

## **CONSULTA AL MERCADO N°90007426 SISTEMA DE ESCANEO DE VULNERABILIDADES WEB**

### **I. Introducción**

El Banco cuenta con una serie de sitios web públicos incluyendo el sitio web institucional, base de datos estadísticos, repositorios digitales, entre otros. Dada la importancia de la información, es crucial asegurar la integridad y seguridad de estos sitios web.

Por lo antes señalado, el Banco requiere realizar una exploración del mercado para identificar y evaluar plataformas potenciales para apoyar el escaneo de vulnerabilidades web en los sitios públicos del Banco, que permita realizar en ellos análisis exhaustivos y automatizados.

### **II. Objetivo**

El Banco busca soluciones tecnológicas que faciliten la detección, análisis y reporte de vulnerabilidades. La plataforma deseada debe ser capaz de ejecutar escaneos regulares y consistentes sin la necesidad de intervención manual, proporcionando informes detallados y comprensibles que puedan ser utilizados para mejorar las medidas de seguridad.

Para asegurar la efectividad y seguridad de la plataforma de escaneo de vulnerabilidades web que se busca implementar, se consideran importantes las siguientes funcionalidades:

1. La plataforma debe ser accesible y utilizable exclusivamente a través de un navegador web desde la red interna del Banco.
2. Permitir la ejecución automática de escaneos de vulnerabilidades en intervalos regulares o según sea configurado por el usuario, asegurando evaluaciones continuas.
3. Debe permitir seleccionar el tipo o nivel de intensidad del escaneo a realizar.
4. Es esencial que la plataforma incluya mecanismos para evitar bloqueos o dar continuidad al servicio frente a bloqueos gatillados por controles de ciberseguridad implementados en el Banco.
5. La Herramienta debe proporcionar notificaciones y alertas de seguridad en tiempo real.
6. Contar con capacidades de analítica y reportería, permitiendo generar informes detallados y personalizados sobre las vulnerabilidades obtenidas en el último escaneo como en los anteriores.

7. La plataforma debe ser capaz de detectar una gran variedad de vulnerabilidades incluyendo la actualización de vulnerabilidades conocidas e incluir un analizador de alta precisión minimizando al máximo los falsos positivos y falso negativos.

### III. Proceso de Consulta

El presente proceso de consulta se ajustará al siguiente Calendario de Actividades:

ACTIVIDADES	FECHA
Publicación de la Consulta al Mercado	Ju.05.09.2024
Comunicación de Interés de los proveedores en participar de este proceso	Vi.13.09.2024
Recepción de consultas y aclaraciones por parte de proveedores	Ma.24.09.2024
Respuestas a consultas por parte del Banco	Vi.27.09.2024
Presentación de Respuesta al Cuestionario por parte del Proveedor	Vi.11.10.2024
Reunión con proveedores en forma individual	Ma.15 y Mi.16.10.2024
Cierre de la Consulta al Mercado	Mi.23.10.2024

Los proveedores interesados en participar en este proceso de Consulta al Mercado deberán comunicarlo a la Encargada del Proceso de Consulta, Sra. Cecilia Krebs, al correo electrónico [ckrebs@bcentral.cl](mailto:ckrebs@bcentral.cl) con copia al Encargado Técnico, Sr. Fabián Estefanía, al correo electrónico [festefania@bcentral.cl](mailto:festefania@bcentral.cl), indicando en el asunto **INTERÉS EN PARTICIPAR: 90007426 Sistema de Escaneo de Vulnerabilidades Web**, hasta la fecha límite establecida en el Calendario de Actividades.

En caso de que el Proveedor tenga consultas u observaciones respecto de este proceso y su Cuestionario, deberá formularlas en la fecha establecida en el calendario que se adjunta, al correo electrónico: [ckrebs@bcentral.cl](mailto:ckrebs@bcentral.cl) con copia a [festefania@bcentral.cl](mailto:festefania@bcentral.cl), indicando en el asunto **PREGUNTAS: 90007426 Consulta Sistema de Escaneo de Vulnerabilidades Web**, las que serán respondidas a todos los proveedores que hayan manifestado interés en participar, sin indicar el autor de las preguntas u observaciones formuladas.

Posteriormente el Proveedor deberá enviar sus respuestas al Cuestionario detallado en el numeral V de este documento, en la fecha establecida en el Calendario antes señalado, a los siguientes correos electrónicos: [ckrebs@bcentral.cl](mailto:ckrebs@bcentral.cl) con copia [festefania@bcentral.cl](mailto:festefania@bcentral.cl), indicando en el asunto **RESPUESTA: 90007426 Consulta Sistema de Escaneo de Vulnerabilidades Web**.

Una vez recibidas las respuestas al cuestionario, el Banco podrá solicitar mayores antecedentes o aclaraciones a todos o parte de los proveedores, en forma individual.

Una vez evaluadas las respuestas al cuestionario, el Banco podrá requerir individualmente a los proveedores participantes, o parte de ellos, la realización de una reunión, para complementar o aclarar algunos aspectos específicos de los productos y/o servicios informados en sus respuestas, la que será realizada en las fechas indicadas en el Calendario de Actividades, la cual será coordinada oportunamente.

#### **IV. Consideraciones adicionales**

- Se hace presente que este proceso de Consultas al Mercado no constituye una Licitación o Cotización, por lo que los proveedores deben abstenerse de enviar propuestas económicas formales, ya que no está considerada ninguna adjudicación.
- Esta solicitud se efectúa sólo para efectos informativos y no compromete en ningún caso al Banco Central de Chile para adquirir o contratar los Productos y/o Servicios consultados.
- En caso de que el Banco Central de Chile requiera la adquisición o contratación de estos Productos y/o Servicios, se iniciará un Proceso de Licitación o Cotización a través de su Departamento de Adquisiciones, estableciendo las condiciones técnicas, administrativas, legales y económicas, bajo las cuales sería contratada por el Banco la provisión de los Productos y/o Servicios.

#### **V. Cuestionario**

1. En el numeral VI siguiente se solicita la información general de la Empresa respecto de las aplicaciones ofrecidas y sus antecedentes, incluyendo en este último los datos de contacto.
2. Funcionalidades de la plataforma:
  - a) ¿Cuáles son las principales funcionalidades de su plataforma?
  - b) ¿Permite ajustar el nivel de tráfico de red o solicitudes que generará la ejecución del escaneo de vulnerabilidades en los activos seleccionados?
  - c) ¿Permite la ejecución automática de escaneo de vulnerabilidades en intervalos regulares?
  - d) ¿La solución permite rotar un stock de sitios en periodos determinados?
  - e) ¿Existe algún requerimiento técnico que deba cumplir el Banco previo a escanear un sitio web?
  - f) ¿Cuentan con mecanismos para evitar bloqueos o dar continuidad al servicio ante controles de ciberseguridad implementados en el Banco que puedan bloquear el tráfico? Comente al respecto.
  - g) ¿Cómo se visualizan los resultados del escaneo? ¿Incluye detalles sobre la presentación de vulnerabilidades detectadas, su severidad y recomendaciones específicas para su mitigación?

- h) ¿La solución implementa notificaciones y alertas de seguridad?
- i) ¿La solución cuenta con actualizaciones de su base de vulnerabilidades? ¿con cuanta regularidad?
- j) ¿La solución cuenta con perfilamiento y controles de acceso por roles?
- k) ¿La solución cuenta con mecanismos de integración con otras herramientas? Ej: Single Sign-On.
- l) ¿Qué tipo de soporte técnico ofrece la empresa?
- m) ¿Desde donde (lugar geográfico) se realizan los análisis?
- n) ¿La Solución dispone de la capacidad de interrumpir el análisis de manera inmediata?
- o) ¿La solución dispone de asistencia de evaluación de informes y análisis asistida por IA?
- p) ¿La cobertura de la solución permite entre otros cubrir los principales riesgos de seguridad de OWASP?
- q) ¿La solución dispone de resumen de vulnerabilidades con sus niveles de gravedad (puntuación CVSS), junto con recomendaciones de mitigación?
- r) ¿La Solución permite integrar autenticación de dos factores?

## VI. Experiencia y Antecedentes de la Empresa

### 1) Experiencia de la Empresa

Años en el mercado	
Años de Experiencia en servicios/productos similares – Escaneo de vulnerabilidades web	
Número de empleados total	
Número de consultores total	(número - especialidad)
Número de consultores certificados total	(número - especialidad)
Certificaciones de la Empresa, si las tiene	
Indicar representaciones o “ <i>partnership</i> ”, si las tiene	
Indicar alianzas para prestar los servicios consultados (por si no está en condiciones de proveer la totalidad de los módulos o de los servicios en forma autónoma)	

### 2) Clientes de la Empresa en Chile con los módulos de la Aplicación

Clientes activos – Escáner de vulnerabilidades web	(Indicar número y listar los tres principales, especificando modalidad SaaS u On-Premise)
--	---

3) Antecedentes de la empresa

Razón Social:	
RUT:	
Domicilio:	

Contacto Comercial

Nombre:	
Correo electrónico:	
Teléfono móvil:	

Santiago, 5 de septiembre de 2024

Departamento de Adquisiciones  
Gerencia de Gestión Contable y Planificación