BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0194-2020-GTI240-N

ASUNTO: INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE – HERRAMIENTA DE ANALISIS ESTÁTICO DE CODIGO FUENTE

---

1. **NOMBRE DEL ÁREA:**
   Subgerencia de Servicios de Tecnologías de Información

2. **RESPONSABLE DE LA EVALUACIÓN:**
   Miguel Tejada Malaspina
   Patricia López Concha
   Gabriela Miranda Córdova
   Julio Rivera Zárate

3. **CARGOS:**
   Subgerente de Servicios de Tecnologías de Información
   Jefe Departamento de Gestión y Calidad
   Especialista en Gestión y Calidad
   Especialista en Gestión y Calidad

4. **FECHA:**
   2020-09-24

5. **JUSTIFICACIÓN:**

   Para reforzar el proceso de desarrollo de software en una etapa temprana, lo que permitirá tomar acciones preventivas y correctivas a tiempo, se considera necesaria la adquisición de la suscripción anual de 1 licencia para el uso de una herramienta de análisis estático de código fuente, la cual es de tipo SAST (Static Application Security Testing). Esta herramienta permitirá revisar el código fuente de las aplicaciones que se desarrollan en la Gerencia de Tecnología de Información y del Fondo de Empleados del Banco, a través de una inspección continua. De esta manera, se tendrá un código fuente limpio, estandarizado, fácil de mantener en el tiempo, así como detectar vulnerabilidades en una etapa temprana para su corrección.

   Gerencia de Tecnología de la Información:
   Departamento de Gestión y Desarrollo de Soluciones de Tecnologías de Información

   Dado que se ha definido la necesidad de reforzar el proceso de desarrollo de software en una etapa temprana, la herramienta de análisis estático de código fuente permitirá a los desarrolladores cumplir con los siguientes objetivos:

   - Cumplimiento de estándares de programación.
   - Encontrar y corregir código incorrecto o que no cumpla con el comportamiento deseado.
   - Detectar y corregir código difícil de ser mantenido en el tiempo.
   - Encontrar y rastrear las inseguridades en el código fuente, como inyección SQL, contraseñas codificadas y errores mal administrados para su corrección.

- Detectar y corregir fragmentos de código sospecho que deben revisar y clasificar, esto permite que se familiaricen con prácticas de codificación segura.
- Revision de información relacionados a la vulnerabilidad, dado que este tipo de herramienta proporciona descripciones detalladas de problemas y aspectos destacados del código que explican por qué dicho código está en riesgo. Además, sugiere que se sigan instrucciones, se verifique una solución y se asegure su aplicación.
- Corregir errores del código fuente en la etapa de desarrollo. Por lo tanto, reduce el tiempo de revisión en el proceso de control de calidad y evita el retrabajo en caso dicho código tuviera que ser devuelto al ambiente de desarrollo para su corrección.

Por lo indicado, es necesario que este departamento cuente con acceso para el uso de la herramienta de análisis estático de código fuente.

Departamento de Gestión y Calidad
Dado que una de las funciones del departamento de Gestión y Calidad es certificar la calidad del código fuente de las aplicaciones que se desarrollan en la Gerencia de Tecnología de Información y del Fondo de Empleados del Banco, es necesario que cuente con una herramienta de análisis estático de código fuente que le permita hacer las revisiones necesarias para validar la calidad del código fuente. En tal sentido, dicha herramienta proporciona la información necesaria para tener la capacidad de saber en cada análisis de código fuente si una aplicación está lista para pasar a producción "en términos de calidad".

Por lo indicado, es necesario que este departamento cuente con el acceso para el uso de dicha herramienta.

Departamento de Redes, Telecomunicaciones y Base de Datos
Dado que una de las funciones de este Dpto., es garantizar la eliminación de riesgos de vulnerabilidad que pueden ser introducidos en el código fuente de las aplicaciones desarrolladas en el Banco, es necesario que cuenten con una herramienta de análisis estático de código fuente que sirva de apoyo para dicho fin.

Los especialistas en seguridad serán los administradores de la herramienta de análisis estático de código fuente. Por lo tanto, se encargarán de lo siguiente:

- Creación de usuarios y contraseñas.
- Creación y asignación de perfiles de usuario para el ambiente de Desarrollo y Calidad; y configurar los accesos.
- Configurar las reglas de validación para cada lenguaje de programación, que certifiquen que el código fuente esté limpio de vulnerabilidades y asignar de acuerdo al perfil de cada usuario.

Por lo indicado, es necesario que este departamento cuente con acceso para el uso de dicha herramienta.

Fondo para Enfermedades, Seguros y Pensiones del BCRP (FE)
Con el objetivo de reforzar el proceso de desarrollo de software en una etapa temprana, es necesario que los desarrolladores del Fondo de Empleados cuenten con una herramienta de análisis estático de código fuente que también les permita cumplir con los objetivos determinados:

- Cumplimiento de estándares de programación.
- Encontrar y corregir código incorrecto o que no cumpla con el comportamiento deseado.
- Detectar y corregir código difícil de ser mantenido en el tiempo.
- Encontrar y rastrear las inseguridades en el código fuente, como inyección SQL, contraseñas codificadas y errores mal administrados para su corrección
- Detectar y corregir fragmentos de código sospecho que deben revisar y clasificar, esto permite que se familiaricen con prácticas de codificación segura.
- Revisión de información relacionados a la vulnerabilidad, dado que este tipo de herramienta proporciona descripciones detalladas de problemas y aspectos destacados del código que explican por qué dicho código está en riesgo. Además, sugiere que se sigan instrucciones, se verifique una solución y se asegure su aplicación.
- Corregir errores del código fuente en la etapa de desarrollo. Por lo tanto, reduce el tiempo de revisión en el proceso de control de calidad y evita el retrabajo que se ocasionaría en caso dicho código tuviera que ser devuelto al ambiente de desarrollo para su corrección.

Por consiguiente, es necesario que cuenten con el acceso para el uso de dicha herramienta.

6. ALTERNATIVAS:

Actualmente existe en el mercado herramientas para el análisis estático de código fuente que se considera conveniente evaluar Se ha tomado en cuenta las siguientes:

SonarQube Developer Edition
Fortify Static Code Analizer

7. ANÁLISIS COMPARATIVO TÉCNICO:

Para realizar el análisis comparativo se ha definido factores técnicos de evaluación, los cuales representan a los criterios mínimos que la herramienta de software debe cumplir.

	SonarQube Developer Edition	**Fortify Static Code Analizer**
Lenguajes Soportados	Java, JavaScript, C#, TypeScript, Kotlin, Ruby, Go, Scala, Flex, Python, PHP, HTML, CSS, XML, VB.NET, C, C++, Objetive-C, PL/SQL, ABAP, TSQL y Swift	ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic, ASP (with VBScript), COBOL, ColdFusion CFML, Go, HTML, Java (including Android), JavaScript/ AJAX, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Swift, T-SQL, VB.NET, VBScript, Visual Basic y XML
Detección de vulnerabilidades	Sí incluye	Sí incluye

	SonarQube Developer Edition	Fortify Static Code Analizer
Integración con IDE para análisis en tiempo real	Sí Incluye	Sí Incluye
Soporte Fábrica	Sí incluye	Sí Incluye
Soporte local – Proveedor	Sí incluye	Sí Incluye
Licencia	Una licencia, acceso para "n" usuarios. Revisión de 2 Millones de líneas de código fuente (LOC)	Licencia para 10 usuarios. Revisón ilimitada de líneas de código fuente
Tipo de Licencia	Suscripción anual	Suscripción anual
Precio referencial por 1año	$12 272,00 con IGV (Incluye soporte)	$ 34 118,72 con IGV (incluye soporte)

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Costos:

Se muestra un cuadro comparativo del precio de dos productos evaluados:

	Licencia por suscripción anual	Revisión de código fuente	Costo aprox. año 1 (USD)	Costo aprox. año 2 (USD)
SonarQube Developer Edition	1 licencia ("n" usuarios)	2 Millones de líneas de código (LOC)	12,272.00	11,044.80
Fortify Static Code Analizer	10 licencias (10 usuarios)	Sin límite de líneas de código	34,118.72	30,706.85

Costos asociados al producto:

- Suscripción de licencia y Soporte técnico
  - Suscripción de 1 licencia para el uso de una herramienta de análisis estático de código fuente, por el periodo de 1 año, la misma que permitirá la revisión de 2 Millones de líneas de código fuente.
  - El precio referencial de la suscrición de licencia anual y el soporte técnico es de USD 12 272,00 incluidos impuestos.

El soporte técnico deberá incluir lo siguiente:

- Se brindará el soporte técnico orientado a asegurar la continuidad operativa de la herramienta a través de la atención de consultas y requerimientos de mantenimiento correctivo y evolutivo.

- El soporte técnico deberá ser brindado por el contratista de lunes a viernes, en el horario de 09.00 a 17.00 horas, vía teléfono o correo electrónico o en forma presencial (previa coordinación).
- El tiempo de respuesta a una solicitud de soporte técnico, no deberá ser mayor de cuatro (4) horas, vía teléfono o correo electrónico o internet. En caso presencial, no deberá ser mayor a 24 horas.
- El soporte técnico incluirá la instalación y configuración de las licencias al inicio de la contratación.
- El mantenimiento de la licencia debe incluir: actualización de versiones, parches (fixes) y service packs.

- Hardware necesario para su funcionamiento
  La licencia por suscripción de la herramienta de análisis estático de código fuente será integrado a la plataforma informática con la que cuenta el Banco Central de Reserva del Perú.

- Tiempo en que se va a entregar la suscripción con las condiciones exigidas por el Banco Central de Reserva del Perú
  El plazo de entrega será no mayor de 20 días calendario, contados a partir del día siguiente de la firma del contrato.

Beneficios:

- Reducir el tiempo de revisión del código fuente en el proceso de control de calidad debido a que dicho código fuente será analizado de manera automatizada durante el proceso de desarrollo, permitiendo al programador detectar errores y vulnerabilidades para su corrección oportuna
- Evita el tiempo de retrabajo de los programadores porque la revisión oportuna disminuye la posibilidad de que el código fuente sea devuelto al ambiente de desarrollo para su corrección.
- Con el uso de esta herramienta se podrá hacer un análisis automatizado del código fuente de los scripts de base de datos, lo que permitirá optimizar dicho código fuente y por ende optimizar el tiempo de respuesta en la obtención del resultado de la ejecución de los mencionados scripts de base datos.
- Revisar una cantidad definida de líneas de código fuente al año. Se ha realizado un cálculo aproximado de las líneas de código que han sido modificadas o creadas en el Banco en los dos últimos años y se ha determinado que son aproximadamente 2 millones de líneas de código fuente (2M).

9. CONCLUSIONES:

Por los motivos antes señalados, se concluye que la suscripción de 1 licencia para el uso de una herramienta de análisis estático de código fuente incluyendo el servicio de soporte técnico, es más beneficiosa porque cubre el requerimiento determinado de revisión continua de 2 millones de líneas de código fuente (2M) por el periodo de un (1) año. Asimismo, es beneficio contar con una herramienta que realice el análisis automatizado de las líneas de código fuente porque permite detectar vulnerabilidades y corregir errores de dicho código fuente en la etapa de desarrollo. Por lo tanto, reduce el tiempo de revisión en el proceso de control de calidad y evita el retrabajo que se ocasionaría en caso dicho código tuviera que ser devuelto al ambiente de desarrollo para su corrección. De esta manera se tendrá código fuente limpio, estandarizado y fácil de mantener en el tiempo.

10. FIRMAS:

Departamento de Gestión y Calidad

Lima, 28 de septiembre de 2020

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Gabriela MIRANDA CORDOVA
Especialista en Gestión y Calidad
Departamento de Gestión y Calidad

Patricia Pilar LOPEZ CONCHA
Jefe de Departamento de Gestión y Calidad
Departamento de Gestión y Calidad

VISADO POR:

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración