Firmado Electrónicamente por:
JORGE SILVANO GUTIERREZ MENDOZA
CONTRATO ADMINISTRATIVO DE SERVICIOS
DIVISIÓN DE ARQUITECTURA DE INFORMACIÓN Y APLICACIONES
Fecha y hora: 20/12/2022 09:16

INFORME N.º 000052-2022-SUNAT/1U4100

ASUNTO : INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE LA SOLUCION PARA FORTALECER LA AUTOMATIZACION EN EL DESPLIEGUE DE PASES A PRODUCCION

LUGAR : Lima, 20 de diciembre de 2022

SUNAT
V° B°
1U4100
REG. 1548
ENZO JULIO BENAVIDES VALENTIN
ENCARGADO (E)
19/12/2022 20:39:50

1. NOMBRE DEL ÁREA

DIVISIÓN DE ARQUITECTURA DE INFORMACIÓN Y DE APLICACIONES

2. RESPONSABLES DE LA EVALUACIÓN

ENZO JULIO BENAVIDES VALENTIN
JORGE SILVANO GUTIERREZ MENDOZA

3. CARGOS

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

4. JUSTIFICACIÓN

De acuerdo con el PEI (2022-2024)[1], la SUNAT tiene como Objetivos Estratégicos "[OIE.04]: Fortalecer la capacidad de gestión interna", en ese sentido, la División de Gestión de Infraestructura Tecnológica encargada de administrar el inventario de software y sus respectivas licencias de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT) y quien debe proporcionar herramientas de software a las unidas orgánicas para el buen desarrollo y desempeño de sus funciones, evalúa la necesidad de la unidad orgánica: Gerencia de Arquitectura perteneciente a la Intendencia Nacional de Sistemas de Información.

La Gerencia de Arquitectura es una unidad orgánica dependiente de la Intendencia Nacional de Sistemas de Informacion, encargada de la conducción de la investigación tecnológica y del diseño de la arquitectura de la información, de aplicaciones y de infraestructura tecnológica de la SUNAT.

En ese contexto, Actualmente la Intendencia Nacional de Sistemas de Informacion - INSI, no cuenta con una solución para automatizar la gestión de la seguridad dentro del flujo de integración continua de los sistemas de información de SUNAT. Esto conduce a que se realice buena parte del trabajo en forma manual.

[1] Fuente: https://www.sunat.gob.pe/legislacion/superin/2021/anexo-B2-rs059-2021.pdf

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
V° B°
1U4100
REG. 1548
ENZO JULIO
BENAVIDES VALENTIN
ENCARGADO (E)
19/12/2022 20:39:50

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) y herramientas de análisis de seguridad de aplicaciones dinámico (DAST)	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 debe permitir la personalización de la interfaz (look&feel) para que se ajuste con información propia de nuestra organización.	10	10	10	10
Funcionalidad:	10	10	10	10

SUNAT V° B° 1U4100 REG. 1548
ENZO JULIO BENAVIDES VALENTIN
ENCARGADO (E)
19/12/2022 20:39:50

Debe soportar las siguientes integraciones con herramientas de pipeline (CI/CD servers): - Jenkins - GitLab - Gradle				
Funcionalidad: D 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 V° B° 1U4100 REG. 1548
ENZO JULIO BENAVIDES VALENTIN
ENCARGADO (E)
19/12/2022 20:39:50

MicroFocus Fortify	Veracode	HCL AppScan
S/. 2,000,000.00	S/. 3,000,000.00	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)** 1548 – Enzo Julio Benavides Valentin