

AMPLIACIÓN CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI) a través de la Dirección Nacional de Tecnología, convoca a proveedores nacionales e internacionales a participar en el proceso de elaboración del Estudio de Mercado para la “**ADQUISICIÓN DE HERRAMIENTA DE VALIDACIÓN DE CÓDIGO ESTÁTICO**”

Este estudio de mercado será utilizado para la definición del presupuesto referencial previo a la publicación del proceso de adquisición.

El precio referencial de los bienes deberá considerar los siguientes aspectos:

- Las especificaciones técnicas detalladas adelante;
- Los precios cotizados deben estar en valor DDP Delivered Duty Paid/ Entregado con derechos pagados, incluyendo todos los derechos de aduanas e impuestos;
- La vigencia de la cotización no debe ser menor a 120 días;
- La fuente de financiamiento será realizada con recursos del Banco Interamericano de Desarrollo, por lo que los oferentes deberán pertenecer a los países miembros del BID;
- El plazo total del contrato es de hasta 754 días calendario, contados a partir del día siguiente de la suscripción del contrato

Las cotizaciones deben ser remitidas en formato digital (firmadas), al correo institucional programaintax@sri.gob.ec hasta el día 01 de febrero de 2024, con los siguientes datos:

Datos del oferente:

Razón Social:

RUC / ID:

Dirección:

Teléfono:

Fecha de emisión de la cotización:

Vigencia de la cotización: (no debe ser menor a 120 días)

Firma de responsabilidad.

Datos del contratante:

A nombre de: Servicio de Rentas Internas

RUC: 1760013210001

Formato Presentación Cotización:

Propuesta Económica:

Presupuesto total del proyecto:				
DESGLOSE DE COMPONENTES				
Tipo de recurso	Descripción producto / servicio	Cantidad	Costo unitario	Total
Software	Suscripciones de software de herramienta de código estático con soporte de fábrica por 1 año.	1		
Software	Renovación de las suscripciones con soporte de fábrica (1 año adicional)	1		
Servicios	Implementación, migración, pruebas y transferencia de conocimientos	1		
Subtotal				\$ 0,00
IVA (12 %)				\$ 0,00
Total				\$ 0,00

Nota: Los oferentes deberán garantizar el entendimiento y el cumplimiento de todas las especificaciones técnicas y servicios conexos requeridos.

Listado de países elegibles

- Lista de países miembros cuando el financiamiento provenga del Banco Interamericano de Desarrollo: Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Territorios elegibles

- Guadalupe, Guyana Francesa, Martinica, Reunión – por ser Departamentos de Francia.
- Islas Vírgenes Estadounidenses, Puerto Rico, Guam – por ser Territorios de los Estados Unidos de América.
- Aruba – por ser País Constituyente del Reino de los Países Bajos; y Bonaire, Curazao, Sint Maarten, Sint Eustatius – por ser Departamentos de Reino de los Países Bajos.
- Hong Kong – por ser Región Especial Administrativa de la República Popular de China.

Servicio de Rentas Internas

ESPECIFICACIONES TECNICAS

1. INFRAESTRUCTURA ACTUAL

El SRI dispone de un servidor de aplicaciones, y espacio en bases de datos para la operación de su actual herramienta de validación de código estático Sonarqube edición Enterprise, tanto en la operación como para pruebas. Esta herramienta hasta diciembre de 2023 ha cubierto un análisis de 9'047.697 líneas de código de los diferentes lenguajes de programación, en los proyectos y mantenimientos que tiene la Institución.

El SRI dispone de:

- Aplicaciones desarrolladas para jboss que van desde la versión 4.3.0 hasta el jboss EAP 7.4.10 y también para la versión Red Hat Single Sign-On 7.3.8 GA.
- Aplicaciones desarrolladas en código java que utilizan jdk que va desde la versión 1.6 hasta la 1.8.
- Desarrollos pl/SQL
- Aplicaciones desarrolladas con python 3.11
- Automatización de la ejecución de validación de código estático con ansible

Estas aplicaciones al momento forman parte del core tributario del SRI en sus diferentes líneas de control, cumplimiento, devolución, entre otras; las cuales no serán migradas a nuevas tecnologías en un mediano a largo tiempo.

El código fuente de las aplicaciones que tiene el SRI se encuentra alojado en los repositorios para control de versiones: SVN (Subversion) 1.8.19 y GitLab Community Edition 15.9.3.

Las aplicaciones cuentan con los siguientes plugins de SonarQube en su edición Enterprise, para la validación de código estático:

- Análisis de código con Maven, Ant, Gradle, en donde se presentan problemas de accesibilidad basados en wcag2, mejores prácticas de programación en función del lenguaje de programación
- Análisis de vulnerabilidades de librerías de terceros con dependency-check
- Análisis de cobertura de código con Junit, pytest
- Análisis de vulnerabilidades en el código fuente analizados con Security SonarAnalyzer basado en las mejores prácticas de cwe, owasp, sans-top25

Los reportes generados de las diferentes validaciones se encuentran centralizados en la herramienta, y son generados a demanda por los diferentes usuarios y de forma concurrente.

El SRI, para alojar la herramienta de validación de Código Estático, cuenta actualmente con la siguiente infraestructura:

AMBIENTE DE PRODUCCIÓN

- Un servidor de aplicaciones
 - Sistema Operativo Red Hat Enterprise Linux release 8.0 (Ootpa)
 - Memoria de 8GB
 - 2 Cores
 - Disco Duro de 100GB

- Un servidor de base de datos Oracle 12c
 - Sistema Operativo Oracle Solaris en SPARC (64 bits)
 - Memoria de 60GB
 - 1 Cores
 - Disco Duro de 40GB

AMBIENTE DE PRUEBAS

- Un servidor de aplicaciones
 - Sistema Operativo Red Hat Enterprise Linux release 7.3 (Maipo)
 - Memoria de 8GB
 - 2 Cores
 - Disco Duro de 80 GB

- Un servidor de base de datos Oracle 12c
 - Sistema Operativo Oracle Solaris en SPARC (64 bits)
 - Memoria de 60GB
 - 1 Cores
 - Disco Duro de 40GB

Estos ambientes, son utilizados de la siguiente forma:

- Ambiente de **PRODUCCIÓN**, en donde se ejecuta la validación de código estático de los 355 proyectos de las diferentes aplicaciones que tiene la Institución.

sonarqube Projects Portfolios Issues Rules Quality Profiles Quality Gates Administration

Administration

Configuration Security Projects System Marketplace Support

SonarSource license

In case of any issue or question about licenses, please send an email to contact@sonarsource.com.

Edition	Type	Expiration
Enterprise Edition	PRODUCTION	November 27, 2024

Lines of Code

Up to 20,000,000

9,047,697 lines currently analyzed 20M

Features included

- Analysis of ABAP
- Analysis of APEX
- Analysis of C/C++
- Analysis of Cobol
- Analysis of Objective-C
- Analysis of PL/I
- Analysis of PL/SQL
- Analysis of RPG
- Analysis of Swift
- Analysis of T-SQL
- Analysis of VB.NET
- Analysis of VB6
- Branch Analysis
- Executive Reporting
- Parallel Processing
- Portfolios Management
- Project Transfer
- SonarLint Smart Notifications
- Vulnerability Analysis

Dichos proyectos, tienen su código fuente en los siguientes lenguajes de programación: java, xml, html, jsp, plsqlopen, css, javascript, pl/sql, Python.

- Ambiente de **PRUEBAS**, en donde se ejecutan las pruebas de las diferentes versiones de la herramienta, previo a su aplicación en el ambiente de PRODUCCIÓN, con el fin de revisar incompatibilidades, mejoras, diferentes formas de ejecución, entre otras validaciones previas a aplicar la última versión en PRODUCCIÓN. Este ambiente, también es utilizado para probar nuevos o mejorados plugins y que el equipo de Desarrollo pueda ejecutar también sus validaciones previas de los diferentes aplicativos en caso de requerirlo.

Projects Portfolios Issues Rules Quality Profiles Quality Gates Administration More Q

Administration

Configuration Security Projects System Marketplace Audit Logs Support

SonarSource license

Here you can set or update your SonarQube license.
In case of any issue or question about licenses, please check the documentation on [License Administration](#), or send an email

[Set new license](#)

Edition	Type	Expiration
Enterprise Edition	PRODUCTION	November 26, 2024

Lines of Code

Up to 20,000,000

8,984,854 lines currently analyzed 20M

Notification threshold
Corresponding to 3,000,000 lines of code before limit
Once you reach this point, you will receive an email when you are approaching your limit of authorized lines of analysis.

[Edit notification threshold](#)

In order to determine how much each project contributes, the license takes into account the number of [lines of code](#) on the largest branch of that project. Lines of test code do not count towards your license usage.

2. SERVICIOS REQUERIDOS

2.1 ALCANCE

Suscripciones de software y soporte de fábrica

- Suscripciones de software de la herramienta para cubrir 17'284.532 líneas de código, con una vigencia de 365 días calendario con renovación por un año adicional, y utilizada por 124 usuarios que pueden realizar los análisis de forma concurrente con sus roles definidos.
- Soporte de fábrica de la herramienta por dos años en modalidad 5x8 (Ocho horas al día por 5 días a la semana). La renovación del soporte de fábrica se realizará anualmente

Implementación/migración/pruebas y transferencia de conocimientos

- Implementación de la solución en los ambientes requeridos.
- Migración de información de la herramienta actual a la nueva.
- Pruebas tanto en el ambiente pruebas como en el ambiente de producción.
- Transferencia de conocimientos impartida de forma presencial para 50 funcionarios del SRI.

2.2 METODOLOGÍA DE TRABAJO

Cláusulas generales

- Todas las actividades que impliquen cambios en la configuración de la Herramienta de Validación de Código Estático deberán ser informados al Administrador del Contrato, y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.
- El personal técnico del contratista deberá contar con todos los medios y recursos necesarios para la ejecución ágil y oportuna atención de todos los trabajos que son parte del objeto del presente contrato; incluyendo, pero no limitado a: equipo portátil, dispositivos de acceso a Internet (ej. módems), medios removibles de almacenamiento (ej. USB Flash Drives, USB External Hard Drives, etc.), “patchcords”, y demás artículos o herramientas que se requieran, según cada caso.
- Cualquier acceso que necesite el contratista para cumplir de manera exitosa con los trabajos objeto del presente contrato deberá ser solicitado previamente al Administrador del Contrato con al menos de 5 días calendario de antelación.
- Toda documentación entregada al SRI se dará por recibida únicamente cuando ésta no tenga observaciones, cumpla debidamente con el requerimiento del SRI y aprobación por parte del Administrador de Contrato.
- Todos los gastos incurridos en el cumplimiento del contrato están a cargo del contratista. El SRI no incurrirá en ningún gasto adicional.

Suscripciones de software y soporte de fábrica

- Las suscripciones de software de la herramienta para cubrir las 17'284.532 líneas de código y 124 usuarios concurrentes deberá ser activado e incluirá el soporte de fábrica necesario para el normal funcionamiento de la solución.
- Durante el periodo de vigencia del soporte de fábrica el SRI debe tener acceso a:
 - Portal para seguimiento de tickets con credenciales de acceso para cada usuario que requiera acceder al soporte
 - Nuevas versiones del sistema y actualizaciones.
 - Acceso para abrir casos directamente con el fabricante.
 - Acceso a la base de conocimientos del fabricante.

Implementación/migración/pruebas

- El contratista deberá entregar al Administrador del Contrato el Plan de Implementación/migración/pruebas que incluirá al menos:
 - Arquitectura de la solución a ser implementada, incluyendo la versión de software y servidores que requiera para su funcionamiento.
 - Cronograma de trabajo.
- El contratista emitirá un cronograma de actividades para la instalación de la nueva herramienta en ambiente de pruebas y posterior su traslado al ambiente de producción; migración de los proyectos de la antigua herramienta, incluyendo la modificación de las automatizaciones existentes para su ejecución y la integración con los repositorios de control de versiones.
- El contratista solicitará al administrador del contrato los permisos de firewall necesarios a los equipos donde se alojará la nueva herramienta.
- El contratista deberá desplegar en la infraestructura del SRI o en la nube la totalidad del software de Herramienta de Validación de Código Estático.
- La implementación del licenciamiento de software de la Herramienta de Validación de Código Estático deberá ser realizado en su totalidad por el contratista en los ambientes de pruebas, y producción que incluya migración de la herramienta actual a la nueva, pruebas tanto en ambiente de pruebas y producción.
- En esta fase el contratista en base al Plan de Implementación/migración/pruebas iniciará con las actividades de Instalación de la nueva herramienta, ya sea, on premise o nube de manera remota o presencial en las instalaciones del Servicio de Rentas Internas en la Plataforma Gubernamental de Gestión Financiera en horario de oficina, de 08h00 a 17h00 en días laborables.
- El contratista deberá entregar un plan de continuidad de la herramienta y un plan de recuperación de desastres, los cuales serán revisados y aprobados por el Administrador del Contrato en la fase de Implementación /migración/pruebas.

Transferencia de Conocimientos:

- El proveedor debe proporcionar transferencia de conocimientos para 50 personas del SRI, permitiendo comprender y aprovechar al máximo las funcionalidades de la Herramienta de Validación de Código Estático implementada.
- La transferencia de conocimientos debe impartirse presencial en un espacio adecuado gestionado por el contratista para 4 grupos de hasta 15 personas con una duración mínima de 30 horas.
- La transferencia de conocimientos deberá incluir los materiales, facilidades y talleres necesarios para la correcta asimilación del contenido y la generación de las destrezas necesarias en los asistentes. Esta actividad no representará costos adicionales para el SRI.

- La logística de la transferencia será de responsabilidad del contratista (un computador para cada participante).
- La transferencia de conocimientos será en idioma español, o con el correspondiente traductor.
- La transferencia de conocimientos debe incluir todos los temas necesarios para que los funcionarios estén en capacidad de operar y administrar la solución adquirida por el SRI y el temario debe contener información sobre arquitectura, configuración, administración, contingencia y troubleshooting de la herramienta adquirida.

Soporte de fábrica

- Las actividades necesarias para la atención de requerimientos podrán ser realizadas remota o presencialmente según lo requiera el personal técnico del SRI.
- El administrador del contrato podrá acceder a toda la información de los tickets reportados.
- Todo requerimiento ingresado deberá tener un número de caso proporcionado por el contratista o fabricante para poder hacer el seguimiento posterior y el contacto del especialista asignado.
- El contratista deberá suministrar el procedimiento de apertura, seguimiento, escalamiento y cierre de casos de soporte con el fabricante, donde se describa el procedimiento de ingreso, seguimiento y cierre de casos de soporte, además deberá incluir el escalamiento en niveles jerárquicos en caso de no tener respuesta de acuerdo con el SLA establecido, el escalamiento debe incluir números telefónicos y correos electrónicos de los involucrados. Además, debe contener el acceso a la base de conocimientos del fabricante.
- Para la atención de requerimientos, el Contratista deberá cumplir con lo establecido en el ACUERDO DE NIVEL DE SERVICIO.
- En caso de controversia sobre la prioridad de un incidente o requerimiento de soporte técnico, prevalecerá el criterio del SRI.
- Si la atención de un caso requiere el levantamiento de información, la ejecución de algún comando, la captura u obtención de datos o la obtención de registros de eventos ("logs"), es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsible para obtener estos(as), sin perjuicio del cumplimiento del ACUERDO DE NIVEL DE SERVICIO.

Acuerdo de nivel de servicio

- El contratista debe garantizar el cumplimiento del SLA establecido, así como el seguimiento de las actividades relacionadas con el objeto del contrato, siendo parte fundamental en la comunicación con el fabricante.
- El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace el soporte técnico y el momento en que inicia el análisis técnico del ingeniero especialista designado. La notificación informativa de recepción del requerimiento no es aceptada como el inicio del análisis técnico.

- La tabla de tiempos de respuesta, a continuación, establece los umbrales máximos aceptables de tiempo de espera para cada prioridad. El tiempo de respuesta está medido en horas consecutivas salvo que se indique lo contrario.

Prioridad	Requerimiento de soporte técnico
1	1 hora
2	4 horas
3	8 horas
4	16 horas

Tabla 2. Tiempos de respuesta por prioridad.

- La tabla a continuación establece los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO.

PRIORIDAD	NIVEL DE SOPORTE	DESCRIPCIÓN
1	Crítico	Se refiere a incidentes en las que la herramienta de validación de código estático está completamente inoperable.
2	Alto	Se aplica a incidentes que, aunque no sean tan urgentes como las críticas, aún tienen un impacto significativo en el funcionamiento de la herramienta. Puede incluir problemas recurrentes o situaciones en las que una función importante de la herramienta no esté operativa.
3	Medio	Se refiere a incidentes que tienen un impacto moderado en la operatividad de la herramienta, pero que no representan una afectación inmediata o crítica.
4	Bajo	Corresponde a incidentes o requerimientos menores, ajustes de configuración, consultas o solicitudes de información o funcionalidades adicionales que no son urgentes.

Tabla 1. Descripción de los niveles de prioridad.

2.3 PRODUCTOS Y SERVICIOS ESPERADOS

SUSCRIPCIONES DE SOFTWARE Y SOPORTE DE FÁBRICA

- Herramienta de Validación de Código Estático de tipo on-premise o que únicamente envíe la metadata a la nube y que el código fuente se quede en los servidores de la Institución, para **17'284.532 líneas de código** y permita detectar errores, code smells y vulnerabilidades de seguridad.
- Independiente de las versiones de java, jboss que tienen las diferentes aplicaciones antiguas y nuevas de la Institución. Es decir, que la herramienta pueda realizar la validación de código estático en todos los aplicativos que disponga la Institución en sus diferentes versiones de jdk y jboss.
- Poseer analizadores de código para cubrir como mínimo los siguientes lenguajes: java, xml, html, jsp, plsql, css, javascript, Python. Los analizadores deben tener reglas que contengan las mejores prácticas de programación en los distintos lenguajes, accesibilidad basados en la WCAG.
- Identificar las vulnerabilidades en librerías de terceros
- Tener análisis de ramas (Branch Analysis), es decir, revisar la calidad de código de cada rama creada por aplicación; para garantizar que el código entregado coincida con las mejores prácticas y estándares. Este análisis debe ser comparado contra el master para identificar las incidencias nuevas creadas en la programación del código fuente.
- Revisar vulnerabilidades de seguridad en el código fuente de las aplicaciones basados en los estándares internacionales OWAS y SANS.
- El contratista habilitará a los 124 usuarios concurrentes en la herramienta, los mismos que contarán con diferentes roles como al menos los siguientes: Administrador, ejecutor y visualizador.
- Tener compatibilidad con los repositorios de código fuente que la Institución utiliza para control de versiones: SVN (Subversion) 1.8.19 y Gitlab Community Edition 15.9.3, con el fin de tener una integración continua que permita enviar el código del ambiente de desarrollo a pruebas y se pueda realizar la validación de código estático en la herramienta.
- El acceso a la herramienta deberá ser a través de LDAP seguro, de tal forma que los usuarios puedan utilizar sus credenciales actuales.
- Contar con reglas de PMD, Checkstyle, Findbugs, Seguridad, Accesibilidad, que puedan ser activadas, desactivadas y personalizadas conforme la institución lo requiera.
- Gobernar los proyectos:
 - **Organizar el Portafolio:** Organizar una amplia gama de aplicaciones y proyectos por jerarquía; estableciendo categorías y definiendo profundidad de estas.
 - **Consolidación de Métricas:** Obtener acceso a la proyección detallada de métricas, las tendencias y los dashboards.
 - **Gestión de Informes:** Generar, exportar y programar informes en formato PDF para garantizar la visibilidad de las métricas claves a todas las partes interesadas. Obtener información rápida y actualizada, sin importar el número de proyectos.

- Integrar la validación de código estático de tal manera que no se pierda las automatizaciones realizadas en ansible para el despliegue de artefactos en los ambientes de prueba
- El contratista debe garantizar el soporte de fábrica de la herramienta 5x8 permitiendo enviar tickets de consultas, problemas durante el tiempo de vigencia del contrato, así como debe velar para que la atención a los tickets abiertos se encuentre dentro del Acuerdo de Nivel de Servicio definido.

IMPLEMENTACION/PRUEBAS/MIGRACION

- El contratista configurará todos los plugins, reglas, plantillas, actualizaciones, parches; para que la herramienta genere los correspondientes reportes referentes a: calidad de código, errores, vulnerabilidades, cobertura, vulnerabilidades en librerías de terceros.
- Se debe implementar un ambiente de pruebas en donde se debe realizar previamente la instalación de la nueva herramienta, y que también sirva para realizar las pruebas de últimas versiones, parches, etc; previo a aplicarlos en ambiente de producción.
- El contratista realizará las configuraciones necesarias para la integración con los repositorios de control de versiones que tiene la Institución; con el fin de que las revisiones de calidad de código se puedan realizar y se generen los reportes correspondientes.
- Configurar o modificar los scripts de automatización de la ejecución de código estático y despliegue en los servidores del ambiente de certificación para la continuidad de las pruebas.
- El contratista realizará todas las configuraciones necesarias en los 53 proyectos migrados de SonarQube, para que los mismos puedan ser evaluados en la nueva herramienta y generar sus correspondientes reportes de la validación de código estático. Contar con una migración transparente de proyectos existentes en la actual herramienta utilizada por la institución, hacia la nueva herramienta.
- El Administrador del contrato realizará en conjunto con un equipo de personas del SRI y el contratista; diversas pruebas de:
 - Acceso a la herramienta.
 - Identificación de roles: Administrador, ejecutor y visualizador, entre otros.
 - Aplicación y uso de la plantilla genérica para ejecución de la validación de código estático.
 - Ejecución de la validación de código estático en proyectos migrados y generación de reportes.
 - Creación de nuevos proyectos, ejecución de validación de código estático y generación de reportes.
- El contratista migrará del ambiente de pruebas a producción, los 53 proyectos antiguos y generará el “Memoria Técnica” de los pasos realizados en la Instalación y Configuración / Pruebas.

- El Administrador del contrato realizará en conjunto con un equipo de personas de la Gestión de Control de Calidad (QA) y el contratista; las mismas pruebas efectuadas en el ambiente de pruebas, pero en ambiente de producción, con el fin de verificar que no exista ninguna incompatibilidad o errores de ejecución.

Requisitos para el servicio de nube:

En el caso que el servicio sea provisto en la nube, debe cumplir con los siguientes requisitos:

SEGURIDAD DE DATOS

- Cifrado en tránsito y en reposo (TLS/SSL, cifrado de disco, etc.).
- La información generada durante la vigencia del contrato será de propiedad del SRI. Al finalizar el servicio, toda la información, incluidos los logs y pistas de auditoría, será entregada al SRI.
- Garantía del fabricante indicando que la información y logs se borraron de la nube permanentemente cuando el servicio terminó.
- Políticas y procedimientos de respaldo y almacenamiento redundante.

LOGS Y PISTAS DE AUDITORÍA

- Registro y gestión de logs y pistas de auditoría, sobre las actividades y transacciones efectuadas dentro del servicio o aplicación.
 - Almacenamiento de los registros de auditoría durante la vigencia del contrato.
- La herramienta debe permitir obtener logs de auditoría de los eventos detectados durante el tiempo de vigencia del contrato. La herramienta debe permitir exportar los logs de auditoría en formatos csv o Excel.

CONTROL DE ACCESO

- Gestión de claves seguras y control de acceso.
- Autenticación fuerte de usuarios (autenticación multifactorial).
- Control de acceso basado en roles y políticas de autorización.
- Auditoría y registro de actividades de usuarios.

SEGURIDAD PERIMETRAL

- Detección y prevención de intrusiones (IPS).
- Firewalls y filtrado de tráfico.
- Protección contra ataques distribuidos (DDoS).
- Protección de capa 7 para aplicaciones mediante firewalls de aplicaciones (WAF).

CONTINUIDAD Y RECUPERACIÓN

- Procedimientos de recuperación ante desastres.
- Una recuperación de datos que asegure la disponibilidad y la integridad de la información en caso de pérdida, borrado o corrupción accidental o maliciosa.

MONITOREO Y DETECCIÓN

- Monitoreo constante de eventos de seguridad y actividad anómala.
- Herramientas de análisis de seguridad y correlación de eventos.
- Automatización que permita detectar y responder a las amenazas en la nube de forma rápida y eficaz.

ACTUALIZACIONES Y PARCHES

- Proceso de gestión de vulnerabilidades.
- Políticas de actualización y aplicación de parches.

SEGREGACIÓN DE DATOS

- Aislamiento lógico de datos entre clientes.

GESTIÓN DE INCIDENTES

- Planes y procesos para la notificación y gestión de incidentes de seguridad.
- Transparencia y auditoría que permita al cliente acceder a los registros e informes sobre las actividades y los incidentes de seguridad que afecten al servicio de nube.

TRANSFERENCIA DE CONOCIMIENTOS

- La transferencia de conocimientos se deberá impartir de acuerdo con el siguiente detalle:

Tiempo	Horas diarias (Máximo)	Número de participantes	Método	Entregable
Mínimo 30 horas	4 horas diarias	Hasta 50 participantes	Presencial con acceso remoto a laboratorio 4 grupos de máximo 15 personas	Certificado de Asistencia

3. GLOSARIO DE TÉRMINOS TÉCNICOS

- **Análisis de Código Estático:** Es el que se realiza sin ejecutar el código, mediante una serie de métodos de análisis que se ejecutan sobre el código fuente de una aplicación para detectar posibles problemas potenciales, previo a la salida a producción del código.
- **Checkstyle:** Revisa la calidad de código, a través del chequeo de la sintaxis del código fuente que ha sido desarrollado, en base a las mejores prácticas y estándares establecidos.

- **Dashboards:** Muestra de manera visual los datos. Es un panel de gestión de datos, que muestra toda la información que se necesita de una manera consolidada, clara y visual.
- **Dependency-check:** Muestra un informe que identifica dependencias vulnerables, junto con sus vulnerabilidades y exposiciones comunes.
- **Findbugs:** Busca y encuentra errores de código, a través de un conjunto de reglas, por ejemplo, encuentra código duplicado entre otros errores.
- **Firewall:** Sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.
- **Gitlab Community Edition:** Es una herramienta que controla las versiones del código fuente. Es una suite completa que gestiona, administra, crea y conecta los repositorios con diferentes aplicaciones y hacer todo tipo de integraciones con ellas.
- **Jboss:** Es un servidor web que facilita a las empresas la gestión y la administración de los entornos web de cualquier tamaño.
- **JDK:** El kit de desarrollo de Java (JDK) es una colección de herramientas de software que se pueden utilizar para desarrollar aplicaciones de Java.
- **Metadata:** Es datos acerca de los datos, consiste en información que caracteriza datos, describe el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos.
- **On-premise:** Es un modelo donde la Infraestructura Informática está localizada y gestionada directamente en las instalaciones físicas de la Institución que contrata este modelo y no en la nube.
- **OWASP:** Proyecto abierto de Seguridad de Aplicaciones Web (Open Web Application Security Project - Estándar de Verificación de Seguridad en Aplicaciones).
- **PMD:** Analizador de código fuente estático de código abierto que informa sobre los problemas encontrados dentro del código fuente de una aplicación. PMD incluye conjuntos de reglas incorporados por defecto y admite la capacidad de escribir reglas personalizadas.

- **Ramas o Branch:** Es una versión específica de código sobre el cual se va a realizar el análisis de código estático, antes de generar la versión definitiva (master).
- **SANS:** SysAdmin, Audit, Network & Security - la fuente más confiable para el entrenamiento, certificación e investigación en el campo de la seguridad de la información.
- **SLAs:** Es un acuerdo a nivel de servicio que establece cómo y en qué condiciones el Contratista proveerá del soporte de la herramienta por 365 días calendario con renovación por un año adicional al Servicio de Rentas Internas.
- **SVN (Subversion):** Es una herramienta que controla las versiones del código fuente. Es decir, maneja ficheros y directorios a través del tiempo. Tiene un árbol de ficheros en un repositorio central.
- **Troubleshooting:** Es el proceso de diagnóstico del origen de un problema. Es usado para solucionar problemas de software y otros muchos productos.
- **WCAG:** Pautas de accesibilidad al contenido web (Web Content Accessibility Guidelines - WCAG) son documentos que explican cómo hacer el contenido Web accesible para personas con discapacidad.

4. PLAZO DE EJECUCIÓN

El plazo total de ejecución del contrato será de hasta 754 días calendario, contados a partir del día siguiente de la suscripción del contrato desglosado de la siguiente manera:

Licenciamiento y soporte de fábrica

- El plazo para la entrega de las suscripciones de software activadas y soporte de fábrica de la Herramienta de Validación de Código Estático para el primer año será de hasta 15 días calendario contados a partir del día siguiente laborable de la suscripción del contrato y su vigencia será de 365 días calendario desde su activación.
- El plazo para la entrega de las suscripciones de software activadas y soporte de fábrica de la Herramienta de Validación de Código Estático para el segundo año será hasta el vencimiento de la vigencia de las suscripciones del primero año, y su vigencia será de 365 días calendario.
- El plazo de entrega del procedimiento de apertura, seguimiento, escalamiento y cierre de casos con el fabricante será de hasta 15 días calendario contados a partir

del día siguiente laborable de la suscripción del contrato.

- El plazo de entrega del informe consolidado de los casos de soporte atendidos será de hasta 10 días calendario después de finalizado cada período de soporte (anual).

Implementación/migración/pruebas

- El plazo de entrega del plan de implementación/migración/pruebas de la Herramienta de Validación de Código Estático será de hasta 15 días calendario contados a partir del día siguiente laborable de la suscripción del contrato.
- El plazo para la implementación/migración/pruebas de la herramienta de Validación de Código Estático será de hasta 45 días calendario contados a partir del día siguiente laborable de la suscripción del contrato.
- El plazo para la entrega de los documentos detallados en la metodología de trabajo relacionados a la implementación/migración/pruebas será de hasta 15 días calendario a partir del siguiente día laborable de la finalización del periodo de implementación, migración y pruebas.

Transferencia de conocimientos

- El plazo para la transferencia de conocimientos de la solución implementada, la entrega de la lista de asistentes y el material con el que se impartió la transferencia de conocimientos será de hasta 15 días calendario contados a partir del día siguiente laborable de la finalización de la implementación/migración/pruebas.

5. FORMA Y CONDICIONES DE PAGO

El Servicio de Rentas Internas pagará al contratista, de la siguiente manera:

SUSCRIPCIONES DE SOFTWARE Y SOPORTE DE FÁBRICA:

- 95% del valor de las suscripciones de software y soporte de fábrica del primer año previa presentación de la planilla de pago y suscripción del acta entrega recepción correspondiente.
- Para la suscripción del acta de entrega recepción correspondiente al primer año de la suscripción de software y soporte de fábrica, el contratista deberá entregar mediante oficio dirigido al administrador del contrato, la documentación que sustente la activación de las suscripciones y soporte de fábrica de la herramienta de Validación de Código Estático y de los componentes necesarios, y se adjuntará:
 - El procedimiento de apertura, seguimiento, escalamiento y cierre de casos con el fabricante.

- 95% del valor de las suscripciones de software y soporte de fábrica del segundo año y previa presentación de la planilla de pago suscripción del acta entrega recepción correspondiente.
- Para la suscripción del acta de entrega recepción correspondiente del segundo año de la suscripción de software y soporte de fábrica, el contratista deberá entregar mediante oficio dirigido al administrador del contrato, la documentación que sustente la activación de las suscripciones y soporte de fábrica de la herramienta de Validación de Código Estático y de los componentes necesarios, y se adjuntará:
 - El informe consolidado de los casos de soporte atendidos en el primer año.
- El 10% del valor de las suscripciones de software y soporte de fábrica al finalizar los 730 días calendario, previa presentación de la planilla de pago y suscripción del acta entrega recepción correspondiente, adjuntando el informe consolidado de los casos de soporte atendidos en el segundo año.

IMPLEMENTACION /MIGRACION Y PRUEBAS / TRANSFERENCIA DE CONOCIMIENTO:

- El 100 % del valor de este rubro se pagará contra entrega, una vez concluidas todas las fases de: implementación, migración, pruebas, transferencia de conocimientos, y previa presentación de la planilla de pago y acta entrega recepción correspondiente.
- Para la suscripción del Acta de Entrega Recepción correspondiente a la Implementación/Migración/Pruebas y Transferencia de conocimientos, el contratista deberá entregar, mediante oficio dirigido al Administrador del Contrato, la siguiente documentación:
 - Documento o comunicación que señale la fecha de finalización de la implementación, migración y pruebas.
 - La memoria técnica de la implementación, migración y pruebas en los ambientes requeridos con el detalle de todas las actividades realizadas y el detalle de los productos implementados.
 - La lista de asistencia a la transferencia de conocimiento debidamente firmada.
 - Plan de continuidad y recuperación de desastres
 - Guía de administración de la solución adquirida, donde se indique al menos los siguientes puntos:
 - Actividades administrativas para ejecutar periódicamente o bajo demanda en la solución.
 - Generación y construcción de reportes.
 - Generación de respaldos de la solución.
 - Modificación de plantillas de notificaciones de correo.
 - Apagado, puesta en marcha y reinicio de la solución.
 - Conciliación de sistemas administrados.

6. LUGAR DE ENTREGA

Para cualquier actividad de coordinación con la Institución debe dirigirse a las oficinas del SRI, Dirección Nacional de Tecnología, Bloque 5 piso 1, Plataforma Gubernamental de Gestión Financiera, Av. Río Amazonas y Alfonso Pereira.