



PERÚ

Ministerio
de la Producción

| OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACION

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 021-2022

“Licencias de Software de Análisis de Código Estático y Pruebas de Seguridad de Aplicaciones”

1. NOMBRE DEL ÁREA

Oficina General de Tecnologías de la Información - OGTI

2. CARGO

Giusseppe Jose Contreras Montalvo – Técnico en Infraestructura Tecnológica

3. FECHA

Noviembre – 2022

4. JUSTIFICACION

El Ministerio de la Producción requiere licencias de software de análisis de código estático y pruebas de seguridad de aplicaciones, para realizar el análisis de código y pruebas de seguridad de las aplicaciones web en la fase de desarrollo y calidad.

Las vulnerabilidades de seguridad en las aplicaciones son resultado de defectos de calidad, que pueden ocurrir durante el proceso de desarrollo de la aplicación, por tanto las organizaciones requieren de herramientas que les permitan identificar y solucionar estas vulnerabilidades como parte de las prácticas estándar de gestión del ciclo de vida de la aplicación, incluyendo las fases de diseño, desarrollo y entrega.

Las herramientas utilizadas para analizar la seguridad de las aplicaciones web se pueden agrupar en tres categorías:

Análisis White box: Toda la información relevante sobre el sistema o el software, incluyendo el código fuente, se conoce y está disponible para el responsable del análisis. Comprende las denominadas pruebas estáticas (Static Application Security Testing – SAST). SAST es de naturaleza amplia, pues simula todos los resultados posibles e inspecciona cada línea de código, y se pueden identificar más tipos de vulnerabilidades que con otros métodos de análisis.

Análisis Black box: Consiste en examinar el software o el sistema sin el conocimiento previo del medio ambiente. Este tipo de análisis es similar a lo que un atacante externo podría hacer. Cuando una organización es sensible a amenazas externas, el análisis Black box es generalmente el primer método de análisis, y los riesgos encontrados del mismo son priorizados porque reflejan con mayor precisión el riesgo expuesto al exterior. Comprende las denominadas pruebas dinámicas (Dynamic Application Security Testing – DAST). DAST trabaja atacando la aplicación mediante el uso de técnicas similares a las que un hacker podría emplear, usando muchos escenarios de ataque y monitoreando las respuestas de la aplicación con el fin de diagnosticar las vulnerabilidades. DAST es ideal para llevar a cabo una prueba del sistema de extremo a extremo. Con herramientas automatizadas de este tipo, en sólo minutos se pueden intentar miles de ataques en contra de una aplicación, descubriendo automáticamente los puntos de entrada (superficie de ataque) de la misma.



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

Análisis Gray box: Combina los beneficios de los análisis de tipo White box y Black box, lo que se logra correlacionando los resultados. Se recomienda aplicarlo a través del ciclo de vida de la aplicación para maximizar los resultados.

Desde el punto de vista de Sistemas de Información e Infraestructura Tecnológica, se necesita contar con herramientas del tipo SAST, que automaticen la detección de vulnerabilidades en aplicaciones web para su uso en las etapas de puesta en desarrollo, calidad y producción de las aplicaciones web y auditorías periódicas ante nuevas vulnerabilidades que puedan ser descubiertas.

5. ALTERNATIVAS

Actualmente en el mercado existen diferentes soluciones correspondientes a análisis de código estático y pruebas de seguridad de aplicaciones, para los aplicativos informáticos de la entidad, en merito a ello se toman en cuenta aquellas que sean compatibles e instalables en la plataforma tecnológica de usuario final.

Tomando en consideración las necesidades y requerimientos del Ministerio de la Producción, en base a los nuevos esquemas relacionados con protección ante amenazas no solo conocidas, sino también desconocidas, se ha buscado alternativas de licencias de software de análisis de código estático y pruebas de seguridad de aplicaciones en el mercado local que cumplan dichas necesidades y cuenten con soporte técnico local.

Se considera conveniente evaluar las siguientes soluciones a fin de definir una de ellas:

- FORTIFY SCA.
- HCL APPSCAN SOURCE.

Para la determinación de las soluciones seleccionadas, así como la evaluación técnica, se ha tomado como referencia:

- Información disponible en la página web de cada uno de los fabricantes.
- Información disponible en internet.

6. ANALISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado según los lineamientos establecidos en la "Guía técnica sobre evaluación de software para la administración pública" aprobado por R.M. N° 139-2004-PCM tal como exige el reglamento de la ley N° 28612 -"Ley que norma el uso, adquisición y adecuación del software en la administración pública":

7.1 Propósito de la Evaluación:

Validar que las alternativas seleccionadas sean las más convenientes para el Ministerio de la Producción.

7.2 Identificar el tipo de producto

Licencias de software de análisis de código estático y pruebas de seguridad en aplicaciones.



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

7.3 Especificación del Modelo de Calidad.

La evaluación de las licencias de software de análisis de código estático y pruebas de seguridad en aplicaciones se ha realizado bajo los parámetros establecidos en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

7.4 Selección de métricas

Las métricas fueron identificadas de acuerdo a las funcionalidades que ofrecen las soluciones señaladas en el punto “6”. Alternativas del presente informe

Cuadro N°01: Cuadro comparativo técnico

N°	Atributos	Descripción	Puntaje Máximo	FORTIFY SCA	HCL APPSCAN SOURCE
Atributos Internos y Externos					
1	Funcionalidad	Debe contar con un modelo de licencias en sitio de soluciones de Análisis Estático (SAST - Static Application Security Testing).	4	4	4
		Deberá contar con un modelo de servicios paquetizados por evento o por suscripción de ejecución de pruebas de Análisis Estático (SAST - Static Application Security Testing).	4	4	4
		Debe contar y detallar las características de su modelo de servicios paquetizados por evento o por suscripción de ejecución de pruebas de seguridad en aplicaciones móviles, contemplando pruebas a los archivos binarios de las aplicaciones, mobile pen testing, análisis de código fuente.	4	4	4
		Debe contar con un modelo de servicios paquetizados por evento o por suscripción de ejecución de pruebas de seguridad en aplicaciones móviles en las plataformas iOS, Android.	4	4	4



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

	Debe contar con un modelo ON-PREMISE para las funcionalidades de SAST.	4	4	4
	Debe ser capaz de integrar en un sistema central de gestión de vulnerabilidades los resultados y hallazgos asociados a las pruebas estáticas (SAST).	4	4	4
	Debe basar su portafolio de soluciones en los modelos y enfoques de seguridad aplicativa OpenSMM y BSIMM	4	4	4
	Debe incluir en su solución, de forma automatizada, plantillas de proceso que incluyan a los participantes, artefactos, requerimientos y actividades asociadas a la creación de software seguro desde una perspectiva de riesgo y de certificación PCI. Esto es adicional a la creación de reportes.	4	4	4
	El fabricante deberá tener partners locales certificados y el proveedor deberá indicar los esquemas de soporte en sitio con que cuenta para sus soluciones	4	4	4
	Debe contar con una robusta integración con los IDEs estándar de la organización para incluir en él la posibilidad de realizar escaneo de código, recuperación remota de resultados de escaneos, remediación de código, descripciones y recomendaciones de buenas prácticas de secure coding y la actualización en el	4	4	4



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

		repositorio central de los problemas de seguridad reportados			
2	Fiabilidad	Debe proveer la capacidad de identificar problemas que fueron ocultados, suprimidos o marcados como "no es un problema" de forma deliberada	3	3	3
3	Usabilidad	Debe permitir la personalización de las descripciones de las vulnerabilidades y las recomendaciones en un Repositorio Central para que haya posibilidad de integrar las descripciones con las políticas internas definidas en la organización, por ejemplo: El cliente podrá personalizar la descripción de determinada vulnerabilidad bajo el contexto de la organización y la aplicación, de forma que más adelante sea posible asociar dichas descripciones a las políticas internas que previamente se han definido	3	3	3
		Debe soportar la personalización de visualización de resultados basado en la audiencia (developer, security, etc.)	3	3	3
		Disponibilidad de manuales y capacitación a cargo de especialistas calificados por el fabricante	2	2	2
		Debe soportar la generación de reportes específicamente de dichas regulaciones y clasificaciones	2	2	2
		Debe soportar la autenticación vía LDAP/AD	2	2	2



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

		Debe soportar la capacidad de asignar la revisión y/o remediación de problemas a algún participante de algún proyecto en específico. Debe permitir a un participante de algún proyecto específico el poder visualizar sólo los problemas de seguridad que le fueron asignados	2	2	2
4	Eficiencia	Debe soportar la integración tanto de resultados identificados de forma automática como de forma manual	5	5	5
5	Portabilidad	Debe ofrecer la capacidad de integrarse con el bugtracker JIRA / TFS	5	5	5
6	Capacidad de mantenimiento	Registro de los incidentes de seguridad detectados para tener un claro entendimiento de éstas	5	5	5
		Permanentemente actualización de la solución, incluyendo el suministro de nuevas versiones y parches	5	5	5
		Soporte directo del fabricante	5	5	5
Sub Total			82	82	82
1	Eficacia	Debe contar con la capacidad de habilitar la colaboración de revisión de resultados, correlación de resultados, auditoría, asignación de problemas y creación de defectos sin necesidad de instalar localmente herramientas propias para estos fines	5	5	5
2	Productividad	Debe contar con herramientas que permitan ejecutar escaneos al código fuente sin necesidad de contar con un IDE	4	4	4



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

3	Seguridad	Debe ser capaz de manejar etiquetas de metadatos que permitan asociar los problemas reportados con las políticas de codificación segura definidas en la organización	4	4	4
		Debe ser capaz de llevar un histórico de todos los comentarios y priorizaciones definidos por el usuario	5	5	5
		Sub Total	18	18	18
		Total	100	100	100

7. ANALISIS COMPARATIVO DE COSTO – BENEFICIO:

7.1 Licenciamiento

Se debe incluir licencias con mantenimiento de software (cambios de versión, actualización) por el tiempo del contrato.

La solución ofrecida debe corresponder a las últimas versiones

7.2 Software

Los sistemas operativos instalados en los computadores de trabajo desplegadas (Ms Windows), cumplen con los requisitos exigidos por las soluciones de software evaluados.

7.3 Soporte y mantenimiento externo

El fabricante o proveedor de los productos ofertados debe poseer oficina de representación en Perú, así como personal de soporte técnico que garantice la adecuada y oportuna prestación de la garantía y de servicios. Este servicio debe ser 8x5.

7.4 Costo

No se ha realizado un Análisis de Costos Beneficio, por cuanto en el presente Informe Técnico Previo de Evaluación de Software, sólo se desea establecer el software más adecuado técnicamente de acuerdo al puntaje obtenido en la Evaluación Técnica de las Métricas.

La evaluación formal del análisis de costos se realizará durante el proceso de oficial de compras, según la ley de contrataciones y adquisiciones del estado N° 30225.

8. CONCLUSIONES Y RECOMENDACIONES

De acuerdo a la evaluación técnica de las métricas de las soluciones evaluadas: “FORTIFY SCA” y “HCL APPSCAN SOURCE” han obtenido puntajes aceptables.

En base al análisis realizado, se evidencia que la solución FORTIFY SCA es que alcanza el mayor puntaje, es



PERÚ

Ministerio
de la Producción

| OFICINA GENERAL DE TECNOLOGIAS DE LA INFORMACION

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año del Fortalecimiento de la Soberanía Nacional”

“Año del Bicentenario del Congreso de la República del Perú”

decir, es la que mejor solución se adecua a las necesidades del área usuaria como las licencias de software de análisis de código estático y pruebas de seguridad de aplicaciones para los equipos del parque informático que se necesita para el Ministerio de la Producción.

9. FIRMA

Giusseppe Jose Contreras Montalvo
Oficina General de Tecnologías de la Información