PROGRAMA DE DESARROLLO DE SANIDAD AGROPECUARIA - PRODESA: MEJORAMIENTO DEL SERVICIO DE INOCUIDAD AGROALIMENTARIA DEL SENASACONTRATO DE PRESTAMO N° 5941/OC-PE ESPECIFICACIONES TÉCNICAS

ESPECIFICACIONES TÉCNICAS

"ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PARA APLICACIONES WEB"

UNIDAD EJECUTORA	Programa de Desarrollo de Sanidad Agropecuaria - PRODESA: Mejoramiento del Servicio de Inocuidad Agroalimentaria del SENASA
COMPONENTE	Componente 2: Mejora del Control de la inocuidad agroalimentaria
PRODUCTO	Estrategia de fortalecimiento de capacidades de Analítica Avanzada de Datos implementada
ACCIÓN	Gobierno de datos institucional implementado y operando
RESPONSABLE	Ing. Josué Carrasco Valiente
DIRECCIÓN	Dirección de Insumos Agropecuarios e Inocuidad Agroalimentaria
SOLICITANTE	Ing. Ivan Angeles Nuñez
AREA USUARIA	Unidad de Informática y Estadística

1. ANTECEDENTES

Mediante Resolución DE-137/24 el Banco Interamericano de Desarrollo – BID aprueba el Préstamo No 5941/OC-PE a la República del Perú para financiar parcialmente el proyecto de inversión con CUI No 2593747 "Mejoramiento del servicio de inocuidad agroalimentaria del SENASA", tercera operación individual bajo la Línea de Crédito Condicional para Proyectos de Inversión – CCPLIP de Largo Plazo del Servicio Nacional de Sanidad Agraria – SENASA. El 10 de junio del 2025 se suscribió con el Banco Interamericano de Desarrollo - BID el Contrato de Préstamo N°5941/OC-PE para la ejecución del Proyecto "Mejoramiento del servicio de inocuidad agroalimentaria del SENASA" PE-L1280.

2. FINALIDAD PÚBLICA

El SENASA a través del PRODESA ejecuta el "Programa de Desarrollo de Sanidad Agropecuaria", cuyo objetivo es la "Adecuada prestación del servicio de vigilancia y control de la inocuidad agroalimentaria del SENASA". El logro de dicho objetivo contribuirá al "incremento de la competitividad de los productores agropecuarios por cumplimiento de

estándares de inocuidad". El resultado de las actividades implementadas en el proyecto Mejoramiento del servicio de inocuidad agroalimentaria del SENASA, es "contribuir a elevar el desempeño del sistema nacional de inocuidad alimentaria del Perú a través de un abordaje sistémico, preventivo, basado en riesgo y armonizado internacionalmente de las políticas, planes y programas de gestión de inocuidad del SENASA; cuyo propósito es que los productores agropecuarios accedan a la prestación del servicios de vigilancia y control de la inocuidad agroalimentaria del SENASA.

El SENASA desea garantizar la seguridad, continuidad y confianza en los servicios digitales que la Entidad brinda a la ciudadanía, usuarios y actores vinculados, protegiendo las plataformas web institucionales frente a ataques que puedan afectar la prestación de servicios públicos, la transparencia institucional y la adecuada atención a la población.

Con ello se busca fortalecer la ciberseguridad de la Entidad, alineada a las políticas nacionales de transformación digital y protección de la información.

3. OBJETO DE LA CONTRATACIÓN

Adquirir una solución de seguridad para Aplicaciones Web (WAF), que consta de un licenciamiento para el funcionamiento e implementación gestionado, que permita proteger las aplicaciones y servicios web institucionales frente a amenazas, vulnerabilidades y ataques cibernéticos, tales como inyección de código, cross-site scripting (XSS), robo de información sensible, entre otros.

La solución deberá incluir:

- El despliegue inicial en la infraestructura tecnológica de la Entidad (nube).
- La configuración de políticas de seguridad basadas en mejores prácticas y normativas vigentes (ej. OWASP Top 10, ISO 27001).
- La integración con las aplicaciones web institucionales y sistemas relacionados.
- La documentación técnica y operativa del proceso de implementación.
- Servicio de Gestión
- Monitoreo y Soporte especializado

Garantizando la disponibilidad, confidencialidad e integridad de la información tratada en las plataformas web institucionales.

Objetivo específico

Fortalecer la seguridad de las aplicaciones y servicios web institucionales, que permita prevenir, detectar y mitigar de manera oportuna ataques cibernéticos y vulnerabilidades, asegurando la disponibilidad, confidencialidad e integridad de la información, así como la continuidad operativa de las plataformas web institucional.

4. DESCRIPCIÓN DE LOS BIENES

ITEM	UNIDAD DE MEDIDA	DESCRIPCIÓN	CANTIDAD
1	Unidad	ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PARA APLICACIONES WEB	1

5. CARACTERÍSTICAS GENERALES

La solución de seguridad Firewall para Aplicaciones Web (WAF) debe ser brindada o provista en la nube del fabricante.

SOLUCIÓN DE FIREWALL PARA APLICACIONES WEB (WAF)

- La solución deberá soportar por lo menos 40 aplicaciones y un ancho de banda de 50 Mbps. La implementación de la solución deberá requerir únicamente cambiar la configuración de DNS para los Dominios web que apuntan a los Aplicativos Web. Es decir, no requiere la instalación de hardware o software adicional o hacer cambios en la programación de las aplicaciones.
- La solución deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación.
- La solución deberá ofrecer los siguientes servicios en una única plataforma integrada
    - Web Application Firewall WAF
    - Servicio de Proteccion de APIs u Open API a nivel de swagger file o archivo de API.
    - Protección contra Bots
    - Detección de Backdoors en aplicativos Web
    - CDN con failover y redundancia
    - Servicio de Balanceo Global Aplicativo o Load Balancing
    - Almacenamiento en Cache
    - Optimización de Contenido
    - Servicio de Mitigación de ataques DDoS L3/L4/L7
    - Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques.
    - Capacidad de exportar los eventos de seguridad a una herramienta tipo SIEM
- La solución debe detectar ataques aplicativos de seguridad, incluyendo los mencionados en los informes de OWASP como mínimo los siguientes:
    - Injections: SQL, OS and LDAP
    - Cross Site Scripting
    - Cross Site Request Forgery
    - Predictable Resource Location
    - Remote File inclusions
    - Brute Force Attacks
    - Buffer overflow
    - Information leakage
    - Anti Scrapping
- La solución debe poder comunicar eventos mediante envío de correos de alertas a los destinatarios definidos mediante configuración.
- La solución debe informar y alertar los ataques hacia los aplicativos, pudiendo definir

por política para cada aplicación, qué acciones tomar ante dichos eventos (ejemplo: bloquear el request individual, sólo alertar, bloquear la IP, etc.)

- La solución debe proteger contra ataques de día cero y refinarse continuamente conforme cambie la aplicación o los parámetros de uso de esta., sin impacto de falsos positivos.
- La solución debe permitir la configuración del bloqueo de tráfico proveniente de anonymous proxies hacia las aplicaciones desde el portal de servicios
- La solución debe tener protecciones agnósticas a la dirección IP para validar los origines del tráfico y proteger contra bots avanzados tales como: Web Scraping, Web Application DDoS, ataques de fuerza bruta con IP dinámicas.
- Una vez configurada, la solución tendrá la opción de deshabilitarse/habilitarse sin tener que hacer cambios en la Aplicación o DNS. Sin afectar el servicio a los usuarios.
- La solución de Firewall de Aplicaciones Web en la nube deberá garantizar un SLA del 99.99%
- La solución y/o fabricante deberá contar con la certificación "SOC 2" Tipo II
- Como respuesta a un ataque, deberá ofrecer la opción de únicamente alertar o de bloquear al usuario o la dirección IP origen por un periodo de tiempo.
- Deberá permitir la creación de reglas personalizadas basadas en al menos URL, tasa de peticiones, existencia de algún parámetro o header HTTP, si el cliente es humano o bot, y el contenido del header REFERER.
- La solución debe ser soportada en una CDN (Content Delivery Network)
- La solución debe ubicarse por 3 años consecutivos en los informes de Gartner para las soluciones de Web Application Firewall y/o Web Application and API Protection (WAAP).
- La solución deberá permitir la creación de políticas de seguridad personalizadas, mediante la configuración de una variedad de factores que las desencadenen, además de tener múltiples acciones como bloquear Usuario, Bloquear petición, Bloquear Usuario o poner en cuarenta la URL.
- La solución deberá entregar un análisis detallado de las amenazas, incluyendo:
  - Dirección IP
  - User Agent
  - Locación geográfica
  - Información relevante de la sesión
- La solución deberá contar con un mecanismo de perfilado, dicho mecanismo debe diferenciar entre usuarios humanos, bots legítimos (google, bing) y robots maliciosos como gusanos.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
- La solución deberá contar con una clasificación de bots basada en reputación y/o Machine Learning para la distinción de Bots buenos, malos y sospechosos. Permitiendo el bloqueo de ataques como comment spam, scraping y escaneo de vulnerabilidades, y asegurando el acceso de bots como Google, Facebook y otros.

- La solución deberá detectar y bloquear los intentos de instalar y/o operar backdoors en los Aplicativos Web a través de Sandboxing.
- La solución deberá hacer bloqueos a partir del País de Origen (GeoBlocking)
- La solución deberá contar con un sistema de Seguridad Colaborativa para evitar ataques que han sufrido otros sitios web. (Crowdsourcing y/o nube del fabricante)
- La solución debe detectar y proteger contra amenazas de robo de cuentas.
- La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante.
- La solución debe hacer análisis de los ataques, agregando eventos y alertas individuales en incidentes o "narrativas" de ataques y amenazas, incluyendo detalles útiles para el análisis de los ataques dirigidos, por ejemplo:
  - Herramientas utilizadas.
  - Direcciones IP de origen y porcentaje de ataque o nivel de amenaza por cada una.
  - Vectores de ataque.
  - Aplicaciones y recursos atacados.
  - Historial en el tiempo, incluyendo eventos bloqueados y/o alertados.
  - Muestra de eventos.
  - Integración con información de inteligencia (geolocalización, ataques previos a otros Clientes o código CVE, entre otros).
- La solución debe rastrear la URL de autenticación del sitio web e identificar los accesos de los usuarios.
- Deberá incluir un servicio de Inteligencia Artificial y Machine Learning (en la nube de inteligencia y/o en la solución) para la investigación, correlación de eventos de seguridad y alertas originados por el firewall de aplicaciones web independientemente donde resida ya sea en sitio, en la nube o hibrido.
- La solución deberá permitir la creación de reglas personalizadas para reescribir peticiones (URL Rewrite)
- La solución deberá permitir crear reglas personalizadas para agregar/quitar encabezados en los paquetes HTTP, como, por ejemplo, X-Forward-For, País y/o Ciudad y/o Coordenadas de geolocalización y contar con una mayor visibilidad del origen de las conexiones.
- La solución debe contar para los sitios protegidos la capacidad de proteger las APIs asociadas.
- La solución debe permitir proporcionar la seguridad de APIs para el archivo de la misma, generando un modelo positivo automático para la protección de los riesgos de seguridad asociados.
- El aprendizaje, refinamiento constante y creación de la política, debe continuar durante todo el ciclo de vida del servicio, aunque la aplicación se encuentre en modo bloqueo.
- La solución ofertada debe poder acelerar el delivery del contenido de las

aplicaciones.

- La solución ofertada para la protección de aplicaciones en nube debe ser operada 100% desde la nube, mediante portal web proporcionado por el proveedor del servicio.
- Desde el portal se deben visualizar los cambios solicitados por los administradores. El portal debe permitir configurar el envío de alertas, por tipo o nivel de ataques.
- El proveedor deberá brindar un reporte mensual de la actividad del servicio de Firewall de Aplicaciones Web.

6. DE LA IMPLEMENTACIÓN DE LA SOLUCIÓN:

Adquirir la solución de seguridad para aplicaciones web considerando:

- El despliegue inicial en la infraestructura tecnológica de la Entidad (nube).
- La configuración de políticas de seguridad basadas en mejores prácticas y normativas vigentes (ej. OWASP Top 10, ISO 27001).
- La integración con las aplicaciones web institucionales y sistemas relacionados.
- La documentación técnica y operativa del proceso de implementación.

7. PLAZO DE EJECUCION DE LA SOLUCION

El postor, deberá realizar el despliegue y configuración de la solución de seguridad para aplicaciones web en un máximo de treinta (30) días calendario contados a partir del día siguiente de suscrito el contrato.

8. SOPORTE TÉCNICO:

Contratar un soporte y gestión especializada de la solución de seguridad para aplicaciones web, por el periodo de tres (03) años, contado a partir de la conformidad otorgada por la Entidad, que incluya:

- Monitoreo proactivo y permanente de la solución frente a incidentes de seguridad.
- Actualización periódica de firmas y reglas de protección frente a nuevas amenazas.
- Atención de incidentes y consultas 24x7 bajo acuerdos de niveles de servicio (SLA).
- Soporte correctivo y preventivo durante la vigencia del servicio.
- Reportes periódicos (mensuales) de seguridad (eventos detectados, ataques mitigados, disponibilidad del servicio).

Tipo	Descripción de la Falla	Tiempo máximo de respuesta en la atención
Falla Grave	Se deberá cumplir cualquiera de los siguientes puntos: ✓ Interrupción total del servicio o degradación de la solución ofertada.	04 horas
Falla Leve	Se deberá cumplir cualquiera de los siguientes puntos: ✓ Falla en alguna funcionalidad que no afecta ni pone en riesgo la solución ofertada.	08 horas
Requerimiento	Consultas y/o solicitudes de informes o de cambio de configuración.	24 horas

9. PERFIL DEL PERSONAL CLAVE

Se requiere contar con (01) especialista en ciberseguridad que realice la implementación de la solución, de acuerdo a lo indicado en el punto 6, y que cumpla con las siguientes características:

9.1. Formación Académica

Un (01) ESPECIALISTA EN CIBERSEGURIDAD

Profesional titulado en Ingeniería de Sistemas y/o Redes y Comunicaciones y/o Informática y/o Telecomunicaciones y/o Redes y Comunicaciones de Datos.

Debe contar con certificación oficial del fabricante o carta emitida por el fabricante o representante local de la solución WAF que faculte a los profesionales responsables como Especialista en la administración y soporte de la solución ofertada.

9.2. Experiencia Profesional

- Experiencia General: tres (03) años de experiencia laboral en el sector público y/o privado.
- Experiencia Especifica: dos (02) años de experiencia laboral en instalación, configuración y soporte de soluciones de Firewall de Aplicaciones Web (WAF).

10. TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá brindar una transferencia de conocimiento de ocho (08) horas para cinco (05) personas, sobre la arquitectura y administración del equipamiento.

11. GARANTIA

El proveedor deberá entregar una carta de garantía del fabricante o equivalente en la modalidad 24x7, el cual asegure que la solución ofrecida contará con una garantía de funcionamiento y soporte técnico por un periodo no menor de tres (3) años; además de consignar un canal de comunicaciones en el cual se entregue el soporte técnico del producto ofrecido.

12. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

LUGAR:

Sede Central del SENASA, ubicada en la Av. La Molina N°1915 (REF: Puerta N°01 de la Universidad Agraria), de lunes a viernes en el horario de 9:00 a.m. a 13:00 p.m. y desde las 14:00 p.m. a 17:00 p.m.

PLAZO:

Los bienes serán entregados en un plazo máximo de diez (10) días calendario, contados a partir del día siguiente de suscrito el contrato

La implementación de la solución deberá realizarse en un plazo máximo de veinte días (20) calendarios contados a partir del día siguiente de la entrega del total de los bienes en las instalaciones del SENASA.

La vigencia del licenciamiento de la solución será de tres (03) años, contado a partir de la conformidad otorgada por la Entidad.

13. REQUISITOS DE CALIFICACIÓN

El postor debe acreditar un monto facturado acumulado equivalente al valor de su oferta total en la venta de bienes iguales o similares al objeto de la convocatoria, durante los cinco (5) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: Venta de licenciamiento y/o implementación de Equipo de seguridad Firewall y/o Sistema de prevención de intrusos y/o Protección Antimalware y/o Protección URL y/o Sistema Proxy Cache y/o Web Filter y/o Sistema de control de Acceso a la Red y/o Firewall de Aplicaciones Web (WEB).

Acreditación

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra y su respectiva conformidad o constancias de prestación o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes.

14. FORMA DE PAGO:

La Entidad paga las contraprestaciones pactadas a favor del proveedor, dentro de los diez (10) días calendarios siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato u orden de compra para ello, bajo responsabilidad del funcionario competente.

El pago se efectuará en soles, PAGO UNICO; para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Comprobante de pago.
- Carta de garantía del bien.
- Acta de conformidad/Memorándum o equivalente emitida por el área usuaria.

15. CONFORMIDAD

La conformidad será otorgada por el coordinador de programación y seguimiento de la Unidad de gestión del proyecto (UGP), previo informe de opinión favorable de la Unidad de informática y Estadística del SENASA, en un plazo que no excederá de siete (07) días calendario para el trámite de pago; de existir observaciones, la Entidad las

comunica al proveedor, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (08) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar.

Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la Entidad puede otorgar al contratista periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo.

16. PENALIDAD

Penalidades por mora:

Se aplicará al proveedor la penalidad, en caso de retraso injustificado del contratista en la ejecución **de las prestaciones objeto del contrato**, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{Plazo}}$$

Donde F tendrá los siguientes valores:
Para bienes y servicios: F = 0.40

En caso de cubrir el monto máximo de la penalidad, se podrá resolver el contrato por incumplimiento.

17. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo de tres (03) años, contado a partir de la conformidad otorgada por la Entidad.

18. CONFIDENCIALIDAD

El proveedor, guardará, bajo responsabilidad a que hubiere lugar, estricta confidencialidad respecto de la información que recabe con ocasión de las visitas a las instalaciones de la institución, así como de la información que genere, no pudiendo emplear dicha información para un fin distinto al contratado.

SENASA PERU
Firmado digitalmente por ANGELES NUÑEZ Ivan Pavel FAU 20131373075 hard
Motivo: Soy el autor del documento
Fecha: 17.02.2026 12:19:58 -05:00

Firma

SENASA PERU
Firmado digitalmente por CARRASCO VALIENTE Josue Alfonso FAU 20131373075 hard
Motivo: Soy el autor del documento
Fecha: 19.02.2026 15:30:23 -05:00

Firma