Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 466843 - Lp1923-25 Adquisición de Licenciamiento y Soporte de Solución de Ciberseguridad WAAP para Protección contra Ataques en Capa de Aplicación Weben Nube, también conocido como Cloud WAAP (WEB APPLICATION FIREWALL + API PROTECTION + BOT MANAGEMENT)

Consulta 1 - Ratios Financieros

Consulta	Fecha de Consulta	02-09-2025
Contribuyentes de IRE GENERAL: Deberán cumplir con el siguiente parámetro: Donde dice: a.1 Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). a.2. Endeudamiento: pasivo total / activo total No deberá ser mayor a 0,80 en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). Solicitamos: Son criterios que no pueden ser visto de manera aislada, ya que es importante considerar la identificación de los estándares de Endeudamiento del sector en el que se desempeña, así como también las inversiones para desarrollar de nuestro sector. Estos puntos puede ser parámetro importante para determinados tipos de procesos licitatorios que requieren fuertes cantidades de inversión para el inicio de obras. Ante lo mencionado, solicitamos la consideración de modificar el “Ratio de Liquidez mayor o igual a 0,90" y el "Nivel de Endeudamiento No deberá ser mayor a 0,91". Si bien entendemos que los números de ratios financieros, son estándares establecidos por la DNCP, y en varias consultas realizadas a la DNCP nos mencionan que son solo niveles "sugeridos" por la misma y por ende cambiarlos queda a cargo de la convocante. A nuestro criterio, realizar esta modificación dará la oportunidad de participar en esta Licitación a más oferentes, con beneficio directo para la Entidad ya que garantizará la posibilidad de obtener los mejores precios y calidad de servicio.		

Respuesta	Fecha de Respuesta	04-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase al Pliego de Bases y Condiciones.		

Consulta 2 - 1) Datos sensibles / mensajes de error

Consulta	Fecha de Consulta	09-09-2025
Solicitamos a la convocante considerar modificar el requerimiento “Debe incluir una protección que enmascare o bloquee información confidencial proveniente de la aplicación incluyendo mensajes de errores del servidor y número de tarjetas de crédito.” porque al listar “número de tarjetas de crédito” se introduce una categoría específica de datos que puede restringir soluciones equivalentes y mezclar requisitos de DLP con controles de WAAP. Proponemos mantener la exigencia de enmascaramiento/bloqueo de mensajes de error del servidor, sin enumerar tipos de datos particulares, a fin de preservar la neutralidad tecnológica.		

Respuesta	Fecha de Respuesta	25-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.		

Consulta 3 - 2) GraphQL – “importar SDL Schemas”

Consulta	Fecha de Consulta	09-09-2025
Solicitamos a la convocante considerar modificar el requerimiento "La solución debe poseer la capacidad de importar SDL Schemas, para brindar protección para APIs que empleen GRAPHQL." porque exigir importación de esquemas obliga a un enfoque técnico específico y excluye mecanismos de protección equivalentes. Sugerimos admitir alternativas funcionales de protección de GraphQL (p. ej., validaciones de consulta por profundidad, tamaño, etc.) sin condicionar la solución a la importación de SDL.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 4 - 3) Schema Enforcement (formatos)

Consulta	Fecha de Consulta	09-09-2025
Solicitamos a la convocante considerar modificar el requerimiento "La solución debe realizar Schema Enforcement en XML y JSON validando el método, endpoint, query parameters, header parameters, cookie parameters y body parameters." porque limitarlo a XML y JSON descarta implementaciones modernas que emplean otros formatos. Pedimos flexibilizar el requisito para mantener JSON y admitir al menos uno entre XML o YAML, preservando la validación de método, endpoint y parámetros.		

Respuesta	Fecha de Respuesta	25-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.		

Consulta 5 - 4) Portal de gestión – métricas mostradas

Consulta	Fecha de Consulta	09-09-2025
Solicitamos a la convocante considerar modificar el requerimiento **"El portal debe mostrar como mínimo la siguiente información relacionada con el plan adquirido: Número de aplicaciones adquiridas / número de aplicaciones aprovisionadas Ancho de banda adquirido / ancho de banda promedio / ancho de banda pico Periodo de Subscripción. Servicios adicionales contratados."** porque centrarse en “plan” y “ancho de banda” puede no reflejar métricas operativas clave de todos los fabricantes. Solicitamos que el portal reporte indicadores del servicio efectivamente prestado (por ejemplo, aplicaciones/subdominios protegidos, volumen de tráfico inspeccionado y solicitudes procesadas, periodo de suscripción y funcionalidades activas), manteniendo trazabilidad y transparencia.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 6 - 5) Notificaciones ante falla de servidores de origen

Consulta	Fecha de Consulta	09-09-2025

Solicitamos a la convocante considerar modificar el requerimiento “El servicio deberá permitir crear notificaciones que puedan ser enviadas por correo o SMS en caso de falla de alguno de los Servidores de origen.” porque exigir SMS como canal obligatorio limita integraciones operativas modernas y puede excluir soluciones equivalentes. Proponemos que se admitan canales configurables (p. ej., correo electrónico y webhooks HTTP, entre otros), manteniendo la capacidad de alertamiento sin imponer un medio específico.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 7 - 6) Servicio administrado por el fabricante (7x24x365)

Consulta	Fecha de Consulta	09-09-2025

"Solicitamos a la convocante considerar modificar el requerimiento “La solución debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365” porque condiciona el modelo de implementación y no contempla la experiencia del adjudicatario en implementaciones similares. Proponemos que:

La implementación sea responsabilidad del proveedor adjudicado, en coordinación con el cliente, respaldada por experiencia comprobable (referencias o certificaciones de implementaciones exitosas previas de alcance y complejidad similares).

La administración y operación 7x24x365 puedan ser realizadas por el proveedor y/o por el cliente, según el SLA definido en el contrato."

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 8 - 7) Implementación y materiales del fabricante

Consulta	Fecha de Consulta	09-09-2025

Solicitamos a la convocante considerar modificar el requerimiento "El servicio administrado debe proporcionar asistencia durante la fase de implementación de las aplicaciones por parte del fabricante.
El proveedor deberá dar acceso web y/o entregar los manuales de uso u otros materiales requeridos para la utilización del software adquirido."
porque asigna la implementación al fabricante y puede limitar la competencia. Solicitamos aclarar que la implementación será responsabilidad del proveedor adjudicado, en coordinación con el cliente, incluyendo transferencia de conocimiento y provisión de documentación/acceso web necesarios.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se aclara que la implementación será responsabilidad del proveedor adjudicado con asistencia del fabricante, en coordinación con el cliente, incluyendo transferencia de conocimiento y provisión de documentación/acceso web necesarios.

Consulta 9 - 8) Estándares y certificaciones

Consulta	Fecha de Consulta	09-09-2025

Solicitamos a la convocante considerar modificar el requerimiento **"El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad:

ISO/IEC 27001:2013 (Information Security Management Systems).

ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)

ISO 27017:2015 (Information Security for Cloud Services)

ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds)"**
porque incluye versiones desactualizadas y omite marcos de privacidad/controles relevantes. Solicitamos actualizar a las revisiones vigentes y admitir certificaciones complementarias de privacidad y controles de servicio (p. ej., ISO/IEC 27701, revisiones 2019/2022 donde corresponda, y SOC 2 Type II), manteniendo equivalencias verificables.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 10 - 9) Modelo de integración “basado en API, sin cambios de DNS o BGP”

Consulta	Fecha de Consulta	09-09-2025

Solicitamos a la convocante considerar modificar el requerimiento:

**"La solución debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente con las siguientes características:
En la arquitectura basada en API no se requiere compartir el certificado digital.
En la arquitectura basada en API los requerimientos van directamente a la aplicación."**

Dado que se enfoca únicamente en el patrón de integración y no incorpora atributos críticos de una solución WAAP en la nube, tales como disponibilidad del servicio, presencia regional (PoPs) y mecanismos de continuidad operativa ante la caída de un punto de presencia.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene el requisito de integración basada en API sin cambios de DNS/BGP, por ser un modelo seguro y eficiente.

Consulta 11 - 10) Volumen de tráfico (TB/mes)

Consulta	Fecha de Consulta	09-09-2025

Solicitamos a la convocante precisar el volumen mensual estimado de tráfico HTTP/HTTPS a proteger (TB/mes), con promedio y picos. Esta métrica impacta directamente en el dimensionamiento y licenciamiento de la plataforma WAAP.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: El tráfico aproximado seria de ±10 Gbps/mes

Consulta 12 - 11) Métrica de solicitudes (requests)

Consulta	Fecha de Consulta	09-09-2025
Solicitamos el total de solicitudes mensuales y los picos de RPS (tanto global como por aplicación). Esta información es crucial, ya que ciertos módulos, como la gestión de bots y la limitación de tasas (rate limiting), se licencian por volumen de solicitudes o picos de RPS.		

Respuesta	Fecha de Respuesta	25-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: La cantidad aproximada de solicitudes mensuales global seria de ±25.000.000		

Consulta 13 - 12) Distribución de políticas

Consulta	Fecha de Consulta	09-09-2025
“El portal de servicios debe permitir la distribución de una política de seguridad de una aplicación a otra permitiendo configurar la distribución de forma periódica.” Solicitamos a la convocante modificar el texto, ya que la exigencia de que la distribución sea de forma “periódica” presupone un mecanismo de programación automática en el portal que no es necesario en todos los fabricantes o no están disponibles, lo cual limita la participación de más oferentes.		

Respuesta	Fecha de Respuesta	25-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.		

Consulta 14 - 13) Nivel de Partner

Consulta	Fecha de Consulta	09-09-2025
Solicitamos a la convocante modificar el requerimiento “Debido a la criticidad del servicio, el proveedor local deberá contar con el mayor nivel de certificación/partnership de la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.” Solicitamos a la convocante modificar este requerimiento, ya que condicionar la calificación del proveedor local al “mayor nivel de partnership” responde principalmente a criterios comerciales y no necesariamente refleja la capacidad técnica ni la calidad del servicio que se prestará al cliente. Lo que mejor asegura la calidad de un proveedor es su experiencia real en proyectos críticos y el nivel de certificación técnica de su personal y del proveedor.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 15 - 14) Certificación Técnica

Consulta	Fecha de Consulta	09-09-2025
Solicitamos que el requerimiento “El proveedor local deberá contar como mínimo con 2 técnicos certificados con las certificaciones del producto vigente a la fecha de apertura de ofertas” Solicitamos a la convocante modificar este requerimiento, ya que contar únicamente con 2 técnicos certificados resulta insuficiente para un servicio que debe brindarse 24x7x365. Ante permisos, turnos rotativos o indisponibilidades, se pone en riesgo el tiempo de respuesta.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 16 - Requerimientos Experiencia

Consulta	Fecha de Consulta	09-09-2025
se solicita: El proveedor debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a desarrollo, mantenimiento y/o implementación de software, comprobable con en el objeto de su Constitución o Constancia de RUC. Experiencia mínima de tres (3) años (2022, 2023 y 2024) demostrable en el rubro de software orientado a la ciberseguridad, específicamente trabajos relacionados al objeto de la contratación. Presentar diez (10) referencias verificables, cumpliendo con lo siguiente: 1. Cada referencia deberá corresponder a trabajos relacionados a desarrollo, implementación y/o actualización de software relacionados al objeto de la contratación (pudiendo ser en el marco de la provisión de otros bienes o servicios TIC, pero demostrable en cada caso). 2. Constancias, facturas y/o contratos emitidos por entidades privadas, públicas y/o mixtas de al menos tres (3) provisiones, instalaciones y/o actualizaciones relacionados al objeto de la contratación en infraestructuras dentro del territorio nacional, 3. Cumplir al menos uno de los siguientes requisitos: a) La sumatoria de referencias representa mínimo el sesenta por ciento (60%) del monto referencial de la contratación. b) Una referencia individual representa al menos el cuarenta por ciento (40%) del monto referencial. La Convocante sumará el monto indicado en cada documento para verificar el cumplimiento de este requisito. La evaluación se realizará aplicando el sistema CUMPLE o NO CUMPLE. Consulta1: en el punto 1 es que solicitan 10 referencias verificables, pero el punto 2 solicitan 3 constancias, estas ultimas 3 constancias forman parte de las 10 referencias verificables? Consulta 2: Cuando mencionan relacionados al objeto de la contratación ¿a que hacen referencia?		

Respuesta	Fecha de Respuesta	25-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Consulta 1: Las 3 constancias forman parte de las 10 referencias verificables. Consulta 2: "Relacionados al objeto de la contratación" se refiere a trabajos de desarrollo, implementación y/o actualización de software de ciberseguridad		

Consulta 17 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
2 La solución debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente con las siguientes características:
- En la arquitectura basada en API no se requiere compartir el certificado digital.
- En la arquitectura basada en API los requerimientos van directamente a la aplicación.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que:
No es requisito de seguridad indispensable
Limita la concurrencia de oferentes: Exigir obligatoriamente un modelo API restringe innecesariamente la participación de proveedores.Algunas marcas líderes (Fortinet, Palo Alto, F5, Check Point, Radware, etc.) ofrecen mecanismos equivalentes que no requieren, y al imponerlo como requisito obligatorio se descartan soluciones robustas y probadas.
Interoperabilidad y flexibilidad: Al dejarlo como opcional, se permite que el oferente proponga la arquitectura más adecuada (API o tradicional) de acuerdo con la infraestructura existente del cliente.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 18 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
16 La solución debe proveer una página de bloqueo por defecto la cual es mostrada a usuarios identificados como atacantes que intentan acceder la aplicación, debe permitir también la opción de personalizar la página de bloqueo por medio de redireccionamiento a un sitio web específico.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que se trata de una característica cosmética o de conveniencia operativa, no un requisito esencial de seguridad.
La funcionalidad de mostrar o personalizar una página de bloqueo no es indispensable para la protección de aplicaciones.
El objetivo de seguridad (bloquear al atacante) se cumple igualmente con un simple rechazo de conexión o código de error estándar.
De esta manera se garantiza seguridad efectiva, sin limitar innecesariamente la concurrencia de oferentes

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 19 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
23 La solución debe contar con un mecanismo que permita visualizar los subdominios y/o URLs que invocan los scripts de java (JS) desde el navegador de los usuarios que consumen las aplicaciones, así como el nivel de amenaza de los mismos y si es que estos cuentan o no con certificados de seguridad.
Solicitamos amablemente este requerimiento pueda contemplar alternativas de soluciones como HTTP Header Protection, CSRF Protection, MiTB Defense, Cookie Security y Bot Mitigation.
El objetivo principal del requerimiento es proteger la integridad de las aplicaciones frente a amenazas en el navegador del usuario y la ejecución de scripts externos.
Los mecanismos mencionados (HTTP headers, CSRF, MiTB Defense, Cookie Security, Bot Mitigation) cumplen la misma función de prevención de explotación de scripts, robo de datos o manipulación del navegador.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 20 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
24 La protección del lado del cliente debe proveer el descubrimiento y monitoreo continuo de todos los servicios de terceros, incluyendo un seguimiento detallado de las actividades.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que si bien es una funcionalidad interesante, no constituye un requisito de seguridad esencial ni universal en la mayoría de arquitecturas actuales de protección de aplicaciones.
También de esta forma se asegura mayor flexibilidad, más competencia en la licitación y optimización de costos, sin afectar el nivel de seguridad requerido.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene como obligatorio por ser un requisito de seguridad proactiva en entornos cloud.

Consulta 21 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
25 La protección del lado del cliente debe tener como mínimo las siguientes funcionalidades:
- Bloquear automáticamente dominios sospechosos según su nivel de amenaza y permitir dominios legítimos con excepciones.
- Evaluación del nivel de amenazas.
- Notificaciones en tiempo real para cada nuevo descubrimiento y cambios en servicios existentes.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo en el marco de la licitación, la funcionalidad de protección del lado del cliente con bloqueo automático de dominios, evaluación de amenazas y notificaciones en tiempo real constituye un valor agregado en términos de ciberseguridad avanzada, pero no necesariamente una condición indispensable para la correcta operación del servicio solicitado. Convertir este requisito en opcional permitiría ampliar la participación de oferentes que, si bien cumplen con las demás necesidades y requerimientos establecidos en la licitación. De esta manera, se fomenta la competencia

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene como obligatorio por ser una funcionalidad crítica para la defensa contra amenazas modernas.

Consulta 22 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
27 La solución debe poseer la capacidad de importar SDL Schemas, para brindar protección para APIs que empleen GRAPHQL.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que la capacidad de importar SDL Schemas para brindar protección específica a APIs que empleen GraphQL representa una funcionalidad de nicho, ya que este tipo de implementación aún no es predominante en la mayoría de entornos productivos. Existen múltiples mecanismos alternativos de protección a nivel de API (como validación de parámetros, control de acceso y limitación de consultas) que cumplen adecuadamente con las necesidades de seguridad sin requerir necesariamente la importación de dichos esquemas. Por ello, exigir esta característica como obligatoria podría restringir la participación de soluciones técnicamente robustas que, si bien no soportan directamente este requerimiento, ofrecen un nivel de protección equivalente mediante otros enfoques ya validados en la industria.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene como obligatorio para garantizar la protección efectiva de APIs GraphQL.

Consulta 23 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
28 La solución debe soportar descubrimiento de la API a través de machine learning, generando un archivo de OpenAPI.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que el soporte para el descubrimiento de APIs mediante machine learning con generación automática de archivos OpenAPI constituye una funcionalidad avanzada que no resulta imprescindible para garantizar la seguridad ni la operatividad de las interfaces. Existen mecanismos convencionales de documentación y descubrimiento de APIs, tales como el versionado manual de OpenAPI o el uso de herramientas estándar de integración continua, que cumplen con el objetivo de mantener un control adecuado sobre los servicios publicados. Hacer obligatorio este requerimiento implicaría limitar la participación a soluciones que integren técnicas de machine learning, aun cuando otras soluciones con enfoques más tradicionales puedan ofrecer resultados igual de efectivos, auditables y compatibles con estándares de la industria.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene como obligatorio por ser un valor agregado significativo para la gestión moderna de APIs.

Consulta 24 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
53 Desde el portal se deben poder configurar múltiples puertos de servicio para una aplicación o dominio específico, teniendo la posibilidad de configurar los siguientes tipos:
- TCP: Tráfico NO http.
- HTTP: Tráfico HTTP sin encriptación.
- HTTPS: Tráfico HTTP encriptado.
Solicitamos amablemente pueda considerarse como opcional al TCP atendiendo que el soporte para puertos TCP no-HTTP representa un escenario de uso particular que no resulta indispensable para la operación de la mayoría de las aplicaciones y servicios web contemplados en este proyecto. En cambio, los protocolos HTTP y HTTPS cubren de manera completa los requerimientos funcionales y de seguridad necesarios, siendo además los más utilizados y estandarizados en la industria. Por tanto, la exigencia de TCP no-HTTP debería establecerse como opcional, permitiendo que los oferentes puedan cumplir con el objetivo del requerimiento únicamente mediante la configuración de HTTP/HTTPS.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 25 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
54 El servicio debe permitir configurar desde el portal y por cada aplicación chequeos de salud de tipo TCP, HTTP y HTTPS.

Solicitamos amablemente pueda considerarse como opcional al TCP atendiendo que los chequeos de salud en protocolos HTTP y HTTPS son suficientes para garantizar la disponibilidad y correcto funcionamiento de la mayoría de las aplicaciones y servicios que se contemplan en este proyecto, dado que representan los protocolos estándar de comunicación en entornos modernos. La verificación mediante TCP, aunque útil en ciertos casos específicos, no aporta un beneficio sustancial adicional respecto a la supervisión basada en HTTP/HTTPS, ya que estos ya permiten evaluar no solo la conectividad sino también la respuesta lógica de la aplicación. Por ello, se solicita que el chequeo de salud de tipo TCP sea opcional, evitando requerirlo como condición restrictiva cuando los otros dos mecanismos cubren ampliamente las necesidades operativas y de seguridad.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 26 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
67 La solución, a través del portal, y por cada aplicación, debe permitir la creación de reglas para, remover, reescribir e insertar encabezados en el response.
Solicitamos amablemente este requerimiento fuera OPCIONAL atendiendo que la capacidad de remover, reescribir e insertar encabezados en las respuestas a nivel de aplicación es una funcionalidad avanzada que, si bien puede resultar útil en escenarios muy específicos de integración o personalización, no es indispensable para la correcta operación ni para la seguridad de los servicios contemplados en este proyecto. La mayoría de las necesidades de control y gestión de tráfico ya se resuelven mediante configuraciones estándar de HTTP/HTTPS y a través de las propias aplicaciones, sin requerir modificaciones directas de encabezados en el response. Por ello, se considera que este requerimiento debería ser opcional, reconociéndolo como un valor agregado pero no como condición obligatoria y limitante para varios fabricantes del rubro .

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene como obligatorio por ser una funcionalidad útil para personalización y seguridad.

Consulta 27 - EETT

Consulta	Fecha de Consulta	09-09-2025

Donde DICE:
88 El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad:
- ISO/IEC 27001:2013 (Information Security Management Systems).
- ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)
- ISO 27017:2015 (Information Security for Cloud Services)
- ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds)
Solicitamos amablemente aceptar cumplimiento de uno de los requerimientos dejando la solicitud como 27001 y/o 27032 y/o 27017 y/o 27018.
Los estándares ISO/IEC 27001, 27032, 27017 y 27018 corresponden todos al ámbito de la seguridad de la información, la ciberseguridad y la protección de datos en servicios en la nube, pero tienen alcances específicos y en muchos casos complementarios. Exigir el cumplimiento simultáneo de los cuatro introduce una barrera excesiva, dado que cada uno por sí mismo, o en combinación con otro, ya garantiza un marco robusto de seguridad reconocido internacionalmente. Por ejemplo, la certificación ISO 27001 asegura la gestión integral de la seguridad de la información; la ISO 27017 y 27018 extienden controles específicos a entornos cloud y protección de datos personales; y la ISO 27032 aporta lineamientos de ciberseguridad. Por lo tanto, permitir que el oferente acredite al menos una de estas certificaciones —o una combinación parcial— asegura igualmente el cumplimiento de buenas prácticas internacionales sin excluir soluciones técnicamente sólidas.
Donde DICE:
88 El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad:
- ISO/IEC 27001:2013 (Information Security Management Systems).
- ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)
- ISO 27017:2015 (Information Security for Cloud Services)
- ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds)
Solicitamos amablemente aceptar cumplimiento de uno de los requerimientos dejando la solicitud como 27001 y/o 27032 y/o 27017 y/o 27018.
Los estándares ISO/IEC 27001, 27032, 27017 y 27018 corresponden todos al ámbito de la seguridad de la información, la ciberseguridad y la protección de datos en servicios en la nube, pero tienen alcances específicos y en muchos casos complementarios. Exigir el cumplimiento simultáneo de los cuatro introduce una barrera excesiva, dado que cada uno por sí mismo, o en combinación con otro, ya garantiza un marco robusto de seguridad reconocido internacionalmente. Por ejemplo, la certificación ISO 27001 asegura la gestión integral de la seguridad de la información; la ISO 27017 y 27018 extienden controles específicos a entornos cloud y protección de datos personales; y la ISO 27032 aporta lineamientos de ciberseguridad. Por lo tanto, permitir que el oferente acredite al menos una de estas certificaciones —o una combinación parcial— asegura igualmente el cumplimiento de buenas prácticas internacionales sin excluir soluciones técnicamente sólidas.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 28 - EETT - soporte tecnico

Consulta	Fecha de Consulta	09-09-2025

para la solicitud 89 El proveedor de las soluciones ofertadas deberá brindar soporte técnico en sitio y/o remoto, en idioma español, 24/7 con un mínimo de 330 horas garantizadas durante el período de licenciamiento de 36 meses.
Consultamos amablemente de estas 330horas ¿deberán ser consideradas horas de ingenieros del fabricante propuesto? ¿Cuántas horas? Recordamos que se tenga en cuenta que el costo de las horas directamente desde el Fabricante es sustancialmente más elevado que las horas del técnico certificado por el fabricante (que pueda residir localmente) para cumplir este requerimiento. Resulta importante que puedan mencionar si serán necesarios y acotar cuantas horas se asumen para el desarrollo del proyecto.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Las 330 horas garantizadas deben ser proporcionadas por personal técnico certificado por el fabricante, pudiendo ser remoto o local. No se especifica un número fijo de horas de ingenieros del fabricante, pero se debe garantizar la capacidad de respuesta durante la vigencia del contrato.

Consulta 29 - EETT

Consulta	Fecha de Consulta	09-09-2025

para la solicitud 91 El proveedor local deberá contar como mínimo con 2 técnicos certificados con las certificaciones del producto vigente a la fecha de apertura de ofertas
Consultamos amablemente si serán aceptadas certificaciones del fabricante para demostrar la capacidad técnica.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 30 - 15) El Pliego de Bases y Condiciones exige lo siguiente:

Consulta	Fecha de Consulta	09-09-2025

"La solución debe soportar un modelo de integración basado en API que no requiera cambios de DNS o BGP para proteger las aplicaciones y que cuente con las siguientes características:
En la arquitectura basada en API no se requiere compartir el certificado digital.
En la arquitectura basada en API los requerimientos van directamente a la aplicación.”
Al respecto, la redacción actual limita la integración únicamente al modelo API sin cambios de DNS o BGP, lo cual restringe la participación de soluciones disponibles en el mercado que emplean un modelo de protección basado en redireccionamiento de tráfico mediante cambios controlados de DNS. Este enfoque es ampliamente utilizado en arquitecturas WAAP en la nube y habilita atributos críticos como balanceo global, continuidad operativa y resiliencia multi-PoP.
Adicionalmente, consideramos fundamental que la especificación contemple la presencia regional a través de múltiples puntos de presencia (PoPs), incluyendo al menos un PoP local en Paraguay, a fin de garantizar baja latencia, mayor disponibilidad y la posibilidad de desvío automático del tráfico hacia PoPs regionales en caso de fallas. Esta condición asegura que el servicio mantenga su operación aun ante la caída de un PoP específico, reforzando la resiliencia y continuidad de la solución.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 31 - Especificaciones Técnicas: La solución debe incluir protección para 10 aplicaciones como mínimo y con ancho de banda superior a 100 Mbps

Consulta	Fecha de Consulta	09-09-2025

En el PLIEGO DE BASES Y CONDICIONES, en la sección Suministros requeridos – especificaciones técnicas. El item 5 del Detalle de los bienes y/o servicios dice: "La solución debe incluir protección para 10 aplicaciones como mínimo y con ancho de banda superior a 100 Mbps". Solicitamos amablemente a la convocante aclare si las aplicaciones son iguales APIs. Considerando que el pliego también pide protección de APIs.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Las "aplicaciones" están relacionadas a app móvil y aplicaciones web, mientras que las "API's" esta relacionadas a los servicios.

Consulta 32 - Especificaciones Técnicas: La solución debe incluir protección para 10 aplicaciones como mínimo y con ancho de banda superior a 100 Mbps

Consulta	Fecha de Consulta	09-09-2025

En el PLIEGO DE BASES Y CONDICIONES, en la sección Suministros requeridos – especificaciones técnicas. El item 5 del Detalle de los bienes y/o servicios dice: "La solución debe incluir protección para 10 aplicaciones como mínimo y con ancho de banda superior a 100 Mbps". Solicitamos amablemente a la convocante aclare si la solución debe considerarse para hasta 100Mbps. Suponiendo el caso que una oferta sea hasta 101Mbps no será igual a una oferta de 1000Mbps.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 33 - Especificaciones Técnicas: La solución debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365

Consulta	Fecha de Consulta	09-09-2025

En el PLIEGO DE BASES Y CONDICIONES, en la sección Suministros requeridos – especificaciones técnicas. El item 83 del Detalle de los bienes y/o servicios dice: "La solución debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365". Además, en el punto 89 del PBC dice: "El proveedor de las soluciones ofertadas deberá brindar soporte técnico en sitio y/o remoto, en idioma español, 24/7 con un mínimo de 330 horas garantizadas durante el período de licenciamiento de 36 meses ". Solicitamos amablemente a la convocante que especifique la cantidad de horas de soporte del fabricante a considerar para el soporte por 36 meses.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Las 330 horas garantizadas deben ser proporcionadas por personal técnico certificado por el fabricante, pudiendo ser remoto o local. No se especifica un número fijo de horas de ingenieros del fabricante, pero se debe garantizar la capacidad de respuesta durante la vigencia el contrato.

Consulta 34 - Especificaciones Técnicas: El proveedor local deberá tener la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información o equivalente para garantizar y/o proteger la confidencialidad, integridad y disponibilidad de la información de la contratante por parte del soporte local.

Consulta	Fecha de Consulta	09-09-2025

"En el PLIEGO DE BASES Y CONDICIONES, en la sección Suministros requeridos – especificaciones técnicas. El item 94 del Detalle de los bienes y/o servicios dice: ""El proveedor local deberá tener la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información o equivalente para garantizar y/o proteger la confidencialidad, integridad y disponibilidad de la información de la contratante por parte del soporte local"". Y considerando el punto 88 del PBC que dice: ""El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad:
- ISO/IEC 27001:2013 (Information Security
Management Systems)."" Solicitamos amablemente a la convocante que aclare si serán aceptadas certificaciones ISO del fabricante ya que el bien del servicio requerido por la convocante es gestionado en la nube y por el fabricante. Lo solicitado encuentra sustento legal en virtud en lo establecido en el artículo Art. 45 de la Ley N° 7021/22 que dispone: “En los procedimientos de contratación será obligación de las convocantes elaborar las bases y condiciones del llamado con la mayor amplitud de acuerdo con la naturaleza específica del contrato con el objeto de que concurra el mayor número de Oferentes (...), en concordancia con lo establecido en el artículo 58 del nuevo Decreto Reglamentario N° 2264/2024, el cual dispone: “Las especificaciones técnicas que deban contener las bases de la contratación, se establecerán con la mayor amplitud de acuerdo con la naturaleza específica del contrato, con el objeto de que concurra el mayor número de oferentes."

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 35 - Especificaciones Técnicas: Debido a la criticidad del servicio, el proveedor local deberá contar con el mayor nivel de certificación/partnership de la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.

Consulta	Fecha de Consulta	09-09-2025

En el PLIEGO DE BASES Y CONDICIONES, en la sección Suministros requeridos – especificaciones técnicas. El item 94 del Detalle de los bienes y/o servicios dice: "Debido a la criticidad del servicio, el proveedor local deberá contar con el mayor nivel de certificación/partnership de la marca ofertada, para garantizar el buen servicio y respaldo del soporte local". Solicitamos amablemente a la convocante aclare si serán consideradas cartas del fabricante garanizando el nivel de partner.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 36 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025

Buenos días, consultamos a la convocante si, en el punto referido a App Protect Core, 100 Mbps Base Plan, serán igualmente consideradas soluciones que no requieran la definición de un throughput fijo en Mbps, sino que operen bajo un esquema de protección “per application”, lo cual brinda mayor flexibilidad y escalabilidad.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 37 - Especificaciones Técnicas / Punto 92

Consulta	Fecha de Consulta	10-09-2025

En el PBC se solicita: “Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS”.
CONSULTA: solicitamos amablemente a la convocante aceptar también como evidencia documental la copia de contrato laboral con las facturas correspondientes para el personal técnico solicitado, es decir, evidenciadas con los certificados de inscripción en IPS y/o contrato laboral con facturas. La exigencia exclusiva de inscripción en IPS restringe innecesariamente la participación de oferentes que cuentan con personal técnico calificado bajo otras modalidades de contratación legalmente válidas, como los contratos laborales a plazo determinado o los contratos de prestación de servicios profesionales.
Entendemos que la finalidad del requisito es asegurar la disponibilidad real y comprobada de personal idóneo, lo cual igualmente queda garantizado con la propuesta alternativa planteada. Ampliar las formas de evidencia favorece la libre concurrencia y la igualdad de oportunidades entre oferentes, en concordancia con los principios que rigen los procesos de contratación pública.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 38 - Especificaciones Técnicas / Punto 93

Consulta	Fecha de Consulta	10-09-2025

En el PBC se solicita: “Debido a la criticidad del servicio, el proveedor local deberá contar con el mayor nivel de certificación/partnership de la marca ofertada, para garantizar el buen servicio y respaldo del soporte local”.
CONSULTA: se solicita amablemente a la convocante la modificación de esta condición de manera que se acepte la participación de oferentes que cuenten con un nivel intermedio o superior (Gold, Platinum o superior) de partnership con la marca ofertada. Exigir el “mayor nivel de certificación/partnership” limita injustificadamente la competencia, ya que en muchos casos solo un número muy reducido de empresas en el país ostentan dicho nivel. Esta situación puede atentar contra los principios de igualdad, libre competencia y concurrencia, establecidos en la normativa de contrataciones públicas.
Los programas de partnership de fabricantes de soluciones tecnológicas (incluidas WAAP/WAF) suelen estructurarse en niveles (ej. Authorized, Silver, Gold, Platinum, etc.), donde los niveles intermedios ya garantizan:
• Capacitación técnica certificada.
• Acceso a soporte oficial del fabricante.
• Respaldo en actualizaciones, parches y escalamiento de incidentes críticos.
Por tanto, exigir exclusivamente el máximo nivel no agrega un valor diferencial proporcional a la criticidad del servicio, ya que el fabricante brinda el mismo soporte de segundo y tercer nivel a todos sus partners acreditados.
Lo solicitado encuentra sustento legal en virtud de lo establecido en el artículo Art. 45 de la Ley N° 7021/22 que dispone: “En los procedimientos de contratación será obligación de las convocantes elaborar las bases y condiciones del llamado con la mayor amplitud de acuerdo con la naturaleza específica del contrato con el objeto de que concurra el mayor número de Oferentes”.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 39 - Especificaciones Técnicas / Punto 88

Consulta	Fecha de Consulta	10-09-2025

En relación con lo establecido en el Punto 88 de las EETT del PBC, donde se indica que: “El servicio debe contar, como mínimo, con los siguientes estándares de seguridad y calidad:
- ISO/IEC 27001:2013 (Information Security Management Systems).
- ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)
- ISO 27017:2015 (Information Security for Cloud Services)
- ISO 27018:2014 (Information Security Protection of Personally identifiable information (PII) in public clouds)”.
Solicitamos amablemente a la entidad convocante confirmar si nuestra interpretación es correcta: entendemos que la expresión “el servicio” hace referencia al servicio ofrecido por el fabricante de la solución, y que por tanto, no se requiere que el proveedor local cuente directamente con dichas certificaciones, siempre que el servicio proporcionado por el fabricante cumpla con los estándares mencionados.

Respuesta	Fecha de Respuesta	25-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remítase a lo establecido en Adenda Nº:1.

Consulta 40 - Técnicos certificados

Consulta	Fecha de Consulta	10-09-2025

En el punto 91 de las Especificaciones Técnicas del PBC, se requiere contar como mínimo con 2 técnicos certificados.
Se solicita respetuosamente a la convocante aceptar como mínimo 1 técnico certificado para el proveedor local, considerando que en el punto 90 de las EETT ya se exige que el soporte del fabricante de las tecnologías consideradas debe incluir un Responsable de Cuenta Técnica dedicado exclusivamente para ANDE.
La obligación de contar con dos técnicos certificados puede restringir la participación de oferentes, además, ya se requiere que el fabricante de la tecnología incluya un Responsable de Cuenta Técnica (TAM) dedicado exclusivamente para ANDE, lo que asegura la disponibilidad de soporte avanzado, especializado y prioritario. Un técnico certificado local, sumado al Responsable de Cuenta Técnica del fabricante, es suficiente para garantizar la instalación, soporte y mantenimiento adecuados de la solución. Lo requerido es en concordancia con el artículo Art. 45 de la Ley N° 7021/22 que dispone: “En los procedimientos de contratación será obligación de las convocantes elaborar las bases y condiciones del llamado con la mayor amplitud de acuerdo con la naturaleza específica del contrato con el objeto de que concurra el mayor número de Oferentes”.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se mantiene el requerimiento de al menos 2 técnicos certificados por el fabricante, dado el carácter crítico del servicio y la necesidad de garantizar redundancia en la capacidad técnica local.

Consulta 41 - Especificaciones Técnicas / Punto 83

Consulta	Fecha de Consulta	10-09-2025

Donde dice: “La solución debe ser un servicio de seguridad administrado por el fabricante con disponibilidad 7x24x365”.
Consultamos a la convocante si puede ser aceptado que el servicio de seguridad administrado con disponibilidad 7x24x365 pueda ser del oferente y/o fabricante.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 42 - Especificaciones Técnicas / Punto 5

Consulta	Fecha de Consulta	10-09-2025
Donde dice: “La solución debe incluir protección para 10 aplicaciones como mínimo y con ancho de banda superior a 100 Mbps” Solicitamos amablemente a la convocante aclarar si nuestra interpretación es correcta: entendemos que se deben cotizar 10 aplicaciones y que cada una de ellas con un mínimo de 100 Mbps.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: La solución debe incluir protección para al menos 10 aplicaciones, con un ancho de banda mínimo de 100 Mbps en conjunto.		

Consulta 43 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si el requisito de agregar un número limitado de aplicaciones (10 a 19) podrá ser considerado como opcional, y en cambio si serán aceptadas soluciones que permitan crecimiento ilimitado en cantidad de aplicaciones protegidas, siempre dentro de la misma suscripción.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. Se aceptarán soluciones que permitan un crecimiento elástico en el número de aplicaciones protegidas dentro de la misma suscripción, siempre que se cumpla con el mínimo exigido de 10 aplicaciones y el ancho de banda establecido.		

Consulta 44 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Con respecto al módulo de Attack Analytics, consultamos si es posible considerar como alternativa tecnologías que incorporen de forma nativa y centralizada el análisis de amenazas y correlación de eventos, sin requerir módulos adicionales.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 45 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si será aceptada una propuesta que contemple un servicio de protección integral de APIs y aplicaciones web (WAAP) bajo un único licenciamiento unificado, en lugar de la separación en módulos como API Security Add-on, App Protect Core y Attack Analytics.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 46 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos a la convocante si es posible eliminar el requisito del límite de 600 millones de requests anuales, y en su lugar aceptar propuestas que ofrezcan esquemas de requests ilimitados o elásticos, más adecuados para escenarios de crecimiento futuro.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 47 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos a la convocante si es posible eliminar el requisito del límite de 600 millones de requests anuales, y en su lugar aceptar propuestas que ofrezcan esquemas de requests ilimitados o elásticos, más adecuados para escenarios de crecimiento futuro.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 48 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si, en la evaluación técnica, se priorizarán soluciones que cuenten con certificaciones internacionales de ciberseguridad y compliance (ej. ISO 27001, SOC 2, PCI DSS, HIPAA), de manera que se garantice el cumplimiento regulatorio en sectores críticos		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 49 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si serán igualmente aceptadas soluciones que, además de protección WAF y API, incorporen bot management y DDoS protection como parte de la misma suscripción, lo cual permite una cobertura de amenazas más amplia sin necesidad de adquirir módulos adicionales.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Sí, se aceptarán soluciones que incluyan gestión de bots y protección DDoS dentro de la misma suscripción, siempre que cumplan con los requisitos técnicos mínimos establecidos.		

Consulta 50 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025

Buenos días, consultamos si será requisito que la solución incluya un único licenciamiento centralizado (WAAP) que cubra simultáneamente WAF, API Security, Bot Management, DDoS Mitigation y Attack Analytics, en lugar de separar los módulos por SKU, de manera a simplificar la administración y evitar sobrecostos en módulos adicionales.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 51 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025

Consultamos si podrán ser consideradas solamente soluciones que ofrezcan protección nativa contra bots maliciosos y ataques automatizados, sin requerir la adquisición de un módulo aparte.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 52 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025

Con respecto al licenciamiento, consultamos si será requisito que la solución pueda escalar automáticamente en volumen de tráfico (requests) sin límites anuales predefinidos, de manera a garantizar continuidad del servicio sin necesidad de adquirir paquetes adicionales.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Sí, se aceptarán soluciones con escalado automático en volumen de tráfico, siempre que cumplan con los requisitos técnicos mínimos establecidos.

Consulta 53 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025

Consultamos si será condición que la plataforma cuente con un portal de gestión unificado con visibilidad completa de aplicaciones y APIs protegidas, evitando la necesidad de múltiples consolas de administración.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 54 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si será requisito que la plataforma ofrezca protección de APIs mediante descubrimiento automático y clasificación de endpoints expuestos, de manera a cubrir APIs desconocidas o “shadow APIs”.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 55 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si se considerarán válidas únicamente las soluciones que permitan protección híbrida (on-premise y cloud) en un mismo licenciamiento, sin necesidad de contratar productos distintos.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 56 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si será necesario que la solución cuente con certificación PCI DSS nivel 1 para WAF y API Security, considerando que gran parte del tráfico a proteger involucra información sensible.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 57 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	10-09-2025
Consultamos si será condición que la solución cuente con soporte técnico directo 24x7 en idioma español y portugués, garantizando cobertura regional y evitando dependencia de terceros.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 58 - Ratios Financieros

Consulta	Fecha de Consulta	12-09-2025

Contribuyentes de IRE GENERAL: Deberán cumplir con el siguiente parámetro: Donde dice: a.1 Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). a.2. Endeudamiento: pasivo total / activo total No deberá ser mayor a 0,80 en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). Consulta: Hemos analizado con detenimiento los criterios financieros establecidos en los pliegos de esta licitación. Comprendemos la importancia de los indicadores de liquidez y endeudamiento para asegurar la solidez de los oferentes. Sin embargo, queremos proponer una consideración basada en la naturaleza de nuestro sector. Los criterios como el "Ratio de Liquidez mayor o igual a 0,90" y el "Nivel de Endeudamiento No deberá ser mayor a 0,92" podrían no reflejar completamente la realidad de las empresas que requieren de grandes inversiones iniciales para la ejecución de obras.

Nuestra solicitud se fundamenta en los principios establecidos en la Ley N° 7021/2022 "De Suministro y Contrataciones Públicas", que busca la máxima participación de oferentes calificados para obtener las mejores condiciones para el Estado.

Principios Rectores (Art. 5°): La ley se rige por principios como la Competencia, que busca fomentar la participación de la mayor cantidad posible de oferentes calificados; la Eficiencia, que implica el logro de los objetivos con el uso óptimo de los recursos públicos; y el Valor por Dinero, que exige la mejor relación costo-beneficio. La exclusión de empresas solventes debido a criterios financieros excesivamente rígidos limita la competencia y podría privar a la entidad convocante de ofertas más ventajosas.

Capacidad para Contratar (Art. 39): Este artículo establece que para participar en las contrataciones públicas, los oferentes deben contar con la habilitación empresarial y profesional exigible por las leyes. Si bien la entidad puede requerir indicadores financieros, estos deben ser proporcionales y coherentes con la naturaleza del contrato, no convertirse en una barrera de entrada para empresas con capacidad técnica demostrada.

Prohibición de Barreras a la Competencia (Art. 42): La ley prohíbe el establecimiento de requisitos que constituyan un obstáculo desproporcionado a la competencia. Requisitos financieros que no se ajustan a la realidad del sector pueden ser considerados una barrera que limita injustamente la participación, yendo en contra del espíritu de la normativa.

Ajuste del Pliego de Bases y Condiciones (Art. 73): Este artículo permite a la convocante modificar los pliegos antes del plazo de presentación de ofertas, siempre que se garantice que las modificaciones no alteren la igualdad y transparencia del proceso. El ajuste de los ratios financieros es una modificación que busca ampliar la participación sin afectar la calidad, lo que se alinea con el propósito de este artículo.

La Dirección Nacional de Contrataciones Públicas (DNCP), como ente normativo de la ley, promueve una aplicación flexible y razonable de los requisitos, de forma que se fomente una mayor concurrencia. Un enfoque flexible permitirá a su entidad contar con un abanico más amplio de ofertas, lo que se traduce en una mayor competencia, mejores precios y una calidad de servicio superior.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 59 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025

Consultamos si será requisito que la plataforma tenga la capacidad de integrarse con SIEMs y SOARs líderes de la industria de forma nativa (Splunk, QRadar, ArcSight, etc.), sin requerir desarrollos adicionales.

Respuesta	Fecha de Respuesta	17-09-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 60 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025
Consultamos si se valorará de manera prioritaria que la solución ofrezca protección DDoS a nivel L3, L4 y L7 incluida en la misma suscripción, asegurando cobertura total frente a ataques volumétricos y de aplicación		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 61 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025
Consultamos si será requisito que la solución deba incluir de forma nativa un sistema de reputación global de IPs y amenazas basado en inteligencia de más de 1 trillón de transacciones diarias, para garantizar máxima precisión en la detección de ataques.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 62 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025
Buenos días, consultamos si será requisito que la solución WAAP cuente con certificaciones de cumplimiento PCI DSS nivel 1 para entornos financieros y de comercio electrónico, emitidas directamente al fabricante de la solución, y no a través de terceros.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 63 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025
Consultamos si será requisito que la solución WAAP ofrezca de manera nativa un mecanismo de descubrimiento automático de APIs Shadow y huérfanas, con capacidad de generar en tiempo real un archivo OpenAPI actualizado, para prevenir riesgos de APIs no documentadas.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 64 - Consultas sobre las EETT de la Solución de Ciberseguridad WAAP

Consulta	Fecha de Consulta	12-09-2025
Buenos días, consultamos si será requisito que la solución deba contar con un historial comprobado de al menos 3 años consecutivos apareciendo en el cuadrante de Líderes de Gartner para WAAP, garantizando así madurez y continuidad de la tecnología.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.		

Consulta 65 - Solicitud de ampliacion de plazos

Consulta	Fecha de Consulta	16-09-2025
Solicitamos ampliacion de plazos de 10 dias para presentar la oferta, debido a la complejidad y la cantidad de consultas a responder.		

Respuesta	Fecha de Respuesta	17-09-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a los plazos establecidos en el SICP (Sistema de Información de las Contrataciones Públicas).		

Consulta 66 - Plazo de Contratacion

Consulta	Fecha de Consulta	19-09-2025
Favor Indicar claramente en dias, el plazo de contratacion del Servicio Waap. 1) En el PBC en: "DATOS DE LA CONVOCATORIA, item. Tiempo de funcionamiento de los bienes", se indica "No Aplica". 2) Posteriormente en: "CONDICIONES CONTRACTUALES, Item: Periodo de validez de la Garantía de Cumplimiento de Contrato", se indica 2.1) "Plazo de Garantía de los Bienes; Mil noventa y cinco (1095) días corridos", para posteriomente indicar 2.2) "Totalizando la cobertura de dicha garantía ... la vigencia del contrato: Mil doscientos quince (1215) días corridos" a la cual a esta ultima se deberia restar los 30 dias plazo de entrega + más treinta (30) días corridos posteriores al plazo de vigencia, dando 1215-30-30 = 1.115 dias. Por tanto existe una diferencia entre 1.095 dias y 1.115, de 60 dias. Una respuesta clara, ayuda a determinar correctamente el precio a ser ofertado. Gracias		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado. El plazo de contratación del servicio WAAP será de 1.215 días corridos, conforme a lo establecido en las Condiciones Contractuales. Este plazo incluye la vigencia completa del contrato.		

Consulta 67 - Reconsideración Ratios Financieros

Consulta	Fecha de Consulta	22-09-2025

Contribuyentes de IRE GENERAL: Deberán cumplir con el siguiente parámetro: Donde dice: a.1 Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). a.2. Endeudamiento: pasivo total / activo total No deberá ser mayor a 0,80 en promedio, en los 3 (tres) últimos años (2022, 2023 y 2024). Consulta: Hemos analizado con detenimiento los criterios financieros establecidos en el pliego de esta licitación. Comprendemos la importancia de los indicadores de liquidez y endeudamiento para asegurar la solidez de los oferentes. Sin embargo, queremos proponer una consideración basada en la naturaleza de nuestro sector. Los criterios como el "Ratio de Liquidez mayor o igual a 0,90" y el "Nivel de Endeudamiento No deberá ser mayor a 0,92" podrían no reflejar completamente la realidad de las empresas que requieren de grandes inversiones iniciales para la ejecución de obras. En nuestra industria, es habitual que se manejen estándares de endeudamiento distintos, alineados con los altos costos de capital necesarios para iniciar los proyectos. Hemos consultado a la Dirección Nacional de Contrataciones Públicas (DNCP) y nos han confirmado que estos niveles son sugeridos, lo que otorga a la entidad convocante la flexibilidad para ajustarlos según las necesidades específicas del proyecto. Consideramos que adaptar estos criterios no solo permitirá que más empresas calificadas puedan participar, sino que también beneficiará a la entidad. Un mayor número de competidores se traduce en la posibilidad de recibir ofertas más competitivas, asegurando los mejores precios y una calidad de servicio excepcional. Agradecemos de antemano su atención a esta propuesta y esperamos que consideren estas observaciones para enriquecer el proceso de licitación.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en el Pliego de Bases y Condiciones publicado.

Consulta 68 - Sobre Experiencia Requerida

Consulta	Fecha de Consulta	26-09-2025

Se considera para calificar la experiencia del oferentedel, item "Experiencia Requerida (PBC pag.19)", en cuanto a: Certificaciones ISO, Experiencia minima, Referencias verificables y uno de los Requisitos solicitados. Si los partner o representantes locales presentan la documentacion previa del fabricante o compañia internacional requeridos, como asi la cadena de autorizacion del fabricante al parter o representante local autorizado, por supuesto con los Tecnicos Locales Certificados. Considerando que lo solicitado solo puede ser proveido del exterior.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.

Consulta 69 - Planilla de EETT Nº 160525-1, item 8

Consulta	Fecha de Consulta	29-09-2025

En item 8 de las EETT "Las políticas de seguridad deben implementar filtros de seguridad que soporten modelos de seguridad positivos y negativos.". Los modelos de seguridad positivos y negativos, se refieren a lista blancas o negras?, si no es asi a que se refiere ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Sí, se refiere a la capacidad de implementar listas blancas (modelo positivo) y listas negras (modelo negativo) en los filtros de seguridad.

Consulta 71 - Planilla de EETT Nº 160525-1, item 6

Consulta	Fecha de Consulta	29-09-2025
En item 6 de las EETT dice: "La política de seguridad de la solución deberá establecerse a medida y ajustada a cada aplicación. No debe ser genérica, ni basada en políticas por defecto o mejores prácticas.". Consulta indicar las aplicaciones en las que debe personalizarse la politica de seguridad.		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. La política de seguridad debe personalizarse para cada una de las 10 aplicaciones mínimas que serán protegidas por el servicio WAAP.		

Consulta 73 - Planilla de EETT Nº 160525-1, item 14

Consulta	Fecha de Consulta	29-09-2025
En item 14 de las EETT dice: "Debe proveer protección basada en modelos de seguridad positivo que evalúe los requerimientos hacia la aplicación, contra una lista que contenga la URI y métodos permitidos, bloqueando todos aquellos requerimientos que no se encuentren explícitamente definidos." Consulta: Cuando indica "modelo de seguridad positivo", y posteriormente menciona una "lista de URI y metodos permitidos". Se refiere a una lista blanca o positivo indica acciones de seguridad personalizadas que indicará la convocante ?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Correcto, el modelo de seguridad positivo se implementa mediante una lista blanca de URI y métodos permitidos. La convocante proporcionará la lista base durante la implementación.		

Consulta 75 - Planilla de EETT Nº 160525-1, item 16

Consulta	Fecha de Consulta	29-09-2025
En item 16 de las EETT dice: " .... página de bloqueo por defecto la cual es mostrada a usuarios identificados como atacantes que intentan acceder la aplicación, debe permitir también la opción de personalizar la página de bloqueo por medio de redireccionamiento a un sitio web específico". Consulta: Como las amenazas son multiples y variadas, por no decir infinitas, la personalizacion debe realizarse por cada amenaza ?, o se debe hacer por agrupamiento y tipos de amenazas?. Cual es la cantidad maxima de personalizacion de amenazas que se establece ?. En el PBC no se indica.		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. La personalización de la página de bloqueo debe poder realizarse por tipo de amenaza o agrupamiento, sin límite máximo de personalizaciones, siempre que sea configurable desde el portal.		

Consulta 76 - Planilla de EETT Nº 160525-1, item 18

Consulta	Fecha de Consulta	29-09-2025

En item 18 de las EETT dice: "La solución deberá permitir al administrador, crear acciones personalizadas de manera a incorporar patrones específicos que desee tratar como eventos de seguridad". Consulta: como las amenazas pueden ser infinitas, no existentes aán etc. Una vez establecidas las configuraciones dinamicas que provee una solucion con IA. Como se dirime que bloqueo o acciones se realizaran si el administrador incorpora acciones personalizadas que no pueden competir con una IA Global que autoaprende y tiene una mayor Base de Datos, de ataques que ocurren a nivel mundial?. De buena Fe al administrador puede incorporar patrones que contradicen o son mas limitados que una IA. Cual prevalece ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Las acciones personalizadas del administrador prevalecen sobre las acciones automáticas de la IA, según lo permitido en el ítem 18 de las EETT.

Consulta 78 - Planilla de EETT Nº 160525-1, item 20

Consulta	Fecha de Consulta	29-09-2025

En item 20 de las EETT dice: "La solución debe estar basada en una tecnología de WAAP que utilice un modelo de seguridad positivo, que aprenda automáticamente los patrones de actividades legítimas de los usuarios, construya automáticamente políticas de seguridad diseñadas para permitir esas actividades y bloquee cualquier acción que se desvíe de estos patrones de comportamiento legítimo.". A su vez en Item 18 habilita al administrador a crear acciones, idem a consulta 76. Cual prevalece?, lo creado por el administrador o la IA del Waap ?. Indicarlo

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Las configuraciones manuales del administrador (ítem 18) tienen prioridad sobre las políticas automáticas de IA (ítem 20).

Consulta 79 - Planilla de EETT Nº 160525-1, item 21

Consulta	Fecha de Consulta	29-09-2025

En item 21 de las EETT dice: "Debe incluir una protección que enmascare o bloquee información confidencial proveniente de la aplicación.". Consulta: Como se determina que una informacion es confidencial, a fin de que el Waap lo pueda enmascarar?. Por principio todo es confidencial, pero por ejemplo: un reconocimiento a un funcionario, que posteriormente la misma convocante publicita en las redes sociales no es confidencial. Indicar como aplica el criterio.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. La información confidencial será definida por la convocante durante la implementación. El WAAP debe permitir configurar patrones o campos sensibles (ej. datos personales, financieros) para enmascarar o bloquear.

Consulta 81 - Planilla de EETT Nº 160525-1, item 22

Consulta	Fecha de Consulta	29-09-2025

En item 22 de las EETT dice: "La solución debe poseer un mecanismo de Fingerprinting ...". El Navegador Tor impide que se genere una huella digital diferente para cada usuario. Consulta: como debe cubrirse este requisito para el cual es ineficaz el Fingerprinting ?.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. El mecanismo de fingerprinting debe complementarse con otras técnicas de identificación (ej. comportamiento, cookies, headers) cuando el navegador Tor impida la generación de huellas únicas.

Consulta 82 - Planilla de EETT Nº 160525-1, item 15

Consulta	Fecha de Consulta	29-09-2025

En item 15 de las EETT dice: "La solución debe incluir protección basada en inteligencia de amenazas con la posibilidad de activarse o desactivarse y que permita crear excepciones de IP que deban ser excluidas de dichas listas". Los pasos para que la inteligencia de Amenazas sea efectiva son: Descubirmiento, recoleccion y analisis, procesamiento, analisis en profunidad, distribucion dentro de la convocante y retroalimentacion. Consulta 1: La convocante tiene los RRHH para realizar estos pasos para que la inteligencia de amenazas sea efectiva?, o la misma debe ser automatica y provista por el fabricante ?. Consulta 2: Cual es el criterio para activar y sobre todo desactivar esta inteligencia ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. La inteligencia de amenazas debe ser automática y provista por el fabricante. El criterio de activación/desactivación será definido por la convocante según el nivel de riesgo y falsos positivos.

Consulta 84 - Planilla de EETT Nº 160525-1, item 1

Consulta	Fecha de Consulta	30-09-2025

En item 1 de las EETT consulta: a) Se pueden instalar agentes ?, 2) Que se debe considerar ante rollback por errores de propagacion del DNS ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. a) No se requieren agentes según el ítem 1 de las EETT.
b) El proveedor debe garantizar un plan de rollback en caso de fallos en la propagación DNS.

Consulta 86 - Planilla de EETT Nº 160525-1, item 2

Consulta	Fecha de Consulta	30-09-2025

En item 2 de las EETT consulta: 1) se pueden compartir certificados digitales en este modelo?, 2) Los requerimientos van directamente hacia la aplicación sin pasar por intermediarios?, 3) Que medidas de seguridad se deben considerar en este flujo API-directo ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. No se comparten certificados en el modelo basado en API (ítem 2). Las solicitudes van directo a la aplicación. Debe implementarse autenticación, cifrado y monitoreo continuo.

Consulta 88 - Planilla de EETT Nº 160525-1, item 3

Consulta	Fecha de Consulta	30-09-2025

En item 3 de las EETT, consulta: Como se debe tratar las vulnerabilidades nuevas no catalogadas ?

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. La solución debe detectar y bloquear vulneraciones basándose en comportamiento anómalo y aprendizaje automático, no solo en firmas conocidas.

Consulta 89 - Planilla de EETT Nº 160525-1, item 4

Consulta	Fecha de Consulta	30-09-2025
En item 4 de las EETT, consulta: a) Hay algun SIEMs que se deba soporta nativamente (Splunk, Sentinel, QRadar)?, b) Qué protocolos/formato de logs se deben considerar ?, c) Con que qué frecuencia se deben los eventos?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.		

Consulta 91 - Planilla de EETT Nº 160525-1, item 5

Consulta	Fecha de Consulta	30-09-2025
En item 5 de las EETT, consulta: a) Cómo se escala en terminos tecnicos y economicos cuando aumentas las aplicaciones y el ancho de banda requerido no satisface?, b) Existen límites de throughput por aplicación?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.		

Consulta 92 - Planilla de EETT Nº 160525-1, item 6

Consulta	Fecha de Consulta	30-09-2025
En item 6 de las EETT, consulta:a) Qué elementos de la aplicacion se pueden personalizar o estan permitidos (URI, headers, métodos)?, b) Se pueden duplicar políticas entre aplicaciones?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.		

Consulta 93 - Planilla de EETT Nº 160525-1, item 7

Consulta	Fecha de Consulta	30-09-2025
En item 7 de las EETT, consulta: a) Cómo se indica el cambio entre modo activo y monitoreo?, b) Se debe generar un log al respecto ?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. a) El cambio debe poder realizarse desde el portal por aplicación. b) Sí, debe generarse un log de auditoría por cada cambio.		

Consulta 95 - Planilla de EETT Nº 160525-1, item 11

Consulta	Fecha de Consulta	30-09-2025
En item 11 de las EETT, consulta: Para tráfico proveniente de redes TOR, como se requiere evaluar esta trafico ?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.		

Consulta 96 - Planilla de EETT Nº 160525-1, item 17

Consulta	Fecha de Consulta	30-09-2025
En item 17 de las EETT, consulta: a) Cómo se requieren las reglas de rate limiting (por IP, cookie, método, path)?, b) Qué acciones debe ejecutar la regla: bloqueo, alerta, retraso?, c) Cómo se define el tiempo de bloqueo o enfriamiento?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. a) Debe permitir reglas por IP, cookie, método, path. b) Acciones: bloqueo, alerta, retraso. c) Tiempo de bloqueo: configurable por regla.		

Consulta 98 - Planilla de EETT Nº 160525-1, item 19

Consulta	Fecha de Consulta	30-09-2025
En item 19 de las EETT, consulta: a) ¿Qué condiciones deben activan el bloqueo automático (número de intentos, severidad u otro)?, b) Cuánto tiempo debe permanece bloqueada una IP por defecto?, c) Se debe registran los eventos de bloqueo ?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. a) Se activa por número de intentos y severidad. b) Tiempo de bloqueo: configurable. c) Sí, todos los eventos de bloqueo deben registrarse.		

Consulta 99 - Operación y soporte Waap

Consulta	Fecha de Consulta	30-09-2025
Respecto al soporte exigido (24/7 en español, hotline 10 minutos, técnicos certificados), ¿qué nivel de involucramiento esperan del fabricante directamente versus del partner local?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Se espera soporte directo del fabricante para incidencias técnicas graves y del partner local para gestión operativa y comunicación.		

Consulta 100 - Protección de APIs y aplicaciones Waap

Consulta	Fecha de Consulta	30-09-2025
Además de las 10 aplicaciones mínimas, ¿prevén un uso intensivo de APIs (REST/GraphQL) que requiera discovery automático y schema enforcement, o el foco principal estará en aplicaciones web tradicionales?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Se prevé un uso intensivo de APIs REST/GraphQL, por lo que se requiere discovery automático y schema enforcement.		

Consulta 101 - Integracion Waap

Consulta	Fecha de Consulta	30-09-2025
En los requerimientos se menciona tanto la integración vía DNS como la posibilidad opcional de API. ¿Cuál es el método que esperan priorizar en este proyecto?		

Respuesta	Fecha de Respuesta	02-10-2025
Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Se priorizará la integración vía DNS, aunque debe estar disponible la opción basada en API.		

Consulta 102 - Punto 23 (Visualización de subdominios/URLs JS desde el navegador)

Consulta	Fecha de Consulta	30-09-2025

El requerimiento solicitado constituye una funcionalidad muy específica que en la práctica solamente un fabricante ofrece de manera nativa, lo cual limita la concurrencia. Además, la dependencia de visibilidad del lado del navegador introduce riesgos de compatibilidad y sobrecarga en la puesta en producción.
Solicitud: Que este requerimiento sea considerado opcional, admitiendo que el objetivo de seguridad puede cumplirse con mecanismos estándar equivalentes (HTTP Header Protection, CSRF, MiTB Defense, Cookie Security, Bot Mitigation, etc.).

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Los ítems 23, 24, 25, 27, 28 y 67 son obligatorios según las EETT y no pueden ser considerados opcionales. Su cumplimiento es esencial para garantizar la protección integral WAAP solicitada.

Consulta 103 - Puntos 24 y 25 (Protección del lado del cliente – descubrimiento continuo, bloqueo y notificaciones en tiempo real)

Consulta	Fecha de Consulta	30-09-2025

Estas funcionalidades corresponden a capacidades avanzadas y no universales en entornos WAAP. Su exigencia como obligatorias restringe la competencia a un único fabricante, generando un sesgo tecnológico. Además, su despliegue requiere configuraciones complejas que pueden retrasar la puesta en producción y encarecer innecesariamente el servicio.
Solicitud: Que las funcionalidades de los puntos 24 y 25 se consideren opcionales o de valor agregado, de modo que los oferentes que dispongan de ellas puedan presentarlas, pero no excluir a otras soluciones igualmente robustas que cumplen los objetivos principales de protección de aplicaciones y APIs.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Los ítems 23, 24, 25, 27, 28 y 67 son obligatorios según las EETT y no pueden ser considerados opcionales. Su cumplimiento es esencial para garantizar la protección integral WAAP solicitada.

Consulta 104 - Punto 27 (Importación de SDL Schemas para GraphQL)

Consulta	Fecha de Consulta	30-09-2025

La exigencia de importación de SDL Schemas obliga a un enfoque técnico único que no es predominante en la industria, y en la práctica solo un fabricante lo soporta. Existen alternativas reconocidas y equivalentes (validación de consultas por profundidad, tamaño, control de parámetros y rate limiting) que permiten proteger APIs GraphQL sin requerir SDL.
Solicitud: Que este punto sea considerado opcional, permitiendo la acreditación de mecanismos alternativos de protección para GraphQL.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Los ítems 23, 24, 25, 27, 28 y 67 son obligatorios según las EETT y no pueden ser considerados opcionales. Su cumplimiento es esencial para garantizar la protección integral WAAP solicitada.

Consulta 105 - Punto 28 (Descubrimiento de API por machine learning con generación de OpenAPI)

Consulta	Fecha de Consulta	30-09-2025

El soporte obligatorio de machine learning para descubrimiento de APIs constituye una funcionalidad avanzada y de nicho, disponible únicamente en un fabricante. Imponerlo como obligatorio restringe la concurrencia y genera riesgos operativos, ya que estos mecanismos pueden producir falsos positivos/negativos y requerir entrenamiento adicional antes de la puesta en marcha.
Solicitud: Que este punto se establezca como opcional, aceptando mecanismos de descubrimiento convencionales (manuales, CI/CD, integración con repositorios) como alternativa válida.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Los ítems 23, 24, 25, 27, 28 y 67 son obligatorios según las EETT y no pueden ser considerados opcionales. Su cumplimiento es esencial para garantizar la protección integral WAAP solicitada.

Consulta 106 - Punto 67 (Reglas para remover, reescribir e insertar encabezados en el response)

Consulta	Fecha de Consulta	30-09-2025

La capacidad de manipular encabezados de respuesta es una funcionalidad avanzada de integración, no esencial para la seguridad básica. Exigirla como obligatoria restringe la competencia a un número muy limitado de soluciones, y puede generar riesgos de compatibilidad con aplicaciones legadas en producción.
Solicitud: Que este punto se considere opcional, reconociéndolo como un valor agregado pero no como condición excluyente.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Los ítems 23, 24, 25, 27, 28 y 67 son obligatorios según las EETT y no pueden ser considerados opcionales. Su cumplimiento es esencial para garantizar la protección integral WAAP solicitada.

Consulta 107 - Riesgos con mecanismos de seguridad Client-Side

Consulta	Fecha de Consulta	30-09-2025

Cuando se implementan soluciones WAAP con mecanismos de seguridad Client-Side, surgen inconvenientes técnicos y riesgos operativos que deben ser considerados, tales como:
1. Fragmentación de seguridad: integración incompleta entre WAAP y client-side (ej. CSP, reCAPTCHA, JS de protección).
2. Falsos positivos y negativos: headers y payloads no estándar que generan bloqueos indebidos o dejan pasar tráfico malicioso.
3. Dependencia del navegador y dispositivo: fallas en navegadores obsoletos o móviles.
4. Riesgos de manipulación del cliente: atacantes que alteran o deshabilitan scripts client-side.
5. Problemas de rendimiento y experiencia de usuario: mayor latencia y errores en funcionalidades legítimas.
6. Desalineación en actualizaciones: incompatibilidades entre versiones que pueden derivar en vulnerabilidades.
Estos puntos, lejos de mejorar la seguridad, pueden afectar la eficacia, la integración y la experiencia del usuario final, además de generar retrasos y riesgos en la puesta en producción.
Solicitud: Que los requerimientos citados en las consultas 102, 103, 104, 105 y 106 se consideren opcionales, permitiendo que los oferentes puedan presentar soluciones robustas, reconocidas internacionalmente y probadas en entornos críticos, aunque no cuenten con todos estos mecanismos específicos. Esto aumentaría la participación de oferentes, beneficiaría directamente a la entidad convocante con mejores precios y condiciones, y mantendría el nivel de seguridad requerido.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.

Consulta 108 - Especificaciones Técnicas de la Solución de ciberseguridad WAAP para protección contra ataques en capa de aplicación web

Consulta	Fecha de Consulta	01-10-2025

En relación al ítem de especificaciones técnicas obligatorias del llamado sobre “Suscripción de Licencias de Firewall de Aplicaciones Web (WAF)”, específicamente donde se indica:

“El servicio debe contar al menos una combinación de los siguientes estándares de seguridad y calidad o similares:

ISO/IEC 27001:2013

ISO/IEC 27032:2012

ISO/IEC 27017:2015

ISO/IEC 27018:2014”

Solicitamos se aclare lo siguiente:

¿Cuál es la cantidad mínima de certificaciones requeridas para que se considere cumplido este requisito?

¿La combinación puede incluir cualquiera de las certificaciones mencionadas o debe obligatoriamente incluir la ISO/IEC 27001:2013?

¿Se aceptarán certificaciones equivalentes o similares emitidas por organismos internacionales reconocidos, en caso de no contar con todas las certificaciones mencionadas?

¿Las certificaciones deben estar a nombre del fabricante del servicio en la nube, del proveedor local o del producto específico ofertado?

Agradeceremos la aclaración correspondiente para asegurar el cumplimiento cabal de los requisitos exigidos y la correcta preparación de la oferta técnica, conforme los principios de igualdad y libre competencia establecidos en el artículo 4 de la Ley 7021/22.

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1. Las especificaciones no establecen un número mínimo explícito. El requisito (ítem 88) indica que el servicio debe contar con "al menos una combinación" de los estándares mencionados o similares. Se recomienda priorizar la ISO 27001 por ser la base de los sistemas de gestión de seguridad con cualquiera de las demás citadas.

Consulta 109 - Soluciones WAAP

Consulta	Fecha de Consulta	01-10-2025

En relación con los requerimientos técnicos especificados en las consultas N.º 102, 103, 104, 105 y 106, que aluden a la implementación de mecanismos de seguridad del tipo Client-Side en soluciones WAAP, solicitamos se sirvan aclarar si tales requerimientos son de cumplimiento obligatorio o si podrán ser considerados como criterios opcionales o de valoración técnica, permitiendo la presentación de soluciones alternativas con niveles equivalentes o superiores de seguridad.

Motiva esta solicitud el hecho de que la exigencia de funcionalidades Client-Side conlleva riesgos operativos y técnicos que podrían comprometer la eficacia de la solución, entre los cuales se mencionan:

Fragmentación de la arquitectura de seguridad, ante la integración parcial entre los módulos WAAP y los scripts client-side (como CSP, reCAPTCHA o JavaScript propietario).

Aumento de falsos positivos y negativos, derivados del tratamiento de headers y payloads no estándar que pueden bloquear tráfico legítimo o permitir la evasión de controles.

Dependencia tecnológica del navegador o dispositivo del usuario final, lo que podría ocasionar fallos en navegadores desactualizados o plataformas móviles.

Mayor superficie de ataque por la posibilidad de manipulación o desactivación de scripts por parte de atacantes con acceso al entorno del cliente.

Impacto en el rendimiento y la experiencia del usuario, con latencias adicionales y potenciales interrupciones de funcionalidades legítimas.

Problemas de compatibilidad y mantenimiento, especialmente en entornos donde las actualizaciones de scripts y servicios no están sincronizadas.

Dado el carácter restrictivo que implican estos requerimientos y sus potenciales efectos adversos en la operación del servicio, consideramos que su exigencia obligatoria podría limitar injustificadamente la participación de oferentes que cuentan con soluciones robustas, reconocidas internacionalmente y desplegadas en infraestructuras críticas, pero que optan por arquitecturas alternativas server-side o híbridas.

Solicitud específica: se solicita que dichos requerimientos sean considerados como opcionales o bien sujetos a puntaje técnico, de modo a garantizar la pluralidad de ofertas, fomentar la competencia y permitir a la entidad convocante acceder a mejores condiciones técnicas y económicas, sin menoscabar la seguridad requerida. Resguardando los principios de igualdad y libre competencia establecidos en el artículo 4 de la ley 7021/22

Respuesta	Fecha de Respuesta	02-10-2025

Sírvanse considerar para la elaboración de sus ofertas lo siguiente: Remitirse a lo establecido en la ADENDA Nº1.