AVISO DE CONTRATACIÓN PÚBLICA PREVISTA

El Banco Central del Ecuador, en cumplimiento de lo dispuesto en:

- El "Acuerdo Comercial entre la Unión Europea y sus Estados Miembros por una parte y Colombia, el Perú y Ecuador, por otra"
- El "Acuerdo Comercial entre el Reino Unido de Gran Bretaña e Irlanda del Norte, por una parte y de la República de Colombia, la República del Ecuador y la República de Perú, por otra"
- El "Acuerdo de Complementación Económica N° 75 entre la República de Chile y la República del Ecuador";

Se procedió a realizar la verificación correspondiente y se determinó que, el proceso para la contratación signado con el código SIE-BCE-2025-034, cuyo objeto de contratación es **"CONTRATACIÓN DE SUSCRIPCIÓN DE HERRAMIENTA DE SOFTWARE PARA LA GESTIÓN DE VULNERABILIDADES"**, se encuentra cubierto por los Acuerdos antes citados; por lo que, se genera el siguiente aviso de contratación pública prevista:

DATOS DE LA ENTIDAD CONTRATANTE:

NOMBRE DE LA ENTIDAD CONTRATANTE:	Banco Central del Ecuador
RUC:	1760002600001
DIRECCIÓN:	Provincia: Pichicha Ciudad: Quito Dirección: Av. 10 de Agosto N11-409 y Briceño Código Postal: 170409
CONTACTO INSTITUCIONAL: (información necesaria para ponerse en contacto y obtener toda la documentación pertinente relativa a la contratación)	Nombres: Carolina Alulema Correo electrónico institucional: aalulema@bce.ec
COSTO POR EDICIÓN Y CONDICIONES DE PAGO:	USD 0,00

INFORMACIÓN DE LA CONTRATACIÓN:

<table>
<tr><td>OBJETO DE LA CONTRATACIÓN:</td><td>“CONTRATACIÓN DE SUSCRIPCIÓN DE HERRAMIENTA DE SOFTWARE PARA LA GESTIÓN DE VULNERABILIDADES”</td></tr>
<tr><td>CÓDIGO DEL PROCEDIMIENTO:</td><td>SIE-BCE-2025-034</td></tr>
<tr><td>CÓDIGO CPC NIVEL 5:</td><td>73310</td></tr>
<tr><td>CÓDIGO CPC NIVEL 9:</td><td>733100</td></tr>
<tr><td>TIPO DE PROCEDIMIENTO DE CONTRATACIÓN:</td><td>SUBASTA INVERSA ELECTRÓNICA.</td></tr>
<tr><td>TIPO DE COMPRA:</td><td>Servicio</td></tr>
<tr><td>COMPRENDE NEGOCIACIÓN</td><td>Si</td></tr>
<tr><td>PRESUPUESTO REFERENCIAL:</td><td>USD 344.999,97 (TRESCIENTOS CUARENTA Y CUATRO MIL NOVECIENTOS NOVENTA Y NUEVE CON 97/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA) sin incluir impuestos.</td></tr>
<tr><td>PLAZO DE EJECUCIÓN:</td><td>El plazo de ejecución del contrato es de 1145 días calendario, distribuidos de la siguiente manera:
50 días calendario contados a partir del siguiente día de la fecha de suscripción del contrato, para la entrega de la implementación del agente en 100 activos de la infraestructura de TIC del BCE y el certificado de activación de las licencias de la herramienta de software para la gestión de vulnerabilidades con el fabricante, previa suscripción del acta entrega-recepción parcial.
1095 días contados a partir del siguiente día de la fecha de suscripción del acta entrega-recepción parcial de la entrega de la implementación del agente en 100 activos de la infraestructura de TIC del BCE y el certificado de activación de las licencias de la herramienta de software para la gestión de vulnerabilidades con el fabricante, donde se dispondrá del servicio de soporte técnico local y mantenimiento de la Contratación de Suscripción de Herramienta de Software para la Gestión de Vulnerabilidades.</td></tr>
<tr><td>CANTIDAD DE LA MERCANCÍA O SERVICIO OBJETO DE CONTRATACIÓN:</td><td>
<table>
<tr><th>Características, Requisitos Funcionales o Tecnológicos</th><th>Código CPC</th><th>Cantidad</th></tr>
<tr><td>Plataforma para Gestión de Vulnerabilidades para 2000 activos por 3 años</td><td>733100011</td><td>1</td></tr>
<tr><td>Plataforma para Remediación Automática de Vulnerabilidades para 1200 activos por 3 años</td><td>733100011</td><td>1</td></tr>
<tr><td>Compliance de CIS Control para 1200 activos por 3 años</td><td>733100011</td><td>1</td></tr>
<tr><td>Soporte Técnico Local por 3 años</td><td>733100011</td><td>1</td></tr>
<tr><td>Mantenimiento Preventivo por 3 años</td><td>733100011</td><td>1</td></tr>
</table>
</td></tr>
</table>

CARACTERÍSTICAS DEL SERVICIO	CANTIDAD
Licencias para Gestión de Vulnerabilidades en activos por tres años	2000
Licencias para la Remediación Automática de Vulnerabilidades en activos por tres años	1200
Licencias para Compliance de CIS control por tres años	1200
La solución de Gestión y Remediación de Vulnerabilidades, así como el Compliance de CIS Control pueden estar centralizadas en una misma plataforma simplificando la gestión, o pueden ser distintas plataformas siempre y cuando se integren de manera nativa	1
La solución de Gestión y Remediación de Vulnerabilidades puede ser entregada como un servicio Software-as-a-Service (SaaS) en una nube propietaria del fabricante y/o proveedor para todos sus servicios y aplicaciones requeridas en este documento o como una solución on-premise.	1
Deberá colectar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y/o agentes.	1
El oferente deberá ofrecer constante mantenimiento y actualización a la plataforma durante todo el periodo de tiempo que dure el contrato del servicio.	1
Las actualizaciones del servicio deben ser transparentes para el administrador de la solución, sin afectar ninguno de los datos almacenados o servicios suministrados.	1
La plataforma que brinde los servicios debe contar con al menos una de las siguientes certificaciones: • SOC 2 • FedRamp Moderate • Privacy Shield Framework • CloudStar • PCI ASV • ISO/IEC 27001: 2013 • ISO/IEC 27017: 2015 • ISO/IEC 27018: 2019 • GDPR	1
La solución debe permitir descubrir, evaluar y priorizar vulnerabilidades/configuraciones en toda la infraestructura de la red, incluyendo estaciones de trabajo, servidores, dispositivos de red, telecomunicaciones y seguridad, hipervisores, máquinas virtuales. y nubes (Azure, GCP, AWS).	1
La solución se debe licenciar por IP o HOST y debe proveer capacidades de descubrimiento e inventario con acceso a agentes, escáneres, sensores para contenedores, sensores de descubrimiento pasivo.	1
La solución para la gestión de vulnerabilidades debe ofrecer soporte para su despliegue en al menos los siguientes sistemas operativos: Windows 10/11, Windows Server 2003/2008/2012/2016/2019/2022 and later	1

		(x86, x64), Red Hat Enterprise Linux 5.x,6.x 7.x, 8.x, 9.x, Solaris 10.x, Solaris 11.x	
		La solución debe detectar y analizar vulnerabilidades en las principales versiones de Bases de Datos, al menos: Microsoft SQL Server, MySQL, Oracle, Sybase, PostgreSQL.	1
		Toda comunicación entre componentes, transferencia y sincronización de datos de la solución debe estar cifrada de extremo a extremo, haciendo uso como mínimo de TLS 1.2, certificados firmados con RSA 2048 bits y algoritmo de firma SHA256 con el fin de garantizar la seguridad de la información del BCE.	1
		La solución para la remediación automática de vulnerabilidades, debe ofrecer soporte para su despliegue en al menos los siguientes sistemas operativos: Windows 10/11, Windows Server /2016/2019/2022 and later (x86, x64)	1
		Deberá ser capaz de integrarse con soluciones SIEM y SOAR a través de APIs estándar o conectores predefinidos, como: Splunk, IBM QRadar, Microsoft Sensitel, LogRhythm, Siemplify, Simlane, entre otros, para centralizar y correlacionar eventos de seguridad.	1
		La solución deberá soportar la integración con sistemas de ticketing “BMC Remedy, entre otros”.	1
		La solución debe permitir la distribución eficiente de parches a gran escala minimizando el impacto en la red y en los sistemas.	1
		La solución debe contar con la capacidad de ejecutar escaneos automáticos en los sistemas para identificar parches faltantes.	1
		La solución debe permitir la programación y automatización de la aplicación de parches durante ventanas de mantenimiento configurables.	1
		La solución debe recopilar información sobre el inventario de activos.	1
		La solución debe monitorear y reportar cambios en la configuración de los sistemas, asegurando que estos se mantengan dentro de las políticas de seguridad.	1
		La solución debe permitir la implementación de los agentes a través de la GPO o por línea de comandos.	1
		La solución deberá proporcionar administración vía interfaz gráfica WEB utilizando HTTPS.	1
		La solución debe permitir definir diferentes perfiles y roles de usuarios para la administración.	1
		La solución debe proporcionar controles jerárquicos de acceso de usuarios basados en roles que permitan la delegación de responsabilidades para reflejar la estructura organizacional.	1
		Debe presentar la clasificación de riesgo y priorizar las vulnerabilidades a corregir en	1

orden de criticidad no solo desde CVE, sino también en relación al contexto de desempeño y la situación del entorno.	
La solución debe permitir exportar informes al menos a dos de los formatos HTML, MHT, PDF, DOC, CSV o XML.	1
La solución debe permitir generar informes al menos de: resumen ejecutivo, informe técnico, informe de remediación.	1
La solución deberá presentar paneles de control predefinidos y personalizables que contengan datos estadísticos, gráficos de tendencias, información relevante mediante filtros, índices de riesgos, resultados en tiempo real de las vulnerabilidades existentes	1
El agente debe poder parchearse el mismo	1
La remediación en los activos que no se puedan automatizar, deberá ser gestionada y reportada para remediar de manera manual como actividad correctiva	1
La plataforma debe incluir capacidades para auditoría de cumplimiento basadas en benchmarks CIS.	1

SOPORTE TECNICO LOCAL

- El soporte técnico local del oferente deberá estar disponible 24 horas al día, todos los días del año (24x7x365) durante el período que dure el servicio contratado, sin límite de horas técnico invertidos en la solución del problema
- El soporte técnico local deberá ser realizado por personal técnico especializado en la plataforma en sitio o remoto, previa coordinación con el Banco Central del Ecuador.
- El oferente deberá dar asistencia técnica para la revisión, monitoreo y afinamiento de los elementos de la solución cuando el personal de la institución reporte la existencia de incidentes de seguridad informática o de problemas de seguridad informática asociados a la solución o cualquiera de sus componentes o a servicios tecnológicos que dependan del mismo.
- Como productos entregables de los servicios de soporte técnico local, la empresa oferente debe entregar al Banco Central del Ecuador la siguiente documentación:
  - Ordenes de trabajos debidamente firmadas, las misma que deben incluir el nombre de la persona que realiza el requerimiento, el nombre del técnico asignado, la fecha del requerimiento, la descripción del problema.
  - Reporte anual de las órdenes de trabajo realizadas.
  - Informe técnico del soporte técnico realizado con el detalle del trabajo realizado.
- El tiempo de respuesta para el servicio de soporte técnico local y el tiempo de solución deberá ajustarse al SLA determinado por el Banco Central del Ecuador y descrito en el numeral 10.2 de este documento.
- Las penalidades aplicarán al incumplimiento del Acuerdo de Nivel de Servicio – SLA y corresponde al soporte técnico local en períodos anuales, mismas que serán calculadas en base al porcentaje establecido y descritas en el numeral 16.2 de este documento.

	- El servicio de actualización de versiones y parches deberá realizarse de acuerdo a las normas y recomendaciones emitidas por el fabricante
	- El oferente deberá prestar el servicio remotamente o en sitio, el Banco Central del Ecuador definirá la modalidad del soporte.
	- Como producto entregable, la empresa oferente deberá entregar al BCE un informe técnico con el detalle del trabajo realizado en el servicio de soporte técnico local.
	
	MANTENIMIENTO PREVENTIVO
	
	- El mantenimiento preventivo de software se lo realizará anualmente, de acuerdo al cronograma que se elaborará de mutuo acuerdo con el Administrador del Contrato posterior a la suscripción del contrato.
	- El servicio de mantenimiento preventivo deberá ser provisto por el oferente conforme las normas y recomendaciones emitidas por el fabricante, de manera remota o en sitio en las instalaciones de Quito y Guayaquil de acuerdo a la definición dada por el Banco Central del Ecuador, sin límite de horas de técnico invertidos.
	- Las actividades mínimas a realizarse como parte del servicio de mantenimiento preventivo de hardware o software son:
	  - Respaldo de configuraciones,
	  - Revisión de logs de funcionamiento,
	  - Revisión de versiones de software,
	  - Ajustes y calibración de los sistemas, entre otros.
	- Como productos entregables para validar el cumplimiento de las actividades de mantenimiento preventivo de software, la empresa oferente deberá entregar al BCE la siguiente documentación:
	  - Ordenes de trabajo debidamente firmadas, las mismas que deben incluir el nombre de la persona que realiza el requerimiento, el nombre del técnico asignado, la fecha del mantenimiento, el proceso del mantenimiento a seguir.
	  - Informe técnico del mantenimiento preventivo realizado con el detalle del trabajo realizado en el mantenimiento.

CONDICIONES DE PAGO:	El valor del contrato se pagará de la siguiente manera: • 91% del valor total del contrato, previa la entrega del informe de implementación del agente en 100 activos de la infraestructura de TIC del BCE, la entrega del certificado de activación de las licencias de la herramienta de software para la gestión de vulnerabilidades con el fabricante, suscripción del acta entrega-recepción parcial, informe favorable del Administrador del contrato y presentación de la factura correspondiente; y, • 9% del valor total del contrato, por el servicio de soporte técnico local y mantenimiento, se realizará mediante 3 pagos vencidos anuales, previo informe de los casos de atención del soporte técnico efectuado,

	informe del mantenimiento preventivo, informe favorable del Administrador del contrato, y presentación de la factura correspondiente.
IDIOMA O IDIOMAS EN QUE PODRÁN PRESENTARSE LAS OFERTAS O LAS SOLICITUDES DE PARTICIPACIÓN	Español
FECHA LÍMITE PARA LA PRESENTACIÓN DE SOLICITUDES DE PARTICIPACIÓN:	Según cronograma del proceso que se publicará en el portal institucional del SERCOP.
DIRECCIÓN PARA LA PRESENTACIÓN DE SOLICITUDES DE PARTICIPACIÓN:	La oferta se deberá presentar a través del Portal CONTRATACIÓN PÚBLICA hasta la fecha y hora indicadas en el cronograma
FECHA DE LA PRESENTACIÓN DE LAS OFERTAS:	Según cronograma del proceso que se publicará en el portal institucional del SERCOP
DIRECCIÓN PARA LA PRESENTACIÓN DE OFERTAS	La oferta se deberá presentar a través del Portal CONTRATACIÓN PÚBLICA hasta la fecha y hora indicadas en el cronograma
IDIOMA PARA LA PRESENTACIÓN DE OFERTAS	Español
CONDICIONES PARA LA PARTICIPACIÓN DE PROVEEDORES	Los requisitos están incluidos en el pliego de condiciones que se pone a disposición de todos los proveedores interesados al mismo tiempo que se hace el aviso de la contratación prevista.

Dado en Quito, en la fecha constante en la firma del delegado de la Máxima Autoridad

Firmado electrónicamente por:
PAULO CRISTOBAL BERMEO MANCERO
Validar únicamente con FirmaEC

Mgs. Paulo Cristóbal Bermeo Mancero
GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN
BANCO CENTRAL DEL ECUADOR

DESCRIPCIÓN	NOMBRE	CARGO	FIRMA
Revisado por:	Octavio Fernando Albuja Romero	Subgerente de Aseguramiento Tecnológico	Firmado electrónicamente por: OCTAVIO FERNANDO ALBUJA ROMERO Validar únicamente con FirmaEC
	Amparo Carolina Alulema Ortiz	Responsable de la Gestión Interna de Compras Públicas	Firmado electrónicamente por: AMPARO CAROLINA ALULEMA ORTIZ Validar únicamente con FirmaEC
Elaborado por:	Lenin Ricardo Bravo Rey Experto de Aseguramiento de la Calidad y Seguridad Informática / Zonal	Experto de Seguridad Informática	Firmado electrónicamente por: LENIN RICARDO BRAVO REY Validar únicamente con FirmaEC