

TÉRMINOS DE REFERENCIA

SERVICIO DE ACCESO DEDICADO A INTERNET PARA LA SEDE CENTRAL

1. OBJETIVO

El objetivo del proceso es contratar a un Proveedor de Servicios de Internet (ISP) con comprobada experiencia en el mercado de las telecomunicaciones para brindar al Programa Integral Nacional para el Bienestar Familiar - INABIF el Servicio de Acceso Dedicado a Internet para la Sede Central.

2. MODALIDAD DE CONTRATACIÓN

A Suma Alzada

3. ÁREA USUARIA SOLICITANTE

Unidad de Tecnologías de la Información

4. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Contar con un enlace dedicado para el acceso a Internet desde la Sede Central, con la finalidad de brindar accesos y servicios a los ciudadanos y servidores del INABIF; buscando elevar los niveles de eficiencia y satisfacción de los usuarios internos y externos.

5. REQUERIMIENTOS TÉCNICOS MÍNIMOS

5.1. GENERALIDADES

Brindar el acceso de Internet a la Sede Central del INABIF, complementado con el servicio de seguridad de borde, que permita minimizar los éxitos de ataques provenientes desde Internet; de acuerdo al siguiente cuadro:

Nº	Nombre de Sede	Dirección	Ancho de Banda	Medio de Enlace
1	Sede Central	Av. San Martín Nº 685 – Pueblo Libre	500 Mbps	Fibra Óptica (Principal)
			500 Mbps	Fibra Óptica (Contingencia)

Para llevar a cabo este proyecto, el proveedor de servicios de Internet deberá realizar de forma integral los trabajos de instalación, configuración y pruebas hasta dejar operativo los servicios y equipos ofrecidos a satisfacción del INABIF. Así mismo, el INABIF brindará los espacios en los gabinetes de comunicaciones y puntos de energía en los PDU. Los cables de energía, adaptadores, transceivers, cableado estructurado (Cobre o Fibra), entre otros, para realizar la interconexión entre los equipos de INABIF y los equipos entregados como parte del servicio, serán por parte del proveedor.

Los enlaces mencionados, deberán trabajar en modo **Activo – Pasivo**. **Todo el equipamiento que son parte del servicio de internet y seguridad será proveído por el postor.**¹

Asimismo, todos los componentes que forman parte del mencionado servicio, tales como cableado, equipos y accesorios, deberán ser nuevos, de primer uso y con vigencia tecnológica al inicio del contrato.

Todos los equipos propuestos, que sean parte de la solución, no deberán tener una antigüedad mayor a tres (3) años de fabricación; el personal de Tecnologías de la Información del INABIF, podrá realizar la verificación de estos, previa coordinación con el contratista, en cualquier momento durante la ejecución del contrato. ~~Deben ser nuevos, de primer uso, de tecnología vigente,~~ **El equipamiento deberá ser nuevo o de primer uso, o vigente y no deberá tener una antigüedad mayor a tres (3) años de fabricación y de uso exclusivo para la Entidad², es decir equipos que no tengan la condición End Of Order (EOO) o Last Service Extension Date (LSED) o End Of Support (EoS) o End Of Life (EoL) o similares no se aceptarán equipos que se encuentren catalogados como EoL (End of Life), EoS (End of Support) o términos equivalentes, asegurando que los equipos estén plenamente vigentes y cuenten con soporte técnico y actualizaciones del fabricante al momento de su implementación, no deberá tener una antigüedad mayor a tres (3) años de fabricación^{3 4}**, al menos durante el primer año de contrato y que se encuentren en condiciones operativas.

5.2. DEL ENLACE DEDICADO A INTERNET DESDE LA SEDE CENTRAL

La coordinación para una visita técnica podrá efectuarse en coordinación con el área técnica en el siguiente correo electrónico institucional: william.arce@inabif.gob.pe, las visitas podrán ser programadas hasta un (01) día antes de la presentación de ofertas.⁵

a. Enlace principal / contingencia

- a.1. Ancho de banda: 500Mbps.
- a.2. El enlace será del tipo simétrico y dedicado al 100%, sin utilizar esquemas de acceso compartido o enlaces del tipo asimétrico.
- a.3. Overbooking nacional: 1:1.
- a.4. El postor, tiene que asegurar la comunicación constante durante toda la ejecución del servicio, para ello deberá contar con salidas internacionales de al menos (02) dos proveedores TIER I, con capacidad mínima de 100 Gbps, tanto como para su salida principal como para su salida de contingencia (100 % fibra óptica), para ello el postor deberá presentar ~~en su propuesta~~ **para el INFORME FINAL DE**

¹ ABSOLUCIÓN DE CONSULTA 136 - WIN EMPRESAS S.A.C.

² ABSOLUCIÓN DE CONSULTA 35 - AMERICA MOVIL PERU S.A.C.

³ ABSOLUCIÓN DE CONSULTA 36 - AMERICA MOVIL PERU S.A.C.

⁴ ABSOLUCIÓN DE CONSULTA 137 - WIN EMPRESAS S.A.C.

⁵ ABSOLUCIÓN DE CONSULTA 61 - FRAVATEL EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA

IMPLEMENTACIÓN⁶, un diagrama de la salida internacional detallando los nombres de los proveedores TIER I.

- a.5. El ~~servicio debe incluir un componente en HA activo-pasivo de seguridad de borde (Secure Access Service Edge – SASE).~~⁷

Se acoge la consulta. Se confirma que la solución de seguridad podrá ser implementada mediante una solución del tipo Secure Access Service Edge (SASE) o Next Generation Firewall (NGFW) en alta disponibilidad (HA), siempre y cuando cumpla con las características detalladas en la absolución de consulta N° 37.⁸

Se acepta una opción SASE o NGFW en HA on-premise, siempre que NGFW cumpla al menos con los siguientes requisitos técnicos:

- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para: "Enterprise Network Firewall" en los últimos 10 reportes.
- Throughput de prevención de amenazas de 4gbps y 256 Mil nuevas sesiones/conexiones por segundo.
- NGFW u otro componente, 4x1G interfaces bypass para la optimización de tráfico.

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades".^{9 10}

- a.6. La administración de los equipos de seguridad debe ser compartida entre el proveedor y el personal de la Unidad de Tecnologías de Información del INABIF. La administración por parte del personal de la UTI-INABIF será únicamente para la generación de usuarios, reglas y políticas internas; cualquier otra configuración, a solicitud del INABIF, deberá ser realizada por el personal del SOC/NOC del proveedor.
- a.7. En el caso de que se requiera el apagado de los equipos que forman parte de la solución ofertada, esta será requerida al contratista a través de la central de atención al cliente.
- a.8. Una vez finalizado el plazo contractual, se realizará la devolución del total de los equipos que hayan sido entregados y/o instalados en el INABIF, por parte del proveedor, para lo cual se realizará previamente una coordinación para su recojo.
- a.9. El servicio brindado por el proveedor debe considerar la gestión de los equipos de acceso a Internet en coordinación con el personal de la Unidad de Tecnologías de la Información del INABIF. La gestión de los equipos routers será únicamente del contratista, brindándose solo acceso de lectura al personal de la UTI-INABIF,

⁶ ABSOLUCIÓN DE OBSERVACIÓN 09 - AMERICA MOVIL PERU S.A.C.

⁷ ABSOLUCIÓN DE CONSULTA 138 - WIN EMPRESAS S.A.C.

⁸ ABSOLUCIÓN DE CONSULTA 181 - WIN EMPRESAS S.A.C.

⁹ ABSOLUCIÓN DE CONSULTA 37 - AMERICA MOVIL PERU S.A.C.

¹⁰ ABSOLUCIÓN DE CONSULTA 82 - GLOBAL LINK ONE S.A.C.

designado para este fin. En caso de necesitarse algún cambio de configuración durante la operación del servicio este deberá ser solicitado por el personal autorizado de la UTI-INABIF, quien realizará las coordinaciones correspondientes con el contratista. En el caso de los equipos de seguridad, la administración será compartida, es decir, será realizado por el proveedor y la Entidad.

- a.10. Asignación de números de IP públicos deberán ser bajo el protocolo IPv4 e IPv6, las mismas que incluye la dirección de red, la dirección de broadcast y la dirección del router.

Para el servicio de Internet de última milla, el proveedor deberá brindar 32 direcciones IPv4 e IPv6.

Asimismo, solo en el caso de SASE, se deberá considerar lo señalado en el inciso 5.3.b.5.¹¹

En cuanto al pool de direcciones IPv6, tanto para SASE como para NGFW, no será necesario añadir direcciones IP adicionales, siempre que se cumplan las características descritas en la absolución de la absolución de consulta N°37.

Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹²

- a.11. El proveedor deberá cambiar la IP publica de salida a internet cuando el INABIF lo solicite.

Se menciona que el proveedor deberá cambiar la IP pública de salida a Internet cuando INABIF lo solicite y se cumpla en los tiempos estipulados en los SLA.

El cambio de IP pública es fundamental para garantizar la continuidad operativa y evitar que la dirección IP pública del INABIF pueda ser bloqueada o incluida en listas negras que influyan en el desempeño operativo.

Si bien este cambio implica una actualización en la configuración de NAT y las políticas de seguridad, este proceso es una práctica común en la administración de redes y debe ser gestionado a través de los distintos equipos propuestos por el postor como parte del servicio.¹³

Las características mencionadas y señaladas se refieren a la posibilidad de cambiar la dirección IP pública de salida hacia internet, la cual estará incluida dentro del Pool de 32 dirección IPv4 e IPv6 provistas por el postor y que serán asignadas a la entidad como parte del servicio.¹⁴

Asimismo, se menciona que no será necesario añadir direcciones IP adicionales a lo solicitado en bases.¹⁵

La capacidad se refiere a cambiar la dirección IP Publica que corresponde a los

¹¹ ABSOLUCIÓN DE CONSULTA N° 139 - WIN EMPRESAS S.A.C.

¹² ABSOLUCIÓN DE CONSULTA 38 - AMERICA MOVIL PERU S.A.C.

¹³ ABSOLUCIÓN DE CONSULTA N° 141 - WIN EMPRESAS S.A.C.

¹⁴ ABSOLUCIÓN DE CONSULTA 39 - AMERICA MOVIL PERU S.A.C.

¹⁵ ABSOLUCIÓN DE CONSULTA 39 - AMERICA MOVIL PERU S.A.C.

enlaces de Internet instalados.¹⁶**Se acoge la consulta**

Se aclara que para el servicio de Internet (última milla) el proveedor deberá brindar 32 direcciones IPv4 como IPv6, de acuerdo a lo señalado en el inciso 5.3.b.5 en el caso de SASE.¹⁷

- a.12. El servicio debe contemplar la gestión de segmentación y priorización del tráfico de acceso a Internet, a través de la funcionabilidad de Calidad de Servicio (QoS), podrá ser suministrada por el componente seguridad de borde (SASE **o NGFW de igual o superior característica siempre que cumpla con las características descritas en la absolución de la consulta N°37**) propuesto por el contratista de acuerdo con los requerimientos del INABIF.

Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{18 19}

Se aclara que este punto hace referencia a la calidad de servicio (QoS). El cual podrá ser manejado por el equipo propuesto por el postor, ya sea a través de una solución SASE o un equipo de seguridad perimetral.

Esto garantiza que la administración del tráfico pueda realizarse de manera eficiente dentro de los parámetros definidos, permitiendo una mejor gestión del ancho de banda y priorización de tráfico según las necesidades de la Entidad.²⁰

- a.13. El servicio deberá comprender acceso y uso irrestricto de todos los protocolos TCP/IP.
- a.14. El proveedor deberá contar con una red principal o backbone propia con redundancia e implementado en su totalidad con fibra óptica, incluido la última milla para el servicio.
- a.15. **Opcionalmente^{21 22}**, el servicio deberá incluir un componente en nube con GUI en idioma español para la gestión y el análisis de logs se realizará a través de un "Data Lake", que se integre con el componente SASE y que genere de manera automatizada informes; asimismo, debe disponer un catálogo de al menos 12,500 aplicaciones, un catálogo de amenazas de al menos 19,500 threats, lo mismo que permitirá la visualización de un inventario de dispositivos y un cuadro de mando de red donde se permita visualiza en un único dashboard: el promedio de Throughput en el tiempo de la sede y de los usuarios, y los datos del enlace principal como secundario referente al total de Bytes de subida, total de Bytes de bajada, pérdida de paquetes de subida/bajada, paquetes descartados de subida y

¹⁶ ABSOLUCIÓN DE CONSULTA 84 - GLOBAL LINK ONE S.A.C.

¹⁷ ABSOLUCIÓN DE CONSULTA N° 140 - WIN EMPRESAS S.A.C.

¹⁸ ABSOLUCIÓN DE CONSULTA 40 - AMERICA MOVIL PERU S.A.C.

¹⁹ ABSOLUCIÓN DE CONSULTA 85 - GLOBAL LINK ONE S.A.C.

²⁰ ABSOLUCIÓN DE CONSULTA N° 142 - WIN EMPRESAS S.A.C.

²¹ ABSOLUCIÓN DE CONSULTA 86 - GLOBAL LINK ONE S.A.C.

²² ABSOLUCIÓN DE CONSULTA 182 - WIN EMPRESAS S.A.C.

bajada. El contratista deberá brindar el acceso de lectura/escritura de este componente, el cual debe accederse mediante un usuario y contraseña con MFA.

- a.16. Entregar reportes mensuales al INABIF por el servicio utilizado (SLA, utilización del ancho de banda, estadísticas de fallas ocurridas, tickets generados, tickets atendidos, tiempos de respuesta del servicio técnico, disponibilidad del enlace) en documento físico o electrónico al cierre del ciclo de facturación; este es requisito indispensable para el otorgamiento de la conformidad del servicio.

Se confirma y aclara que la disponibilidad del enlace se podrá ver en la gráfica que brinde la herramienta monitor.²³

b. Enlace de contingencia

- b.1. El ancho de banda del enlace de contingencia deberá ser del 100% de ancho de banda del enlace principal.
- b.2. Overbooking nacional 1:1.
- b.3. La ruta del enlace de contingencia deberá ser distinto al del enlace principal, no podrá ser el mismo enlace físico y deberá partir desde un nodo de acceso diferente y con destino independiente en la red del contratista.
- b.4. El enlace de contingencia deberá ser por medio de fibra óptica partiendo desde otro nodo, con una ruta distinta.
- b.5. El consumo por el uso de este servicio será por demanda y solo cuando ocurra un problema en el enlace principal.

Se aclara que el servicio solicitado es un escenario de Activo-Pasivo, es decir, solo si el enlace principal fallara, entrara en funcionamiento la contingencia, hasta que se restablezca el enlace Principal.²⁴

- b.6. Activación automática del enlace de contingencia ante una interrupción del enlace principal, y debe retornar de forma automática al esquema principal, luego de haberse solucionado la interrupción o problema del enlace en mención.
- b.7. El contratista debe proporcionar los equipos de comunicación para cada uno de los enlaces el principal y el de contingencia.
- b.8. El contratista debe entregar, al término de la instalación, un informe final de implementación el cual debe contener información sobre la tecnología de transporte empleada y conexión a la red institucional; los tipos de reportes que se pueden obtener respecto al consumo del ancho de banda y los reportes que se generen para la gestión de la red.
- b.9. El contratista deberá entregar los planos impresos; en formato A0 o A1, y en formatos digital de AutoCAD, PDF; donde se muestre las dos rutas (principal y contingencia), el mismo que se entregado con el informe final de implementación

²³ ABSOLUCIÓN DE CONSULTA N° 143 - WIN EMPRESAS S.A.C.

²⁴ ABSOLUCIÓN DE CONSULTA N° 144 - WIN EMPRESAS S.A.C.

del servicio.

Se confirma que se permitirá poder entregar un plano en formato AutoCAD o PDF.²⁵

- b.10. Todos los componentes relacionados a la implementación del servicio serán brindados por el proveedor, sin costo adicional para el INABIF.

5.3. **CARACTERÍSTICAS DE LOS EQUIPOS MÍNIMOS A SER INCLUIDOS**

Para efectos de la correcta prestación del servicio, es necesario que todos los componentes relacionados a la implementación del servicio sean brindados por el proveedor sin costo adicional para el INABIF.

Se aclara que los equipos se encontrarán en modalidad de alquiler.²⁶

Se confirma que, una vez finalizado el plazo contractual, procederá a la devolución del total de los equipos que le hayan sido entregados y/o instalados. Para ello, se comunicará al contratista para disponer del retiro de equipos dentro de los diez días calendarios de finalizado el contrato o de haber sido notificado.²⁷

a. Equipo de enrutamiento de tráfico (Router)

- a.1. El/los equipos de enrutamiento de tráfico de red deben garantizar la capacidad de rendimiento y procesamiento del servicio contratado.
- a.2. El/los equipos de proporcionados para el cumplimiento del servicio deberán contar con soporte y licenciamiento de fábrica, el cual será provista por el mismo contratista, durante la vigencia del servicio, contado a partir del día siguiente de suscrita el Acta de Conformidad de Instalación del Servicio.
- a.3. Los equipos de enrutamiento deben soportar los anchos de banda contratados como mínimo.
- a.4. Es necesario que los equipos puedan tener funcionalidades de control de acceso a nivel de capa 3. Estas características son por cada equipo de cada enlace.
- a.5. Deberán contar con una capacidad mínima de memoria RAM de 512MB y memoria FLASH de 32MB.

b. Equipo de Seguridad de Borde (SASE)

Se acepta una opción SASE o NGFW en HA on-premise, siempre que NGFW cumpla al menos con los siguientes requisitos técnicos:

- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para:

²⁵ ABSOLUCIÓN DE CONSULTA N° 145 - WIN EMPRESAS S.A.C.

²⁶ ABSOLUCIÓN DE CONSULTA N° 72 - WIN EMPRESAS S.A.C.

²⁷ ABSOLUCIÓN DE CONSULTA N° 73 - WIN EMPRESAS S.A.C.

"Enterprise Network Firewall" en los últimos 10 reportes.

- **Throughput de prevención de amenazas de 4gbps y 256 Mil nuevas sesiones/conexiones por segundo.**
- **NGFW u otro componente, 4x1G interfaces bypass para la optimización de tráfico.**

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades".^{28 29 30 31 32 33}

- b.1. EL PROVEEDOR deberá considerar dos (02) componentes en Activo-Pasivo que incluya los siguientes criterios técnicos:
- Cuatro (04) puertos 1GE/2.5GE;
 - Dos (02) puertos USB; y
 - Agregación de hasta (03) interfaces WAN.
- b.2. El servicio de seguridad deberá contar con un punto de presencia en Perú, y redundancia en otro punto fuera del territorio nacional, **de manera opcional toda vez que presente una solución SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolución de consulta N°37.³⁴** El proveedor opcionalmente podrá entregar una página web con el estatus de salud de sus puntos de presencia. **No es obligatorio su presentación.³⁵**
- b.3. Deberá ser nombrado líder en el cuadrante mágico de Gartner para "single-vendor SASE" del 2024.
- b.4. Como parte de la propuesta, se deberá proporcionar al menos 10(diez) cuentas de acceso al portal del fabricante, para acceder, de manera gratuita, a los cursos "Expert" SASE. **La habilitación de las cuentas, se deberá acreditar en el INFORME FINAL DE IMPLEMENTACIÓN.³⁶**
- b.5. Se debe considerar treinta y dos (32) direcciones IP públicas IPv4 ubicadas en Lima, registradas bajo el ASN del fabricante de la solución ofertada. Dicho ASN deberá ser independiente de cualquier operador local y su direccionamiento IP.

No será necesario considerar IP Pool IPv6 para SASE o NGFW.

²⁸ ABSOLUCIÓN DE CONSULTA 37 - AMERICA MOVIL PERU S.A.C.

²⁹ ABSOLUCIÓN DE CONSULTA 87 - GLOBAL LINK ONE S.A.C.

³⁰ ABSOLUCIÓN DE CONSULTA 183 – WIN EMPRESAS S.A.C.

³¹ ABSOLUCIÓN DE CONSULTA 184 – WIN EMPRESAS S.A.C.

³² ABSOLUCIÓN DE CONSULTA 185 – WIN EMPRESAS S.A.C.

³³ ABSOLUCIÓN DE CONSULTA 186 – WIN EMPRESAS S.A.C.

³⁴ ABSOLUCIÓN DE CONSULTA 88 - GLOBAL LINK ONE S.A.C.

³⁵ ABSOLUCIÓN DE CONSULTA N° 10 - AMERICA MOVIL PERU S.A.C.

³⁶ ABSOLUCIÓN DE CONSULTA N° 11 - AMERICA MOVIL PERU S.A.C.

Adicionalmente, se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolució de consulta N°37.^{37 38}

- b.6. Desde el gestor de la solució, el personal con rol de administrador de la entidad podrá modificar las direcciones IP púlicas, pudiendo seleccionar IPs de Lima-Perú o de otros países, con al menos 80 opciones de ubicaciones geográficas distintas. Esto permitirá optimizar las comunicaciones de la entidad, **no será necesario esta característica siempre que el postor considere una solució SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolució de consulta N°37.^{39 40}**
- b.7. La actualización de la plataforma, así como los mantenimientos, deberán ser realizados por el fabricante. Este deberá llevar a cabo actualizaciones al menos dos veces al mes.
- b.8. Deberá incluir la generació de perfiles de usuario para la priorizació del ancho de banda, visibilidad de tráfico de manera granular basado en top aplicaciones, top categorías, top destinos.

Se confirma y aclara que una herramienta de monitoreo de enlaces o dashboard de un router no es capaz de gestionar la priorizació del ancho de banda o brindar visibilidad de acuerdo con las necesidades específicas de INABIF.^{41 42}

- b.9. Así mismo, deberá brindar visibilidad de la siguiente informaci3n:
- El Throughput de subida y bajada del tráfico;
 - El tamaño de cola;
 - El número de paquetes descartados;
 - Top Hosts y Top Aplicaciones;
 - Distancia, Jitter, Packet Loss; y
 - Perfiles de ancho de banda.

No será necesario la presente característica, siempre que se presenten soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolució de consulta N°37.^{43 44}

- b.10. Priorizació y gesti3n de ancho de banda para aplicaciones críticas de negocio. La asignaci3n de ancho de banda deberá ser porcentual, por prioridades y permitir

³⁷ ABSOLUCI3N DE CONSULTA 89 - GLOBAL LINK ONE S.A.C.

³⁸ ABSOLUCI3N DE CONSULTA 187 - WIN EMPRESAS S.A.C.

³⁹ ABSOLUCI3N DE CONSULTA 90 - GLOBAL LINK ONE S.A.C.

⁴⁰ ABSOLUCI3N DE CONSULTA 188 - WIN EMPRESAS S.A.C.

⁴¹ ABSOLUCI3N DE CONSULTA 91 - GLOBAL LINK ONE S.A.C.

⁴² ABSOLUCI3N DE CONSULTA 189 - WIN EMPRESAS S.A.C.

⁴³ ABSOLUCI3N DE CONSULTA 92 - GLOBAL LINK ONE S.A.C.

⁴⁴ ABSOLUCI3N DE CONSULTA 190 - WIN EMPRESAS S.A.C.

opciones como no limitar, limitar siempre y limitar cuando exista congestión del circuito.

No será necesario el cumplimiento de esta característica, cuando el contratista brinde soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.⁴⁵

- b.11. El servicio deberá reconocer por lo mínimo 12,500 aplicaciones y permitir crear aplicaciones customizadas.

Dicha característica será opcional para el NGFW y se considerará 3,500 aplicaciones para la opción SASE. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolución de consulta N°37.^{46 47}

- b.12. La actualización de la plataforma y los componentes de hardware deberá ser realizado por el fabricante, lo mismo que los mantenimientos. El fabricante deberá realizar actualizaciones al menos dos veces por mes.

- b.13. La visualización de las aplicaciones y prioridades deberá ser en tiempo real con uno o tres segundos de actualización. En el caso de las prioridades, se deberá poder tener historial de mínimo tres (03) meses.

No será necesario la presente característica toda vez que el contratista cumpla con brindar soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.^{48 49}

- b.14. Detalle de la utilización de los enlaces por top usuarios, top aplicaciones y por ubicación (país) de la sede.

No será necesario la presente característica toda vez que el contratista cumpla con brindar soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.^{50 51}

- b.15. A continuación, se detallan las funcionalidades de ciberseguridad requeridas:

Filtrado WEB

- Basado en categorías;
- Basado en URL o Dominio;

⁴⁵ ABSOLUCIÓN DE CONSULTA 93 - GLOBAL LINK ONE S.A.C.

⁴⁶ ABSOLUCIÓN DE CONSULTA 94 - GLOBAL LINK ONE S.A.C.

⁴⁷ ABSOLUCIÓN DE CONSULTA 191 - WIN EMPRESAS S.A.C.

⁴⁸ ABSOLUCIÓN DE CONSULTA 95 - GLOBAL LINK ONE S.A.C.

⁴⁹ ABSOLUCIÓN DE CONSULTA 192 - WIN EMPRESAS S.A.C.

⁵⁰ ABSOLUCIÓN DE CONSULTA 96 - GLOBAL LINK ONE S.A.C.

⁵¹ ABSOLUCIÓN DE CONSULTA 193 - WIN EMPRESAS S.A.C.

- Basado en URL personalizado por la entidad; y
- Deberá incluir, la opción de búsqueda de dominios que permita consultar el URL o dominio a fin de obtener su categoría.

Filtrado de Aplicaciones

- Basado en categorías;
- Basado en aplicación predefinida;
- Basado en aplicación personalizada por la entidad; y
- Basado en grupo de aplicaciones personalizadas.

No será necesario la presente característica toda vez que el contratista cumpla con brindar soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.^{52 53}

- b.16. Deberá incluir un catálogo de aplicaciones ~~no menor a 12,500~~ **de 3500** aplicaciones **para la opción SASE. Para la solución NGFW, será opcional, siempre que el contratista cumpla con las funciones detalladas en la absolución de consulta N°37.^{54 55}**

- b.17. Las aplicaciones predefinidas deberán disponer de una descripción de tallada, una categoría, una definición de riesgo, un análisis de cumplimiento ISAE 3402, PCI-DSS, ISO 27001, SOC 1/2/3, y un análisis de seguridad que incluya: TLS Enforcement, RBAC, MFA, SSO, HTTP Security Headers. **Para la opción de NGFW será opcional toda vez que cubra las funciones detalladas en la absolución de consulta N° 37.^{56 57}**

- b.18. IPS (Intrusion Prevention System) que incluya las siguientes categorías:

- Crypto Mining;
- Phishing;
- Ransomware;
- Privilege Escalation;
- Web Application Attack; y
- Restricciones de geolocalización.

Se acoge la consulta de forma parcial.

⁵² ABSOLUCIÓN DE CONSULTA 97 - GLOBAL LINK ONE S.A.C.

⁵³ ABSOLUCIÓN DE CONSULTA 194 – WIN EMPRESAS S.A.C.

⁵⁴ ABSOLUCIÓN DE CONSULTA 98 - GLOBAL LINK ONE S.A.C.

⁵⁵ ABSOLUCIÓN DE CONSULTA 195 – WIN EMPRESAS S.A.C.

⁵⁶ ABSOLUCIÓN DE CONSULTA 99 - GLOBAL LINK ONE S.A.C.

⁵⁷ ABSOLUCIÓN DE CONSULTA 196 – WIN EMPRESAS S.A.C.

Dicha característica será opcional para el NGFW. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.

Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{58 59}

- b.19. Deberá disponer de un motor de Next Generation Anti Malware que permita la protección de archivos de 10MB y de los siguientes tipos: APK, Archives (ZIP, 7ZIP, TGZ, RAR, ARJ, ARC, ZOO), BAT, BIN, CAB, Calendar (ICS, IFB, iCalendar), CMD, CRX, CSV, DEB, DLL, DMG, EXE, FLASH (SWF), Fonts (EOT, WOFF, WOFF2), HTA, JAVA (JAR, CLASS), MACH-O, Microsoft Office (DOC, DOCx, PPT, PPTx, XLS, XLSx), MS-Access (ACCDB), MSI, OFT, PDF, PKG, PS1, PY, RTF, SH, Torrent, VB-Scripts, EXE, MacOS, BIN, MSI, ZIP, TAR, RAR, OLE (.doc, .ppt, .xls), OpenXML (.docx, .pptx, .xlsx), Win32 portable executable
- b.20. Event Viewer
- Historial 3 meses
 - Nombre de regla
 - Contador de eventos
 - Subtipo de evento
 - IP origen
 - Sitio destino (nombre)
 - País de origen
 - Tipo Sistema operative
 - IP destino
 - Acción
 - Fecha y Hora
 - Inspección TLS
 - Aceleración
 - Puertos
 - País de destino
- b.21. Debe incluir capacidades de XDR tanto a nivel de seguridad como a nivel de red (network). Así mismo, debe incluir en los logs de seguridad información MITRE ATT&CK que catalogue el nivel de ataque. **Dicha característica será opcional para el NGFW. Se aceptarán soluciones SASE o NGFW de igual o superiores**

⁵⁸ ABSOLUCIÓN DE CONSULTA 100 - GLOBAL LINK ONE S.A.C.

⁵⁹ ABSOLUCIÓN DE CONSULTA 197 – WIN EMPRESAS S.A.C.

características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.^{60 61}

- b.22. Deberá incluir capacidades de XDR tanto a nivel de seguridad como a nivel de red (network). Así mismo, deberá incluir en los logs de seguridad información MITRE ATT&CK que catalogue el nivel de ataque. **Dicha característica será opcional para el NGFW. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolución consulta N°37.^{62 63}**
- b.23. Dentro de las capacidades de XDR deberá incluir un dashboard que incluya el siguiente análisis: evaluación del riesgo del cliente, Top 5 las historias de eventos más críticos, Top 5 eventos por Indicadores de Ataque, Top 5 por técnicas de MITRE. Así mismo deberá incluir fuentes de inteligencia de amenazas de Virtus Total, AbuseIPDB, IPQualityScore, UrlScan, AlienVault, Twitter, Shodan e IBM X-Force Exchange, y los incidentes podrán ser simplificados en cuanto a contenido mediante un resumen realizado por IA. **Dicha característica será opcional para el NGFW. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolución de consulta N°37.^{64 65}**
- b.24. Se solicitan 270 usuarios de acceso seguro ZTNA para la interconexión de los usuarios de los centros de atención de INABIF, dicho componente deberá contar con las siguientes características:

Se acoge parcialmente la consulta.

El postor podrá considerar características distintas para ZTNA, siempre que cumplan con las funciones detalladas en la absolución de la consulta N°104:

1. Que sea una solución de ZTNA, que permita tres sesiones simultáneas por usuario remoto o que el postor considere 810 usuarios remotos.

2. Que tenga habilitado MFA para la autenticación robusta.

3. Que considere filtrado de navegación, inspección IPS, protección DNS, antimalware, para que el tráfico del usuario remoto sea inspeccionado y controlado antes de llegar al perímetro de INABIF.

⁶⁰ ABSOLUCIÓN DE CONSULTA 101 - GLOBAL LINK ONE S.A.C.

⁶¹ ABSOLUCIÓN DE CONSULTA 198 – WIN EMPRESAS S.A.C.

⁶² ABSOLUCIÓN DE CONSULTA 102 - GLOBAL LINK ONE S.A.C.

⁶³ ABSOLUCIÓN DE CONSULTA 199 – WIN EMPRESAS S.A.C.

⁶⁴ ABSOLUCIÓN DE CONSULTA 103 - GLOBAL LINK ONE S.A.C.

⁶⁵ ABSOLUCIÓN DE CONSULTA 200 – WIN EMPRESAS S.A.C.

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades".^{66 67 68 69 70 71}

Se aclara que la cantidad de buzones de correo debe ser distinta a la cantidad de usuarios remotos ZTNA, no deben ser iguales.⁷²

La aclara o precisa que la cantidad de usuarios remotos solicitado (270) es distinta a la cantidad de buzones de correo (2700). Se confirma que dicha cantidad será la necesaria para cubrir el plazo del servicio para la presente necesidad de INABIF.⁷³

- Acceso por cliente para sistemas operativos sin fin de vida comercial como Windows, MacOS, Linux, Android e IOS.
- Cada licencia por usuario deberá permitir tres (03) sesiones simultáneas para Windows, Linux, MacOS, Android o IOS.

Se acoge parcialmente la consulta.

Considerar que el acceso remoto guarde compatibilidad con Windows, Linux, MacOS, Android o iOS es relevante para INABIF porque asegura que los usuarios puedan conectarse a los sistemas de manera segura, independientemente del dispositivo o sistema operativo que utilicen. Esto facilita la implementación de políticas de seguridad uniformes, mejora la accesibilidad de los empleados y colaboradores, y garantiza la continuidad de los servicios sin importar las plataformas utilizadas, contribuyendo a una mayor flexibilidad y eficiencia operativa.

Sin embargo, para garantizar la pluralidad de postores dicho termino podrá ser considerado opcional siempre que cumplan con las funciones detalladas en la absolución de la consulta N° 104.⁷⁴

- El agente ZTNA deberá permitir el logo de INABIF para los usuarios de Windows, y mostrar el tiempo de conexión del usuario y la siguiente información:
 - ✓ Evaluar la conexión a través de un feedback con una opción directa desde el cliente.
 - ✓ Deberá mostrar la cantidad de los datos transferidos, tanto enviados como recibidos expresado en Megabytes.

⁶⁶ ABSOLUCIÓN DE CONSULTA 104 - GLOBAL LINK ONE S.A.C.

⁶⁷ ABSOLUCIÓN DE CONSULTA 106 - GLOBAL LINK ONE S.A.C.

⁶⁸ ABSOLUCIÓN DE CONSULTA 107 - GLOBAL LINK ONE S.A.C.

⁶⁹ ABSOLUCIÓN DE CONSULTA 112 - GLOBAL LINK ONE S.A.C.

⁷⁰ ABSOLUCIÓN DE CONSULTA 111 - GLOBAL LINK ONE S.A.C.

⁷¹ ABSOLUCIÓN DE CONSULTA 207 – WIN EMPRESAS S.A.C.

⁷² ABSOLUCIÓN DE CONSULTA 105 - GLOBAL LINK ONE S.A.C.

⁷³ ABSOLUCIÓN DE CONSULTA 202 – WIN EMPRESAS S.A.C.

⁷⁴ ABSOLUCIÓN DE CONSULTA 203 – WIN EMPRESAS S.A.C.

- ✓ Mostrar la dirección IP Local o LAN del usuario remoto, la dirección IP brindada por el fabricante, la conexión al POP, archivo PAC, y datos de la identidad del usuario como "last reported" y el estado.
- ✓ Mostrar la distancia del usuario remoto al POP al cual se conecta expresado en ms (milisegundos).

No se acoge la consulta.

Se aclara que Zero Trust Network Access es una tecnología ofrecida por diversos fabricantes que asegura una conexión segura para los usuarios remotos, algo que los agentes de VPN no pueden garantizar de manera similar. Mientras que ZTNA se basa en un enfoque de autenticación y autorización estrictos, verificando continuamente a cada usuario y dispositivo independientemente de su ubicación, las VPN solo crean un túnel seguro para la transmisión de datos, sin evaluar de manera constante la confiabilidad del usuario o el dispositivo.⁷⁵

- Con la finalidad de evitar el robo de información mediante exposición de credenciales, la plataforma deberá considerar la característica de MFA (Multi Factor Authentcator)
- Protección de al menos 75 categorías de navegación. El agente ZTNA para Windows podrá ser customizado con el logo de la entidad.

Se acoge parcialmente la consulta.

Colocar el logo en el agente de ZTNA permite reforzar la identidad corporativa, brindando una experiencia más personalizada y alineada con la imagen institucional. Además, ayuda a generar confianza en los usuarios al interactuar con una solución de acceso seguro que representa oficialmente a la organización.

Sin embargo, para garantizar la pluralidad de postores el término "El agente ZTNA para Windows podrá ser customizado con el logo de la entidad" será opcional siempre que cumplan con las funciones detalladas en la absolución de la consulta N° 104.⁷⁶

- Deberá incluir dentro de la interface de usuario la opción de búsqueda de dominios o "Domain Lookup" que permita ingresar el URL y mostrar la categoría a la que pertenece.
- Catálogo de aplicaciones no menos a ~~12,500~~ aplicaciones las cuales deberán disponer un análisis de cumplimiento ISAE 3402, PCI-DSS, ISO 27001, SOC 1/2/3, y un análisis de seguridad que incluya: TLS Enforcement, RBAC, MFA, SSO, HTTP Security Headers.

⁷⁵ ABSOLUCIÓN DE CONSULTA 201 – WIN EMPRESAS S.A.C.

⁷⁶ ABSOLUCIÓN DE CONSULTA 204 – WIN EMPRESAS S.A.C.

Dicha característica será opcional para el NGFW y se considerará 3,500 aplicaciones para la opción SASE. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre en cuanto cumplan con las funciones detalladas en la absolución de consulta N°37.^{77 78 79}

Se acoge parcialmente la consulta.

El postor hace referencia a un criterio técnico, pero formula su pregunta en relación con otro criterio técnico distinto, lo que genera dudas y puede llevar a interpretaciones erróneas. Es necesario aclarar la consulta para asegurar una comprensión precisa y evitar posibles confusiones en la evaluación.

Sin embargo, para garantizar la pluralidad de postores el termino referido y consultado será opcional siempre en cuanto cumplan con las funciones detalladas en la absolución de la consulta N° 104.^{80 81}

- ✓ Deberá disponer un módulo de IPS que permita la inspección del tráfico de los usuarios remotos ZTNA, que a su vez considere al menos las siguientes categorías: Ataques de Crypto Mining, Phishing, Ransomware, Privilege Escalation, Web Application Attack.

Se acoge parcialmente la consulta.

Las categorías IPS listadas son consideradas por INABIF para mejorar el orden y la claridad durante la gestión de las amenazas, facilitando su clasificación, priorización y respuesta. Esto permite una detección más eficiente, un análisis más preciso de los incidentes de seguridad y una mejor toma de decisiones frente a posibles riesgos.

Sin embargo, para garantizar la pluralidad de postores el término "que a su vez considere al menos las siguientes categorías: Ataques de Crypto Mining, Phishing, Ransomware, Privilege Escalation, Web Application Attack" será opcional siempre que cumplan con las funciones detalladas en la absolución de consulta N° 104.^{82 83 84}

- ✓ Protección DNS que permita el control de: Dynamic DNS, DNS Tunnelling, Phishing, DGAs, C&C, dominios maliciosos.
- ✓ Incluir XDR tanto para seguridad como para networking. Así mismo deberá incluir fuentes de inteligencia de amenazas de Virtus Total,

⁷⁷ ABSOLUCIÓN DE CONSULTA 108 - GLOBAL LINK ONE S.A.C.

⁷⁸ ABSOLUCIÓN DE CONSULTA 109 - GLOBAL LINK ONE S.A.C.

⁷⁹ ABSOLUCIÓN DE CONSULTA 110 - GLOBAL LINK ONE S.A.C.

⁸⁰ ABSOLUCIÓN DE CONSULTA 205 – WIN EMPRESAS S.A.C.

⁸¹ ABSOLUCIÓN DE CONSULTA 206 – WIN EMPRESAS S.A.C.

⁸² ABSOLUCIÓN DE CONSULTA 111 - GLOBAL LINK ONE S.A.C.

⁸³ ABSOLUCIÓN DE CONSULTA 207 – WIN EMPRESAS S.A.C.

⁸⁴ ABSOLUCIÓN DE CONSULTA 208 – WIN EMPRESAS S.A.C.

AbuseIPDB, IPQualityScore, UrlScan, AlienVault, Twitter, Shodan e IBM X-Force Exchange, y los incidentes podrán ser simplificados en cuanto a contenido mediante un resumen realizado por IA.

- ✓ Deberá validar la postura de seguridad del dispositivo considerando: versión permitida del antivirus de la entidad, encriptación de disco, gestor de parche utilizado por la entidad, certificado de la entidad instalado en el dispositivo, DLP usado por la entidad.

b.25. Todos los componentes descritos deberán ser gestionados desde una única consola de administración, para el monitoreo y su configuración.

b.26. Para evaluar la solución de seguridad ~~es necesario que el postor presente en la etapa de presentación de ofertas,~~ **se acreditará con la presentación del ANEXO N° 03**, la documentación técnica que acredite el cumplimiento de la solución descrita en el numeral ~~4.3.2,~~ **5.3.b.**

"Para evaluar la solución de seguridad es necesario que el postor presente en la relación de documentos a presentar con el "Cronograma de Actividades", la documentación técnica que acredite el cumplimiento de la solución descrita en el numeral 5.3.b".^{85 86 87 88}

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades"

5.4. SOLUCIÓN DE ANTISPAM

Se requiere el servicio de antispam basado en Nube para el dominio principal y 2,700 buzones de correo para Zimbra.

a. Características técnicas mínimas:

- a.1. Servicio antispam en NUBE (no requerir hardware).
- a.2. Salvaguardar la reputación del dominio de correo @inabif.gob.pe
- a.3. Contar con protección Anti-Relay.
- a.4. El acceso al antispam en nube debe ser registrado con un correo del dominio del Programa Integral Nacional para el Bienestar Familiar - INABIF.
- a.5. La suscripción debe estar inscrita a nombre del Programa Integral Nacional para el Bienestar Familiar - INABIF.
- a.6. Contar con protección, que evite que terceros hagan uso y envíen correo a nuestro a nombre de un o más usuarios del Programa Integral Nacional para el Bienestar Familiar - INABIF.

⁸⁵ ABSOLUCIÓN DE CONSULTA 13 - AMERICA MOVIL PERU S.A.C.

⁸⁶ ABSOLUCIÓN DE CONSULTA 146 - WIN EMPRESAS S.A.C.

⁸⁷ ABSOLUCIÓN DE CONSULTA 147 - WIN EMPRESAS S.A.C.

⁸⁸ ABSOLUCIÓN DE CONSULTA 148 - WIN EMPRESAS S.A.C.

- a.7. Detectar ataques de SPAM en cuanto ellos emergen para una protección inmediata y continua.
- a.8. Las firmas de SPAM deben actualizarse regularmente, durante todo el periodo de licenciamiento del contrato del producto.
- a.9. Capacidad de crear listas blancas y negras por remitente o destinatario.
- a.10. Capacidad de etiquetar correo considerado como: SPAM, probable SPAM o Bulk.
- a.11. Detectar y bloquear el SPAM, independiente del lenguaje, formato o contenido del mensaje.
- a.12. Garantizar un porcentaje de falsos positivos cercano a cero.
- a.13. Contar con un espacio de cuarentena para el almacenamiento de SPAM.
- a.14. Debe trabajar a nivel de SMTP, POP3 e IMAP.
- a.15. Capacidad para soportar la gestión de usuarios ilimitados concurrentes, deberá incluir soporte técnico local, e incluir la configuración de licencia para uso.
- a.16. Deberá contar con una plataforma en la nube con certificado SSL de acceso seguro.
- a.17. El sistema antispam debe permitir ingresar a la plataforma en la nube con un usuario maestro y permitir crear usuarios con permisos restringido.
- a.18. La interfaz web debe ser intuitiva, facilita el uso y la configuración según el requerimiento del administrador.
- a.19. El sistema antispam debe permitir sincronizar con el Active Directory y sincronización LDAP, brindar protección antispam para correos entrantes y correos salientes y permitir crear o modificar grupos de usuarios.
- a.20. El sistema antispam debe permitir asignar permisos a grupos de usuarios o usuarios individuales.
- a.21. El sistema antispam debe contar con un filtrado de correo entrante y saliente.
- a.22. Deberá permitir y visualizar todos los correos en cuarentena con la finalizadas de elegir que correo se libera y va a lista blanca, o que correo se queda en la lista negra.
- a.23. El sistema antispam debe permitir liberar correos en cuarentena.
- a.24. El sistema antispam debe integrar una lista blanca y lista negra de correos en cuarentena.
- a.25. El sistema antispam debe permitir configurar las opciones de detección de SPAM.
- a.26. El sistema antispam debe informar sobre los correos electrónicos no deseados.
- a.27. El sistema antispam debe permitir ver correos electrónicos en cola, en la cola de entrega.

- a.28. Deberá permitir crear destinatarios locales con la finalidad que el usuario del correo reciba notificaciones de los correos en su cuenta de antispam y pueda decidir liberar los correos.
- a.29. El sistema antispam debe permitir borrar el caché de correo electrónico entrante y saliente.
- a.30. El sistema antispam debe contar con un registro de búsqueda de correos electrónicos entrantes.
- a.31. El sistema antispam debe brindar el registro de búsqueda de correos electrónicos salientes.
- a.32. El sistema antispam debe contar con bloqueo de dominios por países.
- a.33. El sistema antispam debe permitir crear alias de dominio para su identificación.
- a.34. Deberá permitir configurar los ajustes del dominio basado en la configuración de los MX.
- a.35. Permitir configurar restricciones de tamaño de correo electrónico entrante y saliente.
- a.36. El sistema antispam debe permitir configurar las configuraciones de 'extensiones bloqueadas'.
- a.37. El sistema antispam debe permitir visualizar las solicitudes de liberación de los usuarios.
- a.38. Permitir visualizar las solicitudes de listas blancas y negras de los usuarios.
- a.39. El sistema antispam debe permitir ver los destinatarios de la lista blanca y lista negra.
- a.40. El sistema antispam debe contar con una lista blanca y lista negra de remitentes.
- a.41. El sistema antispam debe permitir visualizar el historial de inicio de sesión de los usuarios.
- a.42. El sistema antispam debe permitir visualizar y descargar los archivos adjuntos de correo electrónico sin que este haya llegado a la bandeja de entrada del correo electrónico.

Se acoge la consulta. Se considerará opcional la funcionalidad que permite visualizar y descargar los archivos adjuntos de correos electrónicos retenidos antes de llegar a la bandeja de entrada.

Esto se debe a que las soluciones antispam estándar ya permiten seguimiento de logs, cuarentena y análisis de correos retenidos, asegurando la seguridad sin encarecer innecesariamente la solución. Esta modificación fomenta la pluralidad de postores sin comprometer los objetivos del servicio.⁸⁹

⁸⁹ **ABSOLUCIÓN DE CONSULTA 211 - WIN EMPRESAS S.A.C.**

- a.43. El sistema antispam debe controlar el número de cuentas de administrador de correo electrónico
- a.44. El sistema antispam debe permitir gestionar los informes en tiempo real referente al SPAM.
- a.45. El sistema antispam debe ser de la última versión lanzada al mercado por el fabricante de la solución y además debe contemplarse las actualizaciones correspondientes durante el periodo contractual; sin que esto signifique costo alguno para el Programa Integral Nacional para el Bienestar Familiar - INABIF.
- a.46. Capacidad de bloqueo de SPAMmers conocidos por dominio o dirección de correos.
- a.47. Capacidad de realizar excepciones a las reglas de filtrado para usuarios determinados.
- a.48. Poseer filtros basados en idiomas para bloquear SPAM que no sea en español.
- a.49. Umbral de SPAM ajustable para personalizar los niveles de eficacia y precisión.
- a.50. Cuarentena basada en Web para usuarios o administradores.
- a.51. Filtros antifraude para proteger contra mensajes falsos que buscan datos personales (Phishing) y fraude por correo electrónico.
- a.52. Capacidad de enviar notificaciones al administrador. Considerar como mínimo el envío de mensajes por red, y/o SMTP.
- a.53. El sistema antispam deberá:
- Integrarse perfectamente con ZIMBRA.
 - Analizar correos electrónicos en tiempo real.
 - Utilizar inteligencia artificial para detectar patrones de SPAM.
 - Proporcionar informes detallados sobre el correo electrónico filtrado.
 - Permitir la personalización de las políticas de filtrado.
 - Bloquear correos electrónicos provenientes de dominios sospechosos.
 - Tener capacidad de aprendizaje automático.
 - Ofrecer protección contra phishing.
 - Escanear adjuntos en busca de malware.
 - Tener una tasa de falsos positivos muy baja.
 - Permitir la creación de listas blancas y negras.
 - Filtrar correos electrónicos basados en la reputación del remitente.
 - Tener la capacidad de analizar contenido en múltiples idiomas.
 - Ofrecer opciones de cuarentena para correos sospechosos.

- Proporcionar alertas en tiempo real a los administradores.
 - Integrarse con herramientas de seguridad adicionales.
 - Utilizar técnicas de análisis heurístico.
 - Soportar la autenticación de correo electrónico (SPF, DKIM, DMARC).
 - Actualizar sus bases de datos de amenazas constantemente.
 - Permitir la recuperación de correos electrónicos marcados incorrectamente como SPAM.
- a.54. El sistema antispam debe ofrecer soporte técnico especializado y escanear enlaces en correos electrónicos para detectar amenazas.
- a.55. El sistema antispam debe ser fácil de implementar y gestionar.
- a.56. El sistema antispam debe proporcionar análisis detallados de encabezados de correo y soportar la integración con sistemas de directorio como Active Directory.
- a.57. El sistema antispam debe permitir la configuración de reglas específicas por usuario o grupo.
- a.58. El sistema antispam debe incluir funcionalidades de protección de datos sensibles y ser escalable para grandes organizaciones.
- a.59. El sistema antispam debe tener una interfaz de usuario intuitiva.
- a.60. El sistema antispam debe permitir la personalización de mensajes de rechazo y ofrecer análisis de comportamiento anómalo.
- a.61. El sistema antispam debe garantizar la disponibilidad y continuidad del servicio.
- a.62. El sistema antispam debe ser compatible con múltiples dispositivos y plataformas y ofrecer funciones de auditoría y trazabilidad.
- a.63. El sistema antispam debe permitir la integración con soluciones de SIEM.
- a.64. El sistema antispam debe proporcionar opciones de archivado seguro, permitir el seguimiento de correos electrónicos entregados y proporcionar estadísticas de uso y efectividad.
- a.65. El sistema antispam debe ofrecer una API para integraciones personalizadas.
- a.66. El sistema antispam debe detectar correos electrónicos de suplantación de identidad (spoofing), permitir la configuración de reglas basadas en palabras clave y ofrecer soporte para la encriptación de correos electrónicos.
- a.67. El sistema antispam debe proporcionar opciones de recuperación ante desastres.
- a.68. El sistema antispam debe analizar el historial de comunicaciones para mejorar la detección, permitir la creación de políticas basadas en la ubicación geográfica y ofrecer opciones de escalado automático.

- a.69. El sistema antispam debe proporcionar opciones de sandboxing para adjuntos sospechosos, ser compatible con tecnologías de contenedores y ofrecer un panel de control centralizado.
- a.70. Deberá garantizar la conformidad con normativas de privacidad y protección de datos.
- b. Autenticación de dominio:**
 - b.1. El sistema de autenticación de dominio debe soportar SPF (Sender Policy Framework).
 - b.2. Deberá ser compatible con DKIM (DomainKeys Identified Mail).
 - b.3. El sistema de autenticación de dominio debe implementar y monitorear políticas DMARC (Domain-based Message Authentication, Reporting, and Conformance).
 - b.4. El sistema de autenticación de dominio debe gestionar múltiples dominios y subdominios.
 - b.5. El sistema de autenticación de dominio debe generar registros SPF y DKIM automáticamente.
 - b.6. Permitirá analizar los registros DNS para asegurar su correcta configuración.
 - b.7. Deberá integrarse con proveedores de DNS para facilitar la actualización de registros.
- c. Monitoreo y reportes:**
 - c.1. El sistema de autenticación de dominio debe generar informes DMARC en formato XML y PDF.
 - c.2. El sistema de autenticación de dominio debe ofrecer desglose de resultados de autenticación por país, proveedor y servidor, permitir la visibilidad completa de los intentos fallidos de suplantación y analizar reportes para identificar fuentes legítimas y no legítimas de correos electrónicos.
 - c.3. El sistema de autenticación de dominio debe identificar y eliminar fuentes no autorizadas de correos electrónicos.
 - c.4. El sistema de autenticación de dominio debe generar reportes automatizados de salud del dominio por correo electrónico, detectar problemas de entregabilidad en correos legítimos, visualizar en tiempo real las amenazas y correos no autenticados y permitir la exportación de reportes en CSV y PDF.
 - c.5. El sistema de autenticación de dominio debe permitir configurar políticas DMARC flexibles como none, quarantine y reject.
 - c.6. El sistema de autenticación de dominio debe soportar la aplicación de políticas personalizadas para subdominios.
 - c.7. El sistema de autenticación de dominio debe auditar los cambios en las configuraciones y políticas de seguridad.

- c.8. El sistema de autenticación de dominio debe identificar servicios en la nube autorizados y no autorizados que envían correos en nombre del dominio.
- c.9. El sistema de autenticación de dominio debe realizar seguimiento y análisis de IPs de envío no autorizadas.
- c.10. El sistema de autenticación de dominio debe monitorear falsificaciones y correos no alineados.
- c.11. El sistema de autenticación de dominio debe soportar políticas de subdominio independiente.
- c.12. El sistema de autenticación de dominio debe implementar políticas DMARC de impacto cero (modo none) para observar resultados sin interferir en la entrega de correos.
- c.13. El sistema de autenticación de dominio debe proteger contra la suplantación de identidad en envíos de terceros.
- c.14. Protección de Marca y Certificaciones:
- c.15. El sistema de autenticación de dominio debe implementar BIMi (Brand Indicators for Message Identification) para mejorar la visibilidad de la marca.
- c.16. El sistema de autenticación de dominio debe permitir la certificación de la marca visual en bandejas de entrada compatibles.
- c.17. El sistema de autenticación de dominio debe prevenir la suplantación de dominios de alto perfil.
- c.18. Gestión de Reputación:
- c.19. El sistema de autenticación de dominio debe mejorar la reputación del dominio al implementar políticas estrictas de autenticación.
- c.20. El sistema de autenticación de dominio debe identificar y eliminar direcciones IP que afecten negativamente la reputación del dominio.
- c.21. El sistema de autenticación de dominio debe monitorear la reputación del dominio y ajustar automáticamente la configuración para mejorar la entregabilidad.
- c.22. El sistema de autenticación de dominio debe soportar análisis de IPs bloqueadas y listas negras.
- c.23. El sistema de autenticación de dominio debe validar periódicamente direcciones IP autorizadas para asegurar la autenticación consistente.
- c.24. Facilidad de Uso y Configuración:
- c.25. El sistema de autenticación de dominio debe proporcionar una interfaz intuitiva y amigable para configurar y gestionar políticas SPF, DKIM y DMARC.
- c.26. El sistema de autenticación de dominio debe ofrecer plantillas automáticas para la creación de registros DNS.

- c.27. El sistema de autenticación de dominio debe implementar un asistente paso a paso con recomendaciones basadas en buenas prácticas.
- c.28. El sistema de autenticación de dominio debe configurar alertas automáticas para cambios críticos en la política de autenticación.
- c.29. El sistema de autenticación de dominio debe actualizar automáticamente los registros de autenticación con un solo clic.
- c.30. El sistema de autenticación de dominio debe permitir la programación de reportes y alertas periódicas, soportar múltiples usuarios con roles y permisos personalizados y configurar alertas de detección de intentos de ataque.
- c.31. El sistema de autenticación de dominio debe detectar automáticamente problemas en la infraestructura de correos.
- c.32. El sistema de autenticación de dominio debe integrar plataformas de gestión de correos electrónicos y sistemas de terceros.
- c.33. El sistema de autenticación de dominio debe almacenar un historial de cambios y auditorías accesibles desde la consola.
- c.34. El sistema de autenticación de dominio debe ofrecer documentación detallada y tutoriales integrados.

d. Escalabilidad y soporte:

- d.1. El sistema de autenticación de dominio debe manejar múltiples dominios en una sola cuenta.
- d.2. El sistema de autenticación de dominio debe escalar según las necesidades de la organización, desde pequeñas hasta grandes empresas.
- d.3. El sistema de autenticación de dominio debe ofrecer soporte técnico 24/7.
- d.4. El sistema de autenticación de dominio debe actualizarse periódicamente con mejoras de seguridad y nuevas funcionalidades.
- d.5. El sistema de autenticación de dominio debe ofrecer soporte multilingüe.
- d.6. El sistema de autenticación de dominio debe contar con una comunidad activa y foros de soporte.
- d.7. El sistema de autenticación de dominio debe ofrecer planes personalizables según las necesidades de la organización.

e. Seguridad de la información:

- e.1. El sistema de autenticación de dominio debe cifrar los datos en reposo y en tránsito.
- e.2. El sistema de autenticación de dominio debe gestionar de manera segura las credenciales y claves DKIM.
- e.3. El sistema de autenticación de dominio debe implementar autenticación multifactor (MFA) para usuarios administrativos.

- e.4. El sistema de autenticación de dominio debe soportar IP whitelisting para limitar el acceso a ubicaciones seguras.
- e.5. El sistema de autenticación de dominio debe gestionar usuarios con autenticación segura.
- e.6. El sistema de autenticación de dominio debe cumplir con normativas de seguridad como GDPR y CCPA.
- e.7. El sistema de autenticación de dominio debe realizar auditorías de seguridad sobre el uso de la plataforma.
- e.8. El sistema de autenticación de dominio debe almacenar reportes de manera segura en la nube.
- f. Integración con servicios externos:**
 - f.1. El sistema de autenticación de dominio debe integrar servicios de correo como Gmail, Microsoft 365 y Yahoo Mail, identificar servicios de terceros que envían correos en nombre del dominio e integrarse con plataformas de monitoreo de seguridad y sistemas SIEM.
 - f.2. El sistema de autenticación de dominio debe proporcionar una API para automatizar el monitoreo y análisis de reportes DMARC.
 - f.3. El sistema de autenticación de dominio debe ser compatible con proveedores de DNS como Cloudflare, GoDaddy, y AWS Route 53.
- g. Optimización de entregabilidad:**
 - g.1. El sistema de autenticación de dominio debe mejorar la entregabilidad al identificar y resolver problemas de autenticación, analizar correos legítimos bloqueados para ajustar las políticas sin impactar la comunicación y recomendar ajustes automáticos para mejorar las tasas de entregabilidad.
 - g.2. Deberá proteger contra la falsificación de direcciones de correo, e identificar y resolver problemas de alineación de correos.
 - g.3. El sistema de autenticación de dominio debe proporcionar un análisis detallado de dominios que fallan la autenticación.
- h. Recuperación ante incidentes:**
 - h.1. El sistema de autenticación de dominio debe alertar y bloquear fuentes no autorizadas en tiempo real, generar reportes de incidentes con recomendaciones para resolver fallos de autenticación.
 - h.2. El sistema de autenticación de dominio debe ofrecer soporte para la recuperación de credenciales DKIM comprometidas.
 - h.3. El sistema de autenticación de dominio debe detectar anomalías en patrones de envío de correos.

- h.4. El sistema de autenticación de dominio debe bloquear automáticamente fuentes sospechosas de envío.
- h.5. El sistema de autenticación de dominio debe mitigar ataques de phishing dirigidos.
- h.6. El sistema de autenticación de dominio debe contar con planes de recuperación ante desastres y realizar copias de seguridad de la información crítica.
- i. Funciones adicionales:**
 - i.1. El sistema de autenticación de dominio debe permitir observar e identificar si el correo de la institución está en cumplimiento con los protocolos de seguridad SPF y DKIM.
 - i.2. Deberá permitir visualizar picos de volumen de email, contar con un informe que detalle las IPs de envío, mostrar la lista de servidores que envían y/o retransmiten correos en nombre del dominio de la institución.
 - i.3. El sistema de autenticación de dominio debe permitir identificar la fuente del correo electrónico mal intencionado para tomar una decisión.
 - i.4. El sistema de autenticación de dominio debe permitir identificar los países en donde se encuentran los servidores que utilizan el dominio de la institución.
 - i.5. Deberá procesar tanto reportes agregados como reportes forenses.
 - i.6. El sistema de autenticación de dominio debe permitir configurar de manera ordenada los protocolos de seguridad SPF, DMARC y DKIM.
 - i.7. El sistema de autenticación de dominio debe permitir configurar BIML.
 - i.8. El sistema de autenticación de dominio debe permitir delegar los protocolos SPF, DMARC y DKIM para ser gestionado desde el propio sistema.
 - i.9. El sistema de autenticación de dominio debe permitir activar políticas restrictivas asegurando sus fuentes de correos mediante la aplicación de protocolo de DMARC.
 - i.10. El sistema de autenticación de dominio debe permitir la compresión del SPF a fin de evitar el exceso de lookups.
 - i.11. El sistema de autenticación de dominio debe permitir gestionar tantos dominios como sean necesarios. Ya sean activos como inactivos.
 - i.12. El sistema de autenticación de dominio debe permitir aplicar políticas para que los correos provenientes de fuentes no autorizadas sean identificados y puestos en cuarentena o rechazados según corresponda.
 - i.13. El sistema de autenticación de dominio debe proveer reportes periódicos y automáticos sobre el nivel de exposición de la infraestructura de envío.
 - i.14. El sistema de autenticación de dominio debe permitir detectar quién envía correos a nombre del dominio que no sea parte del servidor de correos.

- i.15. El sistema de autenticación de dominio debe permitir autorizar el envío de correos sólo a remitentes que pertenezcan a la institución o sean autorizados por ella.
- i.16. El sistema de autenticación de dominio debe contar con un sistema de prevención contra intrusos e inspección de todo tipo de tráfico.
- i.17. Debe contar con una gestión de reputación para el dominio protegido, con doble factor de autenticación para los usuarios, gestión de permisos de administrador de cuenta, usuario de cuenta y usuario de solo lectura.
- i.18. El sistema de autenticación de dominio debe contar con integración API.
- i.19. El sistema de autenticación de dominio debe permitir SSO.
- i.20. El sistema de autenticación de dominio debe incluir un simulador de impacto de políticas de DMARC, permitiendo probar diferentes políticas sin afectar la entrega real de correos.
- i.21. El sistema de autenticación de dominio debe contar con un monitor de cambios DNS automático, que alerte sobre modificaciones que afecten los registros de SPF, DKIM o DMARC.
- i.22. El sistema de autenticación de dominio debe soportar la migración de dominios, permitiendo mover configuraciones de autenticación entre distintos proveedores de DNS sin pérdida de seguridad.
- i.23. El sistema de autenticación de dominio debe detectar y alertar sobre intentos de suplantación mediante dominios homógrafos, utilizando caracteres visualmente similares.
- i.24. El sistema de autenticación de dominio debe generar informes de compliance con regulaciones, como GDPR o CCPA, mostrando el cumplimiento en términos de seguridad de correos electrónicos.
- i.25. El sistema de autenticación de dominio debe ofrecer un módulo de entrenamiento en seguridad para los usuarios, con lecciones sobre detección de phishing y correos maliciosos, basado en reportes forenses reales.
- i.26. El sistema de autenticación de dominio debe contar con una herramienta que optimice automáticamente los registros SPF, sugiriendo correcciones para evitar problemas de lookups.
- i.27. El sistema de autenticación de dominio debe incluir un monitor de reputación en tiempo real, permitiendo la visualización inmediata de cambios en la reputación de los servidores de correo.
- i.28. El sistema de autenticación de dominio debe contar con una función que detecte y corrija automáticamente errores en la configuración DNS, proporcionando recomendaciones para su resolución.
- i.29. El sistema de autenticación de dominio debe consolidar reportes agregados y forenses en un solo panel, con filtros avanzados para facilitar el análisis.

5.5. SOLUCIÓN DE PROTECCIÓN DE APLICACIONES WEB

Se precisa que la solución de protección de aplicaciones Web (WAF), podrá ser brindada desde la nube del fabricante propuesto como solución.⁹⁰

Se aclara que lo siguiente en caso que el postor considere una solución WAF brindada desde la nube del fabricante:

- Las aplicaciones a proteger será el dominio principal considerando todos los subdominios y/o considerando 5 aplicaciones.

- Deberá ser brindado desde la nube del fabricante.

- El ancho de banda promedio de referencia será de 25 Mbps por el total de aplicaciones a proteger.⁹¹

El contratista deberá implementar, configurar y gestionar una solución de seguridad perimetral que cubra los siguientes aspectos:

- 1) Implementar un firewall de aplicaciones web (WAF) con personalización avanzada para proteger contra vulnerabilidades de aplicaciones.
- 2) Mitigar ataques DDoS y bots maliciosos, asegurando la disponibilidad del servicio en todo momento.
- 3) Mejorar el rendimiento de los sistemas mediante balanceo de carga, cacheo dinámico y reducción de latencia.

No se acoge la consulta. La funcionalidad requerida se mantiene como obligatoria, ya que el Web Application Firewall (WAF) es un componente esencial en la protección de aplicaciones web contra ataques cibernéticos. Su implementación no solo protege contra amenazas comunes como inyección SQL, cross-site scripting (XSS) y ataques de denegación de servicio (DDoS), sino que también optimiza el tráfico, mejora el rendimiento y asegura la disponibilidad de los servicios web críticos del INABIF.⁹²

No se acoge la consulta, El requerimiento de cacheo dinámico como parte de la solución de protección de aplicaciones web se mantiene como obligatorio, ya que esta funcionalidad es esencial para garantizar una óptima mejora del rendimiento de los sistemas, contribuyendo significativamente a la reducción de

⁹⁰ ABSOLUCIÓN DE CONSULTA N° 149 - WIN EMPRESAS S.A.C.

⁹¹ ABSOLUCIÓN DE CONSULTA N° 150 - WIN EMPRESAS S.A.C.

⁹² ABSOLUCIÓN DE CONSULTA N° 151 - WIN EMPRESAS S.A.C.

latencia y a la optimización de los tiempos de respuesta de las aplicaciones protegidas.⁹³

- 4) Integrar herramientas de análisis para el monitoreo continuo y generación de reportes detallados.
- 5) Proteger APIs críticas con validación de esquema y autenticación de clientes.
- 6) Se deberá licenciar en base al dominio principal y/o considerando 5 aplicaciones, que serán protegidos con la solución WAF.

Se precisa que la solución de protección de aplicaciones Web (WAF), podrá ser brindada desde la nube del fabricante.⁹⁴

Se acoge la consulta y se que aclara que la cantidad de throughput de tráfico HTTP/HTTPS que debe ser considerado para la protección es de 25 Mbps, generado por un total de 5 aplicaciones críticas del INABIF.

Esta información debe ser tomada en cuenta por los postores para el dimensionamiento adecuado de la solución de protección requerida.⁹⁵

Se confirma que las aplicaciones se encuentran dentro de la red de la entidad.⁹⁶

a. Protección avanzada:

- a.1. Mitigación de ataques DDoS en las capas de red y aplicación. **Esta alternativa es opcional y no obligatoria.⁹⁷**
- a.2. Protección contra inyecciones de código y vulnerabilidades OWASP Top 10.
- a.3. Bloqueo proactivo de bots mediante análisis de comportamiento y listas de reputación.

b. Optimización del rendimiento:

- b.1. Balanceo de tráfico global para optimizar el uso de recursos y garantizar alta disponibilidad. **Esta alternativa es opcional y no obligatoria.^{98 99 100}**

⁹³ ABSOLUCIÓN DE OBSERVACIÓN N° 225 - GTD PERÚ S.A

⁹⁴ ABSOLUCIÓN DE CONSULTA N° 152 - WIN EMPRESAS S.A.C.

⁹⁵ ABSOLUCIÓN DE CONSULTA N° 153 - WIN EMPRESAS S.A.C.

⁹⁶ ABSOLUCIÓN DE CONSULTA N° 154 - WIN EMPRESAS S.A.C.

⁹⁷ ABSOLUCIÓN DE CONSULTA N° 155 - WIN EMPRESAS S.A.C.

⁹⁸ ABSOLUCIÓN DE CONSULTA N° 156 - WIN EMPRESAS S.A.C.

⁹⁹ ABSOLUCIÓN DE CONSULTA N° 157 - WIN EMPRESAS S.A.C.

¹⁰⁰ ABSOLUCIÓN DE OBSERVACIÓN N° 226 - GTD PERÚ S.A

- b.2. Cacheo dinámico para mejorar la velocidad de carga de los servicios web.

No se acoge la consulta. El requerimiento de cacheo dinámico como parte de la optimización del rendimiento se mantiene como obligatorio. Esta funcionalidad es esencial para mejorar la velocidad de carga de los servicios web, optimizando el uso de recursos y garantizando una experiencia de usuario eficiente y de alta calidad.¹⁰¹

c. **Gestión y monitoreo:**

- c.1. Acceso a un portal de gestión con reportes en tiempo real y herramientas de análisis.

No se acepta la consulta. El acceso a un portal de gestión con reportes en tiempo real y herramientas de análisis se mantiene como un requisito obligatorio, ya que es esencial para garantizar la visibilidad, monitoreo continuo y análisis del desempeño del servicio en tiempo real, lo cual es crítico para la correcta gestión y toma de decisiones en la operación del servicio.

Si bien el principio de libertad de concurrencia permite la participación de diversos postores, no exime el cumplimiento de los requisitos técnicos que aseguran la calidad y funcionalidad del servicio. La disponibilidad de un portal de gestión con estas características es un estándar en soluciones modernas y no limita la posibilidad de participación de postores con tecnologías equivalentes que cumplan con este requerimiento.¹⁰²

- c.2. Generación de logs exportables para su análisis en herramientas externas.
c.3. Configuración de alertas y notificaciones sobre intentos de intrusión y estado de la red.

d. **Certificación y seguridad del tráfico:**

- d.1. Administración de certificados SSL/TLS, incluyendo soporte para certificados Wildcard.
d.2. Protección de conexiones HTTPS mediante protocolos avanzados como HTTP/2.

Esta alternativa es opcional y no obligatoria.¹⁰³

5.6. **CARACTERÍSTICAS COMPLEMENTARIAS DEL SERVICIO**

¹⁰¹ ABSOLUCIÓN DE OBSERVACIÓN N° 227 - GTD PERÚ S.A

¹⁰² ABSOLUCIÓN DE OBSERVACIÓN N° 228 - GTD PERÚ S.A

¹⁰³ ABSOLUCIÓN DE CONSULTA N° 158 - WIN EMPRESAS S.A.C.

- a) Tener acceso al Backbone Internacional (medio integro de fibra óptica y tecnología única de transporte).
- b) El proveedor deberá garantizar que el retardo máximo permitido será de 5ms, medido dentro de la red IP del proveedor, el que adicionalmente deberá presentar un esquema en el que se muestren las velocidades de conexión a los Backbone Internacionales de Internet y sus enlaces de intercambio (peering) con otros proveedores nacionales que les permite un intercambio local de datos y el cual será verificado en las pruebas de operatividad y estado del enlace para dar conformidad del servicio ofrecido, esta documentación ~~será necesaria para la firma del contrato.~~ **La documentación señalada será requerida en el INFORME FINAL DE IMPLEMENTACIÓN.**¹⁰⁴

El tiempo de retardo permitido será desde el equipamiento brindado en la sede del cliente hasta el equipo de la salida internacional del proveedor. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁰⁵

El postor que resulte adjudicado con la buena pro deberá cumplir obligatoriamente con al menos dos (02) proveedores TIER 1 para garantizar la redundancia del servicio de conectividad internacional y al menos uno de los proveedores TIER 1 deberá tener una capacidad mínima de 100 Gbps. Estas condiciones tienen como finalidad asegurar la calidad y continuidad del servicio, manteniendo un estándar adecuado de conectividad internacional para las necesidades de la entidad. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁰⁶

Se aclara que la latencia podrá ser medida desde el router instalado en la entidad y el equipo de comunicación ubicado en Centro de datos del postor, y deberá tener una latencia de al menos 15 milisegundos.¹⁰⁷

- c) Posteriormente a esto, el INABIF levantará y entregará al proveedor el Acta de Conformidad de Instalación del Servicio.
- d) Capacidad para monitorear el nivel de uso del ancho de banda a través de su Centro de Gestión.
- e) Soporte técnico: las 24 horas del día los siete (7) días de la semana, durante los 365 días del año, en el periodo de vigencia del contrato.
- f) Con referencia a los routers instalados como parte del servicio, deberán ser de última generación (es decir no tengan condición de End of Life (EoL) ni End of Sale (EoS)), con capacidad de soportar el requerimiento de ancho de banda (tanto para el enlace primario como el de contingencia). El proveedor deberá asignar acceso

¹⁰⁴ ABSOLUCIÓN DE CONSULTA N° 14 - AMERICA MOVIL PERU S.A.C.

¹⁰⁵ ABSOLUCIÓN DE CONSULTA N° 41 - AMERICA MOVIL PERU S.A.C.

¹⁰⁶ ABSOLUCIÓN DE CONSULTA N° 42 - AMERICA MOVIL PERU S.A.C.

¹⁰⁷ ABSOLUCIÓN DE CONSULTA N° 159 - WIN EMPRESAS S.A.C.

de solo lectura a los routers, al personal especializado en redes y seguridad del Inabif.

- g) El proveedor deberá otorgar al INABIF una herramienta de acceso web con un circuito lógico independiente por cada enlace, utilizando el mismo medio de transmisión separando redes lógicas y respetando el ancho de banda del servicio y aparte el ancho de banda de la herramienta web; por lo que, deberá considerar los recursos necesarios dentro de su propuesta técnica a fin de que se garantice el servicio.

El postor garantiza la presentación de la herramienta de acceso web con circuito independiente, al que se hace referencia el numeral indicado de las bases, con el Anexo 03.¹⁰⁸

Se confirma que, por redes lógicas hacen referencia a las interfaces (puertos) o VLANs configuradas en el equipo.¹⁰⁹

Se precisa que el postor debe garantizar el ancho de banda solicitado en las bases (500Mbps), para el adecuado funcionamiento y navegación de los usuarios.¹¹⁰

- h) La herramienta de monitoreo, en la que se podrá medir el nivel de saturación, consumo e históricos, entre otros, no deberá consumir los anchos de banda asignados ni mezclarse con los tráficlos de la Entidad. Asimismo, las gráficas de esta herramienta serán tomadas como válidas para medir el nivel de disponibilidad del servicio contratado.

Se confirma la consulta del postor, lo históricos deberán ser de al menos 6 meses.¹¹¹

Se precisa que se hace referencia al consumo de ancho de banda utilizado.¹¹²

Se aclara que medir la saturación hace referencia al consumo de ancho de banda que se está utilizando, es decir, apreciar en las gráficas si se está llegando al ancho de banda total contratado.¹¹³

Se precisa que el postor debe garantizar el ancho de banda solicitado en las bases (500Mbps), para el adecuado funcionamiento y navegación de los usuarios.¹¹⁴

- i) Se deberá programar, cada seis meses, un mantenimiento preventivo, contados a partir del día siguiente de suscrita el Acta de Conformidad de Instalación del Servicio, previamente coordinado con el INABIF; durante el mantenimiento preventivo se deberá llevar a cabo las siguientes actividades:

¹⁰⁸ ABSOLUCIÓN DE CONSULTA N° 15 - AMERICA MOVIL PERU S.A.C.

¹⁰⁹ ABSOLUCIÓN DE CONSULTA N° 160 - WIN EMPRESAS S.A.C.

¹¹⁰ ABSOLUCIÓN DE CONSULTA N° 161 - WIN EMPRESAS S.A.C.

¹¹¹ ABSOLUCIÓN DE CONSULTA N° 162 - WIN EMPRESAS S.A.C.

¹¹² ABSOLUCIÓN DE CONSULTA N° 163 - WIN EMPRESAS S.A.C.

¹¹³ ABSOLUCIÓN DE CONSULTA N° 164 - WIN EMPRESAS S.A.C.

¹¹⁴ ABSOLUCIÓN DE CONSULTA N° 165 - WIN EMPRESAS S.A.C.

- Revisión de los equipos para su optimización.
- Revisión y limpieza de los equipos, cables y conexiones en los circuitos instalado.
- Actualización de software de los equipos.
- Revisión periódica de los enlaces de nuestra red con el proveedor.
- Medir los parámetros de red (tráfico, velocidad, sincronía, retardo, hops, etc.) usando los equipos necesarios para dicha revisión.
- Medición de los parámetros de red (sincronismo, velocidad de enlace, delay, etc.).
- Optimización de los recursos de red.
- De ser necesario, realizar una optimización de red en la plataforma brindada.

Se aclara que el mantenimiento preventivo deberá ser realizado en los equipos que son físicamente instalados como parte de la solución.¹¹⁵

- j) El cronograma del Plan de Mantenimiento Preventivo deberá ser presentado por el proveedor que obtenga la Buena pro, ~~para el perfeccionamiento del Contrato.~~ **se confirma que el "Cronograma del Plan de mantenimiento preventivo", se efectuara en el INFORME FINAL DE IMPLEMENTACION.¹¹⁶**
- k) Garantizar en todo momento la seguridad lógica del servicio prestado.
- l) El plazo de implementación del servicio no deberá exceder de ciento veinte (120) días calendario, contabilizados a partir del día siguiente de la fecha de suscripción del contrato, lo cual será refrendado con un Acta de Conformidad de Instalación del Servicio emitida por la Unidad de Tecnología de la Información de acuerdo al numeral 8), por la implementación, configuración y puesta en marcha del total de equipos ofertados.
- m) El postor deberá contar con al menos (02) implementadores de soluciones de seguridad de borde, el cual deberá ser ingeniero con Título y colegiatura en Ingeniería de Sistemas o Electrónica o Telecomunicaciones o Redes o Redes y Comunicaciones o Informática o Sistemas e Informática o carreras afines, y debe estar certificado a nivel técnico por el fabricante de la solución de seguridad propuesta, este personal debe ser parte del staff de personal propuesto por el postor, considerándosele un personal clave tanto para la etapa de implementación como para la etapa de soporte durante la duración del contrato.

Se acoge la consulta, se considerará lo solicitado en los requisitos de calificación en el numeral B.3.^{117 118}

- n) La empresa proveedora deberá disponer con equipos de contingencia para el reemplazo en el caso de presentarse alguna falla en el equipamiento, en un plazo

¹¹⁵ ABSOLUCIÓN DE CONSULTA N° 166 - WIN EMPRESAS S.A.C.

¹¹⁶ ABSOLUCIÓN DE CONSULTA N° 16 - AMERICA MOVIL PERU S.A.C.

¹¹⁷ ABSOLUCIÓN DE OBSERVACIÓN N° 167 - WIN EMPRESAS S.A.C.

¹¹⁸ ABSOLUCIÓN DE CONSULTA N° 223 - GTD PERÚ S.A.

máximo de cuatro (04) horas, este aplica para escenarios que no se encuentran en alta disponibilidad, ya que, al tener un HA, el servicio no se ve afectado ante la caída de uno de los equipos.

- o) Se deberá presentar el detalle técnico de cada uno de los equipos que se compone la solución ofertada, tecnología utilizada, así como un diagrama de cómo se integran estos componentes, para brindar el servicio, esta información será presentada al momento de la firma del contrato.

Se deberá presentar el detalle técnico (brochure, datasheet) de los equipos que componen la solución ofertada, en el deberá detallarse la marca, el modelo y un diagrama de red de cómo se integraran las soluciones, en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹¹⁹

Se confirma y aclara que en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el postor deberá presentar un detalle técnico (brochure, datasheet) de los equipos que componen la solución ofertada, en el deberá detallarse la marca, el modelo y un diagrama de red de cómo se integraran las soluciones.¹²⁰

- p) Cabe mencionar que el proveedor ganador, deberá proporcionar todos los equipos y/o accesorios que sean necesario para la puesta en marcha del servicio contratado.
- q) Como parte del servicio de soporte el postor deberá brindar una herramienta para la detección de amenazas NDR en la red de INABIF, con las siguientes características:

- Appliance dedicado de uso específico para la función solicitada. No se aceptarán NGFW o equipamiento similar para el cumplimiento del requerimiento.

Se confirma y aclara que la herramienta NDR será un appliance nuevo, de propósito específico y de uso exclusivo para el INABIF.¹²¹

- Interfaces SFP+: 2 (No deberá incluir transceivers SFP+)
- Interfaces SFP: 8 (No deberá incluir transceivers SFP)
- Interfaces GE RJ45: 8
- Local Storage: 1 TB
- UR: hasta 2UR
- BreachDetection o NDR Throughput: Mínimo 1 Gbps
- Nuevas sesiones por segundo: 32,000
- Maximo Sesiones Concurrentes: 750,000
- La solución propuesta debe soportar el modo de operación de tapping, sin ser intrusiva para la red del cliente.

¹¹⁹ ABSOLUCIÓN DE CONSULTA N° 168 - WIN EMPRESAS S.A.C.

¹²⁰ ABSOLUCIÓN DE CONSULTA N° 169 - WIN EMPRESAS S.A.C.

¹²¹ ABSOLUCIÓN DE CONSULTA N° 224 - GTD PERÚ S.A

- La solución debe poder integrarse con firewalls de la misma marca para poder mitigar amenazas.
- La solución debe soportar más de 3,500 aplicaciones, debe soportar el filtro de aplicaciones por nombre, categoría, subcategoría, tecnología y riesgo.
- La solución debe poder identificar aplicaciones móviles del tipo iOS o Android.
- La solución debe ser capaz de identificar las aplicaciones en la nube, debe proporcionar monitoreo y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características.
- La solución debe soportar al menos 2,000 firmas. Debe soportar firmas personalizadas, manual, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada.
- La solución debe ser compatible con la protección de inyección SQL, CC y ataques XSS.
- La solución debe soportar la detección de anomalías de protocolo, detección basada en la velocidad. Incluyendo HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, etc.
- La solución debe permitir crear listas blancas para el módulo de IPS.
- La solución debe contar con perfiles predefinidos de IPS.
- La solución debe ser compatible con Antivirus basado en flujo: los protocolos incluyen HTTP, SMTP, FTP.
- La solución debe soportar la detección de virus para archivos comprimidos como RAR, ZIP, TAR.
- La solución debe ser compatible con el entorno de ejecución virtual de malware, basado en la nube para encontrar amenazas desconocidas.
- La solución debe ser compatible con la carga de archivos maliciosos en el entorno limitado de la nube para su análisis.
- La solución debe tener una interfaz de usuario web integrada (WebUI) e interfaz de línea de comandos (CLI)
- La solución debe soportar el acceso de administración desde HTTP / HTTPS, SSH, telnet, consola
- La solución debe poder proteger el sistema contra ataques de fuerza bruta en el nombre de usuario y la contraseña
- La solución debe ser compatible con la política de seguridad de contraseña para las cuentas de administrador.
- Admite alertas del tipo correo electrónico, mensaje de texto.
- Logs: incluidos registros de eventos, redes, amenazas, configuración y sesiones.
- Admite SYSLOG estándar
- La solución debe soportar análisis por correlación de amenazas, correlación

entre amenazas desconocidas, comportamiento anormal y comportamiento de aplicaciones para descubrir amenazas o ataques potenciales.

- La solución debe permitir la actualización de la base de datos del modelo de comportamiento de malware en línea en tiempo real.
- La solución debe soportar la detección de más de 2000 familias de malware conocidas y desconocidas, incluidos Virus, Gusanos, Troyanos, Desbordamiento, etc.
- La solución debe ser compatible con la detección avanzada de malware basada en comportamiento
- La solución debe ser compatible para detectar ransomware y malware.
- La solución debe soportar el modelado de comportamiento basado en el tráfico de línea de base L3-L7 para revelar un comportamiento anómalo de la red
- La solución debe soportar la visualización de amenazas de Intranet para los servidores (activos críticos), así como la detección del tráfico anormal relacionado a ellos.
- La solución debe soportar visibilidad para la información básica basada en el host, índice de riesgo, las amenazas y el tráfico anormal.
- La solución debe soportar visibilidad de amenazas, incluido el nombre de amenaza, tipo de amenaza, nivel de riesgo, base de conocimiento, paquete forense, etc.
- La solución deberá contar con licencias incluidas de los siguientes servicios durante el periodo del servicio: Cloud-Sandbox y Antispam.

5.7. GESTIÓN DEL EQUIPAMIENTO

- a) El proveedor debe dar servicio de monitoreo remoto del equipo o equipos en 24x7 (Las 24 horas del día, los siete días de la semana) para garantizar el correcto funcionamiento de estos.
- b) El proveedor será totalmente responsable de la administración, configuración y adecuado funcionamiento del equipamiento instalado. En el caso de los equipos de seguridad de borde, la administración será de forma compartida, es decir será efectuada tanto por el personal técnico del proveedor como por el personal especializado, en redes y seguridad del INABIF, previa capacitación¹²² descrita en el literal o) del numeral 6) de los términos de referencia. ~~en el Punto 5, del presente documento.~~
- c) Los reportes se entregarán de forma mensual; sin embargo, la entidad podrá solicitar los reportes al proveedor en cualquier momento, solo cuando exista una necesidad de información en particular; estos no tendrán costos adicionales y se basarán sobre los equipos que formen parte de la solución y deberán ser

¹²² **ABSOLUCIÓN DE CONSULTA 18 - AMERICA MOVIL PERU S.A.C.**

entregados dentro de un plazo no mayor a cuatro (04) días hábiles de hecha la solicitud.

- d) Entre los reportes requeridos tenemos:
- Consumo de ancho de banda,
 - Usuarios con mayor consumo,
 - Sitios más visitados,
 - Ataques bloqueados,
 - Consumo de tráfico por usuarios, entre otros.

Se acoge la consulta los cambios solicitados serán a nivel de configuración mas no de arquitectura o topología.¹²³

- e) El INABIF podrá solicitar cambios en las reglas y/o configuraciones de los equipos que formen parte de la implementación del servicio. Estas solicitudes serán limitadas a veinte (20) veces al año, y no modificarán el alcance de la propuesta con relación a cambios de equipos o aumento de ancho de banda, no requiriéndose un gasto adicional, para que estas sean atendidas por el proveedor en un plazo no mayor a dos (02) días hábiles de realizada la solicitud. Esto último, sin perjuicio de lo requerido por el INABIF.

5.8. GESTIÓN DEL SERVICIO

- a) ~~El proveedor, al momento de la suscripción del contrato, deberá presentar los~~ **contratista deberá incluir en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION¹²⁴ procedimientos con los que cuenta para el reporte de fallas y la gestión del servicio en general.**

Se acoge la consulta, se le podrá brindar a la entidad un cuadro de escalamiento para la priorización de incidencias, este cuadro indicará los plazos y niveles de escalamiento.¹²⁵

- b) El tiempo de respuesta máximo para la atención de un problema, será no mayor de una
- c) (01) hora, y la resolución en un máximo de cuatro (04) horas, contada desde que el INABIF reporta el incidente al Centro de Servicio del proveedor y/o se le asigne un ticket de atención, para lo cual la empresa deberá brindar la información al INABIF sobre sus puntos de contacto; asimismo deberá considerar lo siguiente:

¹²³ ABSOLUCIÓN DE CONSULTA 170 - WIN EMPRESAS S.A.C.

¹²⁴ ABSOLUCIÓN DE CONSULTA 19 - AMERICA MOVIL PERU S.A.C.

¹²⁵ ABSOLUCIÓN DE CONSULTA 171 - WIN EMPRESAS S.A.C.

Se confirma la consulta, el tiempo de atención de cualquier tipo de avería será computado a partir de la generación de un ticket de atención, luego de producido el incidente.¹²⁶

- El tiempo de atención de cualquier tipo de avería, será computado a partir de la generación de un ticket de atención, luego de producido el incidente, para de este modo facilitar el seguimiento de la falla reportada.
- El tiempo de atención de atención implica la identificación de los problemas, las coordinaciones con el INABIF y toma de acciones por parte del proveedor para la resolución del problema a la brevedad.
- El proveedor deberá garantizar un eficiente sistema de gestión de sus redes de comunicación. El centro de gestión deberá estar en capacidad de realizar acciones de controles preventivos, correctivos y pruebas técnicas.
- El proveedor deberá garantizar el profesionalismo, responsabilidad y conocimientos técnicos de su personal en los centros de llamadas de reportes de fallas, centros de gestión y personal de reparación de averías. Asimismo, deberá contar con el equipamiento necesario para solucionar los problemas técnicos que se presenten. Para la imputación de responsabilidades por la existencia de averías se evaluará previamente si esta deberá recaer sobre el contratista o sobre el INABIF, siendo que, de comprobarse que la referida contingencia fue originada por la Entidad, no se generará ningún tipo de penalidad.
- La imputación de responsabilidades por la existencia de daños irreparables de los equipos se evaluará previamente para determinar si esta recae sobre el contratista o sobre el INABIF, siendo que, de comprobarse que el referido daño fuera originado por un uso negligente imputable a la entidad, será esta quien asuma los costos adicionales por la mencionada contingencia. La indisponibilidad por esta causa no será considerada para el cálculo de penalidades.
- El INABIF se reserva la potestad de constatar la información presentada por el operador.
- Durante el periodo de prestación del servicio, se evaluarán los tiempos de respuestas y la calidad del servicio, a fin de que el INABIF determine las correcciones necesarias si fuera el caso.

Se aclara que "determinar las correcciones necesarias", se refiere a las acciones necesarias para ajustar, mejorar y optimizar aspectos clave del servicio en función de los alcances del contrato. Estas correcciones no son arbitrarias ni imprecisas; más bien, se enmarcan dentro de parámetros claros relacionados con la calidad del servicio, el cumplimiento de los niveles de servicio establecidos y la mejora continua del mismo.¹²⁷

¹²⁶ ABSOLUCIÓN DE CONSULTA 123 - NEXTNET S.A.C.

¹²⁷ ABSOLUCIÓN DE CONSULTA 20 - AMERICA MOVIL PERU S.A.C.

Casos Especiales:

- a) Para el caso de pérdida de servicio por avería de planta externa (corte o ruptura de fibra óptica, imputable al Contratista, se brindará (04) horas adicionales a las (04) horas solicitadas para el tiempo de solución/reparación en casos de averías que no son de planta externa.
- b) Para el caso de avería por degradación de servicio (deterioro, intermitencia), se brindará (04) horas adicionales a las (04) horas solicitadas para el tiempo de solución/reparación en casos de averías que no son de planta externa.

5.9. INFRAESTRUCTURA

- a) El postor deberá ser miembro activo del NAP PERÚ (Network Access Point) con el que podrá utilizar el intercambio de redes entre los proveedores, facilitando una conexión continua de internet con baja latencia el servicio. Para ello, el postor ~~deberá presentar en su propuesta, una constancia del NAP que precise ser miembro de la Asociación,~~ **se confirma que, para la Admisión de las Ofertas, el postor puede incluir en su oferta "Constancia NAP que precise ser miembro de la Asociación", no siendo su presentación Obligatoria.**¹²⁸ ¹²⁹, en calidad de operador ISP, con capacidad de 2 enlaces x 100 Gbps.
- b) El proveedor deberá contar con una red principal o backbone; incluido la última milla de fibra óptica para el servicio.
- c) El proveedor deberá proporcionar los equipos de comunicación para cada uno de los enlaces: Principal y de contingencia. Dichos equipos deberán ser de última generación con capacidad de soportar características de seguridad a solicitud del personal especializado en seguridad del INABIF.
- d) El postor deberá incluir en su servicio, una plataforma de autogestión del DNS (Sistema de Nombres de Dominio) que permitirá al usuario autorizado (Con clave de acceso) poder crear, actualizar, modificar y eliminar configuraciones de los registros del DNS. Para ello, se deberá contar como mínimo, con (02) servidores DNS (Principal y redundado) ubicados en Data Center distintos a nivel nacional (Por seguridad de la información, ~~al menos (01) servidor DNS, deberá estar alojado en el Data center propio del postor, certificado en la norma ANSI/TIA de Diseño o Construcción. El postor deberá presentar en su propuesta el/los certificados ANSI/TIA vigentes a nombre del postor.~~ **Opcionalmente al menos uno de los DNS se encuentre en un DC certificado, siempre que se garantice la redundancia geográfica de los DNS para asegurar la operación del servicio. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el/los certificados ANSI/TIA vigentes a nombre del postor.**¹³⁰

Se aclara y se confirma que el servicio de DNS autogestionable en el DC del proveedor bajo la norma ANTSI/TIA será considerada como una característica

¹²⁸ ABSOLUCIÓN DE OBSERVACION 21 - AMERICA MOVIL PERU S.A.C.

¹²⁹ ABSOLUCIÓN DE OBSERVACION 62 - FRAVATEL EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA

¹³⁰ ABSOLUCIÓN DE CONSULTA 45 - AMERICA MOVIL PERU S.A.C.

opcional. Así mismo, se menciona que para cualquier requerimiento o cambio en los DNS el postor deberá cumplir con los SLA descritos en las bases del proceso.¹³¹

Se aclara y se confirma que la herramienta web autogestionable para la gestión de registros DNS será considerada como una característica opcional. Así mismo, se menciona que para cualquier requerimiento o cambio en los DNS el postor deberá cumplir con los SLA descritos en las bases del proceso.¹³²

- e) El postor deberá contar, con su propio **o tercerizado**¹³³ Centro de Operaciones de Red (NOC - Network Operations Center) y su propio Centro **o tercerizado**¹³⁴ de Operaciones de Seguridad (SOC - Security Operations Center). **Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el/los certificados ANSI/TIA vigentes a nombre del postor.**¹³⁵
- f) los cuales atenderán los requerimientos de las bases y mantendrán una comunicación directa con la entidad. ~~Para ello, el postor deberá presentar en su propuesta, su licencia de funcionamiento de la dirección del inmueble y un certificado vigente emitido por una empresa consultora externa (Certificadora en infraestructura y centros de comando de control) que acredite la operación e infraestructura propia del NOC & SOC.~~ **Opcionalmente, será posible la acreditación de la propiedad del NOC y SOC a través de una constatación notarial y/o licencia de funcionamiento y/o certificado vigente emitido por una empresa consultora externa, en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.**^{136 137}
- g) Considerando la importancia, de que el postor asegure una correcta calidad del servicio, confirme la seguridad de la información y asegure la continuidad del servicio, el cual incluirá como mínimo, el planeamiento de soluciones tecnológicas sobre fibra óptica, radio enlaces, monitoreo, soporte, mantenimiento del servicio y atención al cliente. Para ello, el postor deberá **acreditar con el Anexo N° 3**¹³⁸ ~~de presentar el certificado~~ en la presentación de oferta; y en el caso de consorcio cada miembro deberá **acreditar con el Anexo N° 3**¹³⁹ ~~presentar su propia certificación.~~
- h) Considerando la importancia, de que el postor asegure una correcta calidad del servicio, confirme la seguridad de la información y asegure la continuidad del servicio, el cual incluirá como mínimo, los procesos de Provisión, Instalación, Soporte, Monitoreo, Mantenimiento y Gestión, relacionados a los Servicios Cloud, Acceso Dedicado a Internet, Fibra oscura, Centro de Datos, Interconexión de Sedes y Servicios de Seguridad para clientes. Para ello, el postor deberá ~~de presentar su~~

¹³¹ ABSOLUCIÓN DE CONSULTA 134 - NEXTNET S.A.C.

¹³² ABSOLUCIÓN DE CONSULTA 135 - NEXTNET S.A.C.

¹³³ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

¹³⁴ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

¹³⁵ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

¹³⁶ ABSOLUCIÓN DE CONSULTA 22 - AMERICA MOVIL PERU S.A.C.

¹³⁷ ABSOLUCIÓN DE OBSERVACIÓN 23 - AMERICA MOVIL PERU S.A.C.

¹³⁸ ABSOLUCIÓN DE CONSULTA 24 - AMERICA MOVIL PERU S.A.C.

¹³⁹ ABSOLUCIÓN DE CONSULTA 24 - AMERICA MOVIL PERU S.A.C.

~~certificado~~ **acreditar con el Anexo N° 3¹⁴⁰** en la presentación de oferta; y en el caso de consorcio cada miembro deberá **acreditar con el Anexo N° 3¹⁴¹**. ~~presentar su propia certificación.~~

- i) ~~Considerando la importancia, de que el postor asegure una correcta calidad del servicio, confirme la seguridad de la información y asegure la continuidad del servicio, el cual incluirá como mínimo, la provisión, Instalación, Soporte, Monitoreo, Mantenimiento y Gestión, relacionados a los Servicios Cloud, Acceso Dedicado a Internet, Fibra oscura, Centro de Datos, Interconexión de Sedes y Servicios de Seguridad para clientes. Para ello, el postor deberá de presentar el certificado en la presentación de oferta; y en el caso de consorcio cada miembro deberá presentar su propia certificación.~~¹⁴²

6. REQUERIMIENTO MÍNIMOS DE LA EMPRESA A CONTRATAR

- a) La disponibilidad del servicio del enlace dedicado al Internet debe ser como mínimo en el orden del 99.90%, que está compuesta por dos (02) enlaces de Internet
- b) El enlace de contingencia sólo será necesario ante la caída del enlace principal, por lo que, la contingencia solo es para mantener en actividad los servicios básicos, hasta el restablecimiento del principal.
- c) De haber alguna afectación del servicio debido a causas externas, ajenas al proveedor podrá ser reportada a las centrales del proveedor a fin de brindar la atención sin que implique penalidad.
- d) El proveedor deberá indicar el procedimiento con los que cuenta para el reporte de fallas y la gestión en general. El tiempo de respuesta máximo para la atención de un problema, será no mayor de una (01) hora, y la resolución en un máximo de cuatro (04) horas, contados desde que el INABIF reporta el incidente al Centro de Atención/Servicio del proveedor y se le asignará un ticket de atención. Dicho reporte será vía llamada telefónica o vía correo electrónico, para lo cual la empresa deberá dar la información sobre los puntos de contacto a la institución.
- e) El proveedor garantizará la disponibilidad en todo momento del ancho de banda de acceso a internet contratado.
- f) El overbooking contratado no podrá ser variado durante la vigencia del contrato.
- g) El proveedor deberá presentar a un Coordinador de Soporte o quien haga a su vez en la organización del Contratista, quien se considerada un personal clave para el desarrollo del servicio, con quien se coordinará los reportes de averías, el cual deberá contar con experiencia mínima de 2 años en reportes en general.

Se acoge la consulta, se confirma que lo que se solicita en este párrafo es que la entidad cuente con los contactos y escalamientos al momento de reportar una

¹⁴⁰ ABSOLUCIÓN DE CONSULTA 25 - AMERICA MOVIL PERU S.A.C.

¹⁴¹ ABSOLUCIÓN DE CONSULTA 25 - AMERICA MOVIL PERU S.A.C.

¹⁴² ABSOLUCIÓN DE CONSULTA 26 - AMERICA MOVIL PERU S.A.C.

avería para una adecuada atención del servicio.¹⁴³

Se aclara que el coordinador de soporte con 2 años de experiencia no será considerado como personal clave para el presente proceso. Así mismo, el presente inciso hace referencia a los contactos y el proceso de escalamiento para el reporte de averías en el servicio.¹⁴⁴

Se acoge la consulta. El presente punto no hace referencia a un personal onsite dedicado.¹⁴⁵

- h) El proveedor informará sobre cualquier mantenimiento físico o lógico que afecte el desempeño del servicio de Internet y/o Enlace entre Sedes contratado (equipos de última milla, cableado, servidores, etc.). Para ello, elaborará cronogramas que serán entregados a INABIF con la debida anticipación.
- i) La modalidad de la contratación del servicio es a todo costo. El proveedor deberá de incluir en su propuesta todos los componentes necesarios para el servicio de enlace dedicado de acceso a Internet, como para el enlace dedicado entre sedes (medios de enlace, FO, cables, routers, modems, patch cords, entre otros). Igualmente deberá incluir la instalación y programación del equipo de acceso necesario para la prestación del servicio.
- j) Los horarios de implementación son con coordinación previa, pudiendo ser fuera de horario de oficina, a fin de no afectar las labores diarias de la entidad.
- k) El proveedor deberá contar con un Centro de Operaciones de Seguridad (SOC) y Centro de Operaciones de Red (NOC) propio **o tercerizado, Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION¹⁴⁶**, donde monitoreen (7x24) los equipos instalados, y se deberá presentar la documentación que lo acredite. El proveedor es el responsable de la actualización oportuna de los parches, firmware de los equipos y deben hacer copias de respaldo de la configuración y políticas de los equipos instalados.
- l) Asimismo, el proveedor debe garantizar la seguridad de sus redes y sistemas de información ante intrusos de cualquier tipo que puedan afectar la imagen del INABIF. La protección de seguridad mencionada se refiere a la implementación de equipos de seguridad para la protección de las redes internas del INABIF y sistemas de información ante intrusos; dichos equipos fueron indicados en el punto 5.3; de ser el caso el proveedor podrá brindar equipamiento adicional como mejora de su propuesta.
- m) El proveedor deberá tomar las previsiones del caso a fin de no perjudicar el inicio

¹⁴³ ABSOLUCIÓN DE CONSULTA 172 - WIN EMPRESAS S.A.C.

¹⁴⁴ ABSOLUCIÓN DE CONSULTA 173 - WIN EMPRESAS S.A.C.

¹⁴⁵ ABSOLUCIÓN DE CONSULTA 174 - WIN EMPRESAS S.A.C.

¹⁴⁶ ABSOLUCIÓN DE CONSULTA 47 - AMERICA MOVIL PERU S.A.C.

de las labores diarias en INABIF, en el momento de la implementación del servicio.

Se aclara que la frase "el inicio de las labores diarias en INABIF" hace referencia específicamente a las labores operativas del día a día realizadas dentro de la Entidad como actividades rutinarias relacionadas con el servicio que brinda la entidad

Asimismo, se precisa que el momento de la implementación del servicio estará formalizado mediante la suscripción del acta de instalación, la cual establecerá la fecha oficial de inicio de la prestación del servicio. Este procedimiento garantiza claridad y orden en la ejecución de las obligaciones contractuales.¹⁴⁷

n) El proveedor deberá entregar un informe final con los detalles técnicos y de infraestructura de las telecomunicaciones implementadas en el INABIF, al día siguiente de culminado el proceso de implementación.

o) Capacitación como parte del servicio:

- La capacitación ~~oficial~~, **deberá ser no oficial y serán basados en curricula oficial de la marca y podrán ser grabados de forma opcional. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{148 149 150 151}**, deberá realizarse en la ciudad de Lima, por un personal certificado por la marca ofertada, en un ambiente virtual que proveerá el proveedor y reúna las condiciones para el dictado de clases teóricas-prácticas, incluye capacitación grabada que será brindada al personal a capacitar además de guías y/o manuales y/o documentación técnica, entre otros.

Las capacitaciones podrán ser teóricas y en caso de incluir parte práctica se podrá utilizar el propio equipamiento brindado parte del servicio con el fin de hacer las demostraciones de acuerdo a lo implementado. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁵²

- La capacitación será dirigida para tres (03) personas; está orientada en el manejo de los equipos que forman parte del servicio (Componente Seguridad de Borde SASE, Solución Antispam) con un mínimo de diez (10) horas o según la cantidad de horas que tengan definidos los fabricantes en sus cursos oficiales, así mismo dichos cursos podrán realizarse de manera virtual (remoto).

Se aclara que la capacitación será no oficial basada en al curricula oficial y será dirigida para tres (03) personas con un mínimo de 10 horas (solución

¹⁴⁷ ABSOLUCIÓN DE CONSULTA 125 - NEXTNET S.A.C.

¹⁴⁸ ABSOLUCIÓN DE CONSULTA 48 - AMERICA MOVIL PERU S.A.C.

¹⁴⁹ ABSOLUCIÓN DE CONSULTA 50 - AMERICA MOVIL PERU S.A.C.

¹⁵⁰ ABSOLUCIÓN DE CONSULTA 51 - AMERICA MOVIL PERU S.A.C.

¹⁵¹ ABSOLUCIÓN DE CONSULTA 74- WIN EMPRESAS S.A.C.

¹⁵² ABSOLUCIÓN DE CONSULTA 49 - AMERICA MOVIL PERU S.A.C.

SASE, solución antispam) y esta podrá ser brindada durante la IMPLEMENTACION DEL SERVICIO y de forma remota y/o presencial.¹⁵³

- Las coordinaciones para asistir a las capacitaciones deben realizarse con las tres (03) personas acordando una fecha y hora que pueda ser factible para ambos lados. Será responsabilidad del personal asistir a las capacitaciones, la conformidad sobre este punto será cuando el personal complete las capacitaciones brindadas.

Se aclara que las capacitaciones serán brindadas por el postor con curricula oficial del fabricante mas no serán oficiales. La grabación de las sesiones será opcional. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁵⁴

Se aclara que las capacitaciones serán brindadas por el postor con curricula oficial del fabricante mas no serán oficiales. Así mismo, las capacitaciones serán brindadas por personal certificado en la solución propuesta. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁵⁵

Se aclara que las capacitaciones serán brindadas por el postor con curricula oficial del fabricante mas no serán oficiales. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁵⁶

7. PLAZO DE EJECUCIÓN

El otorgamiento del Acta de Conformidad de Instalación del Servicio se brindará posterior a la instalación, previa verificación de los servicios que se realizará en conjunto con el proveedor, como máximo en 48 horas.

El Contratista tendrá ciento veinte (120) días calendario como máximo para la implementación del servicio, que incluye la instalación de todos equipos mínimos requeridos en el literal 5.3. del numeral 5. del presente documento, para lo cual deberá hacer entrega de toda la documentación requerida detallada en los TDR con respecto a este plazo. Los ciento veinte (120) días calendario serán contabilizados a partir del día siguiente del **de la fecha de suscripción¹⁵⁷** del contrato ~~perfeccionamiento del Contrato~~ con el INABIF.

Se confirma la consulta, cuando en el párrafo primero del Numeral 7, la frase "Instalación del Servicio" se refiere a la "Instalación del Servicio" señalada en el segundo párrafo del referido numeral.¹⁵⁸

¹⁵³ ABSOLUCIÓN DE CONSULTA 126 - NEXTNET S.A.C.

¹⁵⁴ ABSOLUCIÓN DE CONSULTA 175 - WIN EMPRESAS S.A.C.

¹⁵⁵ ABSOLUCIÓN DE CONSULTA 176 - WIN EMPRESAS S.A.C.

¹⁵⁶ ABSOLUCIÓN DE CONSULTA 177 - WIN EMPRESAS S.A.C.

¹⁵⁷ ABSOLUCIÓN DE CONSULTA N° 28 - AMERICA MOVIL PERU S.A.C.

¹⁵⁸ ABSOLUCIÓN DE CONSULTA N° 127 - NEXTNET S.A.C.

El plazo contractual o de ejecución del servicio será por el lapso de veinticuatro (24) meses, el cual será contabilizado a partir del día siguiente que la Unidad de Tecnologías de la Información, suscriba el Acta de Conformidad de Instalación del Servicio al INABIF, realizada por el Contratista. **El otorgamiento de esta Acta, se brindará posterior a la instalación, previa verificación de los servicios que se realizará en conjunto con el proveedor.**¹⁵⁹

El contratista debe tener en cuenta que los trámites de permisos o autorizaciones que sean necesarios realizar ante la autoridad competente deben de preverse con anticipación de manera que no afecte el plazo de implementación del servicio. Las solicitudes de ampliación de plazo por causas fortuitas o de fuerza mayor serán evaluadas de acuerdo a la Ley de Contrataciones del Estado y su Reglamento.¹⁶⁰

Se confirma que se coordinará para que el proveedor tenga las facilidades para realizar los trabajos de instalación.¹⁶¹

Se confirma que, una vez finalizado el plazo contractual, procederá a la devolución del total de los equipos que le hayan sido entregados y/o instalados. Para ello, se comunicará al contratista para disponer del retiro de equipos dentro de los diez días calendarios de finalizado el contrato o de haber sido notificado.¹⁶²

8. SOBRE LA IMPLEMENTACIÓN

El periodo de instalación comprende la instalación y puesta en marcha del servicio de acuerdo con la propuesta adjudicada; asimismo, se realizará la verificación del servicio contratado en forma conjunta, una vez concluida la instalación del cien por ciento (100%) de los enlaces ofertados por el proveedor.

Para dar inicio al ciclo de Facturación, de todos los servicios, la Unidad de Tecnologías de la Información deberá emitir la Conformidad de Servicio. El periodo de la instalación no está dentro del tiempo de servicio contratado.

El periodo de instalación será contabilizado a partir del día siguiente de la fecha de suscripción del contrato, debiendo presentar un cronograma de actividades antes del inicio de los trabajos técnicos. El cronograma de trabajo de implementación ~~será presentado como documento para el perfeccionamiento del contrato,~~ **deberá presentarse después de la suscripción del contrato, pero se establece que el plazo será de 5 días calendario a partir de la fecha de suscripción del contrato**¹⁶³. Para el ingreso del personal del proveedor ganador, que realice los trabajos en las instalaciones del INABIF, se requiere el envío de la relación del personal con su Documento Nacional de Identidad (DNI) y fecha en que se realizarán los trabajos, con un mínimo de 48 horas de anticipación. **Se confirma que el medio de presentación de la relación del personal que realizará los trabajos de implementación podrá ser adicionalmente por correo**

¹⁵⁹ ABSOLUCIÓN DE CONSULTA N° 03 - AMERICA MOVIL PERU S.A.C.

¹⁶⁰ ABSOLUCIÓN DE CONSULTA N° 75 – WIN EMPRESAS S.A.C.

¹⁶¹ ABSOLUCIÓN DE CONSULTA N° 76 – WIN EMPRESAS S.A.C.

¹⁶² ABSOLUCIÓN DE CONSULTA N° 114 - NEXTNET S.A.C.

¹⁶³ ABSOLUCIÓN DE CONSULTA N° 29 - AMERICA MOVIL PERU S.A.C.

electrónico al funcionario designado por la entidad durante la etapa de formalización del contrato, toda vez que el plazo de implementación inicia al día siguiente de la suscripción del contrato y los accesos que brindará la entidad serán brindados 48 horas posteriores a la solicitud del contratista.¹⁶⁴

Se confirma y aclara que el contenido mínimo que deberá contener el cronograma de trabajo de implementación es el siguiente: Descripción de las actividades, Duración estimada de las actividades, Fechas de inicio y fin, Responsables, Recursos necesarios.¹⁶⁵

Se confirma que el "Cronograma de actividades" y los documentos requeridos, deberá presentarse después de la suscripción del contrato, pero se establece que el plazo será de 5 días calendario a partir de la fecha de suscripción del contrato, y 2 días calendarios para su aprobación.¹⁶⁶

9. LUGAR DE EJECUCIÓN

La prestación e instalación y configuración del servicio se realizará en la Sede Central del INABIF con domicilio legal en Av. San Martín 685 – Pueblo Libre.

10. FORMA DE PAGO

El pago se realizará de forma mensual, el cual será 1/24 parte del monto adjudicado; el proveedor deberá remitir la factura o **Recibos autorizados por SUNAT**¹⁶⁷ correspondiente, adjuntando la documentación anexa solicitada, seguidamente la Unidad de Tecnologías de la Información emitirá una Conformidad de Servicio, en un plazo máximo de siete (7) días de producida la recepción

Una vez emitida la conformidad de servicio, esta será tramitada a la Subunidad de Abastecimiento, a fin de iniciar las gestiones para el pago correspondiente.

Cabe señalar que el mencionado pago, incluye los costos del servicio, otras prestaciones, así como el mantenimiento preventivo y capacitaciones.

Para efectos de la emisión de la Conformidad de Servicio, el proveedor deberá entregar la siguiente documentación:

- a) Factura o **Recibos autorizados por SUNAT**¹⁶⁸ por concepto del servicio prestado.
- b) Lo indicado en el punto 5.2 inciso a.16

Se precisa que, se aceptará el prorrateo correspondiente, el cual se verá reflejado en el primer y último recibo del servicio contratado, sin modificar el importe total del

¹⁶⁴ ABSOLUCIÓN DE CONSULTA N° 30 - AMERICA MOVIL PERU S.A.C.

¹⁶⁵ ABSOLUCIÓN DE CONSULTA N° 128 – NEXTNET S.A.C.

¹⁶⁶ ABSOLUCIÓN DE CONSULTA N° 178 – WIN EMPRESAS S.A.C.

¹⁶⁷ ABSOLUCIÓN DE CONSULTA N° 31 - AMERICA MOVIL PERU S.A.C.

¹⁶⁸ ABSOLUCIÓN DE CONSULTA N° 31 - AMERICA MOVIL PERU S.A.C.

monto total contratado.^{169 170 171}

11. PENALIDAD

Las penalidades se aplicarán por cada día de atraso, hasta por un monto máximo equivalente al 10% del monto del contrato vigente, en concordancia con el artículo 161° y 162° del Reglamento de la Ley de Contrataciones del Estado, tal como lo señalan los términos de referencia.

OTRAS PENALIDADES (163° del Reglamento de la Ley de Contrataciones del Estado)

La siguiente penalidad se aplicará en caso de incumplimiento del requerimiento mínimo expuesto en el presente documento.

Descripción de incumplimiento	Monto	Procedimientos
Cuando la disponibilidad del servicio de internet y/o seguridad no cumpla con el 99.90% como mínimo y se considerará como caída del servicio. (*)	5% del valor de una UIT (Unidad Impositiva Tributaria). Por cada hora o fracción de inoperatividad del enlace.	Informe de la Unidad de Tecnologías de la Información que acredite el supuesto de aplicación de penalidad
En caso culmine la relación entre el contratista y el ingeniero o el coordinador de soporte ofertado, y la Entidad no haya aprobado la sustitución del personal por no cumplir con la experiencia y calificaciones requeridas en las bases.	30% de una (01) UIT por cada día de ausencia del personal y/o por cada día transcurrido de no haber notificado el cambio del personal. ⁸¹	

(*) La aplicación de la mencionada penalidad, será medida de acuerdo con las métricas establecidas en el Acuerdo de Nivel de Servicio.

12. RESPONSABILIDAD DEL CONTRATISTA POR VICIOS OCULTOS

El CONTRATISTA, es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofrecido de conformidad a lo dispuesto por el Artículo 40° de la Ley de Contrataciones del Estado.

El plazo máximo de responsabilidad de EL CONTRATISTA es de un año, a partir de la conformidad otorgada por el ENTIDAD.

13. DOCUMENTOS PARA LA ADMISIÓN DE LA OFERTA^{172 173}

¹⁶⁹ ABSOLUCIÓN DE CONSULTA N° 69 - WIN EMPRESAS S.A.C.

¹⁷⁰ ABSOLUCIÓN DE CONSULTA N° 71 - WIN EMPRESAS S.A.C.

¹⁷¹ ABSOLUCIÓN DE CONSULTA N° 78 - WIN EMPRESAS S.A.C.

¹⁷² ABSOLUCIÓN DE CONSULTA 05 - AMERICA MOVIL PERU S.A.C.

¹⁷³ ABSOLUCIÓN DE OBSERVACIÓN 116 - NEXTNET S.A.C.

- (a) Declaración jurada de datos del postor. (Anexo N° 1).
- (b) Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

- (c) Declaración jurada de acuerdo con el literal
- (d) b) del artículo 52 del Reglamento. (Anexo N° 2) d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3).
- (e) Declaración jurada de plazo de prestación del servicio. (Anexo N° 4)
- (f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5)
- (g) El precio de la oferta en SOLES Adjuntar obligatoriamente el Anexo N° 6. El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

14. REQUISITOS PARA PERFECCIONAR EL CONTRATO¹⁷⁴

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

- (a) Garantía de fiel cumplimiento del contrato.
- (b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- (c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
- (d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- (e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.

¹⁷⁴ **ABSOLUCIÓN DE CONSULTA 06 - AMERICA MOVIL PERU S.A.C.**

- (f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
- (g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- (h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación 6 (Anexo N° 12).
- (i) Detalle de los precios unitarios del precio ofertado.

15. "CRONOGRAMA DE ACTIVIDADES" Y LOS DOCUMENTOS REQUERIDOS¹⁷⁵

(a) Se acepta una opción SASE o NGFW en HA on-premise, siempre que NGFW cumpla al menos con los siguientes requisitos técnicos:

- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para: "Enterprise Network Firewall" en los últimos 10 reportes.
- Throughput de prevención de amenazas de 4gbps y 256 Mil nuevas sesiones/conexiones por segundo.
- NGFW u otro componente, 4x1G interfaces bypass para la optimización de tráfico.

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades".^{176 177 178 179 180 181}

(b) "Para evaluar la solución de seguridad es necesario que el postor presente con el "Cronograma de Actividades", la documentación técnica que acredite el cumplimiento de la solución descrita en el numeral 5.3.b".^{182 183 184 185}

(c) Se solicitan 270 usuarios de acceso seguro ZTNA para la interconexión de los usuarios de los centros de atención de INABIF, dicho componente deberá contar con las siguientes características:

Se acoge parcialmente la consulta.

El postor podrá considerar características distintas para ZTNA, siempre que

¹⁷⁵ ABSOLUCIÓN DE CONSULTA N° 178 – WIN EMPRESAS S.A.C.

¹⁷⁶ ABSOLUCIÓN DE CONSULTA 37 - AMERICA MOVIL PERU S.A.C.

¹⁷⁷ ABSOLUCIÓN DE CONSULTA 87 - GLOBAL LINK ONE S.A.C.

¹⁷⁸ ABSOLUCIÓN DE CONSULTA 183 – WIN EMPRESAS S.A.C.

¹⁷⁹ ABSOLUCIÓN DE CONSULTA 184 – WIN EMPRESAS S.A.C.

¹⁸⁰ ABSOLUCIÓN DE CONSULTA 185 – WIN EMPRESAS S.A.C.

¹⁸¹ ABSOLUCIÓN DE CONSULTA 186 – WIN EMPRESAS S.A.C.

¹⁸² ABSOLUCIÓN DE CONSULTA 13 - AMERICA MOVIL PERU S.A.C.

¹⁸³ ABSOLUCIÓN DE CONSULTA 146 - WIN EMPRESAS S.A.C.

¹⁸⁴ ABSOLUCIÓN DE CONSULTA 147 - WIN EMPRESAS S.A.C.

¹⁸⁵ ABSOLUCIÓN DE CONSULTA 148 - WIN EMPRESAS S.A.C.

que cumplan con las funciones detalladas en la absolución de la consulta N°104:

1. Que sea una solución de ZTNA, que permita tres sesiones simultáneas por usuario remoto o que el postor considere 810 usuarios remotos.

2. Que tenga habilitado MFA para la autenticación robusta.

3. Que considere filtrado de navegación, inspección IPS, protección DNS, antimalware, para que el tráfico del usuario remoto sea inspeccionado y controlado antes de llegar al perímetro de INABIF.

Se acreditará en la relación de documentos a presentar con el "Cronograma de Actividades".^{186 187 188 189 190}

16. DOCUMENTOS PARA ACREDITAR EN EL INFORME FINAL DE IMPLEMENTACIÓN¹⁹¹

(a) "Diagrama de la salida internacional", de acuerdo a lo indicado en el numeral 5.2, sub numeral a.4) de los términos de referencia.¹⁹²

(b) La habilitación de las cuentas, se deberá acreditar en el INFORME FINAL DE IMPLEMENTACIÓN.¹⁹³

(c) El proveedor deberá garantizar que el retardo máximo permitido será de 5ms, medido dentro de la red IP del proveedor, el que adicionalmente deberá presentar un esquema en el que se muestren las velocidades de conexión a los Backbone Internacionales de Internet y sus enlaces de intercambio (peering) con otros proveedores nacionales que les permite un intercambio local de datos y el cual será verificado en las pruebas de operatividad y estado del enlace para dar conformidad del servicio ofrecido, esta documentación será necesaria para la firma del contrato. La documentación señalada será requerida en el INFORME FINAL DE IMPLEMENTACIÓN.¹⁹⁴

(d) El "Cronograma del Plan de mantenimiento preventivo", se efectuara en el INFORME FINAL DE IMPLEMENTACION.¹⁹⁵

(e) El contratista deberá incluir en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION procedimientos con los que cuenta para el reporte de fallas y la gestión del servicio en general. ¹⁹⁶

¹⁸⁶ ABSOLUCIÓN DE CONSULTA 104 - GLOBAL LINK ONE S.A.C.

¹⁸⁷ ABSOLUCIÓN DE CONSULTA 106 - GLOBAL LINK ONE S.A.C.

¹⁸⁸ ABSOLUCIÓN DE CONSULTA 107 - GLOBAL LINK ONE S.A.C.

¹⁸⁹ ABSOLUCIÓN DE CONSULTA 112 - GLOBAL LINK ONE S.A.C.

¹⁹⁰ ABSOLUCIÓN DE CONSULTA 111 - GLOBAL LINK ONE S.A.C.

¹⁹¹ ABSOLUCIÓN DE CONSULTA N° 09 - AMERICA MOVIL PERU S.A.C.

¹⁹² ABSOLUCIÓN DE CONSULTA N° 09 - AMERICA MOVIL PERU S.A.C.

¹⁹³ ABSOLUCIÓN DE CONSULTA N° 11 - AMERICA MOVIL PERU S.A.C.

¹⁹⁴ ABSOLUCIÓN DE CONSULTA N° 14 - AMERICA MOVIL PERU S.A.C.

¹⁹⁵ ABSOLUCIÓN DE CONSULTA N° 16 - AMERICA MOVIL PERU S.A.C.

¹⁹⁶ ABSOLUCIÓN DE CONSULTA 19 - AMERICA MOVIL PERU S.A.C.

- (f) El postor deberá contar, con su propio **o tercerizado** Centro de Operaciones de Red (NOC - Network Operations Center) y su propio Centro **o tercerizado** de Operaciones de Seguridad (SOC - Security Operations Center) los cuales atenderán los requerimientos de las bases y mantendrán una comunicación directa con la entidad. **Opcionalmente, será posible la acreditación de la propiedad del NOC y SOC a través de una constatación notarial y/o licencia de funcionamiento y/o certificado vigente emitido por una empresa consultora externa, en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.**^{197 198}
- (g) Para el servicio de Internet de última milla, el proveedor deberá brindar 32 direcciones IPv4 e IPv6.
- Asimismo, solo en el caso de SASE, se deberá considerar lo señalado en el inciso 5.3.b.5.
- En cuanto al pool de direcciones IPv6, tanto para SASE como para NGFW, no será necesario añadir direcciones IP adicionales, siempre que se cumplan las características descritas en la absolución de la consulta N°37.
- Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.¹⁹⁹
- (h) El servicio debe contemplar la gestión de segmentación y priorización del tráfico de acceso a Internet, a través de la funcionabilidad de Calidad de Servicio (QoS), podrá ser suministrada por el componente seguridad de borde (SASE **o NGFW de igual o superior característica siempre que cumpla con las características descritas en la absolución de la consulta N°37**) propuesto por el contratista de acuerdo con los requerimientos del INABIF.
- Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{200 201}
- (i) El tiempo de retardo permitido será desde el equipamiento brindado en la sede del cliente hasta el equipo de la salida internacional del proveedor. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.²⁰²
- (j) El postor que resulte adjudicado con la buena pro deberá cumplir obligatoriamente con al menos dos (02) proveedores TIER 1 para garantizar la redundancia del servicio de conectividad internacional y al menos uno de los proveedores TIER 1 deberá tener una capacidad mínima de 100 Gbps. Estas condiciones tienen como finalidad asegurar la calidad y continuidad del servicio, manteniendo un estándar

¹⁹⁷ ABSOLUCIÓN DE CONSULTA 22 - AMERICA MOVIL PERU S.A.C.

¹⁹⁸ ABSOLUCIÓN DE CONSULTA 23 - AMERICA MOVIL PERU S.A.C.

¹⁹⁹ ABSOLUCIÓN DE CONSULTA 38 - AMERICA MOVIL PERU S.A.C.

²⁰⁰ ABSOLUCIÓN DE CONSULTA 40 - AMERICA MOVIL PERU S.A.C.

²⁰¹ ABSOLUCIÓN DE CONSULTA 85 - GLOBAL LINK ONE S.A.C.

²⁰² ABSOLUCIÓN DE CONSULTA N° 41 - AMERICA MOVIL PERU S.A.C.

adecuado de conectividad internacional para las necesidades de la entidad. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.²⁰³

- (k) El postor deberá incluir en su servicio, una plataforma de autogestión del DNS (Sistema de Nombres de Dominio) que permitirá al usuario autorizado (Con clave de acceso) poder crear, actualizar, modificar y eliminar configuraciones de los registros del DNS. Para ello, se deberá contar como mínimo, con (02) servidores DNS (Principal y redundado) ubicados en Data Center distintos a nivel nacional (Por seguridad de la información. **Opcionalmente al menos uno de los DNS se encuentre en un DC certificado, siempre que se garantice la redundancia geográfica de los DNS para asegurar la operación del servicio. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el/los certificados ANSI/TIA vigentes a nombre del postor.²⁰⁴**
- (l) El postor deberá contar, con su propio **o tercerizado²⁰⁵** Centro de Operaciones de Red (NOC - Network Operations Center) y su propio Centro **o tercerizado²⁰⁶** de Operaciones de Seguridad (SOC - Security Operations Center). **Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el/los certificados ANSI/TIA vigentes a nombre del postor.²⁰⁷**
- (m) El proveedor deberá contar con un Centro de Operaciones de Seguridad (SOC) y Centro de Operaciones de Red (NOC) propio **o tercerizado, Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.²⁰⁸**
- (n) La capacitación ~~oficial,~~ **deberá ser no oficial y serán basados en curricula oficial de la marca y podrán ser grabados de forma opcional. Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{209 210 211 212}**
213 214
- (o) **Se deberá presentar el detalle técnico (brochure, datasheet) de los equipos que componen la solución ofertada, en el deberá detallarse la marca, el modelo y un diagrama de red de cómo se integraran las soluciones, en la relación de**

²⁰³ ABSOLUCIÓN DE CONSULTA N° 42 - AMERICA MOVIL PERU S.A.C.

²⁰⁴ ABSOLUCIÓN DE CONSULTA 45 - AMERICA MOVIL PERU S.A.C.

²⁰⁵ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

²⁰⁶ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

²⁰⁷ ABSOLUCIÓN DE CONSULTA 46 - AMERICA MOVIL PERU S.A.C.

²⁰⁸ ABSOLUCIÓN DE CONSULTA 47 - AMERICA MOVIL PERU S.A.C.

²⁰⁹ ABSOLUCIÓN DE CONSULTA 48 - AMERICA MOVIL PERU S.A.C.

²¹⁰ ABSOLUCIÓN DE CONSULTA 50 - AMERICA MOVIL PERU S.A.C.

²¹¹ ABSOLUCIÓN DE CONSULTA 51 - AMERICA MOVIL PERU S.A.C.

²¹² ABSOLUCIÓN DE CONSULTA 175 - WIN EMPRESAS S.A.C.

²¹³ ABSOLUCIÓN DE CONSULTA 176 - WIN EMPRESAS S.A.C.

²¹⁴ ABSOLUCIÓN DE CONSULTA 177 - WIN EMPRESAS S.A.C.

documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.²¹⁵

Se confirma y aclara que en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION, el postor deberá presentar un detalle técnico (brochure, datasheet) de los equipos que componen la solución ofertada, en el deberá detallarse la marca, el modelo y un diagrama de red de cómo se integraran las soluciones.²¹⁶

(p) IPS (Intrusion Prevention System) que incluya las siguientes categorías:

- Crypto Mining;
- Phishing;
- Ransomware;
- Privilege Escalation;
- Web Application Attack; y
- Restricciones de geolocalización.

Dicha característica será opcional para el NGFW. Se aceptarán soluciones SASE o NGFW de igual o superiores características a las descritas siempre que cumplan con las funciones detalladas en la absolución de consulta N°37.

Se acreditará en la relación de documentos a presentar en el INFORME FINAL DE IMPLEMENTACION.^{217 218}

²¹⁵ ABSOLUCIÓN DE CONSULTA N° 168 - WIN EMPRESAS S.A.C.

²¹⁶ ABSOLUCIÓN DE CONSULTA N° 169 - WIN EMPRESAS S.A.C.

²¹⁷ ABSOLUCIÓN DE CONSULTA 100 - GLOBAL LINK ONE S.A.C.

²¹⁸ ABSOLUCIÓN DE CONSULTA 197 – WIN EMPRESAS S.A.C.

17. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<u>Requisitos:</u> El proveedor debe contar con la Copia de la Autorización del Ministerio de Transportes y Comunicaciones para brindar el servicio de Conmutación de Datos por Paquete o Copia Simple del Certificado de Registro de Empresas Prestadoras de Servicio de Valor Añadido para prestar los servicios de conmutación de datos por paquete.
	Importante <i>De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.</i> <u>Acreditación:</u> Copia del documento que autoriza al proveedor para brindar el servicio de transmisión de datos (a Internet y/o Enlaces Dedicados) del Ministerio de Transportes y Comunicaciones o entidad competente ó Copia Simple del Certificado de Registro de Empresas Prestadoras del Servicio de Valor Añadido para prestar los servicios de conmutación de datos por paquetes, emitido por el Ministerio de Transportes y Comunicaciones, o mediante Copia Simple del Registro de Empresas Prestadoras del Servicio de Valor Añadido publicado en la página web del Ministerios de Transportes y Comunicaciones. Importante <i>En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.</i>

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'440,000.00 (Un millón cuatrocientos cuarenta mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 120,000.00 (Ciento veinte mil con 00/100 soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes: Transmisión de Datos, Seguridad Perimetral o SASE, Servicios de Telecomunicaciones, Acceso Dedicado a Internet, Transmisión de voz y datos y/o red de contrataciones de datos para sedes y/o interconexión (enlace de datos entre sedes), servicio de línea de contingencia para transmisión de datos y/o servicio de enlace de transmisión de voz y datos para las redes, Servicio de transmisión recepción de datos a través de un Servicio de internet a nivel nacional y/o Internet Dedicado y Enlace de Datos y/o Servicio Integral de Telecomunicaciones y similares.</p> <p>Se considerará como servicio similar "Servicio de Internet en general y/o Interconexión de datos."²¹⁹</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con vócher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁸⁸, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones</p>

²¹⁹ **ABSOLUCIÓN DE CONSULTA 214 – GTD PERÚ S.A**

independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación que lo sustente correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

Importante

Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.

- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se*

	<p><i>hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".</i></p> <p>⁸⁸ Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:</p> <p><i>"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"</i></p> <p>(...)</p> <p><i>"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".</i></p>
--	---

B.3	CALIFICACIONES DEL PERSONAL CLAVE⁸⁹
<p>Importante para la Entidad</p> <p><i>Para las calificaciones del personal se puede considerar al menos uno de los requisitos siguientes:</i></p> <p><i>Esta nota deberá ser eliminada una vez culminada la elaboración de las bases, así como el requisito de calificación, si este no ha sido incluido.</i></p>	
B.3.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>Jefe de Proyecto</p> <p>Un (01) Profesional con título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica y/o Empresarial y de Sistemas. Colegiatura vigente y habilitado</p> <p>- Copia simple de Certificado, Diploma o Constancia en:²²⁰ ²²¹ Capacitación de mínimo 120 horas en gestión de proyectos y certificado de PMP vigente (Project Management Profesional) o SCRUM.</p> <p>- Copia simple de Certificado, Diploma o Constancia²²² ²²³ en Capacitación de mínimo 25 horas en ITIL v4 y certificado ITIL v4</p> <p>-Capacitación de mínimo 40 horas en SCRUM</p> <p>-Certificado ISO 27001, ISO 22301 e ISO 20001</p> <p>Se confirma y aclara que se deberá presentar, para acreditar el requisito de calificación "Capacitación", del Jefe de Proyecto: copia simple de Certificado, Diploma o Constancia en: 1). PMP vigente (Project Management Profesional) o</p>

²²⁰ ABSOLUCIÓN DE CONSULTA 52 - AMERICA MOVIL PERU S.A.C.

²²¹ ABSOLUCIÓN DE CONSULTA 53 - AMERICA MOVIL PERU S.A.C.

²²² ABSOLUCIÓN DE CONSULTA 52 - AMERICA MOVIL PERU S.A.C.

²²³ ABSOLUCIÓN DE CONSULTA 53 - AMERICA MOVIL PERU S.A.C.

SCRUM, y 2) ITIL v4, eliminándose ISO 27001, ISO 22301 e ISO 20001.^{224 225 226 227 228 229}

Implementador de Soluciones de Seguridad de Borde (SASE)

Se precisa que se considera necesario solicitar dos (02) implementadores en caso surgieran imprevistos con el personal clave durante las fases del proyecto que puedan afectar los plazos de finalización.²³⁰

Dos (02) Ingenieros Titulados o Técnicos Titulados o Bachiller de las carreras de Sistemas o Electrónica o Telecomunicaciones o Redes y Comunicaciones o Informática o Sistemas e Informática o Sistemas y Cómputo o Computación e Informática

Se incorporan las carreras de Redes y comunicación de datos, Ingeniería de informática y sistemas, seguridad y auditoría informática, Computación e informática, industrial.²³¹

Deberá contar con Certificación técnica nivel expert del fabricante de la solución de seguridad de Borde propuesta

Se precisa y aclara que el personal clave deberá contar con la certificación técnica nivel expert en cualquier nivel oficial del fabricante de la solución de seguridad de borde propuesta.²³²

Deberá con certificación de la marca propuesta con una certificación del tipo asociado o asociate en la tecnología propuesta o NDR

Se aclara que, los dos (02) implementadores de soluciones de seguridad de borde, deberán contar con certificación de la marca propuesta con una certificación del tipo asociado o asociate en la tecnología propuesta o NDR.²³³

Acreditación:

El Título será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : <http://www.titulosinstitutos.pe/>, según corresponda.

²²⁴ ABSOLUCIÓN DE CONSULTA 52 - AMERICA MOVIL PERU S.A.C.

²²⁵ ABSOLUCIÓN DE CONSULTA 53 - AMERICA MOVIL PERU S.A.C.

²²⁶ ABSOLUCIÓN DE OBSERVACIÓN 64 - FRAVATEL EMPRESA INDIVIDUAL DE RESPONSABILIDAD LIMITADA

²²⁷ ABSOLUCIÓN DE CONSULTA 214 - GTD PERÚ S.A

²²⁸ ABSOLUCIÓN DE OBSERVACIÓN 215 - GTD PERÚ S.A

²²⁹ ABSOLUCIÓN DE CONSULTA 216 - GTD PERÚ S.A

²³⁰ ABSOLUCIÓN DE CONSULTA 54 - AMERICA MOVIL PERU S.A.C.

²³¹ ABSOLUCIÓN DE CONSULTA 180 - WIN EMPRESAS S.A.C.

²³² ABSOLUCIÓN DE CONSULTA 55 - AMERICA MOVIL PERU S.A.C.

²³³ ABSOLUCIÓN DE CONSULTA 56 - AMERICA MOVIL PERU S.A.C.

	<p>Importante para la Entidad</p> <ul style="list-style-type: none"><i>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.</i><i>Incluir o eliminar, según corresponda. Sólo deberá incluirse esta nota cuando la formación académica sea el único requisito referido a las calificaciones del personal clave que se haya previsto. Ello a fin que la Entidad pueda verificar los grados o títulos requeridos en los portales web respectivos.</i> <p>En caso que el Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.4	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>Jefe de Proyecto</p> <p>Deberá contar con experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.</p> <p>Implementador de Soluciones de Seguridad de Borde</p> <p>Deberá contar con experiencia mínima de dos (02) años en implementación de equipos de seguridad y/o soluciones de seguridad.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>Importante</p> <ul style="list-style-type: none"><i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i><i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</i><i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i>



PERÚ

Ministerio
de la Mujer y
Poblaciones Vulnerables

Viceministerio de
Poblaciones Vulnerables

Programa Integral Nacional
para el Bienestar Familiar
INABIF

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.