

ANEXO NO. 1 ESPECIFICACIONES TÉCNICAS

Objeto:					
Renovación del licenciamiento de la solución tecnológica IBM Guardium, incluido actualización y servicios Expertise Connect en ambiente On-premise”;					
No.	REQUERIMIENTOS	DESCRIPCIÓN			
1.	Renovación licencias IBM Security Guardium				
1.1	Cantidad	Número de parte Licencia actual	Descripción	Cantidad	Período de actualización y soporte
		E0A2FZX	IBM Security Guardium Package (Software) per 100 Resource Units Annual SW Subscription & Support Renewal	240	Veinticuatro (24) meses a partir de la fecha en el documento “Prueba de titularidad (POE)”
1.2.	Periodo de Actualización y soporte	Veinticuatro (24) meses a partir de la fecha indicada en el documento “Prueba de titularidad (POE)”.			
		Adicionalmente el servicio debe incluir el suministro de las versiones, releases, parches o medios durante el tiempo de la vigencia de la actualización y soporte. Dicha vigencia debe estar registrada y habilitada en el sitio de Internet del fabricante a nombre de la DIAN.			
		Asistencia técnica vía telefónica, correo electrónico y/o documentación en el sitio web del fabricante durante veinticuatro (24) meses.			
1.3	Conexión	Activar la actualización y el soporte de las licencias de software en la página de soporte técnico del fabricante para lo cual se debe generar el Documento de Titularidad del proveedor de soporte y entregado al Supervisor del contrato durante el tiempo de ejecución del contrato.			

2.	Servicios Profesionales Expertise Connect plataforma Guardium				
2.1	Duración	Bolsa de hasta 420 horas a ejecutarse en los primeros 12 meses a partir de la fecha del documento "prueba de titularidad (POE)" del que trata los puntos 1.2 y 1.3			
2.2	Actividades	<p>Se ejecutarán como mínimo, las actividades preventivas, proactivas y reactivas necesarias para garantizar la operación, estabilidad y mejora continua de la plataforma IBM Guardium. Estas actividades incluyen, pero no se limitan a:</p> <p>a) Actividades Preventivas (Orientadas a evitar problemas y fortalecer la excelencia operacional)</p>			

		<ul style="list-style-type: none"> • Revisión general del estado de la plataforma y sus componentes clave, conforme a mejores prácticas del fabricante. • Evaluación periódica de salud (Health Check) y recomendaciones de mejora. • Revisión de colectores y validación del levantamiento correcto de fuentes. • Identificación de dependencias técnicas para actualizaciones y migraciones. • Recomendación de fixes y actualizaciones necesarias para reducir riesgos operativos. • <p>b) Actividades Proactivas (Orientadas a análisis, mejora continua y planificación)</p> <ul style="list-style-type: none"> • Revisión de problemas conocidos y aplicación de lecciones aprendidas según la base de conocimiento de IBM. • Identificación de oportunidades de optimización a partir de métricas operativas. • Elaboración de planes de mejora y reportes periódicos de avances. • Acompañamiento en la planificación técnica de la evolución de la plataforma Guardium. • <p>c) Actividades de Implementación y Soporte Técnico Especializado</p> <ul style="list-style-type: none"> • Actualización de la plataforma Guardium a la versión estable o recomendada por IBM. • Instalación y actualización de agentes GIM y STAP en servidores y bases de datos. • Validación de tráfico, pruebas de conectividad y aseguramiento de recolección de eventos. • Ajuste de políticas de monitoreo y configuración de casos de uso según requerimientos. • Documentación técnica asociada a cambios, actualizaciones y configuraciones realizadas. <p>d) Actividades técnicas adicionales (opcionales según priorización de la DIAN)</p> <p>El contratista podrá realizar, de manera opcional y sujeto a priorización por parte de la Oficina de Seguridad de la Información actividades técnicas especializadas orientadas a fortalecer la operación, el monitoreo y la seguridad de la plataforma IBM Guardium, entre ellas:</p> <ul style="list-style-type: none"> • Actividades de integración con componentes o servicios relacionados con bases de datos, repositorios y herramientas complementarias. • Actividades de administración avanzada de la plataforma, incluyendo mantenimiento, ajustes de configuración y optimización operativa. • Actividades de ajuste y optimización de políticas de monitoreo, reglas, grupos y perfiles de comportamiento. • Actividades de actualización, validación y mantenimiento de agentes y componentes distribuidos (GIM, STAP u otros).
--	--	--

		<ul style="list-style-type: none"> • Actividades de mejoramiento de arquitectura, revisión periódica del diseño técnico y análisis de salud de la plataforma. • Actividades de creación o ajuste de casos de uso, reglas de monitoreo, alertas y capacidades de analítica avanzada. • Actividades de integración con el SIEM institucional u otras plataformas de seguridad cuando se requiera. • Actividades orientadas a la activación y seguimiento de capacidades avanzadas, tales como analítica de amenazas, riesgo, cumplimiento y correlación a nivel de sesión. <p>La bolsa de 420 horas de servicios Expertise Connect será gestionada bajo demanda por la DIAN, priorizando actividades de:</p> <ul style="list-style-type: none"> • Acompañamiento técnico especializado, • Atención de incidentes de alta complejidad, • Optimización de configuraciones • Soporte a requerimientos de auditoría y entes de control, • Sesiones técnicas de transferencia de conocimiento. <p>El consumo de horas será controlado por la Entidad mediante actas de solicitud y validación del servicio prestado.</p> <p>Estas actividades no constituyen un listado exhaustivo y podrán ejecutarse total o parcialmente conforme las necesidades técnicas, prioridades institucionales y disponibilidad de horas.</p>
2.3	Servicios	<p>El contratista pondrá a disposición de la DIAN servicios especializados del programa Expertise Connect, orientados al soporte avanzado, acompañamiento técnico y gestión integral de incidentes en la plataforma IBM Guardium. Como mínimo, estos servicios incluyen:</p> <ul style="list-style-type: none"> • Punto único de contacto (SPOC) para coordinar requerimientos relacionados con Guardium. • Gestión de casos de soporte (PMR): análisis inicial, escalamiento, seguimiento y cierre, manteniendo al cliente informado del estado del incidente. • Liderazgo en la resolución de incidentes críticos, coordinando los recursos necesarios para su atención. • Evaluación proactiva de potenciales problemas, con recomendaciones basadas en mejores prácticas del fabricante. • Guía técnica y asesoría especializada para implementación, actualización o cambios en la arquitectura de la solución. • Acompañamiento en nuevas iniciativas, proyectos y despliegues relacionados con Guardium. • Análisis de ambientes y validación de implementación posterior a actualizaciones, cambios o nuevas configuraciones. • Información y orientación sobre implementación de fixes, nuevas versiones y roadmap de funcionalidades de IBM.
3. SUSCRIPCIÓN Y SOPORTE		

3.1	Suscripción	Subscripción a descargas de últimas versiones y release disponibles para Software IBM.												
3.2	Soporte	<p>El contratista deberá brindar soporte técnico del producto ofrecido por medio de una línea de contacto que funcione 7x24, que será el punto de contacto que tendrá la Dirección de Impuestos y Aduanas Nacionales (DIAN) a través del supervisor del contrato (funcionario de la Oficina de Seguridad de la Información), con la finalidad de que allí se realice la apertura de tickets de fallas que se presenten en el sistema.</p> <p>En caso de que se presente algún inconveniente y se requiera de soporte deberá ser por medio de un ticket para su pronta solución según la criticidad definida:</p> <table><tr><th>Severidad</th><th>Atención inicial del caso</th><th>Atención inicial</th></tr><tr><td>1 - Sistema o servicio caído</td><td>Máximo 2 horas (7X24)</td><td rowspan="4">Recepción del caso, diagnóstico inicial y asignación de contacto técnico</td></tr><tr><td>2 – Significante</td><td>Máximo 2 horas (5X8)</td></tr><tr><td>3 – El producto, servicio o funcionalidad es utilizable</td><td>Máximo 2 horas (5X8)</td></tr><tr><td>4 – Consulta</td><td>Máximo 2 horas (5X8)</td></tr></table> <p>En el servicio de atención remota se debe atender a través los medios tecnológicos dispuestos para ello, el servicio se activa ante la presencia de un incidente, se deben garantizar los servicios de diagnóstico y solución de alarmas generadas por el sistema, a través de personal capacitado, el cual debe identificar, aislar y resolver los problemas en forma remota.</p> <p>El contratista deberá proporcionar y garantizar el soporte especializado directamente por el fabricante, entregar a la supervisión los canales de contacto y la matriz de escalamiento de casos.</p>	Severidad	Atención inicial del caso	Atención inicial	1 - Sistema o servicio caído	Máximo 2 horas (7X24)	Recepción del caso, diagnóstico inicial y asignación de contacto técnico	2 – Significante	Máximo 2 horas (5X8)	3 – El producto, servicio o funcionalidad es utilizable	Máximo 2 horas (5X8)	4 – Consulta	Máximo 2 horas (5X8)
Severidad	Atención inicial del caso	Atención inicial												
1 - Sistema o servicio caído	Máximo 2 horas (7X24)	Recepción del caso, diagnóstico inicial y asignación de contacto técnico												
2 – Significante	Máximo 2 horas (5X8)													
3 – El producto, servicio o funcionalidad es utilizable	Máximo 2 horas (5X8)													
4 – Consulta	Máximo 2 horas (5X8)													
4	GENERALIDADES													
4.1	Recepción de actualizaciones.	<p>Para la recepción de las actualizaciones el contratista deberá entregar al supervisor del contrato un informe en donde especifique para cada una de las licencias lo siguiente:</p> <ul style="list-style-type: none">- Tipo de producto o plataforma (Guardium).- Fecha que se realizó la actualización.- Vigencia.- Fecha de finalización.- Captura de pantalla o reporte desde el software donde se pueda evidenciar la versión actualizada.												
4.2	Sitio de entrega de los bienes y/o servicios.	Instalaciones de la UAE - Dirección de Impuestos y Aduanas Nacionales DIAN, Carrera 8 # 6C-38 / Edificio San Agustín Bogotá D.C.												

4.3	Tiempo de entrega de los bienes y/o servicios.	La totalidad de los certificados de servicios deben ser entregados dentro de los cinco (5) días siguientes a la firma del acta de inicio.
-----	--	---



FRANCISCO ANDRÉS DAZA CARDONA
Jefe Oficina de Seguridad de la Información

Proyectó: Alvaro Antonio Sarria – Gestor 

Revisó: Javier Ricardo Alfonso Alba – Gestor 
Oscar Orlando Camargo Garzón – Gestor 