"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

ESPECIFICACIONES TÉCNICAS

Unidad Orgánica	Oficina General de Tecnología de la Información
Meta Presupuestaria:	Sec. Fun. 097 - Desarrollo y Mantenimiento de los Sistemas Informáticos
Actividad del POI	5000003 – Gestión Administrativa

1. DENOMINACIÓN DE LA CONTRATACIÓN

Adquisición de dos (02) Firewalls para la interconexión de los locales periféricos y enlaces dedicados a la red WAN del Ministerio de Transportes y Comunicaciones.

2. FINALIDAD PÚBLICA

Asegurar un servicio ininterrumpido de conectividad de datos a todos los dispositivos de red que conforman la infraestructura de la sede central del MTC, permitiendo con ello poder ofrecer servicios de transmisión de datos desde las diferentes entidades del estado mencionadas en el objetivo específico y locales periféricos del MTC.

3. ANTECEDENTES

Con fecha 12 de octubre de 2009, mediante contrato Nro. 104-2009-MTC/10, se adquirieron cuatro (04) equipos Firewall UTM de la marca Fortinet modelo 620b, los cuales actualmente se encuentran en obsolescencia tecnológica y necesita ser reemplazados por equipos más actualizados y de mejor prestancia que ofrezcan los mecanismos adecuados de seguridad, que los equipos anteriores ya no se encuentran en capacidad de ofrecerlo.

4. OBJETIVOS DE LA CONTRATACIÓN

4.1. Objetivo General

Adquisición de dos (2) equipos Firewall para prevención y protección de la red con características de Next Generation Firewall (NGFW) para brindar conectividad de datos entre los enlaces dedicados de los locales periféricos y otras entidades públicas a la Sede Central del MTC.

4.2. Objetivo Especifico

Adquirir dos (2) Firewall de nueva generación para permitir la interconexión de las sedes de RENIEC, SUNARP, Banco de la Nación, PROVÍAS NACIONAL, SUTRAN, PRONATEL; así como los locales de licencias ubicados en la Av. Antenor Orrego, Lince y los locales de ECER (Estaciones de Control del Espectro Radioeléctrico) con la Sede Central del MTC, a través de los enlaces dedicados.

5. CARACTERÍSTICAS Y CONDICIONES DE LOS BIENES A CONTRATAR

5.1. DENOMINACIÓN Y CANTIDADES A CONTRATAR

N°	DESCRIPCION	CANTIDAD	UNIDAD DE MEDIDA
01	FIREWALL	02	UNIDAD

5.2. CARACTERISTICAS TÉCNICAS

Las características técnicas mínimas que debe presentar el bien solicitado deberán ser de acuerdo a lo siguiente:
Los equipos deben ser nuevos, de primer uso y de tecnología vigente.

Jirón Zorritos 1203 – Lima 1
Central telefónica: (511) 615-7800
www.gob.pe/mtc

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
1. Descripción.	a. La solución debe consistir en una plataforma de protección de Red, basada en dispositivos con funcionalidades de Firewall de Próxima Generación (NGFW). b. La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos dos (2) appliances con las mismas características mínimas mencionadas en estas especificaciones. c. El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 años. d. La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS. e. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7. f. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado. g. Los equipos NGFW deberán tener soporte vigente de fábrica durante el periodo de contrato de las prestaciones accesorias, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware. h. Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.
2. Características Técnicas (hardware)	a. Throughput de Next Generation Firewall de 5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes. b. Throughput de Prevención de Amenazas de 2.7 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
	c. No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde. d. El equipo debe soportar como mínimo 1.000.000 sesiones simultaneas y 55.000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte. e. Raqueable en dos (02) unidades de rack como mínimo. f. Debe contar con fuente de poder redundante con capacidad de cambio en caliente. g. Disco de estado sólido interno de 240 GB o superior. h. Mínimo 12 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red i. Mínimo cuatro (04) interfaces de red 1G en formato SFP para el tráfico de datos de la red j. Mínimo cuatro (04) interfaces de red 10G en formato SFP+ para el tráfico de datos de la red k. La plataforma deberá contar con al menos dos (02) interfaces adicionales 10/100/1000 y una (01) interfaz 10G SFP+ dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad.
3. Características Generales	a. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. b. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). c. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones. d. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP. e. Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino. f. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad. g. Soportar túneles GRE como punto inicio o finalización del túnel. h. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel. i. Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo. j. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
4. Alta Disponibilidad	a. La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
	b. Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces. c. Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3). d. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.
5. Funcionalidades	a. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones. b. Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención. c. Permitir el agendamiento de las políticas de seguridad. d. Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa. e. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. f. Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria. g. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules). h. Debe mostrar la primera y última vez que se utilizó una regla de seguridad. i. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad. j. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
6. Descifrado de tráfico SSL/TLS	a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos. b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall. c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3. d. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros. e. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS f. Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI). g. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
	h. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores. i. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).
7. Control de aplicaciones	a. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email. b. Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2 c. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada. d. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389. e. Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación. f. Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros. g. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado. h. Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante. i. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos. j. Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7. k. Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
8. Prevención de amenazas	a. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot. b. Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos c. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante. d. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot. e. Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia. f. Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad. g. Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems. h. Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. i. Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS. j. Los eventos deben identificar el país que originó la amenaza. k. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto. l. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención. m. Debe soportar la creación de firmas de IPS basadas en el formato de Snort.
9. Análisis de malware de día cero.	a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing. b. La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud) c. Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye Firmas o Prefiltros) d. El Next Generation Firewall debe tener capacidad de enviar 100 archivos por minuto al Sandbox Cloud. e. Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras. f. El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
	g. Deberá garantiza la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP. h. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red. i. Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante. j. Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. k. El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB, tanto en IPv4 como en IPv6. l. Debe permitir al administrador la descarga del archivo original analizado por el Sandbox. m. Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. n. Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. o. Permitir la subida de archivos al sandbox de forma manual y vía API. p. Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
10. Identificación de usuarios	a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local. b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente. c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI. d. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM. e. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios. f. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación. g. Debe permitir la definición de grupos dinámicos de usuarios.

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
11. QoS	a. Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto. b. Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables. c. El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad. d. Soportar marcación de paquetes DSCP, inclusive por aplicaciones; e. Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.
12. Filtro de datos	a. Los archivos deben ser identificados por extensión y firmas. b. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones. c. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
13. VPN	a. Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL. b. La VPN IPSec debe soportar como mínimo: • DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard) • Autenticación MD5, SHA-1, SHA-2; • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; • Algoritmo Internet Key Exchange (IKEv1 & IKEv2); c. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN. d. Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo. e. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA). f. Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN. g. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN. h. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: • Antes del usuario se autentique en la estación; • Después de la autenticación del usuario en la estación usando Single Sign On (SSO); • Bajo demanda del usuario; i. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10 y MacOS X. j. Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
14. Consola de administración y monitoreo	a. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante b. Permitir exportar las reglas de seguridad en formato CSV y PDF c. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad. d. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. e. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino) f. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. g. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política. h. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules). i. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup). j. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada. k. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP). l. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración; m. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema. n. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. o. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

SECCIÓN	CARACTERÍSTICAS TÉCNICAS
15. Geolocalización	a. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países. b. Debe permitir la visualización de los países de origen y destino en los registros de acceso.

NOTA: El postor deberá adjuntar en su propuesta para la admisión de la oferta, la hoja técnica, brochure del equipo, modelo ofertado y/o toda información técnica que acredite el cumplimiento de las características técnicas solicitadas en el presente numeral.

5.3. MODALIDAD DE EJECUCIÓN

El presente requerimiento se aplicará la modalidad de ejecución Llave en mano.

5.4. SISTEMA DE CONTRATACION

El sistema de contratación será a Suma Alzada.

5.5. GARANTIA COMERCIAL

El Proveedor, proporcionará una garantía de tres (3) años por cada uno de los bienes adquiridos que componen la solución de seguridad, dicha garantía iniciará al día siguiente de emitida la conformidad de entrega de los Firewall.

5.6. PRESTACION ACCESORIA A LA PRESTACIÓN PRINCIPAL

5.6.1. Mantenimiento

El proveedor deberá brindar hasta dos (2) mantenimientos anuales que consiste en la verificación del estado de operatividad de los equipos e instalación de upgrade del firmware (si fuese publicado por el fabricante).

El cronograma será establecido en coordinación con el responsable de OITSI a cargo de la supervisión del proyecto.

5.6.2. Soporte Técnico

a) Se brindará durante el periodo de garantía y soporte técnico a razón de tres (3) años en la modalidad 24x7x365 incluido domingos y feriados, contabilizadas a partir del día siguiente de emitida la conformidad de entrega de bienes.
b) El plazo máximo para acudir al local del MTC, identificar las causas del incidente y ejecutar la solución de primer nivel será de cuatro (04) horas.
c) El soporte será ON–SITE y ON-LINE y atenderán incidentes relacionados a los equipos, orientación técnica o atender requerimientos técnicos durante cualquier día de la semana.
d) El Proveedor debe contar con el servicio de recepción de incidentes 24x7x365 incluido domingos y feriados, a través de llamadas y de correos, para lo que deberá brindar; un número directo y una dirección de correo electrónico el cual será utilizado por el MTC para reportar las averías.
e) En caso de avería que afecte la operatividad de los Firewall, el proveedor brindará el equipo de respaldo o cambio dentro de las primeras cuatro (04) horas y para solucionar el incidente definitivamente dentro de las cuarenta y ocho (48) horas siguientes.

5.6.3. Capacitación

a) El PROVEEDOR deberá brindar un programa de capacitación al personal técnico de la Oficina de Infraestructura Tecnológica y Seguridad Informática, el mismo que deberá ser realizado en modo virtual.
b) La capacitación deberá desarrollarse de la siguiente manera:
   - Número de horas a capacitar: 8 horas lectivas mínimo.

- Número de personas a capacitar: 02 personas.
- Número de capacitadores: 01 (Personal clave)
- Entrega de certificado de participación por parte del proveedor.
- Temario de la capacitación: Deberá incluir al menos los siguientes temas:
  - ✓ Instalación, configuración y monitoreo de los equipos.
  - ✓ Actualización de versiones y parches
  - ✓ Administración de los equipos instalados.
  - ✓ Solución de problemas
- Manual de errores frecuentes.

c) El PROVEEDOR deberá brindar todo el material teórico sobre la capacitación en formato digital para cada asistente de la capacitación.

5.7. LUGAR Y PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

5.7.1. LUGAR

El Proveedor deberá considerar que la entrega de los bienes será en el Almacén Central del MTC (Jr. Zorritos N°1203, Cercado de Lima).
El horario de atención del almacén es:

	MAÑANA	TARDE
HORARIO	9:00AM – 12:00 HORAS	13:30 –16:30 HORAS

5.7.2. PLAZO

5.7.2.1. DE LA PRESTACIÓN PRINCIPAL

5.7.2.1.1. Plazo de entrega de los bienes.

Los bienes serán entregados en un plazo no mayor a treinta (30) días calendario, contados a partir del día siguiente del perfeccionamiento del contrato.

5.7.2.1.2. Plazo de instalación, configuración y puesta en producción

La instalación, configuración y puesta en producción será en un plazo no mayor a quince (15) días calendario, contados a partir de la entrega de los bienes.

5.7.2.2. DE LA PRESTACIÓN ACCESORIA

5.7.2.2.1. Plazo de prestación (soporte técnico, mantenimiento)

La prestación se realizará en un plazo de tres (3) años, contados a partir del día siguiente de la conformidad otorgada por la instalación, configuración y puesta en producción de los equipos.

6. REQUISITOS Y RECURSOS DEL PROVEEDOR

6.1. REQUISITOS DEL PROVEEDOR

a) Contar con una mesa de ayuda propia para brindar el soporte 24x7x365 incluidos domingos y feriados.
b) El postor deberá acreditar para la suscripción del contrato ser representante o distribuidor autorizado de la marca ofertada, adjuntando una carta del fabricante haciendo referencia al proceso.

6.2. RECURSOS DEL PROVEEDOR

6.2.1. DEL PERSONAL PROPUESTO

6.2.1.1. JEFE DE PROYECTO

Un (01) jefe de proyecto, será el responsable de la gestión durante toda la etapa de implementación del equipamiento ofertado.

Experiencia:
Con experiencia mínima de tres (3) años en la gestión de proyectos de soluciones de infraestructura tecnológica y/o seguridad informática.

Formación académica:
Profesional titulado en Ingeniería de Sistemas y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones.

Contar con Certificación vigente en PMP.

6.2.1.2. ESPECIALISTAS

Dos (2) especialistas, quienes serán los responsables de la instalación, configuración y puesta en producción del equipo ofertado. Asimismo, uno (1) de ellos será responsable de la capacitación al personal de OITSI.

Experiencia:
Con experiencia mínima de tres (3) años en implementación y/o soporte y/o mantenimiento de soluciones de seguridad informática.

Formación académica:
Profesional titulado o bachiller en Ingeniería de Sistemas y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Redes y/o Ingeniería Informática.

Debe contar con certificación técnica del producto ofertado.

El título profesional como la certificación técnica, debe ser presentado como parte de la documentación para perfeccionar el contrato.

7. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

7.1. OTRAS OBLIGACIONES

7.1.1. OTRAS OBLIGACIONES DEL CONTRATISTA

El CONTRATISTA deberá de remitir a la Entidad los siguientes entregables de la prestación principal y de la prestación accesoria siendo los siguientes:

7.1.1.1. ENTREGABLES

7.1.1.1.1. PRESTACIÓN PRINCIPAL

- Entregable Nro. 1: El proveedor deberá entregar los equipos en el almacén del MTC conforme al plazo indicado junto con la guía de remisión de los equipos en donde se precise los datos y número de serie de los mismos.

- Entregable Nro. 2: El proveedor deberá presentar en un plazo de hasta siete (7) días calendario contados a partir del día siguiente de entregado los bienes:
  a) El plan de implementación.
  b) El procedimiento para la gestión de incidentes de los equipos ofertados mediante la mesa de ayuda del proveedor.
  c) El manual de instalación y administración de los equipos ofertados.
  d) El documento en el cual se muestre la vigencia de la garantía y soporte de toda la solución ofertada.
  e) Informe técnico final de la instalación, configuración y puesta en producción de los equipos firewall en alta disponibilidad.

f) Certificado de capacitación a los asistentes del programa de transferencia de conocimiento.

7.1.1.1.2. PRESTACIÓN ACCESORIA

- Entregable Nro. 3: El Proveedor deberá presentar un informe técnico de las atenciones, información de los hechos y/o tickets generados durante la duración del periodo de soporte técnico en un plazo máximo de hasta cinco (5) días calendario posteriores a la culminación de cada semestre contabilizados a partir del día siguiente de la conformidad otorgada por la instalación, configuración y puesta en producción de los equipos.
- Entregable Nro. 4: El proveedor deberá presentar un informe del mantenimiento realizado que incluya el estado de salud u operatividad de los equipos en un plazo de hasta cinco (5) días calendario contabilizados a partir del día siguiente de culminado cada mantenimiento semestral.

La presentación de cada entregable será dirigido a la Oficina General de Tecnología de la Información y debe ser presentados a través de Mesa de Partes Virtual a través de: https://mpv.mtc.gob.pe/ o de forma física en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos Nº 1203 – Cercado de Lima, previa reservas de citas en línea a través de: https://citas.mtc.gob.pe, de lunes a viernes en el horario de 8:30 horas a 17:30 horas, siendo que los remitidos fuera de esa hora serán recepcionados como si hubiesen sido entregados al día siguiente hábil.

7.1.2. OTRAS OBLIGACIONES DE LA ENTIDAD

- ✓ La Entidad se compromete a otorgar la conformidad por las prestaciones principal y accesoria, según lo señalado.
- ✓ La entidad se compromete en realizar el pago de la prestación dentro de los plazos establecidos según normatividad
- ✓ La entidad se compromete a prestar todas las facilidades al CONTRATISTA, para la ejecución de la prestación.

7.2. CUMPLIMIENTO DE PROTOCOLOS SANITARIOS

De acuerdo a lo establecido en el Decreto Supremo No 103-2020-EF y la Resolución Ministerial Nº0258-2020-MTC/01, el CONTRATISTA deberá cumplir con lo establecido en el Anexo I "Protocolo Sanitario Sectorial para la prevención del COVID-19, para los servicios de telecomunicaciones" incluida en dicha resolución.

Asimismo, de conformidad con el numeral 3.2 del Decreto Supremo N° 080-2020-PCM, EL CONTRATISTA deberá contar con el registro y autorización respecto al "Plan para la vigilancia, prevención y control de COVID-19 en el trabajo" en el Sistema Integrado para COVID-19 (SICOVID-19) del Ministerio de Salud.

El CONTRATISTA deberá cumplir con las disposiciones establecidas en la Resolución Ministerial N°972-2020/MINSA, publicada el 27 de noviembre de 2020, Documento técnico: "Lineamientos para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-CoV-2"., así como, los protocolos sanitarios y demás disposiciones que dicten los sectores y autoridades competentes, que resulten aplicables a la presente contratación, bajo responsabilidad del contratista, con el fin de salvaguardar la salud del personal a cargo de la ejecución de la prestación.

7.3. NORMA ANTISOBORNO

El CONTRATISTA, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que puedan constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderado, representantes legales, funcionarios, asesores o personas vinculadas.

Asimismo, se obliga a conducirse en todo momento, durante la ejecución del contrato. 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, participantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en el artículo 11º de la Ley de Contrataciones del Estado y el artículo 7º de su Reglamento.

Además, se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por el MTC.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que el MTC pueda accionar.

7.4. NORMA ANTICURRUPCION

El CONTRATISTA acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anti-corrupción. Sin limitar lo anterior, EL CONTRATISTA se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anti-corrupción, sin restricción alguna.

En forma especial, EL CONTRATISTA declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

7.5. CONFORMIDAD

7.5.1. AREÁ QUE RECEPCIONA Y BRINDARA LA CONFORMIDAD

7.5.1.1. Recepción

La recepción se hará en el almacén central del MTC (léase numeral 8), debiendo contarse con la presencia de un representante de Almacén Central y un representante de la OGTI.

7.5.1.2. Conformidad

7.5.1.2.1. De la prestación principal

La conformidad de la entrega de los bienes será brindada por la Oficina General de Tecnología de la información (OGTI), con el visto bueno del Director de la Oficina de Infraestructura Tecnológica y Seguridad Informática, previa entrega de la documentación técnica solicitada en el ITEM N° 7.1.1.1.1. ENTREGABLES.

7.5.1.2.2. De las prestaciones accesorias

La conformidad de las prestaciones accesorias será brindada por la Oficina General de Tecnología de la información (OGTI), con el visto bueno del Director de la Oficina de Infraestructura Tecnológica y Seguridad Informática, lo cual se realizará al culminar cada periodo de servicio de soporte técnico anual (12 meses), previa entrega de la documentación técnica solicitada en el ITEM N°7.1.1.1.2. ENTREGABLES.

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

7.6. FORMA DE PAGO

La forma de pago se realizará de la siguiente manera:

7.6.1. DE LA PRESTACIÓN PRINCIPAL:

El pago se realizará en moneda nacional, en único pago (100% del monto ofertado de la prestación principal) a la entrega de los equipos y entregables del numeral 7.1.1.1.1. previa conformidad emitida por la Oficina General de Tecnología de la Información – OGTI.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- ✓ Informe del funcionario responsable de la Oficina General de Tecnología de Información (OGTI) emitiendo la conformidad de la prestación efectuada, previa validación de la Oficina de Infraestructura Tecnológica y Seguridad Informática.
- ✓ Comprobante de pago.
- ✓ Presentación de los entregables Nº1 y N°2 indicados en el numeral 7.1.1.1.1.

7.6.2. DE LAS PRESTACIONES ACCESORIAS:

- **Primer pago:** 20% al finalizar los doce (12) meses de iniciada la prestación accesoria, previo informe del estado situacional desarrollado durante dicho periodo.
- **Segundo pago:** 30% al finalizar los doce (12) meses siguientes a la aprobación del informe del estado situacional emitido en el primer pago.
- **Tercer pago:** 50% al finalizar los doce (12) meses siguientes a la aprobación del informe del estado situacional emitido en el segundo pago.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- ✓ Informe del funcionario responsable de la Oficina General de Tecnología de Información (OGTI) emitiendo la conformidad de la prestación efectuada, previa validación de la Oficina de Infraestructura Tecnológica y Seguridad Informática.
- ✓ Comprobante de pago.
- ✓ Presentación de los entregables Nº3 y N°4 indicados en el numeral 7.1.1.1.2

7.7. PENALIDADES APLICABLES

7.7.1. PENALIDADES POR MORA

En la ejecución de la adquisición de la solución, se aplicarán las penalidades por mora de acuerdo a lo establecido en los artículos 161° y 162° del Reglamento de la Ley de Contrataciones del Estado.

Si el contratista incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el Contratista acredite de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de la Entidad no da lugar al pago de gastos

generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

7.7.2. OTRAS PENALIDADES

De acuerdo con el artículo 163 del Reglamento de la Ley de Contrataciones del Estado, además de las penalidades por mora se considerarán las siguientes penalidades:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO (% POR VALOR DEL SERVICIO)	PROCEDIMIENTO
01	Por exceder el tiempo de respuesta máximo de 04 horas desde la comunicación por parte de la Entidad a una atención que no implique un incidente con la operatividad de los equipos Firewall, el mismo que será acreditado con el código de atención o de registro y/o correo electrónico.	1% del valor de una (01) UIT, por ocurrencia.	Mediante informe de la Oficina General de Tecnología de Información (OGTI).
02	Por exceder el tiempo máximo de cuarenta y ocho (48) horas para resolver incidentes para brindar el soporte correctivo reportado por la Entidad. El tiempo se contabiliza desde que el CONTRATISTA genera el ticket de atención al MTC vía correo electrónico.	3% del valor de una (01) UIT, por ocurrencia.	Mediante informe de la Oficina General de Tecnología de Información (OGTI).

UIT: Unidad Impositiva Tributaria.

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

7.8. RESPONSABILIDAD POR VICIOS OCULTOS

El CONTRATISTA es responsable por la cantidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo máximo de tres (3) años contados a partir de la conformidad otorgada.

8. REQUISITOS DE CALIFICACION:

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a **S/. 900,000.00 (novecientos mil y 00/100 soles)**, por la venta de bienes 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 bienes similares a los siguientes: **Firewall UTM, y/o Firewall de siguiente generación, y/o Firewall de aplicaciones web.** Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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 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 suministro, 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.

[1] 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"
(…)
"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".

BICENTENARIO PERÚ 2021

Firmado digitalmente por: MUÑANTE LOAYZA Patrick Javier FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 09/12/2021 08:48:46-0500

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

	Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**. Cuando en los contratos, órdenes de compra 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 compra 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** *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".*
B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Un (1) Jefe de proyecto:** Con experiencia mínima de tres (3) años en la gestión de proyectos de soluciones de infraestructura tecnológica y/o seguridad informática. **Dos (2) Especialistas:** Con experiencia mínima de tres (3) años en implementación y/o soporte y/o mantenimiento de soluciones de seguridad informática. Los especialistas serán los responsables de la instalación, configuración y puesta en producción del equipo ofertado. Asimismo, uno (1) de ellos será responsable de la capacitación al personal de OITSI. 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** • *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.* • *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.*

Importante

Jirón Zorritos 1203 – Lima – Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

- *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 las Especificaciones Técnicas 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 las características y/o requisitos funcionales. 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.*