AVISO DE CONVOCATORIA PROCESO DE SELECCIÓN ABREVIADA DE MENOR CUANTÍA PB-SAMC-2024-0001

La PERSONERIA DE BOGOTÁ ubicada en la Carrera 7 No. 21- 24 se permite convocar alos interesados en participar en el proceso de selección abreviada de menor cuantía PB-SAMC-2024-0001

OBJETO: PRESTAR LOS SERVICIOS DE UN CENTRO DE OPERACIONES DE SEGURIDAD SOC PARA REALIZAR LA GESTIÓN Y EL MONITOREO DE LA SEGURIDAD INFORMÁTICA DE LAS PLATAFORMAS DE LA PERSONERÍA DE BOGOTÁ D.C., DENTRO DEL MARCO DEL PROYECTO NO. 7719

ESPECIFICACIONES TÉCNICAS MÍNIMAS: El contratista deberá desarrollar el objeto contractual de acuerdo con el Anexo Técnico que hace parte integral del presente proceso como Anexo 1, para lo cual debe contar con toda la capacidad logística, operacional y de personal requerido para adelantar la ejecución contractual, de acuerdo con las actividades allí descritas.

De igual manera, se señalan las siguientes especificaciones técnicas del servicio que se pretende adquirir:

Proveedor del servicio de SOC	
Se requiere que el CONTRATISTA brinde los servicios de Security Operation Center - SOC para la detección y contención de amenazas y ataques cibernéticos, a través de monitoreo en tiempo real, correlación de eventos, analítica de eventos, inteligencia de amenazas y apoyo para la gestión de ciber incidentes.	
EL servicio deber tener capacidad operativa 7x24 en español. El SOC se debe encontrar ubicado en el territorio nacional, con el fin de poder garantizar el cumplimiento de las obligaciones contractuales y la prestación de los servicios debe ser en idioma español.	
El contratista deberá prestar su servicio con la solución de Security Information and Event Management de Fortinet SIEM, la cual es la solución licencia por la entidad. Por lo tanto, este debe garantizar que las herramientas usadas sean compatibles con las plataformas de la entidad.	
SOC - Security Operation Center:	
El servicio contempla el monitoreo 7x24 de las plataformas de la Personería de Bogotá y de la sede electrónica pertenecientes a la entidad, además deberá poder identificar diferentes tipos de ataques que se presentan sobre los sistemas de información de la Personería de Bogotá que se encuentren expuestos en la nube y datacenter.	
El SOC deberá tener una arquitectura de seguridad adaptable para lograr combatir el delito cibernético en el panorama de amenazas actual.	
El equipo SOC debe poder: 1. **Prevenir:** Este concepto permite adoptar capacidades de identificación y mitigación temprana, para prevenir la materialización de los riesgos que puedan amenazar los activos de información críticos para la organización.	

2. **Detectar**: identificación y mitigación de riesgos que puedan ya estar presentes en el ecosistema corporativo, integrando las tecnologías de seguridad existentes en el ecosistema. 3. **Responder**: capacidades de prevención y detección, proveer "respuesta continua" y automática a incidentes para la detección y contención de amenazas. 4. **Predecir**: brindar la atención y primera respuesta de las alertas, integrando algunas de las siguientes metodologías de analítica de datos; indicadores de compromiso (IOC) o Business Intelligence (BI) o Redes Neuronales.	
Se debe poder identificar los riesgos potenciales y amenazas sobre las fuentes críticas definidas por la Entidad antes de que un ataque real se pueda presentar.	
El servicio debe tener la capacidad de extraer y procesar logs de múltiples fuentes en plataformas corporativas en nube como Azure y Oracle, a través de Scripts o APIs; las cuales, mediante llaves, paths o links realiza la conexión, identificación y extracción de logs para los sistemas configurados, con el fin de realizar monitoreo de seguridad y disponibilidad acorde con la información que pueda ser obtenida de los registros.	
Definición inicial de fuentes de logs (construcción de inventario en conjunto con la Personería), definición e integración con los centralizadores de logs para las fuentes incluidas en el servicio.	
El contratista deberá garantizar y acordar con la Entidad los medios necesarios para entregar los logs del proceso de retención a la Entidad.	
Activación de la solución y las reglas de correlación estándar de fábrica. Las actividades de activación de la solución son: 1. Definición de inventario de fuentes de logs. 2. Creación de segmento para la Personería de Bogotá. 3. Acompañamiento en instalación de agentes. 5. Creación de reglas de normalización. 6. Creación de reglas de correlación.	
El SOC deberá realizar análisis del comportamiento de la infraestructura administrada y monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación.	
El contratista deberá contar con talento humano y/o personal calificado que considere necesario, incluyendo los roles y responsabilidades del grupo de operaciones del SOC claramente definido, en lo que respecta al monitoreo, correlación, análisis y de tendencias de seguridad y atención de requerimientos, manejo y contención de incidentes de seguridad. Siempre y cuando garantice la operación del servicio 7X24.	
Se deberá brindar acompañamiento remoto o en sitio de ser necesario, con personal certificado de acuerdo con lo estipulado en los requisitos técnicos, aconsejando o guiando a los equipos de respuesta a incidentes de la Entidad	
Administración de la herramienta SIEM	
La herramienta a utilizar será administrada por un equipo especializado desde el Centro de Operaciones de Seguridad, desde el cual se realizará el procesamiento de la información, notificación y reporte de los hallazgos correspondientes a la plataforma monitoreada.	
La operación del SOC debe ser capaz de recopilar datos de registro y eventos de diferentes fuentes, incluyendo sistemas operativos, aplicaciones, bases de datos, firewalls, WAF y otros dispositivos de red, siempre y cuando el licenciamiento lo permite.	

La operación del SOC debe reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir operaciones dentro de la Personería de Bogotá. Así mismo, evidenciar anomalías en el comportamiento de los usuarios para automatizar la detección de amenazas y la respuesta a incidentes y general los alertamientos y reglas correspondientes.	
La operación del SOC debe ser capaz de integrar soluciones de seguridad adicionales a las configuradas en la actualidad, para mejorar la detección y respuesta a amenazas de seguridad siempre y cuando la licencia actual de la entidad lo permita.	
La operación del SOC debe estar en la capacidad de identificar y filtrar falsos positivos y priorizar los casos que deban ser abiertos como incidentes siempre y cuando la licencia actual de la entidad lo permita.	
Correlación de eventos	
La correlación de evento deberá incluir la definición de reglas en la herramienta a través de una revisión conjunta con el equipo de seguridad de la información e infraestructura de la Personería de Bogotá, en la que se realizará el diseño de la arquitectura del servicio acorde con la necesidad de la Entidad.	
Se deben utilizar fuentes de inteligencia externas de amenazas que contengas listas de reputación (IP) y/o dominios catalogados como sospechosos para la validación de conexiones con sitios comprometidos. Con la información recolectada se deberá entregar un informe mensual y notificación cuando ocurra alguna alerta crítica o incidencia que puede o haya afectado a la entidad, en máximo tres horas a partir de la ocurrencia del evento, que incluya como mínimo: ▪ Fecha y hora en la que se descubrió el incidente. ▪ Tipo de incidente. ▪ Prioridad en el tratamiento. ▪ IP origen. ▪ IP afectada. ▪ Detalle del incidente. ▪ Acciones ejecutadas de detención y contención de ataques. ▪ Recomendaciones de remediación.	
El contratista debe realizar un monitoreo a los análisis de tendencia de amenazas y riesgos disponibles en Internet y/o en centros de respuesta a incidentes (SIRT) que permita informar a la Entidad, las alertas, tendencias, ataques y amenazas provenientes desde el ciberespacio y que puedan afectar la infraestructura o los servicios que presta la Entidad.	
El servicio SOC deberá monitorear, correlacionar y analizar los siguientes activos de la entidad: 1. Mínimo 22 servidores incluidos Linux y Windows. 2. 1 dispositivo firewall on premise - PaloAlto. 3. 1 consola de antivirus - trellix. 4. 2 Switch core. 5. 1 WAF on premise - Fortinet 6. 1 WAF Nube - Fortinet 7. 1 Firewall nube - Fortinet 8. 1 Auditor de datos confidenciales - IBM Guardium 9. 4 Bases de Datos Oracle nube 10. 1 Bases de Datos Oracle on premise **Nota:** La Personería de Bogotá proporcionara el licenciamiento correspondiente para el monitoreo de las anteriores fuentes de información.	

Gestión y notificación de incidentes de seguridad	
El contratista debe informar de manera prioritaria e inmediata de acuerdo con la matriz de escalamiento definida y alertar sobre los cambios de seguridad, de configuración y críticos que se generen en las plataformas tecnológicas que se están monitoreando. Para esto se debe hacer una tabla de alertas, prioridad, tiempos, escalamiento.	
El contratista debe realizar seguimiento a los diferentes incidentes hasta tener un cierre confirmado.	
El contratista deberá elaborar reportes de monitoreo, cambios, alertas, tendencias, gestión, métricas, estadísticas que se entregarán de manera periódica (diario, mensual, semestral) y según requerimiento del supervisor.	
La notificación debe incluir detalles sobre el incidente, como la naturaleza del ataque, la fecha y hora en que se detectó, el impacto potencial en la red o sistemas del cliente, así como las medidas que se están tomando para mitigar el incidente.	
El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas y/o correctivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes.	
Se deberá ofrecer el servicio de profesionales especializados del SOC, de forma virtual, o presencial según la criticidad del caso, en incidentes de seguridad a través de una bolsa de 20 horas durante la vigencia del servicio, con el cual se podrá realizar un análisis sobre el resultado del monitoreo realizado y apoyar la contención de incidentes mediante el análisis de los incidentes presentados, entrega de recomendaciones de cierre y en casos que sea requerido, realizar el apoyo técnico con el cual se pueda contener definitivamente el incidente identificado.	
Los requerimientos deberán ser atendidos por un grupo interdisciplinario en Seguridad de la Información y profesionales especialistas, que cuente con las competencias, conocimiento, certificaciones y experiencia necesaria para apoyar las solicitudes generadas.	
Servicio Forense Digital	
Se deberá ofrecer el servicio de análisis forense en los casos que se requieran para determinar las TTP (Tácticas, Técnicas y Procedimientos) en posibles incidentes, desarrollar contenciones y establecer persistencia. La Entidad llevará a cabo la recolección de los artefactos forenses de acuerdo con las indicaciones, procedimientos y herramientas proporcionadas por el CONTRATISTA, quien a su vez realizará el análisis y la construcción del informe. Este servicio se solicitará en caso de ser necesario y tendrá un límite de 20 horas durante la vigencia del contrato.	

PLAZO DE EJECUCIÓN: El plazo de ejecución del contrato será **SIETE (7) MESES**, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, expedición del Registro Presupuestal, aprobación de la garantía única y suscripción del acta de inicio.

PLAZO PARA PRESENTAR OFERTA, LUGAR Y FORMA DE PRESENTACIÓN DE ESTA. El plazo para presentar oferta será el indicado en el cronograma del proceso, el cualse encuentra en la plataforma transaccional SECOP II y en el acto de apertura de este. Sedeberá presentar digitalmente por medio de la plataforma SECOP II.

VALOR ESTIMADO DEL CONTRATO Y PRESUPUESTO OFICIAL: El valor del presupuesto oficial CUATROSCIENTOS NOVENTA Y SEIS MILLONES CUATROSCIENTOS VEINTIOCHO MIL TRECIENTOS TREINTA Y TRES PESOS M/CTE ($496.428.333,00), incluido IVA e impuestos y retenciones aplicables, amparados con el certificado de disponibilidad presupuestal No. 66 del 03 de enero de 2024, rubro presupuestal O23011605560000007719, Fortalecimiento institucional de la

Personería de Bogotá, expedido la Gerencia Financiera.

INDICACIÓN DE TRATADOS INTERNACIONALES QUE APLICAN A LA CONTRATACIÓN: En cumplimiento de lo dispuesto en el numeral 10 artículo 2.2.1.1.2.1.3 del Decreto 1082 de 2015; y en atención al Memorando Explicativo de los capítulos de contratación pública de los acuerdos comerciales negociados por Colombia para Entidades contratantes expedido por el Departamento Nacional de Planeación

Indique si el proceso está cobijado por Acuerdos Comerciales		Entidad. Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
		SI/NO	SI/NO	SI/NO	SI/NO
Alianza Pacífico	Chile	No	No	N/A	No
	México	No	No	N/A	No
	Perú	No	No	N/A	No
Canadá		No	No	N/A	No
Chile		Si	No	No	SI
Corea		No	No	N/A	No
Costa Rica		No	No	N/A	No
Estados Unidos		No	No	N/A	No
Estados AELC		No	No	N/A	No
México		No	No	N/A	No
Triángulo Norte	El Salvador	Si	No	No	Si
	Guatemala	Si	No	No	Si
	Honduras	No	No	Si	No
Unión Europea		Si	No	Si	No
Comunidad Andina		Si	N/a	NO	SI

Motivo por el cual la Personería de Bogotá le da a los bienes y servicios de los Estados con quienes Colombia ha suscrito el acuerdo comercial el mismo trato que a los servicios colombianos, de acuerdo con lo previsto en el Artículo 2.2.1.2.4.1.3., del Decreto 1082 de 2015.

CONVOCATORIA SUSCEPTIBLE A LIMITACION MIPYMES:

El presente proceso de selección es susceptible de limitarse a MIPYME de conformidad con el artículo 5 del decreto1860 de 2021 que modificó y adicionó el artículo 2.2.1.2.4.2.2. del Decreto 1082 de 2015 y reglamentó el artículo 34 de la Ley 2069 de 2020.

En este sentido, la convocatoria del presente proceso se limitará a las Mipyme colombianas con mínimo un (1) añode existencia, cuando concurran los siguientes requisitos:

1. El valor del Proceso de Contratación sea menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), liquidados con la tasa de cambio que para el efecto determina cada dos años el Ministerio de Comercio, Industria y Turismo.

2. Se hayan recibido solicitudes de por lo menos dos (2) Mipyme colombianas para limitar la convocatoria a Mipyme colombianas. Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben recibirestas solicitudes por lo menos un (1) día hábil antes de la expedición del acto administrativo de apertura, o el que haga sus veces de acuerdo con la normativa aplicable a

cada Proceso de Contratación.

Tratándose de personas jurídicas, las solicitudes solo las podrán realizar Mipyme, cuyo objeto social les permita ejecutar el contrato relacionado con el proceso contractual.

NOTA. Las cooperativas y demás entidades de economía solidaria, siempre que tengan la calidad de Mipyme, podrán solicitar y participar en las convocatorias limitadas en las mismas condiciones dispuestas anteriormente.

Para efectos de la limitación los proponentes atenderán a lo establecido en el articulo 2.2.1.2.4.2.4 del Decreto 1082de 2015, modificado por el articulo 5 del Decreto 1081 de 2021**.**

PROCEDENCIA DE PRECALIFICACIÓN: Para el presente proceso no hay lugar a precalificación.

REQUISITOS PARA PARTICIPAR EN LA PRESENTE SELECCIÓN

Podrán participar en el presente proceso de contratación, todas las empresas que produzcan, comercialicen o distribuyan licencias antivirus; legalmente constituidas, nacionales o extranjeras, en forma individual o en Consorcio o en Unión Temporal, que dentro de su objeto social puedan desarrollar las actividades que la Personería de Bogotá,D.C., requiere contratar y que cumplan con los siguientes requisitos:

- Tener capacidad legal para contratar conforme a las normas legales. Las personasjurídicas (nacionales y extranjeras) deberán acreditar que su duración no es inferioral término de ejecución y liquidación del contrato, y un (1) año más, contado a partirde la fecha de cierre del proceso de selección. En el caso de Consorcio o Unión Temporal, todos sus integrantes deberán cumplir con este requisito.
- No encontrarse incurso en causal alguna de inhabilidad e incompatibilidad para contratar, previstas en la Constitución Política, los artículos 8° y 9° de la Ley 80 de 1993, el artículo 18 de la Ley 1150 de 2007, Ley 1296 de 2009 y las consagradas en la Ley 1474 de 2011, Decreto 1082 de 2015 y demás normas pertinentes, ni encontrarse en conflicto de intereses con la Personería de Bogotá, D.C. Dicha situación se entenderá declarada por el proponente bajo juramento con la firma de la propuesta o del contrato, según el caso.
- Estar debidamente inscrito, clasificado y calificado en el Registro Único de Proponentes de la Cámara de Comercio.
- Las calidades y demás requisitos exigidos a los proponentes en el pliego de condiciones deberán acreditarse mediante los documentos expedidos por la entidady/o autoridad que fuere competente conforme a la Ley colombiana y a lo previsto enel documento antes mencionado.

CRONOGRAMA DEL PROCESO DE SELECCIÓN ABREVIADA DE MENOR CUANTÍA

El presente proceso de contratación se adelantará con arreglo al cronograma previsto a través del Portal Único de Contratación www.colombiacompra.gov.co en el **Sistema Electrónico para la Contratación Pública (SECOP II)**. Teniendo en cuenta los siguienteshitos del proceso:

ETAPA	FECHA	DESCRIPCIÓN
Publicación Aviso de Convocatoria Publica	**22 DE FEBRERO 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II

Publicación Estudios y Documentos Previos **Publicación Proyecto de Pliego de condiciones**	**22 DE FEBRERO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Plazo para presentar observaciones al proyecto de pliego de condiciones **HASTA LAS 17:00 HORAS**	**HASTA EL 29 DE FEBRERO DE 2024**	plataforma del SECOP II
Manifestación para limitar Mipyme	**HASTA EL 01 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Respuesta a observaciones y sugerencias al proyecto de pliego de condiciones	**04 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Fecha prevista de publicación del pliego de condiciones Definitivo	**04 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Publicación Acto administrativo de Apertura del proceso de Selección	**04 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Manifestación de interés	**HASTA EL 07 MARZO DE 2024 A LAS 17:00 HORAS**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Presentación de Observaciones al pliego de condiciones definitivo **HASTA LAS 17:00 HORAS**	**HASTA 08 MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II.
Respuesta a las Observaciones al pliego de condiciones **HASTA 19:00 HORAS**	**11 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Plazo Máximo para expedir Adendas **HASTA LAS 19:00 HORAS**	**11 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Presentación de Ofertas –Cierre del proceso 10:00 HORAS	**13 DE MARZO DE 2024**	Podrán ser presentadas en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Apertura de Sobre de requisitos habilitantes y técnicos. **10:02 HORAS**	**13 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Informe de Presentación de Ofertas **10:05 HORAS**	**13 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II
Publicación del Informe de verificación o evaluación de las Ofertas de las Ofertas lista preliminar de habilitantes **19:00 HORAS**	**15 DE MARZO DE 2024**	. Podrán ser consultados en la Página Web www.colombiacompra.gov.co plataforma del SECOP II

Presentación de Observaciones y/o subsanaciones al informe de verificación o evaluación 17:00 HORAS	**HASTA 20 DE MARZO DE 2024**	www.colombiacompra.gov.co SECOP II
Publicación de las respuestas al Informe de verificación o evaluación y publicación de la lista definitiva de habilitantes. 19:00 HORAS	**21 DE MARZO DE 2024**	www.colombiacompra.gov.co SECOP II
Publicación Acto Administrativo de Adjudicación o de Declaratoria de Desierto 19:00 HORAS	**22 DE MARZO DE 2024**	www.colombiacompra.gov.co plataforma del SECOP II
Firma del contrato	**26 DE MARZO DE 2024**	en la plataforma del SECOP II
Entrega de la Garantía Única de Cumplimiento	**27 DE MARZO DE 2024**	www.contratos.gov.cowww.colombiacompra.gov.co o www.contratos.gov.co SECOP II
Aprobación de Póliza e inicio de Ejecución del Contrato	**27 DE MARZO DE 2024**	Podrán ser consultados en la Página Web www.colombiacompra.gov.co

LUGAR DE CONSULTA Y ATENCIÓN A LOS INTERESADOS

Los interesados en participar en el proceso pueden consultar el pliego de condiciones y losestudios y documentos previos en el portal único de contratación www.colombiacompra.gov.co – SECOP II y en las oficinas de la Subdirección de Gestión Contractual, ubicada en la carrera 7ª No. 21-24 Piso 3º en Bogotá D.C, entre las 8:00 a.m.y las 5:00 p.m. de lunes a viernes

Las observaciones y solicitudes de aclaración deberán ser presentadas a través de la plataforma electrónica SECOP II

Dado en Bogotá D.C., a 22 días de febrero de 2024.

HÉCTOR HERNÁN GONZÁLEZ NARANJO
Director Administrativo y Financiero

Elaboró: Daianys PAlacios – Subdirección de Gestión Contractual
Revisó: Ilba Milady Vergas G. – Subdirección de Gestión Contractual