CONTRATACIÓN DEL SERVICIO DE INTERNET DEDICADO CON SEGURIDAD GESTIONADA E INTERCONEXION DE DATOS CON LAS SUBDIRECCIONES REGIONALES DE LA ARCC

1. ÁREA USUARIA

Oficina de Tecnologías de la Información

2. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación de un servicio de internet dedicado con seguridad gestionada e interconexión de datos con las Subdirecciones Regionales de la Autoridad para la Reconstrucción con Cambios (ARCC)

3. OBJETIVO DE LA CONTRATACIÓN

La Autoridad de la Reconstrucción con Cambios, necesita contratar el servicio de internet dedicado con seguridad gestionada, que permita a la Entidad tener una red informática disponible expuesta a internet.

4. FINALIDAD PÚBLICA

Garantizar que la Autoridad Para la Reconstrucción con Cambios continúe manteniendo operatividad en su servicio de internet a fin de seguir trabajando a nivel nacional en sus distintas áreas y ubicaciones, desplegando sus servicios informáticos a sus colaboradores y a la ciudadanía.

5. DESCRIPCIÓN DEL SERVICIO

La Autoridad para la Reconstrucción con Cambios requiere contratar un servicio de internet dedicado con seguridad gestionada e interconexión de datos con las subdirecciones regionales de la Autoridad para la Reconstrucción con Cambios.

5.1. CARACTERÍSTICAS DEL SERVICIO Y TRABAJOS A REALIZAR

5.1.1 Actividades

La Autoridad de la Reconstrucción Con Cambios, necesita contratar el servicio de internet dedicado con seguridad gestionada, que permita a la Autoridad tener una red informática disponible expuesta a internet. El servicio debe tener las siguientes características:

5.1.1.1 Características Generales de los Servicios

- El proveedor deberá suministrar todos los equipos y sistemas de telecomunicaciones necesarios que permitan el correcto funcionamiento de todos los servicios solicitados.
- Las instalaciones en las sedes Oficina Principal y Lima deberán realizarse vía canalizado subterránea, mientras que las instalaciones en las sedes Tumbes, Huaraz, Cajamarca, Piura, Lambayeque y La Libertad deberán realizarse vía canalizado subterránea o aérea
- Para la imputación de responsabilidades por la existencia de daños irreparables en los equipos se evaluará previamente si esta deberá recaer sobre el contratista o sobre la Entidad.
- Todos los servicios deben contemplar la gestión y monitoreo activo de los mismos. Ante la caída del servicio, el centro de gestión del proveedor deberá

comunicarse con el responsable asignado de la Oficina de Tecnologías de la Información de la ARCC. Así mismo, el personal de la OTI debe tener acceso a estas herramientas. El contratista deberá brindar un usuario con perfil de administrador sin ningún tipo de restricción, el Contratista no será responsable por una mala configuración realizada por la entidad.

- El proveedor deberá cumplir con todas las disposiciones regulatorias que conducen a salvaguardar el secreto de las telecomunicaciones exigidas por el ente regulador OSIPTEL, además de contar con las autorizaciones de los ministerios competentes. Se precisa que lo señalado en el término de referencia, obedece a los parámetros de calidad establecidos y/o aceptados por el ente regulador OSIPTEL y el MTC según corresponda.
- El proveedor en la presentación de su oferta deberá indicar la plataforma tecnológica propuesta a fin de cumplir con los requerimientos de la RCC, a través de una Declaración Jurada, siendo el protocolo de comunicación TCP/IP, para lo cual la red de comunicaciones del contratista debe soportar calidad de servicio (QoS) de extremo a extremo, los cuales serán configurados durante la instalación de los enlaces; asimismo deberá presentarse como parte de la oferta.
- El contratista debe instalar en todas las sedes indicadas en los cuadros N° 1 y N° 2, los equipos de comunicaciones, los mismos que deben ser nuevos, de primer uso y no encontrarse en condición de End of Sale (EoS) ni End of Life (EoL) durante el plazo del servicio. Presentar carta del fabricante (también se podrá presentar una carta de distribuidor y/o reseller del postor indicando que los equipos del cuadro 2 no se encuentran en EoS no en EoL).
- Una vez finalizado el plazo contractual, procederá a la devolución del total de los equipos que le hayan sido entregados y/o instalados bajo cualquier modalidad distinta a la venta (incluyendo equipos, accesorios, routers, swicthes y/o cualquier otro de propiedad del contratista) sin mas desgaste que el de su uso normal y diligente, aceptando que en caso de perdida o robo deberán asumir el costo de los mismos.

5.1.1.2 Características Generales del servicio de Internet Dedicado

- Incluir la provisión y configuración de todos los equipos y accesorios necesarios para la implementación del servicio.
- Ancho de banda de 800 Mbps, sin overbooking y simétrico. (se refiere a que la velocidad de subida y bajada deber ser la misma).
- Los enlaces de interconexión que lleguen a la sede central de la ARCC deben ser en su totalidad de fibra óptica del tipo multimodo o monomodo. No se aceptarán equipos convertidores dado que esto representaría un punto adicional de falla
- Para el protocolo IPV4 debe incluir un mínimo de /28 en IP Públicas (donde la ip de red, gw y broadcast están considerados); tomando en cuenta que se aceptará la suma de diferentes segmentos para cumplir con esta cantidad.
- Para el protocolo IPV6 se debe incluir un mínimo de /64 en IP Publicas Públicas (donde la ip de red, gw y broadcast están considerados); tomando en cuenta que se aceptará la suma de diferentes segmentos para cumplir con esta cantidad.
- Se requiere una herramienta de control para monitorear la capacidad, uso y disponibilidad del enlace, basado en plataforma web. Debe guardar estadísticas históricas de tráfico. La herramienta debe también permitir ver el tráfico en detalle.

- Los equipos de comunicaciones que serán instalados para la prestación de los servicios requeridos, deberán ser propiedad del proveedor y deberán ser otorgados como parte del servicio bajo la modalidad de alquiler.
- El proveedor debe considerar en su propuesta todas las condiciones, normas y estándares que aseguren el correcto funcionamiento de los enlaces.
- El proveedor debe tener una red que participe en Internet como mínimo que cumpla con la normativa nacional dispuesta por el Ministerio de Transportes y Comunicaciones para las ISP presentar documento constancia que certifique lo solicitado para la presentación de la oferta.
- El SLA requerido para el servicio no debe ser menor a 99.5%.
- Los proveedores podrán realizar visitas a los campus previa coordinación con el área encargada de la ARCC.

CUADRO N° 1				
Nº	Nombre de Sede	Dirección	Ancho de Banda	Medio de Enlace
1	Oficina Principal	Jr. Santa Rosa 247, Cercado de Lima.	800 MB	Fibra Óptica / Primario

5.1.1.3 Características Generales de la Seguridad Gestionada

- Protección contra ataques de intrusión (IPS).
- Protección contra virus (AntiVirus).
- Control de Aplicaciones.
- Protección contra malware de Zero Day mediante técnicas de Sandboxing (Puede ser en el Datacenter del fabricante o en el Datacenter del ISP).
- Protección contra malware (AntiMalware).
- Protección contra spyware (AntiSpyware).
- Seguridad de protección web (WAF)
- Capacidad de filtrado de páginas web (URL Filtering).
- SSL VPN Client to Site. (Debe estar licenciado la creación de vpn con dispositivos IOS, Android).
- VPN IPSEC Site to Site.
- Inspección del tráfico tanto de entrada y salida.
- Soporte de feature Prevención de fuga de información (DLP).
- Generación de reportes.
- El proveedor deberá brindar un usuario administrador a dicha plataforma, este usuario no debe tener ningún tipo de restricción.

5.1.1.4 Características Generales de la Interconexión de Datos

- **La sede principal y central de la Autoridad Para la Reconstrucción con Cambios es la sede de Lima en Jr. Santa Rosa 247 cercado de Lima, sede en la cual se habilitará la cabecera única de salida a internet y una cabecera de datos MPLS donde ser interconectaran el resto de sedes, el ancho de banda considerado para la cabecera de internet y la cabecera de interconexión de datos debe cumplir con los estipulados en los cuadros 1 y 2 del presente documento.**
- MPLS de forma tal que la conexión debe de tener un enlace principal.
- Incluir la provisión y configuración de todos los equipos y accesorios

necesarios para la implementación del servicio.

- **El requerimiento de un primer traslado de 1 sede durante la vigencia del servicio no conllevara un gasto adicional y será de forma gratuita, en el caso de que la entidad requiera traslados adicionales, estos traslados conllevaran a costos y adendas adicionales.**
- Ancho de banda de 50 Mbps, sin overbooking y simétrico para cada sede desconcentrada de la ARCC.

- El enlace de interconexión que llegue a la Subdirección de la ARCC debe ser en su totalidad de fibra óptica del tipo multimodo o monomodo, no se aceptaran equipos convertidores dado que esto representaría un punto adicional de falla.
- **En la sede principal de Lima la que está ubicada en Jr. Santa rosa 247 cercado de lima se incluirá dos equipos de seguridad perimetral tipo firewall que trabaje a nivel de capa 7 modelo OSI (estarán en alta disponibilidad del tipo activo activo) para la protección de seguridad perimetral del servicio de internet, estos deberán cumplir con las características técnicas y físicas indicas en el presente documento. En las sedes remotas nacionales que se interconectarán mediante MPLS a la cabecera de datos de la sede principal en Lima Jr. Santa rosa 247 solo será necesario considerar equipos de capa 3 tipo routers, en todos estos equipos propuestos por el proveedor se deberá brindar las credenciales a nivel administrador al área técnica de la Autoridad Para la Reconstrucción con Cambios y el proveedor podrá solicitar a la entidad aceptar una carta de responsabilidades en caso se vea perjudicado el servicio por una mala configuración de responsabilidad de la entidad.**
- Se requiere una herramienta de control para monitorear la capacidad, uso y disponibilidad del enlace, basado en plataforma web. Debe guardar estadísticas históricas de tráfico. La herramienta debe también permitir ver el tráfico en detalle.
- Los equipos de comunicaciones que serán instalados para la prestación de los servicios requeridos, deberán ser propiedad del proveedor y no genera ningún gasto adicional para la entidad.
- El proveedor deberá considerar un traslado de cualquiera de las sedes, dentro del territorio nacional (con todo el detalle técnico) durante el tiempo de servicio sin costo adicional para la entidad.
- El proveedor debe instalar en todas las sedes indicadas en el cuadro N° 2, los equipos de comunicaciones (router), los mismos que deben ser nuevos, de primer uso y no encontrarse en condición de End of Sale (EoS) ni End of Life (EoL) durante el plazo del servicio. Presentar carta del fabricante.(también se podrá presentar una carta del distribuidor o reseller y/o fabricante y/o declaración jurada del postor indicando que los equipos del cuadro 2 no se encuentran en EoS no en EoL.)

CUADRO N° 2		
Nº	**DIRECCIÓN**	**ANCHO DE BANDA**
1	**Sede Lima - Camaná** Jr. Camaná 851 piso 5 Cercado de Lima	50 Mbps
2	**Sede Tumbes** Urb. Joé Lishner Tudela – I etapa Mz N, LT. 2	50 Mbps
3	**Sede Huaraz** Jr. Alejandro Tafur N°432 Urbanización Huarupampa Zona H	50 Mbps
4	**Sede Cajamarca** Jr. Tarapacá 652 (A dos cuadras de Plaza de Armas) Cajamarca	50 Mbps
5	**Sede Piura** Av. Los Cocos 381 Urb. Club Grau Ref. A espaldas de Transportes Línea	50 Mbps
6	**Sede Lambayeque** Calle Mangos N° 230 Urb. San Victoria Chiclayo, Lambayeque	50 Mbps
7	**Sede La Libertad** Av. Larco Nº 443 Trujillo, La Libertad	50 Mbps

8	**Sede Arequipa** Av. Cayma 520, Cayma, Arequipa	50 Mbps
9	**Sede Lima – Carabaya** EDIFICIO ITALIA: Jr. Santa Rosa N°191 – Cercado de Lima (piso 3)	50 Mbps

Direccion	Latitud	Longitud	Referencia
Sede Lima - Camaná: Jr. Camaná 851 piso 5 Cercado de Lima	**-12.050958**	**-77.036186**	Jr. Camaná 851 piso 5 Cercado de Lima
Tumbes: Urb. José Lishner Tudela – I etapa Mz N, LT. 2	**-3.561669**	**-80.426082**	
Huaraz: Jr. Alejandro Tafur N°432 Urbanización Huarupampa Zona H.	**-9.5295965**	**-77.5347002**	
Cajamarca: Jr. Tarapaca 652	**-7.15633227**	**-78.52028918**	Dirección Regional de Transporte y Comunicaciones de Cajamarca
Piura: Av. Los Cocos 381 Urb. Club Grau Ref. A espaldas de Transportes Línea	**-5.191604**	**-80.632404**	
Lambayeque: Calle Mangos N° 230 Urb. San Victoria Chiclayo, Lambayeque	**-6.7830156**	**-79.8426079**	
La Libertad: Av. Larco Nº 443 Trujillo, La Libertad	**-8.1180152**	**-79.0355983**	La casa de identidad liberteña
Arequipa: Av. Cayma 520, Cayma, Arequipa	**-16.3868057**	**-71.549088**	
Sede Lima – Carabaya: EDIFICIO ITALIA: Jr. Santa Rosa N°191 – Cercado de Lima (piso 3)	**-12.0487265**	**-77.032039**	Edificio de migraciones

Los elementos y/o accesorios de los que será responsable el proveedor serán todos los relacionados a la operación del servicio solicitado. Los siguientes equipos/accesorios no son parte del servicio solicitado y lo brindará la entidad (para el caso de la sede principal.

- Tomacorrientes
- Energía Estabilizada
- Patch Panel
- Patch Cord
- Switch Lan (donde se conectará el router)
- Tendido de cableado eléctrico
- UPS
- Pozos tierra
- Gabinete o Rack
- Cableado

5.1.1.5 Características mínimas especificas del servicio de internet

ITEM	CARACTERÍSTICAS MÍNIMAS
Ancho de banda	800 Mbps
Simetría	Simétrico
Overbooking	Sin Overbooking
Direcciones IP publicas IPV4	/28
Direcciones IP publicas IPV6	/64
Herramienta de control y monitoreo	Si

ITEM	CARACTERÍSTICAS MÍNIMAS
Normativa Nacional	Que cumpla con lo dispuesto por el MTC para ISP.
Red de acceso – última milla	Fibra óptica del tipo Fibra Multimodo o Monomodo
Proveedor cuenta con NOC propio	Si
Proveedor cuenta con SOC propio	Si

5.1.1.6 Características mínimas especificas del servicio de seguridad gestionada sede central

ITEM	CARACTERÍSTICAS MÍNIMAS
Arquitectura	• Se requiere por lo menos 16 puertos de red Ethernet 100/1000 Mbps. • Se requiere por lo menos 16 puertos de red 1G SFP. • Se requiere por lo menos 2 puertos de red 10G SFP+. • 02 Fuentes de poder AC o DC. Se requiere que el contratista realice una visita a la data center para que valide el tipo de conector de energía a utilizar. Las fuentes deben ser cambiables en caliente. • Alta disponibilidad (02 equipos del mismo modelo) • La solución deberá contar con 32 SFP+ con soporte de 1 a 10GB
Performance	• El Throughput de NGFW (Firewall con control de aplicaciones más IPS activos) debe ser de 4 Gbps como mínimo. Se tomará en consideración mediciones de throughput tomadas con 100% de tráfico http, Enterprise mix o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 25544, 2647 o 1242. En caso, el fabricante tenga publicados múltiples números de desempeño, solamente se aceptará el valor más pequeño. • El Throughput de firewall puro debe ser de como mínimo 52 Gbps, se tomará en consideración la ficha técnica oficial certificada por la marca propuesta. • El throughput de prevención de amenazas (Firewall, control de aplicaciones, IPS y antimalware) debe ser de 4.2 Gbps como mínimo y debe estar medido en condiciones reales o con tráfico mixto. • El throughput de IPS debe ser de 4.2 Gbps como mínimo y debe estar medido en condiciones reales o con tráfico mixto. • En caso de que el fabricante tenga publicados múltiples números de desempeño (Throughput) para cualquiera de las funcionalidades, solamente se aceptara el de valor más pequeño. • El Throughput de VPN IPSec debe ser de 25 Gbps como mínimo. • Debe soportar como mínimo 11’000,000 (once millones) de conexiones o sesiones concurrentes como mínimo. • Debe soportar como mínimo 280,000 (doscientos ochenta mil) nuevas conexiones por segundo. • La solución deberá soportar al menos 1500 usuarios. En caso requerir licencias estas deberán estar incluidas para toda la solución propuesta.

	• Capacidad de Almacenamiento integrado en el equipo 1 disco de 256 GB SSD.
Capacidades	• Debe tener la capacidad de habilitar como mínimo 2 instancias virtuales sobre el mismo dispositivo, de ser el caso deberá contar con el licenciamiento aplicado y disponible por el tiempo de contrato de la solución. • La solución deberá enviar alertas para eventos críticos relacionados con hardware o software.
Filtro URL	• El filtrado de URL debe ser basado en categorías y debe permitir crear grupos personalizados • Debe cubrir más de 80 millones de sitios web en al menos 30 categorías. • Debe incluir un mecanismo permitan al administrador, negar o permitir URLs específicos, que no necesariamente están definidos en una categoría, para poder ser utilizados en la definición de nuevas reglas • Debe permitir la creación de excepciones basadas en la definición de objetos de red. • Debe proveer la opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página. • El Filtrado de URL debe poder integrarse a un mecanismo, o bloque de seguridad, que permita controlar aplicaciones web 2.0. Dicha integración debe ser dentro del mismo dispositivo sin el uso de herramientas de terceros o servidores separados. • El dispositivo debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0 • El dispositivo debe tener la capacidad de identificar y bloquear herramientas de “proxy bypass” sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales) • Debe bloquear Malware sobre sitios Web y Web 2.0 • Debe incluir un método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes • Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL. La solución debe hacer dicha inspección sin la necesidad de utilizar herramientas de terceros, servidores o licencias adicionales • Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando cual URLs a través de la integración con servicios de directorio activo, autenticación vía LDAP, Active Directory y base de datos local. • Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora). • Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad. • Debe permitir publicar los logs de URL con la información de los usuarios con servicios de directorio.
	• Debe incluir soporte a las topologías VPNs site-to-site • Soporte a VPNs client-to-site basadas en IPSEC. • VPNs IPSec debe soportar:DES, 3DES. ;

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

VPN	• Autenticación MD5 y SHA-1.;
	• Diffie-Hellman Group 1 , Group 2, Group 5 y Group 14;
	• Algoritmo Internet Key Exchange (IKE);
	• AES 128, 192 y 256 (Advanced Encryption Standard)
	• Autenticación vía certificado IKE PKI.
	• Las VPN SSL deben soportar:
	  ○ Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB
	  ○ Las funcionalidades de VPN SSL deben ser atendidas con el uso de agente, opcionalmente sin el uso de agente
	  ○ La asignación de dirección IP en los clientes remotos de VPN
	  ○ La asignación de DNS en los clientes remotos de VPN
	• Debe tener la posibilidad de realizar VPNs clientes SSL para acceso remoto, sin necesidad de instalar un cliente.
	• Soporte a VPNs tipo L2TP.
	• La VPN SSL deberá soportar asignación de aplicaciones permitidas por grupo de usuarios
	• Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante.
	• El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.
	• Soporte de conexiones VPN del tipo Client to Site con dispositivos Celulares/móviles.
	• Deberá de permitir la comunicación de la VPN a través de SSL y IPSec.
	• Deberá soportar el acceso VPN SSL mínimo de 50 usuarios concurrentes.
	• Debe poder establecer VPNs IPSec con gateways que tengan direcciones IP dinámicas públicas.

Prevención de Amenazas	• Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS y Antimalware. • Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware o Antimalware). • Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.). • Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP. • Debe contar con funcionalidad de Análisis de archivos sospechosos o detección de malware desconocido en la nube (emulación de sandboxing). • Debe incluir protecciones para el protocolo POP3 e IMAP. • Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP. • Capacidad de actualización automática o manual de firmas. • El IPS debe proveer al menos dos políticas o perfiles predefinidos, para ser usados inmediatamente.

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

	• El administrador debe poder activar automáticamente nuevas firmas, basados en parámetros de configuración definidos previamente (impacto en el desempeño, severidad de la amenaza, tipo de protección: server o client).
	• Deberá poseer habilitado la seguridad de aplicaciones web (WAF), el cual deberá proteger a los servidores web internos de las actividades maliciosas especifica en estos tipos de servidores esto incluye:
	  ○ Cross Site Scripting
	  ○ SQL injection
	  ○ Generic Attacks
	  ○ Trojans
	  ○ Known Exploits
	  ○ Credit Card Detection
	• Deberá poseer los siguientes mecanismos de inspección de IPS:
	  ○ Análisis de patrones de estado de conexiones.
	  ○ Análisis de decodificación de protocolo.
	  ○ Análisis para detección de anomalías de protocolo.
	  ○ Análisis heurístico.
	  ○ IP Desfragmentación.
	  ○ Re ensamblado de paquetes de TCP.

Administración	• La solución debe administrarse desde una única consola gráfica, se prefiere que sea basada en Web en equipos Windows o Linux con navegadores Microsoft Internet Explorer (Windows), Chorme, Mozilla Firefox (Windows/Linux). • La solución deberá soportar acceso via SSH, cliente WEB (HTTPS) o interfaz GUI. • En caso de que sea necesario la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operativos windows. • La solución deberá poder realizar respaldos y restauraciones de las configuraciones.
Autentificación de Usuarios	• La solución deberá poder integrarse con Active Directory de Microsoft, se prefiere que no sea necesario instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectúe por medio de cuentas de usuarios y grupos de administración basadas en el Active Directory. • Administración Basada en Roles: Es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad del de Sistemas y de otras unidades definidas en el Active Directory. La solución deberá permitir la segregación de funciones de forma granular, permitiendo así definir al alcance o posibilidades de gestión para cada administrador. • La solución tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.
Reportes	• Se debe proveer la capacidad de contar con acceso a un sistema de reportes en línea en donde se almacenes los registros de todos los equipos de seguridad provistos para el servicio de internet con una antigüedad de logs de por lo

	menos 2 meses, estos reportes deben ser granulares y generados a demanda del cliente final, además debe contar con indicadores de compromiso y capacidad de generar reportes personalizados por usuarios y por ip. • El sistema de reportes debe contar con una capacidad de 4 TB de almacenamiento como mínimo. • La solución deberá permitir generar reportes en tiempo real. • La solución deberá permitir generar reportes históricos. • La solución deberá permitir generar reportes de actividad de los usuarios, aplicaciones, servicios, equipos. • La solución deberá permitir generar reportes de actividad del malware, virus, spyware detectado. • La solución deberá tener la capacidad de enviar reportes programados por correo electrónico. • La solución deberá permitir exportar los reportes generados en los siguientes formatos al menos: PDF, HTML, XML y CSV.
Credenciales	• Deberá proporcionar las credenciales de nivel administrador a personal de la Oficina de Tecnologías de la Información.

5.1.1.7 Características mínimas específicas del servicio de interconexión de datos

ITEM	CARACTERÍSTICAS MÍNIMAS
Ancho de banda	50 Mbps
Simetría	Simétrico
Overbooking	Sin Overbooking
Herramienta de control y monitoreo	Si
Normativa Nacional	Que cumpla con lo dispuesto por el MTC para ISP.
Red de acceso – última milla	Fibra óptica del tipo Fibra Multimodo o Monomodo
Proveedor cuenta con NOC propio	Si
Proveedor cuenta con SOC propio	Si

5.1.2 Procedimiento

Para la realización de los trabajos, el proveedor deberá tener en cuenta el siguiente procedimiento:

- Tendrá mesas de trabajo técnica de manera conjunta con la Oficina de Tecnologías de la Información antes de la implementación. Debido a la coyuntura que está viviendo nuestro país las coordinaciones de mesas de trabajo técnica y cualquier reunión se podrá realizar remotamente o de manera virtual pudiendo usar cualquier plataforma de comunicación (teams, zoom, u otro) para evitar exponer al personal de ambas partes.
- Enviará por mesa de partes virtual de la Entidad (mesadepartesvirtual@rcc.gob.pe) la lista de actividades, protocolo de pruebas y personal involucrado en la implementación y gestión. Personal de campo deberá contar con todos los seguros e implementos de seguridad

para la realización del trabajo. La lista más el seguro debe de ser enviada con 24 horas a lo mucho al contacto/responsable de la OTI.
- Para los trabajos, se contará con personal de la OTI quien supervisará los trabajos.
- Ejecutará los protocolos de pruebas para el servicio. El monitoreo posterior a la implementación se podrá realizar de manera remota.
- El proveedor deberá resanar cualquier alteración en la infraestructura de la sede donde se realizan los trabajos y deberá mantener la estética del lugar utilizando pintura, drywall, etc. necesarios. La ARC solo garantiza todas las facilidades técnicas cuando se trata de sus instalaciones mas no al edificio donde reside o de otras areas.
- Monitoreo presencial en los días posteriores a la implementación.
- Firma del acta de servicio por parte de la OTI una vez estén estable los servicios.
- El proveedor ganador de la buena pro deberá realizar el protocolo de verificación, certificación necesaria para comprobar el estado de la infraestructura de la ARCC antes del acondicionamiento y de la instalación de los equipos de comunicación que son parte del servicio.
- La omisión en la oferta de algún producto que al momento de las pruebas resulte necesario para la provisión de los servicios, o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al contratista a proveerlo sin cargo alguno. Este alcance cubre a los equipos provistos por el contratista como parte del servicio.

5.1.3 Plan de Trabajo

El proveedor deberá presentar en el plazo de 05 días hábiles posteriores a la suscripción del contrato, un Plan de Trabajo que contenga la siguiente información:

- Metas y objetivos por alcanzar.
- Recursos necesarios.
- Línea de acciones para alcanzar las metas y objetivos (actividades).
- Protocolo de pruebas.
- BoM del equipamiento.
- Layout del equipamiento en visio.
- Topología.
- Plan de bajo nivel.
- Responsable por actividad.
- Cronograma de actividades.
- Riesgos advertidos.

5.1.4 **Requisitos según leyes, reglamentos técnicos, normas metrológicas y/o sanitarias, reglamentos y demás normas** (de corresponder).

No corresponde

5.1.5 **Impacto Ambiental** (de corresponder).

No corresponde

5.1.6 **Seguros** (de corresponder).

No corresponde

5.1.7 Mantenimiento Preventivo

- El proveedor deberá considerar mantenimiento (lógico y físico) preventivos y correctivos durante la ejecución del contrato, la frecuencia será de dos (02) veces en el año.
- 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.
- El cronograma del Plan de Mantenimiento Preventivo de los equipos implementados deberá ser entregado a la suscripción del Contrato.
- La medición de trafico podrá utilizarse aplicativos o equipos o comandos para validar la latencia y ancho de banda solicitado (en caso de internet).

Asimismo, el mantenimiento preventivo consta de:

a) Informar de nuestra presencia al contacto de la sede.
b) Reportar al centro de gestión inicio de mantenimiento y/o encargado residente.
c) Identificar equipo Router y Modem a trabajar con rotulación de CD.
d) Verificar/Identificar conexión de sus interfaces y rotularlos.
e) Tomar fotografías del Equipo para ver estatus antes del mantenimiento.
f) Conectarse al puerto de consola del equipo mediante los emuladores, para la toma de Backups / Configuración del equipo y aplicar comando tipo Show.
g) Apagar el equipo (router y modem) para realizar mantenimiento.
h) Limpieza de hardware.
i) Realizar captura de imágenes durante el mantenimiento.
j) Armar equipo y montarlo al rack de comunicaciones o lugar donde se retiró.
k) Verificar estado de las interfaces y consultar al centro de gestión al acceso remoto.
l) Llenar boleta de atención para ser firmado por el contacto del local.

5.1.8 Soporte Técnico

Entre otras, se podrán considerar como garantía comercial del servicio, las siguientes:

5.1.8.1 Soporte técnico del Internet Dedicado e Interconexión de Datos

El proveedor deberá contar con un Centro de Operación de Red: NOC – Network Operation Center (según 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), que como mínimo cumpla con lo siguiente:

- Soporte para averías, modalidad presencial y en línea (por diferentes medios), del tipo 24x7x365. La atención en línea debe ser inmediata.
- La cantidad de atenciones de las averías deberán ser ilimitadas sujeta al tiempo de la garantía de los equipos.
- El tiempo de resolución de averías del router/internet se encuentra tipificado de la siguiente manera como mínimo:

- Tiempo de respuesta: (30 minutos) desde que el cliente llama, se realiza los primeros descartes y hasta que se genera el ticket de atención.

El tiempo de atención de cualquier tipo de avería será computado a partir de la generación de un tiket de atención o luego de enviado un correo electrónico solicitando la atención, luego de producido el incidente, para de este modo facilitar el seguimiento de la falla reportada.
- Nivel 1 (Grave): La funcionalidad anexa no se encuentra operando en su totalidad.
- Nivel 2 (Severa): El equipo opera con inconvenientes afectando a más de un 20% de los puestos de trabajo o al servicio de operadora.
- Nivel 3 (Leve): El equipo opera parcialmente afectando a menos de un 20% de los puestos de trabajo.
- Nivel 4 (Normal - Cambio de configuración): El equipo opera con normalidad. El evento: afecta el puesto de trabajo de un usuario, no se encuentra contemplado en los niveles 1-2-3 o es considerado cambio de configuración.

Nivel	Tipificación	Tiempo de Resolución
1	Grave	4 Horas
2	Severa	5 Horas
3	Leve	6 Horas
4	Normal	7 Horas

- En caso de falla de hardware, se debe disponer de un equipo de reemplazo en un tiempo máximo de 4 horas. El proveedor deberá realizar el diagnóstico correspondiente para determinar la falla de hardware, siendo válidas soluciones de separe (reemplazo) con equipos similares de forma temporal, hasta tener el equipo definitivo gestionado a través del contrato con el fabricante.
- Se contará con una atención preferencial por parte de los ejecutivos asignados dentro del horario de oficina, el cual será comunicado al Proyecto Especial.
- Se aceptarán como hechos fortuitos ajenos al proveedor y que podrían afectar el servicio, aquellos ocasionados por atentados o desastres naturales. Estos hechos no afectarán el nivel de servicio requerido.
- Toda actividad o provisión de bienes que tenga que ejecutar el proveedor para subsanar la avería que obedezca a causa imputable al contratista será sin costo alguno para la ARCC. En caso la avería sea imputable a la entidad, se confirma que el cliente asumirá el costo de reparación.

5.1.8.2 Soporte técnico de la Seguridad Gestionada

El proveedor deberá contar con un Centro de Operación de Seguridad: SOC – Security Operation Center, que como mínimo cumpla con lo siguiente:

- Soporte para averías, configuraciones en modalidad presencial y en línea (por diferentes medios), del tipo 24x7x365. La atención en línea debe ser inmediata.
- La cantidad de atenciones de las averías deberán ser ilimitadas sujeta al tiempo de la garantía de los equipos.
- El tiempo de resolución de averías y de ejecución de configuraciones se encuentra tipificado de la siguiente manera como mínimo:

Averías del Equipos

- Tiempo de respuesta: (30 minutos) desde que el cliente llama, se realiza los primeros descartes en línea y se compruebe el fallo de los equipos.
- Nivel 1 (Grave): La funcionalidad anexa no se encuentra operando en su totalidad.
- Nivel 2 (Severa): El equipo opera con inconvenientes afectando a más de un 20% de los puestos de trabajo o al servicio de operadora.
- Nivel 3 (Leve): El equipo opera parcialmente afectando a menos de un 20% de los puestos de trabajo.

En todos los casos al comprobarse la falla del equipo, este debe ser reemplazado por otro equipo de las mismas características de acuerdo al tiempo de resolución indicado en el siguiente cuadro.

SLA Equipo Firewall

Nivel	Tipificación	Tiempo de Resolución
1	Grave	4 Horas
2	Severa	5 Horas
3	Leve	6 Horas

Ejecución de Configuraciones

- Tiempo de respuesta: (30 minutos) desde que el cliente llama, se realiza los primeros descartes y hasta que se genera el ticket de atención.

- Nivel 1 (Grave): La configuración de 4 o menos reglas o filtros, habilitación de URL y aplicaciones, sincronización con el AD.
- Nivel 2 (Severa): La configuración de VPNs y servicios complementarios.
- Nivel 3 (Leve): La configuración de reglas con más de 4 filtros y con más de 5 reglas concurrentes.
- Nivel 4 (Normal - Cambio de configuración): Configuraciones complejas que requieren cambio de topología.

SLA Servicios de Configuración Firewall

Nivel	Tipificación	Tiempo de Resolución
1	Grave	1 Hora
2	Severa	2 Horas
3	Leve	4 Horas
4	Normal	7 Horas

- Se contará con una atención preferencial por parte de los ejecutivos asignados dentro del horario de oficina.
- La cantidad de atenciones de configuración de firewall deberá ser ilimitada, sujeta al periodo que dure el servicio.
- El proveedor deberá considerar proactivamente la actualización del firmware del equipo sin incurrir en gastos adicionales ni consumo de horas de la bolsa. Esta actividad debe ser parte del servicio.

5.1.9 Capacitación y/o entrenamiento

El contratista deberá ofrecer un curso integral considerado Técnico para al menos cuatro (4) personas de la Oficina de Tecnologías de la Información de la ARCC, en cursos relacionados a la Gestión de seguridad para Redes corporativas o afines por 24 horas, este curso deberá ser realizada por el proveedor. Este curso deberá ser oficial y con certificado emitido por la marca.

El curso se brindará dentro de los 30 días calendarios posterior a la implementación asimismo no representará algún costo a la entidad.

La transferencia de conocimiento deberá realizarse en las instalaciones de la Oficina de Tecnologías de la Información y podrá ser virtual.

El expositor deberá tener conocimientos sólidos sobre la solución a implementar, la cual deberá acreditar mediante constancia al menos un (01) año de experiencia en implementación y capacitación de proyectos similares, y deberá presentarse para la etapa de suscripción del contrato.

La capacitación o entrenamiento se podrá realizar remotamente o de manera virtual pudiendo usar cualquier plataforma de comunicación(teams, zoom, u otro), para evitar exponer al personal de ambas partes.

5.1.10 Resultados Esperados

No aplica

5.2. REQUISITOS DEL PROVEEDOR

- El proveedor deberá ser partner certificado para trabajar con la solución ofertada o estar habilitado en la venta de productos del fabricante de la solución a ofrecer la cual deberá informar mediante constancia o una declaración jurada la cual deberá estar firmada por un representante de la marca ofertada, presentarlo en los documentos para la admisión de la oferta.
- **El proveedor debe ser miembro activo del NAP Perú o podrá tener un punto de intercambio a través de un miembro activo del NAP, se acreditará mediante reporte de la página web del NAP o certificado o declaración jurada, en los documentos para la admisión de la oferta.**
- El proveedor deberá contar con una red principal o Backbone propia y redundante, que tenga como medio de transporte fibra óptica, se acreditará con una Declaración Jurada.
- El proveedor deberá contar con una red de acceso propia y redundante, que tenga como medio de transporte fibra óptica, se acreditará con una Declaración Jurada.
- Debe contar con un NOC (Network Operations Center) propio, presentar documento que sustente la propiedad.
- Debe contar con un SOC (Security Operations Center) propio, presentar documento que sustente la propiedad.

5.2.1 ANÁLISIS DE VULNERABILIDADES

El POSTOR deberá considerar dentro de su propuesta realizar un servicio de Análisis de vulnerabilidades al pool de direcciones ips públicas ipv6 e ipv4 que nos asignará como parte del servicio. Este análisis deberá iniciar al día siguiente después de concluida la **implementación del servicio de internet.**

- Será realizado bajo la modalidad de Caja Negra.
- El análisis será realizado por un periodo de diez (10) días calendarios como máximo.
- El análisis debe considerar la búsqueda de información confidencial de diseño y exposición externa, vulnerabilidades, posibles amenazas y adicionalmente en caso de encontrar aplicativos webs publicados en dichas direcciones ip publicas analizadas se deberá reportar errores de código o diseño, así como identificar la versión y el tipo del servidor web donde esta alojada la aplicación, para explorar las distintas vulnerabilidades y exploits a los que se encuentra expuesto. Se debe detectar la fuga de información en metadatos de archivos y/o página web. Análisis de fuga de información sobre el código de programación público del servicio web. Debe identificar el tipo de framework de la aplicación a través de su fingerprint para la revisión de vulnerabilidades conocidas. Detección de archivos de configuración que puedan exponer el código del lado del servidor. Se deben evaluar los distintos métodos HTTP de la aplicación web. El análisis debe contemplar las pruebas de credenciales por defecto sobre la aplicación web a través de distintos diccionarios.
- Debe considerar ataques de fuerza bruta a los servicios encontrados en el análisis del rango de direcciones ips publicas ipv4 e ipv6 asignados.
- El servicio debe ser realizado por un Tecnico o Bachiller en Telecomunicaciones y/o Redes y Comunicaciones de Datos con certificación en CyberSecurity Foundation y certificacion eJPT (Penetration Testing).

El postor deberá brindar los siguiente entregables al finalizar el análisis:

- **Informe de Diagnóstico**: donde se presentará el detalle de vulnerabilidades y los hallazgos.
- **Informe ejecutivo:** Donde se informará de manera general el diagnóstico del análisis realizado, lista de vulnerabilidades y una semaforización para indicar su nivel de criticidad.

El plazo máximo para que el postor envié y presente estos documentos es de (diez)10 días después de iniciado el análisis, estos documentos deberán ser remitidos en formato digital mediante un correo dirigido a mesadepartevirtual@rcc.gob.pe.

5.3. EQUIPOS, MATERIALES E INSUMOS

No Aplica

6. PERSONAL CLAVE

El personal del proveedor deberá contar con el siguiente perfil profesional:

Jefe de Proyecto (01 persona):

- Técnico y/o bachiller y/o ingeniero Electrónico, Sistemas y/o de Telecomunicaciones y/o Redes y Comunicaciones y/o Sistemas y/o Informatica, Sistemas y/o informática, Sistemas y Computo.
- Certificación en Project Management Professional vigente.
- Experiencia en al menos tres (03) proyectos de sistemas de Internet y datos o experiencia en proyectos de Sistemas de Seguridad Gestionada en los últimos (03) años. Se aceptará experiencia laboral sea de (02) años en implementación y/o gestión y/o configuración en equipos de seguridad perimetral.

Especialista (01 persona):

- Técnico y/o bachiller y/o ingeniero Electrónica, Sistemas y/o de Telecomunicaciones y/o Redes y comunicaciones y/o Sistemas y/o informática, Sistemas y Computo.
- Experiencia laboral en al menos tres (03) proyectos en implementación de sistemas de internet con seguridad Gestionada en los últimos tres (03) años. Deberá sustentarse con constancias laborales. Se aceptará experiencia laboral sea de dos (02) años en implementación y/o gestion y/o configuración en equipos de seguridad perimetral.
- Certificación vigente de nivel asociado en la especialidad de seguridad de redes. (certificación técnica del firewall solicitado) Deberá sustentar., la certificación deberá ser considerada una certificación oficial técnica en el ámbito de ciberseguridad y no comercial.

Capacitador (01 persona):

- El expositor deberá tener conocimientos sólidos sobre la solución a implementar, la cual deberá acreditar mediante constancia al menos un (01) año de experiencia en implementación y capacitación de proyectos similares, y deberá presentarse para la etapa de suscripción del contrato

  La experiencia del personal 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.

  El capacitador podrá ser personal que implementó el equipo de seguridad perimetral y/o personal que cuente con la certificación oficial de la marca.

7. OBLIGACIONES DEL PROVEEDOR

- Realizar la implementación del servicio.
- Realizar y entregar el informe.
- Cumplir con los alcances del servicio.

8. OBLIGACIONES DE LA ENTIDAD

- Supervisar, verificar y validar el servicio brindado por el postor.
- Revisar el informe y entregables del servicio.
- Realizar el pago correspondiente de acuerdo al TDR.

9. PLAZO DE EJECUCIÓN

Plazo máximo de implementación del servicio de internet será de 45 días calendario.

Plazo de Ejecución es de doscientos sesenta (260) días calendario o hasta que termine el plazo de vigencia de la Institución contado, a partir de suscrito el acta de implementación del servicio.

10. LUGAR DE EJECUCIÓN DEL SERVICIO

Lugar: Cercado de Lima - Lima

- Jirón Santa Rosa 247 Piso 7, Cercado de Lima

11. PENALIDADES.

12.1. Penalidad por mora:

En caso de retaso injustificado en la ejecución de la prestación del servicio por parte del proveedor, la entidad aplicará de forma automática una penalidad por cada día de atraso.

$$\textbf{Penalidad Diaria} = \frac{0.10 \times MONTO}{F \times PLAZO\ EN\ DIAS}$$

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

Donde F tiene los siguientes valores:
F=0.4 para plazos menores o iguales a 60 días
F= 0.25 para plazos mayores a 60 días.
Monto= Monto de la Orden de Compra o Servicios
Plazo en días = Plazo de cumplimiento de la ejecución contractual.
La penalidad máxima aplicable será de hasta el 10% del monto contratado.

12.2. Otras penalidades:

Nº	INCUMPLIMIENTO		PENALIDAD (% UIT)
1	**POR LA INTERRUPCIÓN DEL SERVICIO**		
	Interrupciones en el servicio, no mayores a una (01) hora, no programada imputables al postor (corte parcial, total o decremento en la calidad de las comunicaciones).	Entre dos (02) y cuatro (04) horas interrupciones del servicio al mes	1% UIT
		Más de cuatro (04) horas interrupciones del servicio al mes	2% UIT
2	**POR DEMORA EN LA ATENCIÓN DE AVERIAS/CONFIGURACIONES**		
	Tiempo de respuesta para la atención de averías/configuraciones. (Tiempode atención y plazo para brindar una respuesta para cualquier llamada del Proyecto Especial en la que reporte una avería).	Hasta una (01) hora de retraso	1% UIT
		Hasta dos (02) horas de retraso	2% UIT
		Por más de dos (02) horas de retraso	3% UIT
3	**DEMORA POR REPARACIONES DE AVERÍAS**		
	Tiempo de resolución de averías (Tiempo en que se dará solución al a avería reportada)	Hasta una (01) hora de retraso	1% UIT
		Hasta dos (02) horas de retraso	2% UIT
		Por más de dos (02) horas de retraso	3% UIT
4	**POR REALIZAR TRABAJOS SIN CONTAR CON SEGURO COMPLEMENTARIO DE TRABAJO DE RIESGO VIGENTE**		
	Penalidad aplicada por realizar trabajos sin contar con seguro complementario de trabajo de riesgo de todo su personal.	De 01 a 02 días	30% UIT
		De 03 a 04 días	40% UIT
		Mayor a 05 días	50% UIT

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

13. ENTREGABLE

Luego de implementado la solución, el proveedor tendrá diez (10) días calendario para la presentación del informe final de la implementación del servicio en digital vía correo electrónico, se espera el siguiente contenido como mínimo:

- El BoM de los equipos implementados.
- El inicio y fin del soporte de los equipos (vigencia).
- Pantallazos de la configuración realizada y líneas de comandos de la configuración del equipo de seguridad perimetral y el diagrama de la implementación.
- Saturación del enlace para la conformidad del ancho de banda contratado.
- Pantallazos de las pruebas realizadas con la integración de la red LAN.
- Anexar los protocolos de prueba.
- Topología de red a detalle de lo implementado con detalle de los nodos a donde conectan los servicios.
- Informe de Diagnóstico del análisis de vulnerabilidades realizado como parte del servicio.
- Informe ejecutivo del análisis de vulnerabilidades realizado como parte del servicio.

Así mismo, el proveedor deberá presentar un informe mensual sobre la utilización de la solución (estadísticas de consumo, tickets generados, el consumo de ancho de banda de los enlaces tanto de internet y como el de la red privada lan to lan), la misma que servirá como base de la conformidad mensual de pago; esta documentación deberá presentarlo de manera digital al responsable de la Oficina de Tecnologías de la Información y de manera impresa a Mesa de Partes de la institución.

La entrega del informe mensual deberá ser mensualmente en un plazo máximo de diez (10) días de siguiente mes de prestado el servicio.

14. FORMA DE PAGO

El pago se realizará en soles mediante transferencia electrónica a través del abono directo de los montos correspondientes en la cuenta bancaria abierta en cualquier entidad del Sistema Financiero Nacional, para lo cual comunicará su Código de Cuenta Interbancaria mediante Autorización, en la oportunidad que se da inicio a la relación contractual".

Se realizará el pago mensualmente, contra la conformidad del informe presentado en un plazo máximo de 10 días después de cada mes de servicio prestando.

- Autoridad para la Reconstrucción con Cambios (Jirón Santa Rosa 247, Cercado de Lima).

La Entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguiente a la conformidad del servicio, siempre que se verifiquen las condiciones establecidas en el contrato para ello.
El pago se realizará mediante transferencia electrónica a través del abono directo de los montos correspondientes en la cuenta bancaria abierta en cualquier entidad del Sistema Financiero Nacional, para lo cual comunicará su Código de Cuenta

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

Interbancaria mediante Autorización, en la oportunidad que se da inicio a la relación contractual.

15. CONFORMIDAD DEL BIEN Y/O SERVICIO, PRESENTACIÓN DE INFORME SEGÚN CORRESPONDA

La conformidad del servicio será otorgada por la Oficina de Tecnologías de la Información de la Autoridad de Reconstrucción Con Cambios, en calidad de área usuaria.

16. RESPONSABLES DE LAS COORDINACIONES REFERIDAS A LA CONTRATACIÓN (De corresponder).

Autoridad para la Reconstrucción con Cambios

17. PROPIEDAD INTELECTUAL

No aplica

18. ADELANTOS

No aplica

19. CONFIDENCIALIDAD

El proveedor y el personal a su cargo en el proyecto, no deberán revelar en ningún momento a cualquier persona o entidad alguna información confidencial adquirida en el curso de la ejecución del contrato.

La obligación de confidencialidad no resulta aplicable en los siguientes supuestos:

a) Cuando la información en cuestión haya sido de difusión o acceso publico.
b) Cuando la información en cuestión haya sido publicada antes de haber sido puesta a disposición del postor.
c) Cuando la información en cuestión ya obre en poder del postor y no este sujeta a cualquier otro impedimento o restricción que le haya sido puesto en manifiesto.
d) Cuando la información en cuestión haya sido recibida a raves de terceros sin restricciones y sin que implique incumplimiento de contrato.
e) Cuando la información en cuestión haya sido independientemente desarrollada por el postor, siempre que no se hubiese utilizado para ello otra información confidencial o cuando la información en cuestión deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden.

20. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 146 de su Reglamento.

El plazo máximo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de la presente adquisición es de UN (01) año, contados a partir de la conformidad otorgada por la entidad.

21. ANTICORRUPCIÓN

PROVEEDOR declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato u orden de servicio.

Asimismo, EL PROVEEDOR se obliga a conducirse en todo momento, durante la ejecución del contrato/orden de servicio, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL PROVEEDOR se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas."

Para el logro del objeto de prevención del soborno, queda terminantemente prohibido la oferta, suministro y/o aceptación de regalos y/u hospitalidad, que se consideran o razonablemente puedan percibirse como soborno, conforme a lo estipulado en los lineamientos establecidos en la "Política Antisoborno y Función deCumplimiento" al interior de la Autoridad para la Reconstrucción con Cambios" en concordancia a los Decretos Supremos N° 092-2017-PCM y N° 044-2018-PCM queaprueba el "Plan Nacional de Integridad y Lucha contra la Corrupción.

Así mismo; la Autoridad para la Reconstrucción con Cambios pone a disposición su Política Antisoborno a todas sus partes interesadas en el siguiente link: http://www.rcc.gob.pe/wp-content/uploads/2019/10/Resolución-Direccion-Ejecutiva-108.pdf, como parte de su compromiso frente a la prevención y lucha contra soborno.

22. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos: El postor deberá ser una empresa autorizada por el Ministerio de Transporte y Comunicaciones, para brindar el servicio de internet. **Importante** *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.* Acreditación: Copia de la resolución con la autorización del Ministerio de Transporte y Comunicaciones. (Autorización del Ministerio de Transporte y Comunicaciones para brindar servicios d valor añadido que incluye servicio internet). **Importante**

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

	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.

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: El personal clave para la ejecución del servicio es el siguiente: **Jefe de Proyecto (01 persona):** • Técnico y/o bachiller y/o ingeniero Electrónico, Sistemas y/o de telecomunicaciones y/o redes y/o comunicaciones y/o informática, sistemas y computo. Nota: La habilitación deberá ser acreditada al inicio de la prestación. **Especialista (01 persona):** • Técnico y/o bachiller y/o ingeniero Electrónico, Sistemas y/o de telecomunicaciones y/o redes y/o comunicaciones y/o informática, sistemas y computo. Nota: La habilitación deberá ser acreditada al inicio de la prestación. Acreditación: Los títulos profesionales citados serán verificados por el comité de selección 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. Importante para la Entidad *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.* En caso el título profesional 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.
B.3.2	**CAPACITACIÓN**
	Requisitos: La capacitación del personal clave de la prestación es la siguiente: **Jefe de Proyecto (01 persona):** • Certificación en Project Management Professional vigente. La Certificación debe ser emitida por PMI. **Especialista (01 persona):** • Certificación vigente de nivel asociado en la especialidad de seguridad de redes con Certificación del firewall solicitado, la certificación debe ser oficial de la marca y en ámbito técnico, no se aceptarán certificaciones consideradas comerciales. Acreditación: Se acreditará con copia simple de consignar constancias, certificados, u otros documentos, según

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

	corresponda. **Importante** *Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.*
B.4	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Jefe de Proyecto (01 persona):** • Experiencia en al menos tres (03) SERVICIOS de sistemas de internet y datos o experiencia en proyectos de seguridad gestionada en los últimos tres (03) años, se aceptará experiencia laboral sea de dos (02) años en implementación y/o gestión y/o configuración en equipos de seguridad perimetral. **Especialista (01 persona):** • Experiencia laboral en al menos tres (03) SERVICIOS en implementación de sistemas de internet con seguridad Gestionada en los últimos tres (03) años. Deberá sustentarse con constancias laborales, como especialista o equivalente. Se aceptará experiencia laboral sea de dos (02) años en implementación y/o gestión y/o configuración en equipos de seguridad perimetral. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: 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. Importante • *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.* • *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.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.* • *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.*

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a un S/ 600,000.00 (seiscientos 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. Se consideran servicios similares a los siguientes: internet dedicado. También: se aceptarán cualquier servicio brindado sobre fibra óptica tales como servicio de internet y/o servicios de transmisión de datos y/o transporte de datos, servicio de Ancho de banda y/o servicio de internet en general. Acreditación: 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 voucher 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 pago[1], correspondientes a un

Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

"… 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"

Firmado digitalmente por: ALVITRES TORRES Segundo Sergio FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 25/02/2022 10:43:01-0500

Firmado digitalmente por: CORIGLIANO ZEGARRA Victorio Daniel FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 25/02/2022 11:40:34-0500

	máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 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 sustentatoria 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 Nº 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 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".*

(…)

"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 contaríacon la declaración de un terceroquebrindecerteza, ante la cual debiera reconocerse la validez de la experiencia".

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*