Tenable o equivalente) para 210 activos por 12 meses. Este ítem contempla exclusivamente el costo del derecho de uso del software (SaaS/Suscripción).	1	Global

DESCRIPCIÓN GENERAL DEL SERVICIO:

CONDICIONES MÍNIMAS GENERALES PARA TODOS LOS ITEMS (EXCEPTO ITEM 2 - 3)

No.	DESCRIPCIÓN
1	Se deberá renovar la garantía, licenciamiento y el soporte directamente con el fabricante por doce (12) meses contados a partir de la suscripción del acta de inicio para cada uno de los elementos objeto de la contratación, en los términos establecidos en la ficha técnica y propuesta presentada. Asimismo, el licenciamiento de las soluciones anteriormente descritas deberá contar con una fecha de expiración unificada al 31 de julio de 2027, como se muestra a continuación:
2	Se deberá actualizar el software de todas las plataformas de acuerdo con las recomendaciones del fabricante en cuanto a tener instaladas las últimas versiones más estables, seguras, confiables y funcionales. Estas actividades harán parte de los mantenimientos preventivos y soporte en general.
3	Se deberá prestar servicios de soporte técnico, mantenimiento preventivo y cambio de partes para los elementos de tipo hardware relacionados en la tabla de unidad de medida.

Número de Serie	Modelo	Descripción	Fecha de Vencimiento
FG9H0GTB24900013	FortiGate 900G	FGCATASTRO_01	2026-07-31
FG9H0GTB24900327	FortiGate 900G	FGCATASTRO_02	2026-07-31
FGVM4VTM24003585	FortiGate VM04V	FortiGate VM04 02	2026-07-31
FGVM4VTM18000139	FortiGate VM04V	FGTVM_AZURE	2026-07-31
FGVM8VTM24003354	FortiGate VM08V	FortiGate VM08V OCI	2026-07-31
FGVM8VTM24003854	FortiGate VM08V	FGT VM08 02	2026-07-31
FSA1KFT619000028	FortiSandbox 1000F	FSA_UAECD	2026-07-31
FSMP000000003507	FortiSIEM	FORTISIEM_UAECD	2026-07-31
FV-1KET120900187	FortiWeb 1000E	FWB_UAECD_S	2026-05-15
FV-1KET119900219	FortiWeb 1000E	FWB_UAECD_M	2026-05-15
FVVM040000178185	FortiWeb VM 4 CPU	FWBVM_AZURE	2026-07-31
FVVM04TM21000017	FortiWeb VM 4 CPU	FWBVM04-OCI	2026-07-31
FL-8HFT721900046	FortiAnalyzer 800F	FAZ-UAECD	2026-07-31
FRNFPR0000000218	ELA FortiRecon Pre Pay		2026-07-31

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	4	Se deberán atender e implementar todas las configuraciones solicitadas por la Entidad que permitan mejorar la seguridad y desempeño de cada uno de los elementos objeto de la contratación, bajo las buenas prácticas de fabricante.
	5	Se deberá explicar claramente con un tiempo máximo de cinco (5) días después de firmada el acta de Inicio del contrato, la metodología que se debe seguir para solicitar y prestar el servicio de soporte técnico y mantenimiento, en dicho procedimiento se deben relacionar los canales de comunicación y ANS respectivos.
	6	Se deberá hacer efectiva ante el fabricante la garantía de los componentes de los equipos que deban ser remplazados garantizando el cambio total de cualquier parte, equipos o repuestos que presenten defectos o fallas de material por fabricación, por otros nuevos de iguales o mejores características. Este cambio deberá realizarse en un plazo máximo de 7 días calendario. Mientras se efectúa el cambio del componente defectuoso, el proveedor deberá proporcionar un equipo de iguales o mejores características en calidad de préstamo para no afectar la operación de la entidad. Los repuestos empleados para reemplazar elementos defectuosos deberán ser nuevos y de la misma calidad de las partes cambiadas y deberán tener garantía de un año. El cambio se realizará previa autorización del Supervisor del contrato.
	7	De igual forma, en cualquier caso, el contratista deberá realizar todas las configuraciones, parametrizaciones y demás actividades que garanticen la correcta operación sobre equipos nuevos o en calidad de préstamo, esto sin que se genere ningún costo adicional para la entidad
	8	El proponente deberá realizar la actualización del equipo FortiAnalyzer 800F en mención con el mismo licenciamiento, soporte y garantías del fabricante teniendo en cuenta el end-of-support (EoS) de la plataforma actual. La actualización de la solución deberá ser por uno equipo Fortinet que posea mínimo las siguientes características: - Centralized log and analysis appliance - Interfaces: 4x RJ45 GE y 2x GE SFP - 16 TB self-encrypting storage - Hasta 200 GB/ day de logs. - Analytic Sustained Rate (logs/sec) de 4000 - Collector Sustained Rate (logs/sec) de 6000

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

ESPECIFICACIONES GENERALES PARA EL ÍTEM 2 - Servicio de monitoreo de marca y seguridad SOC

No.	DESCRIPCIÓN
1	La UAECD cuenta actualmente con una solución de monitoreo y correlación de eventos de seguridad FORTISIEM S/N FSMP000000003507, la cual cuenta con capacidad para monitorear y correlacionar 150 dispositivos entre los que se encuentran AP, servidores controladores de dominio, servidores de archivos, servidores de aplicaciones, servidores de bases de datos, servidores web Apache/IIS, servidor Symantec Endpoint Protection, hipervisores, almacenamiento, aplicaciones, firewalls, switches, routers, balanceadores de carga, almacenamiento NAS – SAN, entre otros. El contratista deberá realizar la correlación, monitoreo y casos de uso sobre la plataforma del UAECD, de tal forma que todo el know how y parametrizaciones queden para la entidad. En ningún caso la información de logs deberá salir de la entidad.
2	Las evidencias recopiladas por el SOC son propiedad de la UAECD y podrán ser solicitadas en cualquier momento para atención de requerimientos legales.
3	El proveedor deberá usar la solución de SIEM como herramienta de monitoreo, análisis y correlacionador de eventos. Para acceder al SIEM, que es el núcleo central del monitoreo, se hará a través de una conexión segura utilizando internet, el costo del canal de internet del proponente no generará costos adicionales a la entidad.
4	El contratista deberá realizar todas las actividades y operaciones necesarias sobre el SIEM y sus componentes para los nuevos casos de uso que se requieran garantizando el correcto funcionamiento de este, así como mantener la operación del SOC acorde con las necesidades de la UAECD.
5	El contratista deberá realizar la configuración, desarrollo de conectores necesarios y el parsing para la generación de los casos de uso que la UAECD requiera, los cuales involucrarán los dispositivos monitoreados.
6	El proveedor deberá realizar los scripts y/o desarrollos compatibles sobre el correlacionador eventos (SIEM) para que este se integre con los sistemas que la UAECD requiera.
7	El servicio se prestará para la Unidad Administrativa Especial de Catastro Distrital (UAECD) para sus infraestructuras ubicadas en: la Carrera 30 25-90; y de nubes: Microsoft Azure y Oracle Cloud Infrastructure.
8	El contratista deberá mantener el inventario de dispositivos monitoreados actualizado, ajustándose a los cambios y a la dinámica de las necesidades institucionales sin costo adicional para la Entidad.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	9	En caso de que las plataformas que se relacionan en la Tabla N° 3 Plataformas de seguridad informática de la UAECD, no sean suficientes para el monitoreo del SOC, el contratista podrá integrar al servicio cualquier otra herramienta compatible con el SIEM que considere sin que esto genere un costo adicional para la Entidad. Tabla N° 3 Plataformas de seguridad informática de la UAECD

N.°	Tipo de Equipos o plataformas	Números de Serie
1	FortiSIEM	FSMP000000003507
2	FortiAnalyzer	FL-8HFT721900046
3	FortiGate Nube OCI	FGVM8VTM24003354 FGVM8VTM24003854
4	FortiWeb Nube OCI	FVVM04TM21000017
5	FortiGate Nube Azure	FGVM4VTM18000139 FGVM4VTM24003585
6	FortiWeb Nube Azure	FVVM040000178185
7	FortiGate On-Premise	FG9H0GTB24900013, FG9H0GTB24900327
8	FortiSandbox	FSA1KFT619000028
9	FortiWeb On-Premise	FV-1KET120900187, FV-1KET119900219
10	FortiRecon	FRNFPR0000000218

	10	La Entidad requiere el monitoreo de disponibilidad, seguridad y alertas de las plataformas de servidores físicos, virtuales en infraestructura On-Premise y de nubes que soportan los servidores de infraestructura, de bases de datos, de aplicaciones, de redes y comunicaciones y de seguridad informática para el ambiente de producción principalmente de catastro multipropósito. La plataforma de servidores deberá estar disponible, monitoreada y en operación 7x24 mediante el monitoreo de disponibilidad a través de las plataformas con las que cuenta la Entidad, principalmente el SIEM (sobre el cual también deberá administrar su gestión de cambios), y con aquellas que el proveedor considere necesarias para garantizar el servicio y el cumplimiento de los Acuerdos de Niveles de Servicio - ANS, sin que esto genere un costo adicional para la Entidad.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

11	El proveedor realizará la integración y monitoreo de los dispositivos y activos tecnológicos que conforman la infraestructura tecnológica de la UAECD de acuerdo con la infraestructura para ser monitoreada. Una vez integrada toda la plataforma tecnológica, el proveedor configurará, mantendrá y afinará la herramienta de correlación para mejorar su funcionalidad.
12	A los cinco (5) días hábiles posteriores a la suscripción del acta de inicio, el contratista deberá presentar el plan de trabajo del proyecto que incluya como mínimo: funciones y responsabilidades del personal involucrado, cronograma de trabajo, etapas, resultados esperados, productos a entregar, estrategias para asegurar el logro de dichos productos en los tiempos establecidos y describir los procesos/procedimientos, las técnicas y herramientas que utilizará en la ejecución del contrato, que deberán ser aprobados por el supervisor del contrato. Cualquier cambio en alguno de estos aspectos en el desarrollo del contrato, deberá ser informado y aprobado por el supervisor.
13	A los diez (10) días hábiles posteriores a la suscripción del acta de inicio, el contratista deberá entregar el inventario y diagnóstico del estado de funcionamiento de los equipos objeto del servicio con el fin de identificar las necesidades futuras y roadmap de la plataforma.
14	El contratista deberá contar con un SOC propietario en la ciudad de Bogotá, respaldado adecuadamente con esquemas de contingencia. Este SOC será administrado y operado por el personal del proponente en sus propias instalaciones.
15	Disponer del servicio de protección de marca y riesgos digitales para el monitoreo en esquema 7X24, el cual será por el término de un (1) año contado a partir de la fecha de activación, contemplando el envío de alertas y reportes de eventos e incidentes de seguridad de la exposición de marca de la Unidad Administrativa Especial de Catastro Bogotá - UAECD.
16	Cuando un evento de seguridad ocurre o está en suceso, el SOC deberá identificarlo y estar en la capacidad de relacionar de forma directa o indirecta con otros eventos de seguridad asociados, determinando el patrón de ataque.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	17	El servicio debe incluir informes, en idioma castellano, que la UAECD requiera durante la prestación del servicio, incluyendo como mínimo reportes mensuales (mes cumplido en los primeros cinco (5) días hábiles del mes siguiente) tanto de SOC como de disponibilidad; así como casos específicos sobre eventos de seguridad en la UAECD solicitados por el Supervisor del contrato o canalizados a través del Oficial de Seguridad de la Entidad o la Subgerencia de Infraestructura (a los tres (3) días hábiles posteriores a la mitigación del evento de seguridad). Estos informes pueden referirse a: • Estado y resultados del servicio en el periodo de valoración, de tipo gerencial. • Eventos de actividad sospechosa atendidos durante el periodo. • Cambios realizados sobre la infraestructura monitoreada. • Alertas, ataques, incidentes y tendencias. • Comportamientos más relevantes según la correlación realizada por el proponente. • Incidentes de seguridad presentados. • Estadísticas de la información procesada • Hallazgos realizados sobre la plataforma tecnológica • Análisis y recomendaciones sobre los resultados • Acciones preventivas, tales como instalación de parches, actualización de versiones, modificación de políticas y configuraciones.
	18	El servicio debe permitir la integración del envío de alarmas automáticas, relativas a seguridad, vía correo electrónico a los ingenieros de seguridad informática de la Entidad.

DETALLES DEL MONITOREO – ITEM 2	
No.	**DESCRIPCIÓN**
1	Se deberán generar alertas de todas las amenazas que puedan impactar la infraestructura tecnológica de la UAECD, como las identificadas en los reportes de análisis de tendencia de centros como el CSIRT/CERT o en las bases de datos de conocimiento del proponente. Asimismo, el contratista deberá disponer de servicios de inteligencia ante Ciber Amenazas.
2	El contratista deberá mantener sincronizados todos los relojes de las herramientas de monitoreo con la hora legal colombiana, suministrada por la Superintendencia de Industria y Comercio (http://horalegal.sic.gov.co/)

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	3	El SOC deberá ejecutar actividades permanentes para garantizar el descubrimiento y monitoreo de nuevos dispositivos en la red.
	4	El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Una vez terminado el vínculo contractual, el proponente deberá destruir toda la información a la que tuvo acceso de la UAECD.
	5	Los servicios ofrecidos deberán poder ser visualizados a través de tableros de control que permitan ver métricas en línea de acuerdo con las necesidades del UAECD, como: • Alertas/Incidentes por tipo • Alertas/Incidentes nuevos y resuelto • Tiempo medio de creación de alertas/incidentes • Tiempo medio de solución • Tendencias y top de alertas/incidentes • Cumplimiento de acuerdos de servicio • Nivel de disponibilidad del servicio
	6	El servicio de SOC requerido abarcará la monitorización de eventos de seguridad esenciales para la UAECD, incluyendo, pero no limitándose a eventos relacionados con cuentas privilegiadas, bases de datos, cambios en plataformas Windows y Linux, conexiones, comportamientos sospechosos, auditoría, entre otros. La entidad se reserva el derecho de solicitar ajustes en las categorías de eventos a medida que evolucionen los requisitos de seguridad y las necesidades operativas.

	SOPORTE Y MANTENIMIENTO PARA TODOS LOS ÍTEMS (EXCEPTO ITEM 2 - 3)	
	No.	**DESCRIPCIÓN**
	1	Se deberá prestar soporte técnico cuantas veces así lo requiera la entidad de manera presencial y/o remota en modalidad (7x24x4). El proveedor atenderá los requerimientos de soporte a los equipos reportados y efectuará la asistencia técnica ante la presencia de fallas.
	2	De requerirse un técnico en las oficinas de la entidad, este deberá desplazarse para atender los eventos reportados, de acuerdo con el horario de cubrimiento y tiempos de respuesta solicitados, siempre y cuando la solución del problema reportado no se pueda realizar mediante las conexiones remotas que actualmente la entidad tiene configuradas. Los gastos de transporte del personal ajeno a la entidad deben correr por cuenta del proveedor y no deben generar ningún costo adicional para la Entidad.
	3	Se deberán entregar informes o documentación detallada de todos los proyectos y procedimientos realizados después de los mantenimientos preventivos, correctivos y soporte por cambios de unidades, problemas presentados, actualizaciones, así mismo se debe detallar en el informe las causas, procedimientos preventivos y soluciones futuras inmediatas a los problemas o daños presentados en cualquiera de las herramientas.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

		4	En caso de ser necesario se deberá diseñar y ejecutar el plan de instalación o reconfiguración más recomendado para la Entidad dando el soporte técnico adecuado con los niveles de servicio necesarios para el óptimo funcionamiento, previa presentación del plan de trabajo y aprobación por parte del supervisor.
		5	Se deberán atender todos los incidentes y requerimientos técnicos a que haya lugar, incluidos casos de Security Operation Center - SOC. Una vez solucionada la falla, el proveedor presentará un informe de análisis causa raíz basado en la recopilación de eventos del SIEM, así como también incluirá un plan de mejoramiento o remediación para prevenir que se vuelva a presentar la falla, durante el término de la garantía.
		6	Se deberán atender consultas técnicas sobre funcionamiento de las herramientas, configuración de funcionalidades y características propias de las plataformas, reconfiguración de la solución y requerimientos técnicos.
		7	La metodología de escalamiento de soporte a usar es la siguiente: • 1 nivel: Soporte Técnico del proveedor. • 2 nivel: Soporte Técnico Especializado proveedor. • 3 nivel: Soporte Técnico Fabricante. El soporte técnico presencial se debe brindar en las instalaciones de la entidad en la ciudad de Bogotá. El soporte técnico debe garantizar una adecuada operación de los componentes relacionados en esta ficha técnica, de conformidad con las especificaciones técnicas
		8	**Atención en Sitio:** Cuando se haya determinado el problema y no se encuentre solución telefónica o remota, el proveedor debe asignar un ingeniero para que se desplace a las oficinas de la entidad, de acuerdo con los tiempos definidos en la tabla Acuerdos de Niveles de Servicio – ANS, del presente documento.
		9	**Contactos de soporte técnico:** La entidad en conjunto con el proveedor, deberá identificar los números telefónicos correspondientes de contactos de acuerdo con la matriz de escalamiento suministrada por el proveedor, quienes serán el canal autorizado para acceder a los servicios de soporte técnico. Únicamente las personas que la entidad haya referenciado pueden pedir apoyo, formular consultas y/o solicitar soporte.
		10	**Mantenimiento Preventivo:** Se deben realizar dos (2) mantenimientos preventivos a nivel lógico y físico en las instalaciones de la entidad donde se encuentran instalados los equipos físicos, y de forma remota para las plataformas que se encuentran en la nube; dichas actividades se deben realizar así: • Un (1) mantenimiento preventivo en el segundo semestre del 2026. • Un (1) mantenimiento preventivo en el primer trimestre del 2027. El proveedor deberá entregar la hoja de ruta y el cronograma de las actividades que va a realizar en dichos mantenimientos, estas actividades deberán cumplir con las mejores prácticas del fabricante.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

		11	Se deberá contar con un centro de soporte al cliente 7x24 el cual será el único contacto para la solicitud de servicios, quien igualmente debe contar con un sistema de gestión de mesa de ayuda en donde se respondan y solucionen todas las peticiones de soporte de la entidad, resolviendo los casos o direccionándolos inmediatamente al fabricante.
		12	En los casos de soporte en sitio, el centro de soporte al cliente deberá hacer un seguimiento de la solicitud del servicio, desde el momento de recibo de la llamada hasta la prestación del servicio, para asegurar y verificar que el trabajo de los ingenieros de campo se está haciendo de acuerdo con los estándares técnicos y de servicios ofrecidos a la entidad.
		13	El centro de atención al cliente debe asegurar el cumplimiento del servicio solicitado por la entidad hasta que se haya terminado y solucionado.
		14	Al momento de realizar el mantenimiento preventivo y cambio de partes a los elementos, se deberá verificar que todo residuo que se genere durante esa actividad se disponga de una manera ambientalmente adecuada, y en caso de generarse residuos de los aparatos eléctricos y electrónicos - RAEES objeto del contrato, estos deben ser gestionados con una empresa que cuente con licencia ambiental para este tipo de residuos.
		15	Para el ítem 2, el proveedor hará monitoreo constante del estado de disponibilidad y desempeño de la herramienta de correlación de eventos y generará los reportes correspondientes de caídas que se presenten y que puedan afectar los acuerdos de niveles de servicio y porcentajes de disponibilidad contratados por la UAECD.
		16	Para el ítem 2, se deberá garantizar la disponibilidad, confidencialidad, integridad, no repudio, auditoria y privacidad de los datos y servicios soportados
		17	Para el ítem 2, el servicio se centrará en el tratamiento de eventos, identificación y gestión de incidentes, los cuales contarán con un conjunto de metodologías y atención, procesos que permitirá brindar respuesta oportuna a los riesgos y
			amenazas. Por lo anterior, el personal del servicio del SOC deberá realizar el escalamiento a través de la herramienta de mesa de servicios con que cuente y las comunicaciones por medio de correo electrónico y/o telefónico con el personal de la UAECD a fin de comunicar las incidencias presentadas y las acciones a seguir para solucionarlas. Adicionalmente realizará el seguimiento, apoyo y acompañamiento sobre los eventos hasta que estos sean cerrados adecuada y oportunamente.
		18	Para el ítem 2, se realizará una valoración de las amenazas existentes en la región y el mundo, determinando cuál de estos exponen a un riesgo a la UAECD, resumiendo los resultados en boletines o Informes extraordinarios de SOC.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	19	Para el ítem 2, se realizará seguimiento 7x24 a los ataques originados desde Internet al igual que los originados al interior de la Entidad. El SOC, debe definir la matriz de escalamiento de común acuerdo con los responsables de seguridad informática en la UAECD, clarificando el nivel de escalamiento según el tipo y nivel de incidente.
	20	Para el ítem 2, se deberán analizar las diferentes alertas detectadas para descartar falsos positivos, antes de crear el caso/ticket en la herramienta de mesa de servicios dispuesta para ello.
	21	Para el ítem 2, el contratista deberá informar inmediatamente al equipo de seguridad informática de la UAECD o a la Subgerencia de Infraestructura Tecnológica en su horario laboral, sobre cualquier evento o incidente real que no sea droppeado ni bloqueado y se presente sobre la infraestructura tecnológica de la Entidad. Los incidentes que se presenten fuera del horario laboral de la Entidad deberán ser notificados a la misma al personal que disponga la Entidad para atención 7x24.
	22	Para el ítem 2, el contratista deberá tener desarrollados casos de uso estándar para los tipos de incidentes establecidos.
	23	Para el ítem 2, el contratista deberá contar con procesos de atención a incidentes de seguridad, los cuales contemplen la estimación de los niveles de riesgo asociados.
	24	Para el ítem 2, el contratista deberá contar con procesos definidos para la detección, categorización y alertamiento oportuno de incidentes de seguridad
	25	Para el ítem 2, el contratista deberá definir escenarios de crisis para preparación ante Amenazas Persistentes Avanzadas (APT), ataques de DDoS y ataques focalizados y así definir reglas para detectar, reaccionar y contener ataques dirigidos.
	26	Para el ítem 2, en caso de que el contratista identifique algún tema cuya relevancia podría ameritar un análisis urgente por parte del UAECD, se generará un Informe urgente con la información correspondiente.
	27	El contratista deberá alinearse a las políticas de la UAECD relaciones con el intercambio seguro de información.
	28	El contratista debe contar con la membresía vigente del FIRST (Forum of Incident Response and Security Teams) con vigencia mínima de seis (06) meses para la ejecución del SOC.
	29	El contratista debe contar con la certificación vigente de ISO 27001:2022
	30	El contratista debe entregar una carta dirigida a la entidad donde se evidencia que cuenta con la especialidad de Security Operation ó especialidad en Secure Networking Firewall por parte del fabricante de la solución de SIEM, lo anterior garantizando que el canal o partner posea el aval por parte de la marca para la prestación del servicio SOC.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

GARANTÍA

No.	DESCRIPCIÓN
1	Se deberá extender la garantía, soporte y mantenimiento correctivo directo de fabricante por doce (12) meses contados a partir de la suscripción del acta de inicio para cada una de las plataformas objeto de este contrato y de acuerdo con los niveles de servicios solicitados, a partir del vencimiento de la garantía actual. Asimismo, el soporte y garantía de las soluciones deberá contar con una fecha de expiración unificada al 31 de julio de 2027.

EQUIPO MÍNIMO PARA SOPORTE Y GESTIÓN DE VULNERABILIDADES

Cant	Perfil	Formación académica	Experiencia general
1	Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones, industrial o carreras afines. ● Posgrado en Gerencia de Proyectos y/o Certificación PMP vigente. ● Certificación vigente en ITIL Foundation v3 o superior. ● Certificación vigente en ITIL Strategist Direct, Plan and Improve ● Certificación vigente en ITIL Managing Professional	Experiencia mínima 10 proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática. Tarjeta Profesional con expedición mínima de diez (10) años
1	Ingeniero Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización o maestría en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en SCRUM Foundations Professional (SFPC). ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR LÍDER en la norma ISO/IEC 27001:2022. ● Certificación vigente en LÍDER GESTOR CIBERSEGURIDAD en la norma ISO/IEC 27032:2023. ● Certificación vigente como especialista en seguridad en redes. Emitida por el fabricante de las soluciones del proceso.	Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cinco (5) años como líder o coordinador o gerente de servicios de TI. Certificaciones de Experiencia especifica de mínimo años (5) años en Liderar equipo de operaciones y servicios de seguridad.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	1	Ingeniero Implementador	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación en AUDITOR INTERNO en la norma ISO/IEC 20000-1:2018. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como profesional en nube publica ● Certificación vigente como especialista en seguridad en redes ● Certificación vigente como especialista en seguridad en nube publica ● Certificación vigente como especialista en seguridad de OT ● Certificación vigente como especialista en SASE	Experiencia general de diez (10) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional
	1	Ingeniero de soporte Nivel 2	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Especialización en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en AUDITOR INTERNO en la norma ISO/IEC 27001:2022. ● Certificación vigente como profesional de seguridad en redes ● Certificación vigente como especialista en seguridad en redes ● Certificación vigente como especialista en SASE ● Certificación vigente como especialista en Acceso confianza cero	Experiencia general de siete (7) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cinco (5) años en implementación, soporte y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

1	Ingeniero de soporte Nivel 1	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. ● Especialización en Seguridad de la Información ó informática ó Ciberseguridad. ● Certificación vigente en ITIL Foundation v3 o superior. ● Certificación vigente como Profesional en Operaciones de Seguridad ● Certificación vigente en Seguridad en la Nube y Gestión de Postura de Seguridad en entornos Cloud ● Certificación vigente en Gestión y Análisis de la Superficie de Ataque Externa ● Certificación vigente en Seguridad de Identidades y Gestión de Exposición de Directorios. ● Certificación en Certified in Cybersecurity ISC2	Experiencia general de cinco (5) años a partir de la expedición de la tarjeta profesional, de los cuales mínimo de cuatro (4) años en implementación, soporte y/o monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional

ACUERDOS DE NIVELES DE SERVICIO PARA LA GARANTÍA, SOPORTE Y MANTENIMIENTO DE LOS EQUIPOS DE SEGURIDAD INFORMÁTICA

La medición de los Acuerdo de Niveles de Servicio (ANS) para el servicio de garantía, soporte y mantenimiento de los equipos de seguridad informática son los siguientes:

Nº	TIPO DE FALLA	DESCRIPCIÓN	VALOR/NIVEL DE ACEPTACIÓN	PENALIZACIÓN
1	Incidentes - Pérdida de Servicio	Se entiende como interrupción total del servicio.	≤ 30 minutos calendario	Por cada 2 horas de retraso en la atención de los incidentes que se tengan en el mes, el proveedor deberá dar un día de licenciamiento adicional.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	2	Incidentes - Operación Degradada	Servicio Restringido, Lentitud en el servicio o bajo desempeño. Presencia de fallas presentadas esporádicamente y que pueden causar interrupción en el servicio por periodos cortos.	≤ 2 horas calendario	Por cada 4 horas de retraso en la atención de los incidentes que se tengan en el mes, el proveedor deberá dar dos días de licenciamiento adicional.
	3	Requerimientos y/o fallas no graves.	Se entiende como la que no afecta ni degrada la prestación del servicio. En este nivel se encuentran los requerimientos, consultas, preguntas y sugerencias de mejora sobre el servicio.	≤ 4 horas calendario	Por cada 8 horas de retraso en la atención de las solicitudes que se tengan en el mes, el proveedor deberá dar cuatro días de licenciamiento adicional.

Nota: Cualquier intervención programada y autorizada (ventanas y/o mantenimientos) no se contabiliza dentro de los tiempos de respuesta establecidos en los ANS.

ACUERDOS DE NIVELES DE SERVICIO PARA SERVICIO DE MONITOREO Y SEGURIDAD SOC

La medición de los Acuerdo de Niveles de Servicio (ANS) que se menciona a continuación se realizará de manera mensual, y se basará en los informes de gestión mensual que debe presentar el contratista, así como los específicos por incidentes.

Nº	DESCRIPCIÓN	FORMA DE MEDICIÓN	UNIDAD DE MEDIDA	VALOR/NIVEL DE ACEPTACIÓN	COMPENSACIÓN
1	Monitorización evento crítico[2]	Eventos escalados dentro de una (1) hora calendario[3].	Número	≤ 1	Más de 2% de casos escalados después de una (1) hora. Descuento del 10% en la factura mensual de servicio.

FICHA TÉCNICA

PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA

	2	Monitorización evento alto	Eventos escalados dentro de dos (2) horas calendario.	Número	≤ 2	Más de 2 horas en ser escalados. Descuento del 5% en la factura mensual de servicio.
	3	Monitorización evento medio	Eventos escalados dentro de doce (12) horas calendario.	Número	≤ 12	Más de 12 horas en ser escalados. Descuento del 3% en la factura mensual de servicio.
	4	Monitorización evento bajo o informativo	Eventos escalados dentro de veinticuatro (24) horas calendario.	Número	≤ 24	Más de 24 horas en ser escalados. Descuento del 1% en la factura mensual de servicio.
	• **Entrega mensual de informes de gestión de vulnerabilidades**: Primeros 5 días hábiles. • **Compensación**: El retraso en la entrega generará un descuento del 1% sobre el valor de la factura mensual del Ítem 2.					

2 La definición de evento crítico, alto, medio y bajo/informativo se tomará a partir de categorizaciones de alertas emitidas desde el FortiAnalyzer y el SIEM.

3 El tiempo se empezará a contar desde que el SIEM haga el reporte del evento a través de sus alarmas.

JAVIER ALEJANDRO PEREIRA VARGAS
Subgerente de Infraestructura Tecnológica

Elaboró: Iván García Beltrán - Contratista - Subgerencia de Infraestructura Tecnológica