Firmado electrónicamente por:
JORGE SILVANO GUTIERREZ MENDOZA
CONTRATO ADMINISTRATIVO DE SERVICIOS
DIVISIÓN DE ARQUITECTURA DE INFORMACIÓN Y APLICACIONES
Fecha y hora: 22/05/2024 13:47

INFORME TÉCNICO N.º 000022-2024-SUNAT/1U4100

ASUNTO : Informe Técnico de Evaluación de Software "Solución de análisis de seguridad de aplicaciones para el desarrollo seguro de sistemas de información en la SUNAT."

LUGAR : Lima, 22 de mayo de 2024

SUNAT
Vº Bº
1U4100
REG. 1245
JOHNNY ANTONIO VALDEZ AREVALO
ENCARGADO (E)
22/05/2024 10:53:44

1. NOMBRE DEL ÁREA

DIVISIÓN DE ARQUITECTURA DE INFORMACIÓN Y DE APLICACIONES

2. RESPONSABLES DE LA EVALUACIÓN

JOHNNY ANTONIO VALDEZ AREVALO
JORGE SILVANO GUTIERREZ MENDOZA

3. CARGOS

JEFE DE LA DIVISIÓN DE ARQUITECTURA DE INFORMACIÓN Y DE APLICACIONES
ARQUITECTO TI

4. JUSTIFICACIÓN

La SUNAT, a través de su PEI (2024-2027) ha establecido sus objetivos estratégicos, entre los cuales se encuentra el OEI.01: “Mejorar el cumplimiento tributario y aduanero de los administrados”. Respecto a ello, la Entidad requiere contar con herramientas que permitan mejorar la gestión de la seguridad informática del ciclo de vida de desarrollo de software para los sistemas de información internos y externos que brindan soporte a los servicios ofrecidos a los contribuyentes, con la finalidad de mantener la integridad, disponibilidad y confidencialidad de la información.

En ese contexto, Actualmente, la Intendencia Nacional de Sistemas de Información - INSI, no cuenta con una solución robusta para la ejecución de análisis de seguridad en el código fuente durante el ciclo de vida de desarrollo de software de los sistemas de información de SUNAT. Esto conduce a que potenciales vulnerabilidades y errores en la codificación de los sistemas de información no puedan ser identificados, gestionados y remediados de forma adecuada y oportuna, lo que supone riesgos de seguridad en la información tributaria de los contribuyentes y la información interna de la Entidad. Debido a ello, se requiere fortalecer la seguridad informática de la Entidad con una herramienta nueva, robusta y de nivel empresarial, que permita gestionar el desarrollo seguro de los sistemas de información.

Por lo expuesto y en cumplimiento de la Ley N° 28612 – "Ley que norma el uso, adquisición y adecuación del software en la administración pública" – se ha procedido a elaborar el presente informe de evaluación de software para el logro de los objetivos institucionales y la modernización de la SUNAT.

5. ALTERNATIVAS

Considerando la necesidad del área usuaria en mención, se han buscado alternativas de software en el mercado que lo cumplen, tomando en consideración la disponibilidad en el servicio de atención y soporte local.

En ese sentido, la búsqueda ha dado como resultado los productos que se listan a continuación:

- Microfocus Fortify
- Veracode
- HCL AppScan

SUNAT
Vº Bº
1U4100
REG. 1245
JOHNNY ANTONIO VALDEZ AREVALO
ENCARGADO (E)
22/05/2024 10:53:44

6. ÁNALISIS COMPARATIVO TÉCNICO

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la "Guía Técnica sobre Evaluación de Software en la Administración Pública" aprobado mediante la Resolución Ministerial N° 139-2004-PCM tal como se exige en el reglamento de la Ley N° 28612, donde se aplicó el modelo de calidad de software establecido en el mismo.

a. Propósito de evaluación
Validar que las alternativas seleccionadas en el Ítem 6. sean las más convenientes técnicamente para el uso de la unidad orgánica: Gerencia de Arquitectura.

b. Identificar el tipo de producto
Software para la automatización en el despliegue de pases a producción

c. Identificación del modelo de calidad
Se aplicará el Modelo de Calidad de Software descrito en la parte I de la Guía Técnica sobre Evaluación de Software para la Administración Pública aprobado por Resolución Ministerial N° 139-2004-PCM.

d. Selección de métricas
Las métricas fueron seleccionadas en base al análisis de las características técnicas del software seleccionado en el ítem 6 (alternativas de software), así como información de internet y plantillas de evaluación.

Las métricas consideradas en el "Cuadro Comparativo de Métricas Internas y Externas", donde se han evaluado atributos internos, externos y de uso, se muestran a continuación:

CUADRO COMPARATIVO DE MÉTRICAS INTERNAS Y EXTERNAS:

	Puntaje Max. 100 puntos	MicroFocus Fortify	Veracode	HCL AppScan
ATRIBUTOS INTERNOS	**40**	**40**	**40**	**40**
Funcionalidad: Permite consolidar los resultados que se realicen con herramientas de análisis estático de código (SAST), herramientas de análisis de seguridad de aplicaciones dinámico (DAST) y Software de Análisis de componentes (SCA).	10	10	10	10
Funcionalidad: Debe permitir una herramienta automatizada de análisis de vulnerabilidades de aplicaciones web, API y servicios web	10	10	10	10
Funcionalidad: Permite un análisis modular donde se puedan pre-escanear librerías y sublibrerías de manera separada del proyecto principal. Estas deberán poder ser incluidas luego en el proyecto principal ya escaneadas de manera de mejorar la performance. Esta característica se espera que al menos esté disponible para proyectos Java	10	10	10	10
Funcionalidad: Debe contar con un componente de gestión centralizada de vulnerabilidades que permita a los diferentes actores (desarrolladores, analista de calidad, analistas de seguridad), colaborar y dar seguimiento de remediación a las potenciales vulnerabilidades.	10	10	10	10
ATRIBUTOS EXTERNOS	**30**	**30**	**30**	**30**
Funcionalidad: Interoperabilidad Debe contar con un componente de gestión centralizada de vulnerabilidades que permita a los diferentes actores (desarrolladores, analista de calidad, analistas de seguridad), colaborar y dar seguimiento de remediación a las potenciales vulnerabilidades.	10	10	10	10
Funcionalidad: Debe incluir un modo de escaneo, donde se permite navegar manualmente a las secciones de la aplicación que se deba escanear, es decir, la solución registra información solo sobre los recursos que encuentra mientras navega manualmente por el sitio. La idea, es que una vez que se termine de navegar por el sitio, se pueda auditar los resultados para evaluar las vulnerabilidades de seguridad relacionadas con esa parte del sitio que se registró.	10	10	10	10
Funcionalidad: Debe proveer las actualizaciones a las reglas de la base de conocimientos así las actualizaciones al propio software de la solución	10	10	10	10
ATRIBUTOS DE USO	**30**	**30**	**30**	**30**
Funcionalidad: El componente de gestión centralizada de vulnerabilidades hallazgos debe soportar la creación de webhooks para actualizar sistemas externos.	10	10	10	10
Funcionalidad:	10	10	10	10

SUNAT
Vº Bº
1U4100
REG. 1245
JOHNNY ANTONIO VALDEZ AREVALO
ENCARGADO (E)
22/05/2024 10:53:44

Debe soportar las siguientes integraciones con herramientas de pipeline (CI/CD servers): - Jenkins - GitLab - ArgoCD - Bamboo				
Funcionalidad: Debe proveer un mecanismo automático que facilite y mejore la calidad de las auditorías sobre las vulnerabilidades incluyendo la reducción de falsos positivos (preferentemente basado en machine learning)	10	10	10	10
PUNTAJE TOTAL	**100**	**100**	**100**	**100**

7. ANALISIS COMPARATIVO DE COSTO-BENEFICIO:

A continuación, se ha realizado un análisis de costos referencial de los productos y complementos necesarios para cumplir con la evaluación técnica realizada.

SUNAT Vº Bº 1U4100 REG. 1245
JOHNNY ANTONIO VALDEZ AREVALO
ENCARGADO (E)
22/05/2024 10:53:44

MicroFocus Fortify	Veracode	HCL AppScan
S/. 4,000,000.00	S/. 5,000,000.00	S/. 7,000,000.00

8. CONCLUSIONES:

Del análisis realizado a nivel de atributos requeridos en la solución, la herramienta MicroFocus Fortify, la herramienta Veracode y la herramienta HCL AppScan cumplen con la totalidad de requerimientos solicitados para la institución. Se debe proceder a un proceso de adquisición por concurso para la disponer de la herramienta.

ELABORADO POR AL38 – Jorge Silvano Gutierrez Mendoza	**EVALUADO POR (firma y sello)** 1245 – Johnny Antonio Valdez Arevalo