BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0008-2025-GTI410-N

ASUNTO : Informe técnico previo de evaluación de software – *Contratación por 2 años de suscripciones de una solución DAST (Dynamic Application Security Testing) del BCRP*

---

1. NOMBRE DEL ÁREA:

Dpto. de Ciberdefensa

2. RESPONSABLE DE LA EVALUACIÓN:

Brian Dextre Alarcón.
Leandro Alvarez Figueroa.
Alexander Gamboa Inga

3. CARGO:

Especialista de Ciberdefensa
Jefe de Departamento de Ciberdefensa
Subgerente de Ciberseguridad Interino

4. JUSTIFICACIÓN:

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 vulnerabilidades de Seguridad en las aplicaciones son el resultado de inadecuadas prácticas durante el desarrollo en sus distintas fases. Desde su diseño hasta la construcción de artefactos. Por lo tanto, las organizaciones requieren de controles de Seguridad adicionales que complementen el end-to-end del ciclo de Desarrollo Seguro de Software. Iniciativas como Devops y DevSecops introducen la cultura de implementar controles de Seguridad en todas las fases del Desarrollo.

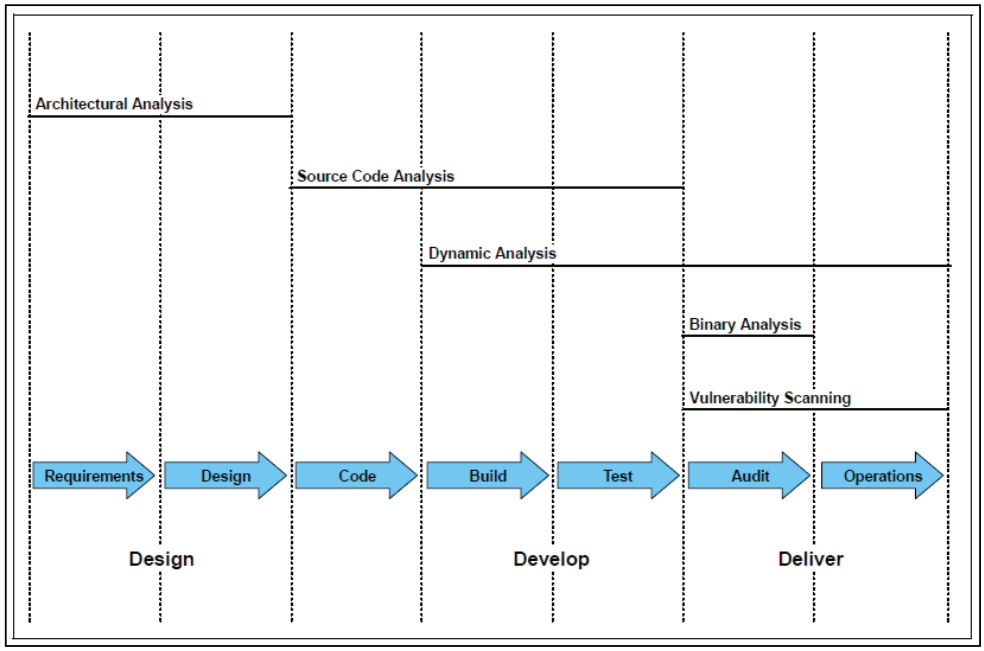

Figura N° 1: The different types of security analysis throughout the software development life cycle
Fuente: *Improving Your Web Application Software Development Life Cycle's Security* (IBM)

Las herramientas de Seguridad utilizadas para analizar la seguridad de las aplicaciones web, móviles y servicios web se pueden agrupar en dos categorías:

Herramientas para pruebas de Seguridad estáticas (SAST):

Las herramientas para pruebas de seguridad estáticas (SAST, por sus siglas en inglés **Static Application Security Testing**) son soluciones diseñadas para analizar el código fuente, el código compilado o los archivos binarios de una aplicación en busca de vulnerabilidades de seguridad sin ejecutarla. Estas herramientas evalúan el código en reposo, lo que permite identificar fallas de seguridad y problemas de calidad en las etapas tempranas del ciclo de desarrollo del software.

Herramientas para pruebas de Seguridad dinámicas (DAST):

Las herramientas para pruebas de seguridad dinámicas (**DAST**, por sus siglas en inglés **Dynamic Application Security Testing**) son soluciones diseñadas para analizar aplicaciones en ejecución y detectar vulnerabilidades explotables en tiempo real. A diferencia de SAST, estas herramientas evalúan cómo la aplicación se comporta y responde a diferentes entradas y condiciones mientras está en ejecución, dichas pruebas son similares a las que realizan los ciberatacantes cuando encuentran servicios expuestos en internet.

En este tipo de pruebas de Seguridad, se manejan dos tipos:

- **Análisis No Autenticado**

Simulan un ataque externo donde el atacante no tiene credenciales válidas y se tiene el objetivo de evaluar las vulnerabilidades accesibles para usuarios anónimos.

- **Análisis Autenticado**

Simulan un escenario donde el atacante tiene credenciales válidas, permitiendo pruebas con diferentes niveles de privilegios.

Desde el punto de vista de infraestructura de TI y Ciberseguridad, se necesita contar con una herramienta de tipo DAST (Dynamic Application Security Testing), que automaticen la detección de vulnerabilidades de Ciberseguridad en las aplicaciones y servicios Web. Esta herramienta se usa en las etapas previas de puesta a producción de nuevas aplicaciones y cambios en aplicaciones existentes (incluyendo tanto las aplicaciones que son de desarrollo propio como los productos adquiridos) y auditorías periódicas ante nuevas vulnerabilidades que puedan ser descubiertas.

El BCRP tiene implementadas diversas aplicaciones web, entre ellas: Portal Web Institucional (www.bcrp.gob.pe), Portal de Series Estadísticas, Biblioteca, Fondo de Empleados, SICAP, SIBFTP, Tienda virtual, LBTR, SACWeb, entre otras, por lo cual es necesario contar con herramientas tecnológicas que permitan detectar las vulnerabilidades de las aplicaciones web previo a su puesta en producción y ante modificaciones que se realicen a las mismas.

- una cobertura básica y eficiente sin intervención constante.

Además, el Banco actualmente se encuentra impulsando las siguientes actividades:

- **Proyectos trimestrales:** Los Proyectos trimestrales implican el desarrollo web de iniciativas nuevas o mejoras sobre aplicaciones existentes, siguiendo las buenas prácticas de Desarrollo Seguro. Sea el camino de nueva iniciativa o mejora, ambos tienen que pasar por pruebas de análisis dinámico, para garantizar que el producto que se implemente y publique sea de calidad y seguro.

- **DevSecOps:** Es una metodología o enfoque de desarrollo de software que combina las prácticas de desarrollo (Dev), seguridad (Sec), y operaciones (Ops) para integrar la seguridad de manera continua y efectiva en todo el ciclo de vida de desarrollo y entrega de aplicaciones.

5. ALTERNATIVAS:

Consideramos las siguientes marcas que brindan soluciones de una solución centralizada DAST (Dynamic Application Security Testing).

- Open Text/Micro Focus Fortify.
- Qualys Web Application Scanning (WAS).

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial NO 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

a. Propósito de evaluación

Comparar alternativas de productos existentes en el mercado.

b. Propósito de evaluación

Suscripciones de Software para la Solución Centralizada DAST (Dynamic Application Security Testing)

c. Identificación del modelo de calidad

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de evaluación de software aprobado por RM NO 139-2004-PCM.

d. Selección de métricas.

Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

Se realizó el análisis para las marcas Open Text/Micro Focus Fortify y Qualys Web Application Scanning

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Detección de vulnerabilidades en las aplicaciones web de la institución.
- Pruebas de black box (DAST).
- Generación de reportes especializados (detalle de vulnerabilidades, recomendaciones de solución) que son analizados por el Departamento de Ciberseguridad y Redes para luego ser derivado hacia el Departamento de Gestión y Calidad para su subsanación o compensación de acuerdo con el hallazgo encontrado.
- Soporte con el Proyecto OWASP (Open Web Application Security Project).
- Herramienta que se actualiza constantemente con las nuevas vulnerabilidades que son descubiertas en la actualidad.
- Múltiples perfiles de escaneo basándose en el tipo de aplicación.
- Soporte a automatizaciones haciendo uso de integraciones con las APIs de la solución.
- Contar con una solución centralizada y automatizada que permita la detección de vulnerabilidades a nivel de la capa aplicación de las aplicaciones desarrolladas por el BCRP.

- Contar con una solución centralizada y automatizada que permita integrarse a flujos de automatización continua.
- Contar con una solución que luego de realizar los análisis de vulnerabilidad, permita la descarga de reportes de vulnerabilidad del tipo técnico, ejecutivo y con capacidad de personalizar de acuerdo con criterios como lo son tipo de vulnerabilidad y severidad descubierta en las aplicaciones web.
- Contar con soporte por parte del fabricante y local para la atención ante posibles errores de la solución o la absolución de dudas a partir de características de la misma solución
- Aumentar la capacidad operativa para la realización de escaneos en simultaneo a las aplicaciones web del Banco que se encuentran en desarrollo o producción, lo que permitirá acelerar la entrega de reportes de vulnerabilidades hacia los equipos de Calidad y Soluciones TI del Banco

Costos:

Las prestaciones requeridas corresponden al periodo de 2 años de servicio.

- Prestación principal: Implementación del servicio
  Implementación del software de una solución centralizada DAST, suscripciones, actualizaciones de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento).

- Prestación accesoria: Servicios del partner (proveedor local)
  Mesa de ayuda y soporte, en el esquema 24x7 y mantenimiento técnico preventivo anual.

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2024.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se solicita la contratación por 2 años de suscripciones de una solución DAST (Dynamic Application Security Testing).

BANCO CENTRAL DE RESERVA DEL PERÚ

ANEXO N° 1

ATRIBUTOS Y MÉTRICAS

N°	Atributos	Puntaje máximo	Open Text/Micro Focus Fortify	Qualys Web Application Scanning (WAS)
1	Detección de vulnerabilidades en las aplicaciones web de la Institución	10	10	10
2	Pruebas de black box (DAST)	10	10	10
3	Generación de reportes especializados (detalle de vulnerabilidades, recomendaciones de la solución)	10	9	9
4	Soporte con estandares como OWASP (Open Web Application Security Project)	10	10	9
5	visualización del progreso de escaneo en tiempo real	10	8	8
6	Integración nativa con soluciones de integración y entrega continua de Software	10	10	10
7	Permitir programar escaneos para que se realice en fechas y horas programadas	10	10	10
8	Ejecución de escaneos simultáneos	10	10	10
9	Consola de gestión centralizada	10	10	9
10	Escalabilidad en los componentes de la solución.	10	9	10
Puntaje Total		100	96	95

Lima, 29 de enero de 2025

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Brian Jason DEXTRE ALARCON
Especialista en Ciberdefensa
Departamento de Ciberdefensa

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Ciberdefensa
Departamento de Ciberdefensa

Marco Antonio GRANADINO CACERES
Subgerente de Ciberseguridad
Subgerencia de Ciberseguridad

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

VISADO POR: