

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y

ACLARACIONES

LPN N°003-2026-MIDAGRI-SENASA-PRODESA

“ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PARA APLICACIONES WEB”

LICITANTE 1					
N°	PÁGINA DDL	NUMERAL DE LAS EETT	LITERAL O SUB NUMERAL	CONSULTAS Y/O ACLARACIÓN	RESPUESTA
1	49	SECCION II Datos de Licitación IAO 1.1 Objeto e ítem 1	Objeto e ítem 1	Texto relevante: “Adquisición de una Solución de Seguridad para aplicaciones Web”, por una (1) unidad. Fundamento: El objeto comprende licenciamiento en nube, implementación y servicios gestionados por tres años, pero el documento emplea indistintamente reglas de bienes, equipos y servicios. Consulta/solicitud: Confirmar la naturaleza y alcance contractual de cada componente (licenciamiento en nube, implementación, soporte y gestión) y precisar qué reglas y formularios corresponden a cada uno, manteniéndose un único lote.	Se precisa, que la solución integral de seguridad para aplicaciones web, comprendiendo el Licenciamiento, Implementación, soporte técnico y transferencia de conocimientos, establecidos en las EETT, manteniéndose la contratación como un único lote. Para efectos de la presentación de la oferta, cada componente deberá ser considerado en el formulario que corresponda de acuerdo con su naturaleza. Ver Enmienda 1
2	51	SECCION II Datos de Licitación c. Preparación	Documentos técnicos a) y Otros documentos a)	Texto relevante: Se exige dos veces poder o vigencia de poder del representante legal, ambos con antigüedad no mayor de 90 días. Fundamento: La duplicidad puede generar interpretaciones distintas sobre el documento y la	Se confirma, será suficiente la presentación de una sola vigencia de poder o documento equivalente del representante legal, siempre que cumpla con las condiciones y antigüedad máxima de noventa (90) días establecidas en las bases, siendo dicho documento válido para acreditar ambos apartados en los que se

		de las Ofertas IAO 12.(j)		fecha de emisión exigibles. Consulta/solicitud: Confirmar que basta presentar una sola vigencia de poder o documento equivalente, emitido dentro de los 90 días previos a la presentación de ofertas, que cumpla ambos apartados.	solicita.
3	51	SECCION II Datos de Licitación c. Preparación de las Ofertas IAO 12.(j)	Documentos técnicos f)	Texto relevante: Se solicita carta del fabricante sobre stock de repuestos y soporte para los equipos ofrecidos. Fundamento: La solución requerida es provista en la nube y no contempla hardware instalado en la Entidad, por lo que el stock de repuestos podría ser inaplicable. Consulta/solicitud: Confirmar que este requisito no aplica cuando la solución ofertada es íntegramente SaaS/nube y no incluye equipos físicos; en tal caso, permitir una carta de continuidad y soporte del servicio por tres años.	Ver Enmienda 2
4	52 y 60	Sección II Datos de Licitación C. Preparación de las Ofertas IAO 12.1(j) e) y Criterio 5.1(c)	Acreditación técnica	Texto relevante: La página 46 permite brochure, URL, datasheet, documentación técnica o carta del fabricante; la página 54 indica que solo para información no detallada podrá usarse declaración jurada complementaria y que no se aceptará únicamente esta. Fundamento: Debe existir una regla uniforme sobre medios probatorios, especialmente para funciones que los fabricantes no publican en fichas comerciales. Consulta/solicitud: Precisar la prelación y combinación de documentos admitidos. Confirmar que una carta del fabricante o representante autorizado se podrá utilizar para validar el cumplimiento de las características.	Se precisa que, para validar el cumplimiento de las especificaciones técnicas, deberá proporcionar información por medio de BROCHURE, URL, DATASHEET, documentación técnica o carta emitida por el fabricante y/o representante autorizado.

5	52, 74-78 y 131	Sección II Datos de Licitación IAO 15.7; Formularios de precios; CGC 5.2	Incoterm y listas de precios	Texto relevante: Se establece DDP 2020 y se incluyen listas para bienes importados, nacionalizados, fabricados localmente y servicios conexos. Fundamento: Una suscripción cloud no se entrega físicamente ni se importa bajo un Incoterm; la selección incorrecta del formulario puede afectar admisibilidad y comparación económica. Consulta/solicitud: Indicar exactamente qué lista(s) de precios debe completar el oferente para licenciamiento cloud, implementación y soporte, y confirmar si DDP 2020 resulta aplicable o solo referencial para componentes físicos.	Se aclara que, tratándose de una solución de licenciamiento en la nube (SaaS) sin desplazamiento físico de bienes, el Incoterm DDP 2020 previsto en la IAO 15.7 y en la CGC 5.2 resulta únicamente aplicable en el supuesto de que el oferente incluya componentes físicos o bienes importados en su propuesta; para una oferta íntegramente cloud, dicha referencia deviene formal y no aplicable en términos logísticos. <u>El oferente deberá utilizar el Formulario “Lista de Precios: Bienes Fabricados en el País del Comprador”</u> (Sección V, Grupos A y B) para cotizar el licenciamiento/suscripción del software, y el <u>Formulario “Precio y Cronograma de Cumplimiento: Servicios Conexos”</u> para la implementación, el soporte técnico y la transferencia de conocimiento. Ver Pliego de Enmienda 1
6	54	Sección II Datos de Licitación IAO 23.1	Firma de la oferta	Texto relevante: La oferta se remitirá en un único PDF y cada hoja deberá estar firmada por el representante autorizado. Fundamento: No se define si se admite firma digital, firma electrónica, rúbrica o firma manuscrita escaneada, ni cómo tratar páginas de catálogos emitidos por terceros. Consulta/solicitud: Precisar las modalidades de firma válidas y confirmar si la exigencia alcanza absolutamente todas las páginas, incluidos catálogos, estados financieros y documentos de terceros, o únicamente los formularios y documentos elaborados por el oferente.	Se precisa que la modalidad de firma válida para la presentación de la oferta es la firma manuscrita escaneada. Asimismo, se confirma que la exigencia de firma alcanza a todas y cada una de las páginas que conforman la oferta, sin excepción, incluyendo formularios, documentos técnicos y económicos, catálogos, fichas técnicas, estados financieros, certificados, cartas del fabricante y demás documentación que sea incorporada como parte de la oferta, aun cuando haya sido emitida originalmente por terceros.
7	54-55	Sección II Datos de Licitación IAO 23.1 y 26.1	Encriptación y entrega de clave	Texto relevante: La oferta debe estar encriptada con clave en poder del oferente hasta el acto virtual de apertura; no se indica el formato de cifrado ni el mecanismo y momento de entrega de la clave. Fundamento: Una diferencia de software o	Se precisa que la oferta deberá ser remitida en formato PDF, en un único archivo adjunto y protegido mediante contraseña. La contraseña permanecerá en poder exclusivo del oferente hasta el inicio del acto público virtual de apertura, momento en el cual deberá ser proporcionada al comité de

				procedimiento puede impedir abrir una oferta presentada oportunamente. Consulta/solicitud: Precisar formatos de cifrado admitidos (por ejemplo, PDF o archivo comprimido), compatibilidad requerida, canal exacto y momento para comunicar la contraseña, así como el procedimiento ante una falla técnica verificable durante la apertura.	evaluación a través del medio habilitado para dicho acto. El oferente será responsable de verificar que el archivo pueda ser abierto correctamente con la contraseña proporcionada.
8	55	Sección II Datos de Licitación IAO 35.2(a)	Artículo omitido en lista de precios	Texto relevante: Para completar un artículo omitido se menciona el precio “promedio o más alto (según lo especificado en los DDL)”, pero no se selecciona una de las dos opciones y permanece texto entre corchetes. Fundamento: La metodología de evaluación debe ser única y conocida antes de ofertar. Consulta/solicitud: Definir expresamente si se utilizará el precio promedio o el precio más alto y eliminar el texto pendiente de edición, indicando además cómo se aplicará en un lote único compuesto por licencia y servicios.	Se precisa que, en caso de que un artículo o componente no sea incluido en la Lista de Precios y la Oferta cumpla sustancialmente con los requisitos, para efectos de la comparación se calculará el costo total equivalente de la Oferta agregando el precio más alto del artículo o componente omitido, conforme a lo establecido en la IAO 31.3. Dicho precio será determinado a partir de las Ofertas que cumplan sustancialmente con los requisitos. Si no fuera posible determinarlo a partir de dichas Ofertas, el Comprador utilizará su mejor estimación, conforme a la IAO 31.3. Ver Enmienda 3
9	56	Sección II Datos de Licitación IAO 44.1	Variación de cantidades $\pm 20\%$	Texto relevante: La Entidad podrá aumentar o disminuir las cantidades en 20%, pese a que el lote contiene una (1) solución con capacidad y servicios definidos. Fundamento: No se identifica qué unidad medible puede variar ni cómo se reajustaría el precio de una solución integral. Consulta/solicitud: Precisar si esta facultad aplica al proceso y, de aplicar, identificar los componentes cuantificables (aplicaciones, ancho de banda, plazo u otros), sus precios unitarios y la fórmula de ajuste contractual.	Se precisa que la facultad prevista en la IAO 44.1 resulta aplicable al presente proceso. Considerando que el objeto de la contratación corresponde a una (1) solución integral de seguridad para aplicaciones web, la variación de cantidades se aplicará sobre la solución integral como unidad de contratación, y no sobre sus componentes de manera independiente. Ver Enmienda 4
10	59	Sección III Criterios de	Capacidad financiera	Texto relevante: Se requieren estados financieros 2025 y 2024 que demuestren la “solidez actual” del oferente, sin ratios ni valores mínimos.	Ver Enmienda 5

		evaluación y Calificación 5.1(a)		Fundamento: Sin parámetros objetivos, la calificación financiera queda abierta a apreciación discrecional. Consulta/solicitud: Precisar los indicadores, fórmulas, periodos y valores mínimos que se evaluarán, o confirmar que la presentación válida de los estados financieros solicitados será suficiente para cumplir el requisito.	
11	59-60	Sección III Criterios de evaluación y Calificación 5.1(b)	Documentos de experiencia	Texto relevante: La Sección III admite contratos u órdenes de servicios, mientras las EETT califican la prestación como venta de bienes y aluden a contratos u órdenes de compra. Fundamento: La solución combina licencias y servicios, por lo que contratos equivalentes podrían documentarse con cualquiera de ambos tipos de orden. Consulta/solicitud: Confirmar que serán válidos contratos, órdenes de compra u órdenes de servicio, con su conformidad/constancia o comprobante cancelado, siempre que acrediten prestaciones iguales o similares.	Ver Enmienda 6 y 7
12	59-60 y 95	Sección III Criterios de Evaluación y Calificación 5.1(b) y EETT 13	Cómputo y moneda de la experiencia	Texto relevante: Se exige facturación acumulada equivalente a una vez el valor de la oferta durante cinco años, considerando los bienes similares: Venta de licenciamiento y/o implementación de Equipo de seguridad Firewall y/o Sistema de prevención de intrusos y/o Protección Antimalware y/o Protección URL y/o Sistema Proxy Cache y/o Web Filter y/o Sistema de control de Acceso a la Red y/o Firewall de Aplicaciones Web (WEB). Consulta/solicitud: Dado que existen algunas terminologías comerciales referentes a las soluciones, se solicita considerar como bienes similares a los siguientes términos: licenciamiento de la solución waf, licencia de seguridad avanzada detección y	Ver enmiendas 8 y 9

				respuesta antimalware y antiransomware, venta de licencia cloud waf, llicencias de web filtering, adquisicion de licencias de software para los equipos de seguridad perimetral (firewall). Por lo que la redacción de los bienes similares quedarían de la siguiente manera: Venta de licenciamiento y/o implementación de Equipo de seguridad Firewall y/o Sistema de prevención de intrusos y/o Protección Antimalware y/o Protección URL y/o Sistema Proxy Cache y/o Web Filter y/o Sistema de control de Acceso a la Red y/o Firewall de Aplicaciones Web (WEB) y/o licenciamiento de la solución waf y/o licencia de seguridad avanzada detección y respuesta antimalware y antiransomware y/o venta de licencia cloud waf y/o licencias de web filtering y/o adquisición de licencias de software para los equipos de seguridad perimetral (firewall).	
13	84	Sección VI Requisitos de los Bienes y Servicios Conexos	Lugar de destino	Texto relevante: El cuadro remite el lugar de destino al numeral 4 de las EETT, pero dicho numeral describe los bienes y no establece la dirección de entrega. Fundamento: La referencia errónea puede producir ofertas con lugar de ejecución distinto. Consulta/solicitud: Rectificar la referencia y confirmar que el lugar aplicable es el señalado en el numeral 12 de las EETT y en la CGC 1.1(n), precisando además qué entrega física se espera tratándose de una solución en nube.	Se aclara que la referencia al numeral 4 de las EETT corresponde a un error material. El lugar de entrega aplicable es el establecido en el numeral 12 de las EETT y en la CGC 1.1(n), correspondiente al Almacén de PRODESA. Ver Enmienda 10 y 11
14	93	Sección VI. Requisitos de los Bienes y Servicios Conexos	Reporte mensual WAF	Texto relevante: El proveedor debe brindar un reporte mensual de actividad del WAF. Fundamento: No se establecen contenido mínimo, fecha, formato, destinatarios, reunión de revisión ni efecto sobre la conformidad.	Se precisa, que el reporte mensual deberá contener como mínimo información relacionada con la operación del WAF, eventos y ataques identificados, acciones de mitigación, utilización del servicio, incidencias relevantes y recomendaciones de seguridad, el resto será definido

		Punto 5 de EETT		Consulta/solicitud: Definir contenido y métricas mínimas, formato, idioma, plazo mensual de entrega, responsables de recepción.	durante el servicio. La Entidad definirá al inicio del servicio el responsable de recepción y el mecanismo de entrega de los reportes.
15	93-94	Sección VI. Requisitos de los Bienes y Servicios Conexos Punto 7 y 12 de las EETT	Plazos de entrega e implementación	Texto relevante: El numeral 7 fija despliegue y configuración en 30 días desde la suscripción; el numeral 12 fija bienes en 10 días y luego implementación en 20 días desde la entrega total. Fundamento: Aunque ambos pueden sumar 30 días, usan hitos distintos y no precisan dependencias a cargo de la Entidad. Consulta/solicitud: Confirmar el cronograma contractual definitivo, hitos de entrega, inicio y fin de implementación, y suspensión/prórroga por falta de DNS, certificados, accesos, inventario o ventanas de cambio que correspondan a la Entidad.	Ver enmienda 11
16	94	Sección VI. Requisitos de los Bienes y Servicios Conexos Punto 10 de las EETT	Transferencia de conocimiento	Texto relevante: Se requieren ocho horas para cinco personas sobre arquitectura y administración del “equipamiento”. Fundamento: La solución es cloud y faltan modalidad, sesiones, materiales, ambiente, evaluación y constancias. Consulta/solicitud: Confirmar que la referencia correcta es la solución cloud y precisar modalidad presencial/remota, número de sesiones, temario, idioma, materiales, laboratorio y entrega de constancias en caso aplicar.	Se precisa que la transferencia de conocimiento corresponde a la solución cloud objeto de la contratación y no a equipamiento físico. Se mantiene el alcance de ocho (08) horas para cinco (05) personas. La modalidad podrá ser virtual o presencial, la programación y demás aspectos operativos serán coordinados con la Entidad durante la implementación.
17	94	Sección VI. Requisitos de los Bienes y Servicios Conexos Punto	Carta de garantía	Texto relevante: Se requiere carta de garantía del fabricante “o equivalente” 24x7 por no menos de tres años y un canal de soporte. Fundamento: No se define quién puede emitir el equivalente ni si el canal debe ser del fabricante o del contratista. Consulta/solicitud: Precisar que equivalente se	Se precisa que “equivalente” aplica también a partner autorizado.

		11 EETT		refiere a un partner autorizado del fabricante en la solución..	
18	135	Sección IX. Formularios de Contrato CGC 29.3 y 29.5	Garantía y reposición	Texto relevante: La garantía dura 36 meses y la reposición de componentes/equipo debe efectuarse en tres días desde la notificación. Fundamento: La solución es cloud y no contempla componentes físicos en la Entidad, por lo que el remedio puede no ser aplicable a una falla del servicio. Consulta/solicitud: Confirmar que la reposición en tres días aplica solo si se ofertan equipos físicos; para SaaS, sustituirla por tiempos de restauración, continuidad, failover y escalamientos acordes con el SLA de soporte.	Se aclara que la obligación de reposición de componentes o equipos en el plazo establecido no es aplicable. Dado que la solución prestada es íntegramente bajo modalidad SaaS/cloud, serán aplicables los mecanismos de acuerdo con el SLA del soporte técnico.
19	133-134	Sección IX. Formularios de Contrato CGC 19.1 y 19.3	Garantía de cumplimiento	Texto relevante: Se exige fianza de 10% vigente hasta la culminación del contrato, sin aceptar otra modalidad. Fundamento: El contrato comprende tres años de servicio; no se precisa fecha de liberación, renovaciones ni reducción tras implementación. Consulta/solicitud: Definir la fecha exacta de culminación y devolución/liberación, condiciones de renovación y posibilidad de reducción proporcional después de la implementación, manteniendo cobertura sobre obligaciones pendientes.	Ver Enmienda 12
20	85-86	Sección VI. Requisitos de los Bienes y Servicios ConexosEE TT 10	Transferencia de conocimiento	Texto relevante: El contratista deberá brindar una transferencia de conocimiento de ocho (08) horas para cinco(5) personas. Fundamento: Indicar a qué si corresponde al servicio principal o conexo. Consulta/solicitud: Definir a qué servicio corresponde, ya sea "Lista de bienes y	Se aclara que la transferencia de conocimiento corresponde a la Lista de Servicios conexos y cronograma de cumplimiento Lista de Servicios conexos y cronograma de cumplimiento: Implementación Soporte técnico y Transferencia de conocimiento.

				cronograma de entregas” o “Lista de servicios conexos y cronograma de cumplimiento” dado que no se indica donde se debe considerar para la presentación de ofertas.	Ver Enmienda 13
LICITANTE 2					
N°	PÁGINA DDL	NUMERAL DE LAS EETT	LITERAL O SUB NUMERAL	CONSULTAS Y/O ACLARACIÓN	RESPUESTA
21	84	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	05	DICE: La solución de seguridad Firewall para Aplicaciones Web (WAF) debe ser brindada o provista en la nube del fabricante. CONSULTA: Respecto a los Requerimientos Generales de la Solución WAF. Sírvase precisar que la plataforma ofertada deberá permitir la gestión y operación centralizada de las funcionalidades solicitadas mediante una arquitectura unificada y una única consola de administración y API de control, incluyendo como mínimo las capacidades de WAF, Bot Management, Rate Limiting, CDN y protección DDoS, sin requerir la implementación de consolas diferenciadas, módulos externos o licenciamientos independientes para la operación de dichas funcionalidades en entornos on-premises o multicloud. Lo anterior permitirá garantizar una administración integral, simplificar la operación, reducir la complejidad de integración y contar con una visibilidad centralizada de la postura de seguridad de las aplicaciones; exceptuándose de este alcance la funcionalidad de DAST, la cual, por su naturaleza y arquitectura especializada para pruebas dinámicas de seguridad de aplicaciones, podrá ser provista mediante una plataforma o módulo independiente.	Se acoge parcialmente, que las funcionalidades establecidas en las EETT deberán permitir una gestión y operación centralizada y encontrarse debidamente integradas a la solución ofertada. La estructura interna de módulos, licencias o SKU utilizada por cada fabricante no constituye por sí misma una restricción, siempre que la oferta incluya la totalidad de funcionalidades requeridas durante todo el periodo contractual, sin generar costos adicionales para la Entidad. Para el componente DAST se mantiene expresamente lo establecido en las EETT respecto a la posibilidad de utilizar una solución del mismo fabricante o de otro fabricante. En caso de que el componente DAST sea de otro fabricante se debe presentar una carta del fabricante a nombre de la entidad indicando el nombre del producto, tipo de licencia y tiempo de licenciamiento de acuerdo al contrato.

22	84	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución deberá ofrecer los siguientes servicios en una única plataforma integrada: • Web Application Firewall WAF • Servicio de Protección de APIs u Open API a nivel de swagger file o archivo de API. • Protección contra Bots • Detección de Backdoors en aplicativos Web • CDN con failover y redundancia • Servicio de Balanceo Global Aplicativo o Load Balancing • Almacenamiento en Cache • Optimización de Contenido • Servicio de Mitigación de ataques DDoS L3/L4/L7 • Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques. • Capacidad de exportar los eventos de seguridad a una herramienta tipo SIEM. CONSULTA: Con relación con los requerimientos de disponibilidad, rendimiento y protección de la plataforma. Sirvase confirmar que la solución ofertada debe procesar la inspección completa de reglas WAF, mitigación DDoS e inspección de tráfico en un único salto de red (Single-Pass) a través de sus nodos perimetrales distribuidos bajo arquitectura Anycast, evitando redirecciones o desvíos innecesarios del tráfico hacia pods o infraestructura secundaria de inspección. Asimismo, considerar que la plataforma cuenta con una capacidad global de mitigación de ataque DDoS de al menos 300 Tbps a fin de garantizar una capacidad suficiente frente a ataques volumétricos de gran escala.	No se acoge la consulta. Las EETT establecen las capacidades funcionales, de seguridad, disponibilidad y mitigación que deberá proporcionar la solución, sin restringir su implementación a una arquitectura específica de procesamiento o red. En consecuencia, no resulta necesario incorporar como requisitos obligatorios una arquitectura denominada “Single-Pass”, el uso específico de Anycast ni una determinada capacidad global expresada en Tbps. Se mantienen las características y capacidades establecidas en las EETT.
23	84	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución deberá ofrecer los siguientes servicios en una única plataforma integrada: • Detección de Backdoors en aplicativos Web CONSULTA: Teniendo en cuenta que en el presente ítem no se especifica el método tecnológico a utilizar, y considerando que en otro numeral de las EETT	Se precisa que La solución deberá contar con capacidades de Sandboxing que permitan el análisis de archivos, objetos o contenidos potencialmente maliciosos, especialmente aquellos asociados a funcionalidades de carga de archivos (File Upload), con la finalidad de detectar y bloquear comportamientos

				relacionada a backdoors se hace referencia al uso de Sandboxing para la detección de backdoors: Sirvase confirmar que para el cumplimiento del requerimiento de "Detección de Backdoors en aplicativos Web" la solución WAF podrá emplear sus mecanismos nativos de inspección profunda de tráfico Capa 7, reglas de firmas, análisis heurístico, protección de subida de archivos maliciosos (File Upload Protection) y/o motores de Inteligencia de Amenazas, garantizando así la coherencia técnica del requerimiento.	relacionados con malware, web shells o backdoors antes de su procesamiento por los Aplicativos Web Protegidos. El Sandboxing podrá ser una capacidad nativa de la solución WAF o proporcionada mediante una solución o licencia de terceros siempre que se encuentre integrada con el WAF, y permita aplicar las acciones de bloqueo y generar las alertas y registros correspondientes. En caso de que el componente Sandboxing sea de otro fabricante se debe presentar una carta del fabricante a nombre de la entidad indicando el nombre del producto, tipo de licencia y tiempo de licenciamiento de acuerdo al contrato.
24	84	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución debe detectar ataques aplicativos de seguridad, incluyendo los mencionados en los informes de OWASP como mínimo los siguientes: • Information leakage CONSULTA: El TDR plantea la protección contra Information leakage (fuga/exposición de información) y habiendo soluciones que solo se limitan a inspeccionar las peticiones (requests) de entrada sin analizar el contenido saliente (responses). Se solicita a la entidad profundizar en este ítem exigiendo Detección de Datos Sensibles (SDD) y DLP en respuestas HTTP/HTTPS.	Se acoge parcialmente la consulta. Para el cumplimiento de la protección contra Information Leakage, la solución deberá contar con mecanismos que permitan detectar y prevenir la exposición de información sensible en las comunicaciones HTTP/HTTPS, incluyendo las respuestas generadas por los aplicativos cuando corresponda. No será obligatorio que dicha funcionalidad se denomine comercialmente "SDD" o "DLP", pudiendo acreditarse mediante capacidades nativas o equivalentes de protección contra fuga o exposición de información de la solución ofertada.
25	85	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución debe proteger contra ataques de día cero y refinarse continuamente conforme cambie la aplicación o los parámetros de uso de esta., sin impacto de falsos positivos. CONSULTA: Para garantizar la mitigación de amenazas de día cero (Zero-Day), Sirvase confirmar que la solución ofertada deberá incorporar un motor de análisis conductual mediante Machine Learning que asigne puntuaciones de probabilidad de ataque (Attack	No se acoge la consulta. El requerimiento de protección contra amenazas de día cero se mantiene en términos funcionales y no será condicionado a una metodología específica de puntuación, nomenclatura comercial o clasificación independiente de Attack Score para SQLi, XSS y RCE. La solución deberá contar con mecanismos tecnológicos que permitan identificar y mitigar amenazas desconocidas o variantes de ataques, conforme a las capacidades exigidas en las EETT.

				Score) categorizadas independientemente para SQLi, XSS y RCE, evitando depender de firmas estáticas o reputación de IP.	
26	85	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución deberá permitir la creación de políticas de seguridad personalizadas, mediante la configuración de una variedad de factores que las desencadenen, además de tener múltiples acciones como bloquear Usuario, Bloquear petición, Bloquear Usuario o poner en cuarentena la URL. CONSULTA: Se observa una repetición en el enunciado al mencionar dos veces la acción "Bloquear Usuario" y en una de ellas lo coparan con "poner en cuarentena la URL". Se solicita a la Entidad en definir formalmente el alcance operativo de la acción "poner en cuarentena la URL" en el ámbito del CWAF o indicar que es algo opcional, como parece ser pues usan el conector "O".	Se precisa que la repetición de la expresión "Bloquear Usuario" corresponde a un error material. La referencia a "poner en cuarentena la URL" deberá entenderse funcionalmente como la capacidad de restringir, bloquear o impedir temporalmente el acceso a una URL o patrón de URL mediante políticas de seguridad, aceptándose denominaciones funcionalmente equivalentes. Ver Enmienda 14.
27	85	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	Punto 5	DICE: La solución deberá permitir la creación de políticas de seguridad personalizadas, mediante la configuración de una variedad de factores que las desencadenen, además de tener múltiples acciones como bloquear Usuario, Bloquear petición, Bloquear Usuario o poner en cuarentena la URL. CONSULTA: Sirvase precisar cuántas acciones de respuesta como mínimo deben ser soportadas de forma obligatoria por la solución WAF para dar por cumplido el requerimiento, considerando que la redacción menciona explícitamente acciones como "Bloquear petición, Bloquear Usuario"	Se precisa que la solución deberá disponer de múltiples acciones de respuesta y mitigación. Para efectos de cumplimiento, deberá permitir como mínimo acciones como bloquear Usuario, Bloquear petición y poner en cuarentena la URL. Ver enmienda 14
28	86	Sección VI. Requisitos de los Bienes y Servicios.	Punto 5	DICE: La solución deberá detectar y bloquear los intentos de instalar y/o operar backdoors en los Aplicativos Web a través de Sandboxing.	Se aclara , se mantiene el requerimiento de Sandboxing para la detección y bloqueo de intentos de instalación y/o

		3. EETT Punto 5		CONSULTA: Teniendo en cuenta que las soluciones de Cloud WAF previenen y bloquean la instalación y/u operación de backdoors en aplicaciones web mediante inspección profunda de firmas, análisis heurístico, reglas de control de subida de archivos (File Upload Protection) e Inteligencia de Amenazas en tiempo real en la Capa 7. Sirvase precisar que la funcionalidad de Sandboxing para la detección y bloqueo de backdoors sea considerada como opcional o, en su defecto, se acepte el cumplimiento del requerimiento mediante mecanismos equivalentes de inspección profunda de tráfico HTTP/HTTPS, análisis heurístico, protección contra subida de archivos maliciosos (Web Shells/RCE) y/o firmas de seguridad nativas de la solución CWAF.	operación de backdoors o web shells en los Aplicativos Web Protegidos. El requerimiento responde a la necesidad de contar con una capacidad adicional de análisis de contenido potencialmente malicioso, particularmente en funcionalidades de carga de archivos, que permita identificar amenazas que podrían no ser detectadas únicamente mediante firmas, reglas de inspección, análisis heurístico, protección de File Upload o Inteligencia de Amenazas. No obstante, el Sandboxing podrá ser una capacidad nativa del WAF o ser proporcionado mediante una solución, motor o licencia de terceros, siempre que se encuentre integrada con la solución WAF y permita realizar el análisis, aplicar las acciones de bloqueo correspondientes y generar las alertas y registros respectivos. En caso de que el componente Sandboxing sea de otro fabricante se debe presentar una carta del fabricante a nombre de la entidad indicando el nombre del producto, tipo de licencia y tiempo de licenciamiento de acuerdo al contrato.
29	86	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	Punto 5	DICE: La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante. CONSULTA: Con la finalidad de garantizar la pluralidad de postores y asegurar la libertad de propuesta de las mejores soluciones especializadas del mercado: Sirvase confirmar que para el cumplimiento del módulo DAST se aceptará la propuesta de un fabricante o marca completamente independiente y diferente al fabricante de la solución Cloud WAF (CWAF) ofertada.	Se precisa que dentro del requerimiento de las EETT se establece que esta capacidad se podrá brindar a través del mismo u otro fabricante. En caso de que el componente DAST sea de otro fabricante se debe presentar una carta del fabricante a nombre de la entidad indicando el nombre del producto, tipo de licencia y tiempo de licenciamiento de acuerdo al contrato.

30	86	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	Punto 5	DICE: La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante. CONSULTA: Teniendo en cuenta que diversas herramientas DAST del mercado estructuran su licenciamiento en función del número de programadores o usuarios activos de la plataforma: Sírvasse precisar la cantidad de desarrolladores, programadores o analistas de la Entidad que harán uso del módulo DAST y gestionarán los escaneos de las 40 aplicaciones web durante el periodo del servicio.	Se precisa que el alcance mínimo requerido para el componente DAST corresponde a cuarenta (40) aplicaciones web durante todo el periodo contractual. Será responsabilidad del postor dimensionar e incluir el modelo de licenciamiento y los accesos administrativos necesarios para cumplir integralmente dicho alcance, independientemente del esquema comercial utilizado por el fabricante ofertado y sin generar costos adicionales para la Entidad. El licenciamiento no deberá limitar la cantidad de escaneos, evaluaciones o aplicaciones por restricciones de usuarios.
31	86	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	Punto 5	DICE: La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante. CONSULTA: Para llevar a cabo un dimensionamiento correcto de la herramienta DAST y de la solución WAF/WAAP, es necesario considerar la relación FQDN/Dominios y Subdominios, pues el costo y las reglas de alcance (Scope Restrictions) de varias soluciones DAST del mercado varían sustancialmente si las 40 aplicaciones web corresponden a un único dominio principal con múltiples subdominios o a 40 dominios/FQDNs independientes de diferentes nombres Por lo tanto, sírvase precisar en precisar a cuántos dominios principales y subdominios (FQDNs) están vinculadas a las 40 aplicaciones web objeto de la presente contratación.	Se precisa que las 40 aplicaciones web se encuentran bajo un único dominio principal, mediante los respectivos subdominios/FQDN

32	96	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante. CONSULTA: Teniendo en cuenta que las soluciones de Cloud WAF/WAAP previenen ataques en tiempo real y proporcionan visibilidad continua de la superficie de ataque mediante módulos de Security Center y API Discovery, y que los módulos de DAST realizan pruebas dinámicas mediante el envío masivo de peticiones HTTP, inyecciones de prueba y rastreo de rutas (crawling). Ejecutar este tipo de escaneos de forma continua sobre los 40 aplicativos web en producción, consume recursos de servidor, genera latencia (delay) en el procesamiento de solicitudes e introduce retrasos perceptibles en los tiempos de respuesta para los usuarios finales durante su operación diaria, aparte que genera complejidad operacional y sobrecostos en la implementación. En virtud de lo antes mencionado, sírvase confirmar que se eliminara la exigencia del módulo de DAST o, en su defecto, se considere opcional, aceptando en su lugar el cumplimiento equivalente mediante las funcionalidades nativas de la solución WAF para el descubrimiento de vulnerabilidades, visibilidad de la superficie de ataque (Security Center) y gestión de riesgo de APIs/Aplicativos en producción.	NO SE ACOGE la consulta. Se mantiene el requerimiento del módulo DAST para las cuarenta (40) aplicaciones web. Las funcionalidades de protección WAF/WAAP, descubrimiento de APIs, monitoreo y visibilidad de superficie de ataque cumplen funciones de prevención y mitigación durante la operación; las herramientas DAST realizan pruebas dinámicas orientadas a identificar vulnerabilidades en las aplicaciones. En consecuencia, dichas capacidades se consideran complementarias y no equivalentes para efectos del presente requerimiento.
33	86	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 5	5	DICE: La solución debe incluir un módulo de DAST (Dynamic Application Security Testing) para las 40 aplicaciones web y por el periodo solicitado, el proveedor podrá incluir la licencia (si fuese el caso) del mismo fabricante de la solución u otro fabricante. CONSULTA: Durante el ciclo de vida de desarrollo de software (DevSecOps) y la vigencia del contrato, es posible que la Entidad dé de baja aplicativos antiguos, cree nuevas plataformas o renombre entornos. Algunas	Se acoge parcialmente la consulta. Durante la vigencia del servicio, las 40 aplicaciones web consideradas en el alcance podrán ser reasignadas o reemplazadas por nuevas aplicaciones web o subdominios que la Entidad implemente en producción, en función de las

				marcas de módulos DAST asignan identificadores de aplicación fijos y rígidos, y cualquier cambio futuro en los activos impediría evaluar los nuevos sistemas sin incurrir en costos adicionales de licenciamiento. En virtud a lo antes mencionado, sírvase confirmar que las 40 aplicaciones web podrán ser reasignadas o reemplazadas de forma flexible durante el periodo del servicio por nuevas aplicaciones o subdominios que la Entidad despliegue en producción.	necesidades institucionales y de la evolución de su plataforma tecnológica. Esta reasignación o reemplazo deberá mantenerse dentro del alcance de 40 aplicaciones web, <u>sin que genere costos adicionales por concepto de licenciamiento, siempre que no se incremente la cantidad máxima de aplicaciones consideradas en la contratación.</u>
34	88	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 9	9.1	DICE: 9.1. Formación Académica Un (01) ESPECIALISTA EN CIBERSEGURIDAD Profesional titulado en Ingeniería de Sistemas y/o Redes y Comunicaciones y/o Informática y/o Telecomunicaciones y/o Redes y Comunicaciones de Datos. Debe contar con certificación oficial del fabricante o carta emitida por el fabricante o representante local de la solución WAF que faculte a los profesionales responsables como Especialista en la administración y soporte de la solución ofertada. CONSULTA: Teniendo en cuenta que existen carreras profesionales universitarias y/o técnicas afines con competencias equivalentes en infraestructura, redes y ciberseguridad, y con el fin de promover la mayor concurrencia de postores y profesionales calificados: Sírvase confirmar que se aceptara la inclusión de las siguientes carreras afines para el perfil del Especialista en Ciberseguridad: Red de computadoras y comunicación de datos Redes de computadora y comunicación de datos Ingeniería Electrónica y Telecomunicaciones Ingeniería Empresarial y de Sistemas	Ver enmienda 15
35	88	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT	9.1	DICE: 9.1. Formación Académica Un (01) ESPECIALISTA EN CIBERSEGURIDAD Profesional titulado en Ingeniería de Sistemas y/o Redes y Comunicaciones y/o Informática y/o Telecomunicaciones y/o Redes y Comunicaciones de	No se acoge la consulta. Se mantiene el requisito de profesional titulado establecido para el Especialista en Ciberseguridad, considerando las responsabilidades de administración, implementación y soporte de la solución objeto de la contratación. Se mantienen las condiciones establecidas en las EETT.

		Punto 9		Datos. Debe contar con certificación oficial del fabricante o carta emitida por el fabricante o representante local de la solución WAF que faculte a los profesionales responsables como Especialista en la administración y soporte de la solución ofertada. CONSULTA: Teniendo en cuenta los Principios de Libre Concurrencia y Competencia que rigen las contrataciones públicas, y considerando que el conocimiento técnico para la implementación y soporte de un WAF se valida mediante la experiencia práctica y la certificación del fabricante, y no por la obtención del título profesional universitario. Sirvase confirmar que se aceptara el grado de Titulado Tecnico, o Bachiller o Titulado profesional en las carreras solicitadas para el perfil del Especialista en Ciberseguridad.	
36	88	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 9	9.1	DICE: 9.2. Experiencia Profesional Experiencia General: tres (03) años de experiencia laboral en el sector público y/o privado. Experiencia Específica: dos (02) años de experiencia laboral en instalación, configuración y soporte de soluciones de Firewall de Aplicaciones Web (WAF). CONSULTA: Teniendo en cuenta los Principios de Proporcionalidad, Libre Concurrencia y Competencia, debido a que la experiencia específica es considerada también experiencia general y considerando que para la correcta ejecución del servicio el factor determinante es la experiencia en soluciones WAF (la cual subsume a la experiencia general): Sirvase confirmar que se aceptara que el tiempo exigido para la Experiencia General del Especialista en Ciberseguridad sea de dos (02) años de experiencia laboral en el sector público y/o privado, igualándolo al tiempo solicitado para la Experiencia Específica	No se acoge la consulta. La experiencia general y la experiencia específica corresponden a criterios distintos de acreditación profesional.

37	89	Sección VI. Requisitos de los Bienes y Servicios. 3. EETT Punto 13	Punto 13	DICE: Se consideran bienes similares a los siguientes: Venta de licenciamiento y/o implementación de Equipo de seguridad Firewall y/o Sistema de prevención de intrusos y/o Protección Antimalware y/o Protección URL y/o Sistema Proxy Cache y/o Web Filter y/o Sistema de control de Acceso a la Red y/o Firewall de Aplicaciones Web (WEB). CONSULTA: Considerando que el objeto de la contratación se encuentra relacionado con soluciones de seguridad de aplicaciones, ciberseguridad, y con la finalidad de promover una mayor pluralidad de postores. Solicitamos confirmar que también serán considerados como bienes similares aquellos relacionados con la venta, servicio, licenciamiento, suscripción, renovación y/o implementación de soluciones de seguridad de aplicaciones y/o ciberseguridad, tales como: Plataforma de Protección y Seguridad de Aplicaciones Soluciones de seguridad de aplicaciones WEB (WAF) Soluciones, licenciamiento, implementación y soporte de solución de seguridad perimetral y/o ciberseguridad.	Ver Enmienda 8
38	72	Sección V. Formularios de la Oferta	Punto 13	DICE: PRECIO Y CRONOGRAMA DE CUMPLIMIENTO: SERVICIOS CONEXOS CONSULTA: Considerando que dentro de los formularios de la oferta se incluye el formato denominado "Precio y Cronograma de Cumplimiento: Servicios Conexos", solicitamos a la Entidad precisar y detallar cuáles son los servicios conexos que deberán ser considerados	Se aclara que los servicios conexos corresponden: 1. <i>Implementación</i> 2. <i>Soporte Técnico y transferencia de conocimiento</i> Ver Enmienda 1 y 13

				y cotizados por el postor en dicho formato. Lo solicitado permitirá a los postores identificar correctamente los servicios que forman parte del alcance de la contratación, realizar una adecuada determinación de costos y presentar ofertas bajo las mismas condiciones.	
--	--	--	--	--	--

EL DOCUMENTO ORIGINAL SE ENCUENTRA EN EL EXPEDIENTE