Nro. Orden	Nombre o Razón Social de la empresa	Tipo Formulación (consulta u observación)	Sección (Especifica o general de las bases)	Numeral (de las bases)	Literal (De las bases)	Página	Consulta u Observación (Descripción de la consulta u observación)	Respuesta	Modificación
1	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	2,6		14	En las bases se señala: Documentación técnica del fabricante de la solución NGFW empleada, que sustente el cumplimiento de los numerales 3.1.1, 3.1.2, 3.1.3 y 3.1.4 de las especificaciones técnicas del Capítulo III de la Sección Específica de las bases. Consulta: Se solicita a la entidad confirmar si será posible realizar el sustento con una carta de fabricante indicando el cumplimiento de dichos puntos.	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, lo cual ofrece mayor detalle, especificidad y objetividad, reduciendo los riesgos de incumplimiento de la solución de la presente contratación.	
2	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	2,6		14	En las bases se señala: Documentación técnica del fabricante de la solución NGFW empleada, que sustente el cumplimiento de los numerales 3.1.1, 3.1.2, 3.1.3 y 3.1.4 de las especificaciones técnicas del Capítulo III de la Sección Específica de las bases. Consulta: Se solicita a la entidad confirmar si se aceptará que el sustento de los puntos requeridos se podrá realizar mediante enlaces web (link) del fabricante en el cual se indique el cumplimiento	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, la misma que debe adjuntarse como parte de la oferta, y no sólo proporcionar enlaces web. Cabe recalcar que la revisión de la oferta se realiza en base a la documentación presentada en ella y un enlace web, link o url es una dirección electrónica que como tal no permite validar el cumplimiento.	
3	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	2,7		14	En las bases se señala: Documentación técnica del fabricante que sustente el cumplimiento de los numerales 3.4.1, 3.4.2, 3.4.3, 3.4.4 y 3.4.5. de las especificaciones técnicas del Capítulo III de la Sección Específica de las bases. Consulta: Se solicita a la entidad confirmar si será posible realizar el sustento con una carta de fabricante indicando el cumplimiento de dichos puntos.	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, lo cual ofrece mayor detalle, especificidad y objetividad, reduciendo los riesgos de incumplimiento de la solución de la presente contratación.	
4	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	2,7		14	En las bases se señala: Documentación técnica del fabricante que sustente el cumplimiento de los numerales 3.4.1, 3.4.2, 3.4.3, 3.4.4 y 3.4.5. de las especificaciones técnicas del Capítulo III de la Sección Específica de las bases. Consulta: Se solicita a la entidad confirmar si se aceptará que el sustento de los puntos requeridos se podrá realizar mediante enlaces web (link) del fabricante en el cual se indique el cumplimiento.	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, la misma que debe adjuntarse como parte de la oferta, y no sólo proporcionar enlaces web. Cabe recalcar que la revisión de la oferta se realiza en base a la documentación presentada en ella y un enlace web, link o url es una dirección electrónica que como tal no valida el cumplimiento.	
5	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3		15	En las bases se señala: Incorporar en la oferta los documentos que acreditan los "Requisitos de Calificación" que se detallan en el numeral 2 del Capítulo III de la presente sección de las bases. Consulta: Se solicita a la entidad confirmar si los documentos para acreditar los requisitos de calificación son los solicitados en las páginas 37 y 38, del Numeral 2, Capítulo III	Se confirma lo indicado por el participante. Los documentos para acreditar los requisitos de calificación se encuentran en el literal a y b del numeral 2 del Capítulo III de la Sección Específica de las bases.	
6	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	4,1		15	En las bases se señala: Incorporar en la oferta el documento que acredita el factor de evaluación establecido en numeral 1 del Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo Consulta: Se solicita a la entidad confirmar si los documentos para acreditar los factores de evaluación se encuentran detallados en la página 39, Numeral 1, Capítulo IV.	Se confirma lo indicado por el participante. Los documentos para acreditar los factores de evaluación se encuentran detallados en el numeral 1 del Capítulo IV de la Sección Específica de las bases. Asimismo se corregirá el texto "FACTORE" por "FACTOR" en el numeral 1 del Capítulo IV - Factores de Evaluación.	CAPÍTULO IV FACTORES DE EVALUACIÓN ... 1) FACTOR DE EVALUACIÓN OBLIGATORIO
7	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	5	i	15	En las bases se señala: Documento del fabricante que indique que el servicio en nube del fabricante cumple con lo requerido en el numeral 3.2.34, debiéndose incluir como referencia uno o más enlaces (links) a la documentación/portal web del fabricante, donde se detalle el cumplimiento. Consulta: Se solicita a la entidad confirmar si para efectos de este punto se aceptará agregar a los enlaces del fabricante una explicación de como en caso de presentarse más enlaces estos se relacionan para lograr el cumplimiento de lo requerido en el numeral 3.2.24.	Se precisa que dicha explicación puede realizarse en el documento del fabricante. Debe recalcarse que lo primordial es la presentación de la documentación del fabricante en la que en el mismo documento se evidencie el cumplimiento de lo requerido en el numeral 3.2.34. Adicional a ello, debe incluir de manera referencial los enlaces al portal web del fabricante, según lo requerido en el literal i del numeral 5 del Capítulo II de la Sección Específica de las bases.	
8	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3,1		19	En las bases se señala: Nota: Se deberá presentar documentación técnica del fabricante de la solución NGFW empleada, que sustente el cumplimiento de los numerales 3.1.1, 3.1.2, 3.1.3 y 3.1.4. Dichos documentos serán parte de la documentación de presentación obligatoria que los postores deberán incluir en sus ofertas Consulta: Se solicita a la entidad confirmar si será posible realizar el sustento con una carta de fabricante indicando el cumplimiento de dichos puntos.	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, lo cual ofrece mayor detalle, especificidad y objetividad, reduciendo los riesgos de incumplimiento de la solución de la presente contratación.	
9	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3,1		19	En las bases se señala: Nota: Se deberá presentar documentación técnica del fabricante de la solución NGFW empleada, que sustente el cumplimiento de los numerales 3.1.1, 3.1.2, 3.1.3 y 3.1.4. Dichos documentos serán parte de la documentación de presentación obligatoria que los postores deberán incluir en sus ofertas Consulta: Se solicita a la entidad confirmar si se aceptará que el sustento de los puntos requeridos se podrá realizar mediante enlaces web (link) del fabricante en el cual se indique el cumplimiento.	No se confirma lo solicitado por el participante. El sustento de los puntos solicitados debe ser realizado con documentación técnica del fabricante, la misma que debe adjuntarse como parte de la oferta, y no sólo proporcionar enlaces web. Cabe recalcar que la revisión de la oferta se realiza en base a la documentación presentada en ella y un enlace web, link o url es una dirección electrónica que como tal no valida el cumplimiento.	

10	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.1		20	En las bases se señala: Para los equipos NGFW a continuación se presentan los requerimientos de throughput mínimo requerido de cada equipo, en cada categoría, tanto para el caso en que se utilice la modalidad de inspección paralela (donde se abre una sola vez el paquete de red y se revisa en forma paralela por los módulos de control de seguridad), como en el caso de la inspección serial (donde cada módulo de inspección abre el paquete en forma sucesiva). Este throughput debe considerar al menos, las siguientes funcionalidades activas simultáneamente, así como la operación con el más alto modo de inspección (en caso la solución tuviese más de un modo de inspección): ✓ Identificación y control de aplicaciones. ✓ Prevención y control de amenazas: IPS, antimalware y control de C&C. (TABLA DE TIPOS DE INSPECCIÓN POR CATEGORÍA) Lo indicado debe haberse medido bajo tráfico mixto empresarial, enterprise mix o mix de aplicaciones, condiciones de pruebas empresarial. Consulta: Se solicita a la entidad confirmar que se aceptarán términos similares, debido que estos cumplen las mismas funciones, como por ejemplo lo siguiente: Antimalware y/o antivirus Control de C&C y/o Antibot y/o Antispyware Aceptan que finalmente se requiera la inspección de la siguiente manera: ✓ Identificación y control de aplicaciones. ✓ Prevención y control de amenazas: IPS, antimalware y/o antivirus y control de C&C y/o Antibot y/o Antispyware.	Se aclara que son aceptables denominaciones similares tal como "antimalware" y "antivirus", así como "Control de C&C", "Antibot" o "Antispyware", siempre que se cumplan con los requerimientos especificados bajo el título "IPS, antimalware y protección contra C&C" según lo establecido en los numerales del 3.2.1 al 3.2.22 del Capítulo III de la Sección Específica de las bases.	
11	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.2		20	En las bases se señala: Cada equipo debe manejar la siguiente cantidad de sesiones como mínimo: (TABLA DE CANTIDADES DE SESIONES POR CATEGORÍA) Consulta: Con la finalidad de permitir una pluralidad de postores que cuenten con diferentes términos en sus documentos de sustento, se solicita a la entidad confirmar que se aceptarán los términos de sesiones y/o conexiones concurrentes y de Nuevas sesiones y/o conexiones.	Se aclara que aceptan denominaciones similares que representen el mis concepto de lo requerido, tal es el caso de los términos sesiones y conexiones.	
12	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.30		22	En las bases se señala: Debe ser capaz de descifrar el tráfico HTTPS, para ello deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, AES128, AES256, CHACHA20-POLY1305; SHA1, SHA256, SHA384. Consulta: Se solicita a la entidad confirmar el requerimiento a la siguiente homologación: Debe ser capaz de descifrar el tráfico HTTPS, para ello deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, AES128, AES256, CHACHA20-POLY1305; SHA1, SHA256, SHA384. En su defecto, se aceptarán soluciones donde los algoritmos de cifrado tengan la siguiente nomenclatura: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256	Se confirma lo indicado por el participante. Se precisa que alternativamente se aceptarán nomenclaturas equivalentes siempre que soporten los algoritmos requeridos en el numeral 3.1.30. Se realizará la precisión correspondiente en el numeral 3.1.30 del Capítulo III - Requerimiento.	3.1.30. Debe ser capaz de descifrar el tráfico HTTPS, para ello deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, AES128, AES256, CHACHA20-POLY1305; SHA1, SHA256, SHA384. Se precisa que alternativamente se aceptarán nomenclaturas equivalentes siempre que soporten los algoritmos requeridos.
13	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.33		22	En las bases se señala: Permitir la adición de firmas personalizadas para reconocimiento de aplicaciones propietarias, mediante CLI o la propia interface gráfica de la solución, sin la necesidad de acciones por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la organización Consulta: Se solicita a la entidad confirmar si se aceptará que lo requerido se pueda realizar mediante CLI o la propia interface gráfica de la solución o una herramienta externa del fabricante ofertado. Finalmente aceptando soluciones que cumplan con lo siguiente: Permitir la adición de firmas personalizadas para reconocimiento de aplicaciones propietarias, mediante CLI o la propia interface gráfica de la solución o el uso de una herramienta propia del fabricante de seguridad ofertante, sin la necesidad de acciones por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la organización.	Se confirma lo solicitado por el participante. Se aceptará que lo requerido se pueda realizar mediante CLI o la propia interface gráfica de la solución o una herramienta externa del fabricante de la solución ofertada. Se realizará la modificación correspondiente en el numeral 3.1.33 del Capítulo III - Requerimiento.	3.1.33. Permitir la adición de firmas personalizadas para reconocimiento de aplicaciones propietarias, mediante CLI o la propia interface gráfica de la solución o una herramienta externa del fabricante de la solución ofertada, sin la necesidad de acciones por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la organización,
14	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.50		23	En las bases se señala: Permitir filtrar de manera optimizada protocolos P2P (Por ejemplo, Kazaa, Gnutella, BitTorrent e IRC), independiente de los puertos TCP utilizados para su comunicación. Consulta: Se solicita a la entidad confirmar si optimizado hace referencia a que se debe de detectar las aplicaciones y estas deben de ser reconocidas independientemente de los puertos TCP utilizados.	Se confirma lo solicitado por el participante. Se agregará la precisión correspondiente en el numeral 3.1.50 del Capítulo III - Requerimiento.	3.1.50. Permitir filtrar de manera optimizada protocolos P2P (Por ejemplo, Kazaa, Gnutella, BitTorrent e IRC), independiente de los puertos TCP utilizados para su comunicación. Se precisa que el filtrado optimizado hace referencia a la detección e identificación de aplicaciones.

15	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.55		23	En las bases se señala: El software de cliente VPN IPSec debe soportar su instalación en Windows y Mac. Consulta: Se solicita a la entidad confirmar si se aceptarán soluciones las cueles cuenten con software de cliente VPN IPSec que soporte su instalación en Windows y/o Mac.	Se precisa que se aceptarán soluciones que cuenten con software de cliente VPN IPSec que soporte su instalación en Windows. Se realizará la modificación correspondiente en el numeral 3.1.55 del Capítulo III - Requerimiento.	3.1.55. El software de cliente VPN IPSec debe soportar su instalación en Windows.
16	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.1.76		24	En las bases se señala: En caso de sincronizar por aplicación del mecanismo de HA, se debe considerar al menos: ✓ Todas las sesiones. ✓ Certificados para desencriptar. ✓ Todos los cambios de configuración. ✓ Todas las tablas de enrutamiento. Consulta: Se solicita a la entidad confirmar si para la sincronización de certificados para desencriptar, se aceptará que se utilice la consola de gestión con la función de distribuir estos certificados en todos los firewalls que se requieran y así mantenerlos sincronizados.	Se confirma lo solicitado por el participante. Se precisa que, para efectos de la sincronización de certificados utilizados para desencriptar, será válido el uso de la consola de gestión con la función de distribución de dichos certificados en todos los firewalls que se requieran, garantizando con ello su adecuada sincronización. Se modificará el numeral 3.1.76 del Capítulo III - Requerimiento.	3.1.76. En caso de sincronizar por aplicación del mecanismo de HA, se debe considerar al menos: - Todas las sesiones. - Todos los cambios de configuración. - Todas las tablas de enrutamiento. Se precisa que, para efectos de la sincronización de certificados utilizados para desencriptar, será válido el uso de la consola de gestión con la función de distribución de dichos certificados en todos los firewalls que se requieran, garantizando con ello su adecuada sincronización.
17	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.4		25	En las bases se señala: Permitir establecer excepciones en las reglas, ya sea por dirección IP origen o IP destino, de forma general y firma a firma. Consulta: Se solicita a la entidad confirmar si se aceptará como una opción para el término de "firma a firma" que la solución permita crear un perfil de Prevencion de Amenazas y sobre este perfil configurado se creen excepciones, para así luego aplicar este perfil a las reglas.	Se confirma lo solicitado por el participante. Se precisa que será aceptable que, para el término de "firma a firma", la solución permita crear un perfil de Prevención de Amenazas y, sobre dicho perfil configurado, establecer las excepciones correspondientes, siempre y cuando se garantice que dichas excepciones se apliquen efectivamente en las reglas mediante el uso del perfil referido. Se agregará la precisión correspondiente al numeral 3.2.4 del Capítulo III - Requerimiento.	3.2.4. Permitir establecer excepciones en las reglas, ya sea por dirección IP origen o IP destino, de forma general y firma a firma. Se precisa que será aceptable que la solución use un perfil de Prevención de Amenazas y, sobre este, se configuren excepciones, siempre que se garantice que dichas excepciones se apliquen efectivamente en las reglas mediante ese perfil.
18	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.7		25	En las bases se señala: Incluir funcionalidades de inspección de IPS que permitan: □Análisis de estado de conexiones. □Análisis de decodificación de protocolo. □Análisis para detección de anomalías de protocolo. □Fragmentación IP. □Reensamblado de paquetes TCP. □Bloqueo de paquetes malformados. Consulta: Se solicita a la entidad confirmar si, en lugar del mecanismo de análisis de decodificación de protocolo especificado en el TDR, se aceptará como opción la implementación de funciones embebidas de "Analizadores de protocolos" (Protocol Parsers). Esta alternativa permite validar el cumplimiento de estándares de protocolo, detectar anomalías en el tráfico (incluyendo paquetes malformados), y recolectar datos relevantes para su posterior inspección por otros componentes del motor IPS. Adicionalmente, se contempla una capa de administración y protección que permita gestionar de forma centralizada tanto los analizadores de protocolos como las protecciones basadas en firmas.	Se confirma lo solicitado por el participante. Se precisa que será aceptable la implementación de funciones embebidas de "Analizadores de protocolos" (Protocol Parsers), siempre que estas cumplan con el objetivo establecido en el TDR respecto al análisis de decodificación de protocolo, garantizando la capacidad de inspección profunda, detección de anomalías y aplicación de firmas de seguridad a nivel de protocolo. Se agregará la precisión correspondiente al numeral 3.2.7 del Capítulo III - Requerimiento.	3.2.7. Incluir funcionalidades de inspección de IPS que permitan: - Análisis de estado de conexiones. - Análisis de decodificación de protocolo. - Análisis para detección de anomalías de protocolo. - Fragmentación IP. - Reensamblado de paquetes TCP. - Bloqueo de paquetes malformados. Se precisa que será aceptable implementar analizadores de protocolos embebidos, siempre que cumplan con el objetivo del TDR: decodificación, inspección profunda, detección de anomalías y aplicación de firmas de seguridad a nivel de protocolo.
19	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.25		26	En las bases se señala: Capacidad de subir (desde la solución NGFW) al menos de 2500 archivos al día, de forma automática al entorno de análisis de malware, en nube. Consulta: Se solicita a la entidad confirmar si se aceptarán soluciones que operen bajo una tasa de envío calculada mensualmente, equivalente a 14,000 archivos por mes. Esta modalidad permite una gestión más flexible de los recursos, manteniendo la capacidad total requerida en el período, y asegurando el cumplimiento funcional del objetivo de análisis automatizado.	No se confirma lo solicitado por el participante. No obstante, como alternativa a lo definido en el requerimiento, se precisa que también será aceptable brindar la capacidad de subir un promedio de 75000 archivos al mes, de forma automática al entorno de análisis de malware, en nube. Se realizará la modificación correspondiente al numeral 3.2.25 del Capítulo III - Requerimiento.	3.2.25. Capacidad de subir (desde la solución NGFW) al menos de 2500 archivos al día o un promedio de 75000 archivos al mes, de forma automática al entorno de análisis de malware, en nube.
20	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.30		27	En las bases se señala: El sistema de análisis de malware, basado en nube, debe permitir: ✓ Exportar el resultado de los análisis de malware desconocido, en los formatos PDF y/o CSV, a partir de la propia interface de administración. ✓ Analizar archivos ejecutables (EXE), ZIP, sobre conexiones cifradas (HTTPS). ✓ Analizar archivos del paquete MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), flash, PDF, bat, rar, hta, vbs, ps1, elf y archivos java. Consulta: considerando la diversidad tecnológica de las soluciones disponibles en el mercado, se solicita a la entidad confirmar si se aceptarán propuestas que permitan el análisis de archivos del paquete MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), flash, PDF, bat, rar, hta Y/O vbs, ps1, elf y archivos java,	Se precisa que se eliminará el requerimiento de realizar el análisis de malware, basado en nube, en archivos HTA. Se realizará la modificación correspondiente al numeral 3.2.30 del Capítulo III - Requerimiento.	3.2.30. El sistema de análisis de malware, basado en nube, debe permitir: - Exportar el resultado de los análisis de malware desconocido, en los formatos PDF y/o CSV, a partir de la propia interface de administración. - Analizar archivos ejecutables (EXE), ZIP, sobre conexiones cifradas (HTTPS). - Analizar archivos del paquete MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), flash, PDF, bat, rar, ~~hta~~, vbs, ps1, elf y archivos java.
21	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.34		27	En las bases se señala: Nota: Se deberá presentar un documento del fabricante que indique que el servicio en nube del fabricante cumple con lo solicitado, debiéndose incluir como referencia uno o más enlaces (links) a la documentación/portal web del fabricante, donde se detalle el cumplimiento. Dicho documento será presentado para el perfeccionamiento del contrato. Consulta: Se solicita a la entidad confirmar si para el sustento de los puntos requeridos se permitirá adjuntar uno o más enlaces (links) y además una explicación de como estos enlaces (links) guardan relación entre sí para sustentar así el cumplimiento de lo solicitado.	Se precisa que dicha explicación puede realizarse en el documento del fabricante. Debe recalcarse que lo primordial es la presentación de la documentación del fabricante en la que en el mismo documento se evidencie el cumplimiento de lo requerido en el numeral 3.2.34. Adicional a ello, debe incluir de manera referencial los enlaces al portal web del fabricante, según lo requerido en el literal i del numeral 5 del Capítulo II de la Sección Específica de las bases.	
22	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.43		28	En las bases se señala: Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS. Consulta: Con la finalidad de brindar una apertura de participación de fabricantes, se solicita a la entidad confirmar si se aceptarán soluciones que permitan identificar amenazas en DNS over HTTPS (DoH) y/o DNS over TLS	Se confirma lo solicitado por el participante. Se aceptarán soluciones que permitan identificar amenazas en DNS over HTTPS (DoH) y/o DNS over TLS Se realizará la modificación correspondiente al numeral 3.2.43 del Capítulo III - Requerimiento.	3.2.43. Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y/o DNS sobre TLS.

23	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.2.46		28	En las bases se señala: Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos del BCRP Consulta: Se solicita a la entidad confirmar si como opción a las estadísticas requeridas se aceptarán soluciones en la cual integre una vista predefinida en donde se muestren a nivel de DNS Security: Total de Ataques (Benignos, Maliciosos detectados y Maliciosos prevenidos), Top de ataques, técnicas utilizadas, usuarios involucrados, dominios maliciosos y una línea del tiempo de ataques y/o acciones maliciosas a nivel DNS realizadas	Se confirma lo solicitado por el participante. Alternativamente se aceptará que la solución integre una vista predefinida en donde se muestren a nivel de DNS Security: Total de Ataques (Benignos, Maliciosos detectados y Maliciosos prevenidos), Top de ataques, técnicas utilizadas, usuarios involucrados, dominios maliciosos y una línea del tiempo de ataques y/o acciones maliciosas a nivel DNS realizadas. Se realizará la modificación correspondiente al numeral 3.2.46 del Capítulo III - Requerimiento.	3.2.46. Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos del BCRP. Alternativamente, se aceptará que la solución incluya una vista predefinida de DNS Security con: total de ataques, top de ataques, técnicas usadas, usuarios, dominios maliciosos y línea de tiempo de acciones maliciosas.
24	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.3.17		29	En las bases se señala: Soportar la identificación de usuarios basada en protocolos como LDAP y RADIUS. Asimismo, permitir la autenticación de administradores a través de diversos mecanismos, tales como passwords locales, tokens y/o smart cards, RADIUS (o TACACS y/o TACACS+) y certificados digitales X.509. Consulta: se solicita a la entidad confirmar si el término "tokens" contempla la aceptación de tecnologías basadas en tokens de autenticación dinámica, tales como RSA SecurID u otras soluciones equivalentes que generen códigos temporales vinculados a credenciales únicas.	Se confirma lo indicado por el participante. Se precisa que el término "tokens" contemplado en las bases incluye la aceptación de tecnologías basadas en tokens de autenticación dinámica, tales como RSA SecurID u otras soluciones equivalentes que generen códigos temporales vinculados a credenciales únicas, en concordancia con los mecanismos de autenticación establecidos.	3.3.17. Soportar la identificación de usuarios basada en protocolos como LDAP y RADIUS. Asimismo, permitir la autenticación de administradores a través de diversos mecanismos, tales como passwords locales, tokens y/o smart cards, RADIUS (o TACACS y/o TACACS+) y certificados digitales X.509. Se precisa que el término "tokens" incluye tecnologías de autenticación dinámica como RSA SecurID u otras equivalentes, que generen códigos temporales ligados a credenciales únicas, según los mecanismos de autenticación establecidos.
25	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.4.1		31	En las bases se señala: Se deberá incluir una herramienta integrada a la solución NGFW proporcionada y/o externa a la misma que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, firmware cerca a la obsolescencia, expiración de licencias Consulta: Se solicita a la entidad confirmar si se aceptará que se realice lo requerido mediante una herramienta o un servicio proporcionado por el fabricante.	Se confirma lo solicitado por el participante. Se aceptará que se realice lo requerido mediante una herramienta o un servicio proporcionado por el fabricante. Se realizará la modificación correspondiente al numeral 3.4.1 del Capítulo III - Requerimiento.	3.4.1. Se deberá incluir una herramienta integrada a la solución NGFW proporcionada y/o externa a la misma que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, firmware cerca a la obsolescencia, expiración de licencias. Se precisa que, alternativamente, se aceptará que se realice lo requerido mediante una herramienta o un servicio proporcionado por el fabricante.
26	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.4.4		32	En las bases se señala: Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red. Consulta: se solicita a la entidad confirmar si se aceptarán soluciones que, mediante el análisis de objetos sin uso en las políticas, se permita filtrar y determinar aquellas políticas que no están siendo utilizadas en los firewalls. Asimismo, se propone considerar la depuración de políticas como una acción opcional, dado que su ejecución automática podría generar impactos no deseados en la continuidad del servicio del BCRP. En ese sentido, se plantea que las acciones de depuración se realicen de forma manual y controlada, previa validación operativa, para garantizar la integridad del servicio.	Se confirma lo indicado por el participante. Se confirma que será aceptable que la solución permita, mediante el análisis de objetos sin uso en las políticas, filtrar y determinar aquellas políticas que no están siendo utilizadas en los firewalls. Asimismo, se precisa que la depuración de políticas debe poder realizarse de forma manual y controlada, previa validación operativa. Se realizará la modificación correspondiente al numeral 3.4.4 del Capítulo III - Requerimiento.	3.4.4. Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red. Se aceptará que la solución pueda identificar políticas no utilizadas en los firewalls y que la depuración deberá hacerse manualmente y de forma controlada, previa validación operativa.
27	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	3.4.5		32	En las bases se señala: Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio. Consulta: Se solicita a la entidad confirmar si esta característica solicitada pueda ser cumplible mediante secciones que se presenten como las indicadas a continuación: - Una sección de sugerencia sobre la Política de Seguridad - Una sección de realizar cambios mas adelante ("Decidir mas tarde") sobre las sugerencias planteadas por la herramienta. - sección de sugerencias rechazadas y/o no tomadas en consideración	Se confirma lo indicado por el participante. Se precisa que será aceptable que la característica solicitada pueda ser cumplida mediante la incorporación de secciones como las indicadas: Una sección de sugerencia sobre la Política de Seguridad. Una sección de realizar cambios más adelante ("Decidir más tarde") sobre las sugerencias planteadas por la herramienta. Una sección de sugerencias rechazadas y/o no tomadas en consideración. Ello, siempre que se garantice el cumplimiento del requerimiento de identificar automáticamente las políticas abiertas sin restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de aplicar correcciones y dar cumplimiento al principio de mínimo privilegio. Se realizará la modificación correspondiente al numeral 3.4.5 del Capítulo III - Requerimiento.	3.4.5. Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio. Alternativamente, se aceptará que la solución cumpla este requerimiento mediante secciones de sugerencias, "decidir más tarde" y sugerencias rechazadas, siempre que se garantice la identificación automática de políticas abiertas (ANY/ALL) para aplicar correcciones según el principio de mínimo privilegio.
28	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	7,1		33	En las bases se señala: Jefe de proyectos Contar con un (01) especialista con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática. Dicho personal debe contar con certificación vigente en Gestión de Proyectos, siendo encargado de gestionar la implementación del servicio. Consulta: Con la finalidad de ampliar la participación de profesionales calificados en el rol de jefe de proyectos, se solicita a la entidad confirmar si, además de la certificación vigente en Gestión de Proyectos, se aceptará como una opción válida la acreditación mediante un Diplomado en Gestión de Proyectos.	Se precisa que en el caso del personal clave con el rol "Jefe de Proyecto" además de certificaciones específicas en Gestión de Proyectos, también se considerará como válido contar con certificado de haber aprobado especializaciones, programas y/o diplomados en gestión y/o dirección de proyectos, con una duración mínima de 120 horas, considerando que es vigente si se obtuvo en los últimos 5 años. No son válidos certificados de sólo asistencia o participación. Se realizará la modificación correspondiente al numeral 7.1 del Capítulo III - Requerimiento.	Numeral 7.1: Jefe de proyecto: Contar con un (01) especialista con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática. Dicho personal, siendo encargado de gestionar la implementación del servicio, debe contar con certificación vigente en Gestión de Proyectos o certificados de especialización, programas o diplomados en gestión y/o dirección de proyectos con una duración mínima de 120 horas, obtenidos en los últimos cinco (05) años. No son válidos certificados de sólo asistencia o participación.

29	THINK NETWORKS PERU S.A.C.	CONSULTA	ESPECÍFICA	10		35	En las bases se señala: Proporcionar cursos oficiales de capacitación teórico/practica, (del fabricante) que permita certificar a nivel experto, profesional o equivalente, sobre la solución propuesta, para el personal técnico del BCRP, con una duración según lo establecido por el fabricante (mínimo de 40 horas lectivas). La capacitación deberá ser programada considerando 07 participantes, en al menos dos (2) grupos y deberá ser realizada dentro del plazo de nueve (09) meses contabilizados a partir de la fecha indicada el acta de conformidad de implementación de la solución, en forma presencial en la ciudad de Lima (sin costos adicionales para el BCRP) o en forma remota, en alguna de las siguientes modalidades: 1) Online y 2) On demand. Las fechas de capacitación se programarán en coordinación con el BCRP. Se deben incluir las constancias de participación correspondientes, así como los vouchers de las evaluaciones de certificación oficial. Consulta: En atención al requerimiento de proporcionar cursos oficiales de capacitación teórico-práctica que permitan certificar al personal técnico del BCRP a nivel experto, profesional o equivalente, se solicita a la entidad confirmar si se aceptará como válida la modalidad de capacitación estructurada en dos niveles secuenciales, conforme al itinerario oficial del fabricante. Esta modalidad contempla que los participantes cursen inicialmente el primer nivel formativo, seguido de su respectiva evaluación, y posteriormente accedan al segundo nivel, culminando con el examen de certificación correspondiente. Dicho enfoque permite alcanzar el nivel experto requerido, cumpliendo con el mínimo de 40 horas lectivas y respetando el diseño curricular establecido por el fabricante para dicho perfil de certificación. La propuesta busca asegurar una formación progresiva, y garantizar que el personal técnico del BCRP reciba una capacitación completa, oficial y certificable, conforme a lo solicitado en las bases.	En el requerimiento no se restringe a algún tipo de capacitación en específico, lo cual dependerá de cada fabricante de la solución, siempre que cumpla con lo establecido en el numeral 10 del Capítulo III de la Sección Específica de las bases. En ese sentido, se considerará aceptable lo propuesto por el participante siempre que: - Permita alcanzar el nivel experto, profesional o equivalente requerido. - Cumpla con el mínimo de 40 horas lectivas en total. - Incluya las constancias de participación correspondientes y los vouchers de las evaluaciones de certificación oficial.	
30	THINK NETWORKS PERU S.A.C.	CONSULTA				37	Dice: Se consideran bienes similares a los siguientes: Venta de equipos, licencias y suscripciones de soluciones Firewall, NGFW (Next Generation Firewall), IPS (Intrusion Prevention System), sandboxing y sus consolas de gestión, así como los servicios de implementación, mantenimiento, capacitación/entrenamiento y soporte técnico correspondientes. CONSULTA: Sirvase confirmar que se aceptara como bienes similares lo siguiente: RENOVACION DE LICENCIAS PARA NGFW, ADQUISICION DE SUSCRIPCION PARA LOS EQUIPOS SEGURIDAD PERIMETRAL; FIREWALL INTERNO; EQUIPO DE PROTECCION Y SEGURIDAD PERIMETRAL FIREWALL	Se precisa que son aceptables denominaciones equivalentes tal como Venta de firewall interno, equipos de protección y seguridad perimetral Firewall y adquisición de suscripción para equipos de seguridad perimetral Firewall. Asimismo también se considerará como equivalentes la renovación de licencias y/o suscripciones para NGFW y/o equipos de seguridad perimetral Firewall. Se realizará la modificación correspondiente al literal a) del numeral 2.1 - Requisitos de Calificación del Capítulo III - Requerimiento.	2.1. Se consideran bienes similares a los siguientes: Venta de equipos, licencias y suscripciones de soluciones Firewall, NGFW (Next Generation Firewall), IPS (Intrusion Prevention System), sandboxing y sus consolas de gestión, venta de firewall interno, equipos de protección y seguridad perimetral Firewall, adquisición de suscripción para equipos de seguridad perimetral Firewall, renovación de licencias y/o suscripciones para NGFW y/o equipos de seguridad perimetral Firewall, así como los servicios de implementación, mantenimiento, capacitación/entrenamiento y soporte técnico correspondientes.
31	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3.1.1		20	CONSULTA: Considerando que todos los requerimientos técnicos establecidos en el TDR se deben cumplir con los equipos ofertados, independientemente del modo de inspección utilizado (paralela o serial), se solicita confirmar y ser explícito con lo siguiente: En caso de que la solución propuesta utilice la modalidad de inspección paralela, esta no debe desactivar las funcionalidades de Overlapping de NAT y traducción de IP6 a IPv4, solicitados en el TDR. Esta consulta se formula en atención a que existen soluciones en el mercado que, al operar de forma forzada —no nativa— en modalidad de inspección paralela, pueden desactivar funcionalidades que se impidan cumplir con los requerimientos técnicos solicitados en el TDR..	Se precisa que la modalidad de inspección paralela debe brindarse, sin necesidad de desactivar alguna de las funcionalidades provistas por los equipos. Se agregará tal precisión al numeral 3.1.1.	3.1.1. Para los equipos NGFW a continuación se presentan los requerimientos de throughput mínimo requerido de cada equipo, en cada categoría, tanto para el caso en que se utilice la modalidad de inspección paralela (donde se abre una sola vez el paquete de red y se revisa en forma paralela por los módulos de control de seguridad), como en el caso de la inspección serial (donde cada módulo de inspección abre el paquete en forma sucesiva). Este throughput debe considerar al menos, las siguientes funcionalidades activas simultáneamente, así como la operación con el más alto modo de inspección (en caso la solución tuviese más de un modo de inspección): ✓ Identificación y control de aplicaciones. ✓ Prevención y control de amenazas: IPS, antimalware y control de C&C. Se precisa que la modalidad de inspección paralela debe brindarse, sin necesidad de desactivar alguna de las funcionalidades provistas por los equipos.
32	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3,2		25	SUSCRIPCIONES DE SEGURIDAD IPS, antimalware y protección contra C&C DICE: 3.2.6. Incluir firmas específicas para el bloqueo de: ✓Vulnerabilidades. ✓Exploits conocidos. ✓Ataques de buffer overflow. ✓Ataques DoS (Denial of Service). ✓Ataques XSS y SQL Injection. 3.2.13. Identificar y bloquear comunicaciones de tipo C&C CONSULTA: Se ha identificado que los requerimientos técnicos de prevención basadas en firmas para los sistemas IPS y C&C, son insuficientes para enfrentar las ciberamenazas modernas. Los ataques actuales, por su naturaleza sofisticada y evasiva, requieren un enfoque avanzado que utilice Inteligencia Artificial (IA) para analizar el comportamiento de la red y detectar anomalías en tiempo real. En línea con la Ley N.º 31814, que declara de interés nacional el uso de la IA para fortalecer los servicios públicos, y dada la importancia estratégica del BCRP, es crucial evaluar los riesgos de no adoptar estas tecnologías. Por ello, se solicita que se confirme si la entidad ha realizado un análisis de riesgo, cualitativo o cuantitativo, sobre las consecuencias de excluir la IA de sus capacidades de IPS y C&C. Omitir esta tecnología aumentaría de manera crítica la exposición de la institución a ciberataques cada vez más frecuentes y complejos. Adicionalmente, se solicita a la entidad confirmar que, si se decide omitir la IA en los requerimientos técnicos descritos y se produce un incidente derivado de esta decisión, los proveedores o contratistas quedarán exentos de la responsabilidad de brindar soporte o realizar la investigación sobre dichos incidentes.	Se aclara que dentro del requerimiento si se han incluido funciones relacionadas con Inteligencia Artificial (IA), tal como se ha establecido en los numerales 3.2.37 y 3.2.44 del Capítulo III de la Sección Específica de las bases.	

33	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3,2		26	SUSCRIPCIONES DE SEGURIDAD Análisis y prevención de malware, basado en nube DICE: 3.2.25. Capacidad de subir (desde la solución NGFW) al menos de 2500 archivos al día, de forma automática al entorno de análisis de malware, en nube. 3.2.26. El ambiente de análisis de malware, basado en nube, deberá emular el malware y archivos sospechosos como mínimo en sistemas operativos Microsoft Windows y opcionalmente Linux, MacOS y Android. CONSULTA: Se ha identificado que, en los requerimientos técnicos, la capacidad de emulación (sandboxing) para detectar malware de día cero en entornos Linux, macOS y Android ha sido definida como opcional. Esta decisión implica que la protección contra amenazas avanzadas y de día cero se limitará únicamente a los entornos Windows. Como resultado, toda la infraestructura basada en Linux, macOS y Android quedará expuesta a un riesgo crítico, sin visibilidad ni capacidad de detección. Por esta razón, se solicita a la entidad que confirme, si se produce un incidente de seguridad en cualquiera de estos sistemas operativos (Linux, macOS, Android) debido a esta omisión en los requerimientos, el proveedor o contratista quedará exento de toda responsabilidad de brindar soporte o realizar la investigación correspondiente a dicho incidente.	No se confirma lo indicado por el participante. Se precisa que los numerales 3.2.25 y 3.2.26 del Capítulo III - Requerimiento, corresponden a requerimientos asociados a la funcionalidad "Análisis y prevención de malware, basado en nube", la cual es aplicable sólo a los equipos de Categoría B, tal como se establece en el numeral 2.6. En tal sentido no corresponde utilizar dichos requerimientos para pretender establecer límites sobre los alcances de la solución completa, cuyos requerimientos incluyen funcionalidades técnicas y responsabilidades del proveedor.	
34	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3.2.45		28	SUSCRIPCIONES DE SEGURIDAD Análisis avanzado del tráfico DNS DICE: Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algorithm), DNS Tunneling y/o Fast Flux Domain. CONSULTA: Se ha identificado que los requerimientos actuales de seguridad DNS son limitados, ya que omiten la detección de ataques críticos como NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS entre otros. Por esta razón, se solicita a la entidad que confirme, si se produce un incidente de seguridad que se originen por las técnicas mencionadas, el proveedor o contratista quedará exento de toda responsabilidad de brindar soporte o realizar la investigación correspondiente a dicho incidente.	No se confirma lo indicado por el participante. Se precisa que el numeral 3.2.45 del Capítulo III - Requerimiento, corresponde a requerimientos asociados a la funcionalidad "Análisis avanzado del tráfico DNS", la cual es aplicable sólo a los equipos de Categoría B, tal como se establece en el numeral 2.6. En tal sentido no corresponde utilizar dichos requerimientos para pretender establecer límites sobre los alcances de la solución completa, cuyos requerimientos incluyen funcionalidades técnicas y responsabilidades del proveedor.	
35	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	9,8		35	DICE: El plazo de implementación se contabiliza a partir del día siguiente de la fecha indicada en el acta de conformidad de la instalación básica de los equipos hasta el 10 de enero de 2026. CONSULTA: Se requiere confirmar si las actividades a realizar en este plazo corresponden solo a las indicadas en el punto 9.3 o sírvase listar el total de las actividades a realizar en este plazo.	Se confirma lo indicado por el participante. Las actividades que se requiere ejecutar en la implementación se encuentran especificadas en el numeral 9.3 del Capítulo III - Requerimiento.	
36	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3.2.37		27	DICE: Captchas falsos y/o codificación de caracteres HTML y/o inyección de un "Java Script" por parte del NGFW en la página solicitada por el usuario, analizando todos los componentes HTML en tiempo real para su análisis basado en IA y su posterior veredicto de benigno o malicioso. CONSULTA: Se solicita a la Entidad confirmar si corresponde sustentar, mediante documentación pública del fabricante, que los equipos ofertados cuenten con capacidad de inspección en tiempo real de todos los componentes HTML en tiempo real, incorporando mecanismos de análisis avanzado y basados en IA que permitan la detección de contenido malicioso.	Se confirma lo indicado por el participante. Se deberá presentar documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido en el numeral 3.2.37 del Capítulo III de la Sección Específica de las Bases, la cual deberá ser presentada para el perfeccionamiento del contrato. Se agregará una nota correspondiente a dicho requerimiento en el numeral 3.2.37 del Capítulo III de la Sección Específica de las Bases. Asimismo, se agregará como requisito para el perfeccionamiento del contrato en el numeral 5 del Capítulo II de la Sección Específica de las Bases.	3.2.37. Debe contar con medidas de antievasión tales como: ✓ Cloaking y/o motores embebidos los cuales prevengan campañas de phishing de día cero que intenten suplantar marcas locales y/o globales, ello mediante deep learning (aprendizaje profundo). ✓ Captchas falsos y/o codificación de caracteres HTML y/o inyección de un "java Script" por parte del NGFW en la página solicitada por el usuario, analizando todos los componentes HTML en tiempo real para su análisis basado en IA y su posterior veredicto de benigno o malicioso. Nota: Se deberá presentar documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido, la cual deberá ser presentada para el perfeccionamiento del contrato. CAPÍTULO II 5. REQUISITOS PARA PERFECCIONAR EL CONTRATO (..) m. Documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido en el numeral 3.2.37 del requerimiento.
37	IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.	CONSULTA	ESPECIFICA	3.2.44		28	DICE: La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial. CONSULTA: Se solicita a la Entidad confirmar si corresponde sustentar, mediante documentación pública del fabricante, que los equipos ofertados cuenten con mecanismos avanzados de detección para el análisis de tráfico DNS, empleando técnicas de inteligencia artificial a fin de identificar amenazas que no puedan ser mitigadas únicamente mediante firmas o reputación de dominio.	Se confirma lo indicado por el participante. Se deberá presentar documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido en el numeral 3.2.44 del Capítulo III de la Sección Específica de las Bases, la cual deberá ser presentada para el perfeccionamiento del contrato. Se agregará una nota correspondiente a dicho requerimiento en el numeral 3.2.44 del Capítulo III de la Sección Específica de las Bases. Asimismo, se agregará como requisito para el perfeccionamiento del contrato en el numeral 5 del Capítulo II de la Sección Específica de las Bases.	3.2.44. La identificación de amenazas avanzadas camufladas en tráfico DNS deberá contar con mecanismos avanzados de detección con el objetivo de identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para ello se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial. Nota: Se deberá presentar documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido, la cual deberá ser presentada para el perfeccionamiento del contrato. CAPÍTULO II 5. REQUISITOS PARA PERFECCIONAR EL CONTRATO (..) n. Documentación técnica del fabricante de la solución NGFW propuesta, que sustente el cumplimiento lo requerido en el numeral 3.2.44 del requerimiento.