ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE EQUIPAMIENTO PARA LA IMPLEMENTACION DE LA NUEVA PLATAFORMA DE DIRECTORIO ACTIVO PARA EL SISTEMA DE ÍNDICE COMBINADO DE ADN

Firma Digital

Firmado digitalmente por LEON RICALDI Jorge Jose Carlos FAU 20131370301 soft
Gerente De Oficina De Redes Y Comunicaciones
Motivo: Doy V° B°

1. OBJETO

Adquisición de Equipamiento para Implementación de la Nueva Plataforma de Directorio Activo para el Sistema de Índice Combinado de ADN.

2. DESCRIPCION DEL OBJETO

Con fecha 08 de julio de 2020, la República del Perú y el Banco Interamericano de Desarrollo (BID) suscribieron el Contrato N° 4959/OC-PE, cuyo objeto es contribuir a la financiación y ejecución del Programa "Mejoramiento de los servicios de justicia en materia penal en el Perú".

El objetivo general del programa es la mejora de la gestión del servicio del Sistema de Administración de Justicia Penal (SAJP), a través del: (i) aumento de la eficiencia del SAJP a través de los medios tecnológicos; (ii) aumento de la calidad de la investigación criminal; y (iii) mejoramiento del acceso a los servicios de administración de justicia penal a través de medios tecnológicos.

El principal impacto de la operación será mejorar la gestión del SAJP, medida en la disminución de la brecha entre procesos de investigación preliminar iniciados y resueltos

El Programa será ejecutado conjuntamente, por el Ministerio de Justicia y Derechos Humanos (MINJUSDH), el Ministerio Público (MP) y el Poder Judicial (PJ).

La Unidad Ejecutora 011, Carpeta Fiscal Electrónica, fue creada mediante Resolución de la Fiscalía de la Nación N° 1049-2020-MP-FN, y con Resolución de la Fiscalía de la Nación N° 1226-2020-MP-FN, se aprueba el Manual Operativo del Programa (MOP) "Mejoramiento de los servicios de justicia en materia penal en el Perú", en el cual se establece, entre otros, la descripción del Programa, beneficiarios, componentes del programa, marco institucional y ciclo operacional.

En ese contexto, la Oficina de Proyectos y Cooperación Técnica Internacional requiere de una solución tecnológica para la nueva plataforma de Directorio Activo que será utilizado por el software "CODIS" que forma parte del Proyecto de Inversión denominado **"Creación del Centro Nacional de Perfiles Genéticos Humanos y fortalecimiento de los laboratorios de ADN de la Unidad de Biología Molecular y Genética de Lima y de las Unidades Médico Legales III de Arequipa y Lambayeque, del Instituto de Medicina Legal y Ciencias Forenses del Ministerio Público".**

3. FINALIDAD PÚBLICA

El presente proceso tiene por finalidad adquirir una nueva plataforma de gestión de accesos a la información segura, escalable y de convergencia simplificada, en el cual se sincronizará para los accesos al Sistema de índice combinado de ADN, dicho esto se requiere contar con elementos de seguridad que protejan ante ataques informáticos.

4. CARACTERÍSTICAS TÉCNICAS

Los equipos ofertados deben ser nuevos (no más de 12 meses de fabricación), sin uso y del modelo más reciente e incorporado todas las últimas mejoras en cuanto a diseño y materiales, enfocados solo al sector Enterprise. Ningún componente podrá presentar adulteraciones ni correcciones. El postor deberá ofertar equipos de última vigencia tecnológica; igualmente no se podrá ofertar versiones Beta o que no sean de venta comercial por parte del fabricante.

Se precisa que la validación del cumplimiento de las características técnicas mínimas de los equipos será al momento de la presentación de los documentos de la admisión de la oferta. Se acreditará el cumplimiento mediante la presentación de una declaración jurada con una relación de los equipos propuestos, donde se indique la marca, modelo y/o código de parte, y

las cantidades ofertadas, indicando el link donde se pueda descargar las fichas técnicas en página del fabricante para la revisión y validación de cumplimiento, adicional como complementario podrá adjuntar las fichas técnicas en idioma español o inglés, también se aceptara carta de fabrica que sustente algún requerimiento técnico que no se encuentre en ficha técnica (firmado por algún representante de la marca e indique algún correo corporativo para la validación).

4.1 CARACTERÍSTICAS

La solución estará compuesta por los siguientes componentes:

A. **UN EQUIPO DE SEGURIDAD PERIMETRAL PARA LA INTEGRACION DEL DIRECTORIO ACTIVO.**
B. **UN EQUIPO DE GESTIÓN Y REPORTES DEL SISTEMA DE SEGURIDAD PERIMETRAL.**
C. **IMPLEMENTACION DE PLATAFORMA DE DIRECTORIO ACTIVO INTEGRADA A EQUIPO DE SEGURIDAD PERIMETRAL.**

Se precisa que todas las funcionalidades y licencias soportadas por los equipos solicitados deben estar habilitadas hasta el fin del periodo de la garantía como mínimo.

A. UN EQUIPO DE SEGURIDAD PERIMETRAL PARA LA INTEGRACION DEL DIRECTORIO ACTIVO.

- **Next Generation Firewall:**

  - ✓ De propósito dedicado de único fabricante en hardware y software.
  - ✓ Estar licenciado como mínimo 3 años y habilitado en simultaneo las funcionalidades de: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios a través de directorio activo y prevención de Bots, Sandboxing.
  - ✓ Debe tener el sistema operativo integrado a IPv4 e IPv6.
  - ✓ Deber poder ingresar al equipo a través de SSH, interfaz Web - SSL.
  - ✓ Debe incluir mínimo 1000 VLANs.
  - ✓ Protección contra ataques de denegación de servicio (DoS), mínimamente para HTTP Flood, UDP Flood, TCP SYN Flood, ICMP Flood, DNS Flood.
  - ✓ Protección para protocolos y tráfico anómalos, y debe tener habilitado mínimamente los siguientes: RIP, BGP, OSPF v2 y v3, IGMP v2 y v3, PIM-SM, PIM-DM.
  - ✓ Debe soportar realizar limites en el ancho de banda, y limitar aplicaciones.
  - ✓ El Gateway debe soportar mínimo 8 interfaces 10/100/1000Mbps RJ-45 y 4 interfaces de 10GbE (incluido sus 4 transceiver de 10Gbps).
  - ✓ El throughput debe ser al menos 7 Gbps para Threat Prevention con las funcionalidades habilitadas: Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot o Antispyware y Protección contra Dia Cero (Sandboxing) con logging activo; medido en condiciones de prueba empresariales o mezcla de trafico empresarial o en transacciones HTTP de 64KB, estos valores deberán estar claramente indicados en los datasheets públicos del fabricante ofertado
  - ✓ Tener un rendimiento para VPN (Gbps): 9 Gbps mínimo.
  - ✓ Debe incluir un Throughput mínimo de 37 Gbps de Firewall en Capa 4 o de Next Generation Firewall (NGFW) medido en condiciones de prueba empresariales o mezcla de trafico empresarial o en transacciones HTTP de 64KB, estos valores deberán estar claramente indicados en los datasheets públicos del fabricante ofertado
  - ✓ Debe ser capaz de manejar al menos 9 millones de conexiones concurrentes o cantidad máxima de sesiones.

- ✓ Debe soportar crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.
- ✓ Soportar que la comunicación entre los servidores de administración y el Gateway debe ser cifrada y autenticada.
- ✓ Debe soportar conectarse modo transparente o modo bridge.
- ✓ Debe soportar redundancia a enlaces.

- **Seguridad IPsec VPN:**
  - ✓ Debe soportar este módulo, y tener mínimamente 200 accesos disponibles, de acceso remoto VPN.

- **Seguridad IPS*:***
  - ✓ Soportar que el IPS y Firewall, deben estar integrados para protección multicapa.
  - ✓ Debe proveer miles de protecciones preventivas y proactivas out-of-the-box.
  - ✓ La solución debe ser miembro activo de la organización global conocida como la "Alianza de Ciberamenazas" (CTA) la cual garantiza un intercambio de inteligencia de amenazas entre terceros para acelerar la detección y mitigación de ataques globales, de tal forma que el fabricante pueda proveer más firmas enriquecidas por esta organización.
  - ✓ Debe tener tecnología de inspección del orden de llegada de los paquetes, de modo que ayude contra ataques relacionados al orden de los paquetes.
  - ✓ Debe poder bloquear amenazas: Protocol misuse, comunicaciones Outbound con malware, Intentos de Tunneling y ataques genéricos.
  - ✓ Debe proteger contra ataques complejos y elusivos.
  - ✓ Contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento y correlación de múltiples elementos.

- **Filtrado URL:**
  - ✓ Soportar filtrado de URL debe ser basado en categorías.
  - ✓ Soportar negar o permitir URLs específicos.
  - ✓ Debe poder filtrar tráfico cifrado HTTPS sin realizar inspección SSL.
  - ✓ Soportar la creación de excepciones basadas en la definición de objetos de red.
  - ✓ Soportar la notificación de bloqueo, y redireccionar al usuario a otra página.
  - ✓ Soportar un mecanismo, o bloque de seguridad, que permita controlar aplicaciones web 2.0 y widgets.
  - ✓ Soportar la identificación y bloquear herramientas de "proxy bypass" sobre protocolos estándar y no estándar.
  - ✓ Soportar bloquear Malware sobre sitios Web y Web 2.0.
  - ✓ Soportar método dinámico en la nube para la categorización de los sitios Web existentes y nuevos sitios emergentes.
  - ✓ Soportar inspección de tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.
  - ✓ Debe poder realizar la implementación de TLS 1.3 para inspección SSL y soportar protecciones al protocolo HTTP.

- **Control de aplicaciones:**
  - ✓ Se requiere que la detección de aplicaciones sea basada en APP-ID (decodificación de protocolos y aplicaciones, junto a detección heuristica) o en base a firmas, en el caso que la solución sea basada en firmas, la base de datos de control de aplicaciones debe contener al menos 6500 aplicaciones
  - ✓ Soportar identificar, permitir o bloquear aplicaciones y páginas Web.

- ✓ Soportar la integracion de control de aplicaciones y filtrado de URL dentro de la misma plataforma que además proporcione una solución de firewall, IPS, etc.
- ✓ Soportar bloquear aplicaciones o sitios al menos por lo siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales y grupos de usuarios.
- ✓ Soportar la integración con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en: usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas
- ✓ Soportar reglas de control de aplicaciones y filtrado de URL: bloquear, monitorear, informar al usuario y preguntar al usuario
- ✓ Soportar el control de ancho de banda de las aplicaciones por regla.

- **Antivirus y Antibot/Anti-Spypware:**
  - ✓ Solución integrada para prevención de virus y amenazas.
  - ✓ Soportar prevención de virus en al menos los siguientes protocolos: HTTP, HTTPS, FTP, POP3 y/o SMTP, en tiempo real.
  - ✓ La solución debe evitar infecciones de malware a través de archivos maliciosos entrantes (Word, Excel, PowerPoint, PDF, etc.) y en tiempo real.
  - ✓ Soportar el escaneo por dirección, e inspección sobre tráfico encriptado SSL.
  - ✓ Soportar descubrimiento de bots dentro de la red institucional y debe bloquear la comunicación que intenten establecer los bots con los atacantes.
  - ✓ Soportar detectar host infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.
  - ✓ Soportar analizar direcciones para descubrimiento de bots, que incluyan al menos, direcciones de: IP de Command and Control, URL y DNS.
  - ✓ Soportar patrones de comunicación de botnets.
  - ✓ Soportar identificación de direcciones de Command and control utilizadas por los criminales para controlar los bots.

- **Identificación de usuarios:**
  - ✓ Soportar proveer tres métodos para obtener las identidades de los usuarios: Sin agente haciendo búsquedas al directorio activo, agente instalado en los equipos del usuario final o portal cautivo.
  - ✓ Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un portal cautivo, a través del protocolo http.
  - ✓ Soportar el uso del protocolo WMI (Windows managemwnt instrumentation).
  - ✓ La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
  - ✓ La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP. Tambien se aceptaran soluciones que para cumplir este requerimiento tengan que instalar un agente en la PC que se integre con el módulo de identificación del usuarios del Firewall.
  - ✓ La solución debe poder integrarse con el directorio activo (AD) sin la necesidad de instalar un agente en el servidor de dominio o en los equipos de los usuarios finales.
  - ✓ Soportar crear reglas de acceso por usuario, debe poder integrase con otras soluciones como: control de aplicaciones y filtrado de URL.

- **Protección de *Sandboxing*:**
  - ✓ Soportar proteger contra ataques de día cero y malware desconocido antes de que una firma de protección estática sea creada.
  - ✓ Debe tener la opción de soportar emulación basada en red. ¨Network based Threat emulation, a través de un equipo dedicado para este fin, donde se realicen los análisis del sandbox.

- ✓ Tener la disponibilidad de despliegue en la nube, de tal forma que en la nube del fabricante se pueda realizar el análisis del sandbox
- ✓ Soportar emular archivos ejecutables, documentos, java y flash. En específico soportar los siguientes tipos de archivos, csv, doc, docx,, exe, jar, pdf, ppt, pptx, rar, rtf, swf, tar, tgz, xls, xlsm, xlsx, zip.
- ✓ Soportar múltiples sistemas operativos de Windows.
- ✓ Soportar detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- ✓ Soportar inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing con la infraestructura anti malware.
- ✓ Soportar realizar una pre-emulación o validación a través de un filtrado estático, en donde se valide si es necesario enviar el archivo a emulación.
- ✓ Soportar detección y prevención inmediata. La solución debe detectar el ataque en la fase de exploit.
- ✓ Soportar anti evasión, para que el malware no pueda detectar su ejecución dentro de un ambiente de Sandboxing y capacidad de detección anti-vm.
- ✓ Soportar detectar malware incluso si este tiene implementados retardos a nivel de shell code o ejecución del Malware.
- ✓ Soportar emular apagados y reinicios de las máquinas, para ver la reacción del Malware una vez esto ocurre.
- ✓ Ser resistente a casos donde el shell-code o malware no se ejecuten si detectan la existencia de un ambiente virtual.
- ✓ Soportar emular actividad real de los usuarios.

B. UN EQUIPO DE GESTIÓN Y REPORTES DEL SISTEMA DE SEGURIDAD PERIMETRAL.

- La administración de las políticas de Seguridad debe realizarse a través de una solución de administración independiente al firewall.
- Soportar gestionar a mínimo 05 firewall de nueva generación.
- Tener la capacidad de administrar las políticas de seguridad y diferentes perfiles de administración.
- Tener la capacidad de generar reportes automáticos y personalizables.
- Opción de segmentar reglas de acceso.
- Tener filtros predefinidos de búsqueda.
- Tener como mínimo 01 disco de 1TB.
- Debe permitir exportar en formato XLSX o PDF los reportes generados
- Debe estar licenciada para procesar/almacenar logs por segundo sin límite, hasta agotar el almacenamiento disponible

C. IMPLEMENTACION DE PLATAFORMA DE DIRECTORIO ACTIVO INTEGRADA A EQUIPO DE SEGURIDAD PERIMETRAL.

- La entidad entregara una máquina virtual para la instalación del directorio activo.
- Se deberá realizar la migración de Netware actual de la entidad, a una infraestructura de Directorio Activo, la cual debe contemplar mínimamente:
  - Exportar la lista de usuarios de Netware a archivos planos (tipo txt o csv).
  - Exportar la lista de grupos de Netware a archivos planos (tipo txt o csv).
  - Exportar las membresías de los grupos a archivos planos (tipo txt o csv).
  - Construir la infraestructura de Unidades Organizativas en el directorio Activo.
  - Planificar e implementar los GPO.
  - Exportar el árbol de directorios del Netware.
  - Importar los usuarios y grupos desde los archivos planos generados.
  - Poblar los grupos desde los archivos planos.

- Construir el árbol de directorios en el servidor Windows, que hará de File Server.
- Asignar os permisos a los directorios.
- Copiar la información.

- Se deberá considerar todas las licencias y software necesarios para la operación del nuevo directorio activo, las cuales deben estar vigentes y con soporte de actualizaciones por 3 años. No se aceptarán software libre, todos deben ser licenciados y con respaldo de soporte del fabricante.
- La nueva plataforma deberá tener políticas granulares y específicas en su operación, con una infraestructura de directorio Activo.
- Se deberá aplicar filtros y bloqueos de aplicaciones que la institución desea controlar, según se detalla mínimamente:
  - Integración con el AD intuitiva y eficiente.
  - Creación de políticas basadas en usuarios, de configuración intuitiva.
  - Creación de reportes basados en usuarios.
  - Creación de reglas de descarga y de carga, con aplicaciones específicas.
  - Bloqueos de aplicaciones web como Facebook y YouTube para el manejo optimo del ancho de banda de la institución, permitiendo en casos especiales a un grupo de usuarios estos servicios cuando sean solicitados.
  - Filtrado de aplicaciones que usan anonimizadores y quieran ocultar el tipo de tráfico que usan, permitiendo así un mejor control del tipo de información que usan.
  - Reportes fáciles de crear y programar para un grupo de ejecutivos, envió reportes por correo semanales, diarios, etc.
  - Instalación e implementación de un dominio de Directorio Activo, para aproximadamente 3000 usuarios simultáneos.
  - Migración de los objetos grupo, manteniendo las membrecías a los grupos.
  - Migración de los equipos cliente al dominio de directorio activo, manteniendo los perfiles de usuario.
  - Instalación configuración de un file server basado en Windows Server.
  - Migración de la data actual al nuevo file server manteniendo los permisos y características actuales.
  - Aplicación de políticas de acuerdo con las que se aplican actualmente.
  - Implementación / Configuración de un servidor de impresión.
  - Asignación de las impresoras de manera automática.
  - Implementar un servicio de actualizaciones automáticas, con servicios de DHCP y DNS, licenciados.
  - Implementar cuotas de almacenamiento y control de archivamiento.
  - Implementar dos controladores de dominio como mínimo, que contemple:
    - Un servidor de Archivos
    - Un servidor de impresión
    - Un servidor de actualizaciones

4.2 INSTALACIÓN Y CONFIGURACIÓN

La instalación, configuración y puesta en producción de los equipos solicitados será realizada por el personal del contratista, para lo cual deberá contar con el personal clave requerido.

PERSONAL CLAVE:

El POSTOR deberá presentar el personal requerido a fin de encargarse de la gestión y las instalaciones, del sistema instalado. Para el adecuado desarrollo de las instalaciones y el soporte técnico, el POSTOR deberá acreditar en su propuesta el siguiente personal requerido, considerando que solo las certificaciones deberán ser presentados para la firma de contrato.

JEFE DE PROYECTOS:

- Un (01) Profesional ingeniero en Ingeniería de Sistemas o Telecomunicaciones o Electrónico.
- Certificaciones PMP, SCRUM MASTER, vigentes.
- Experiencia de 3 años como Jefe de Proyectos de tecnologías de información y/o ciberseguridad.

ESPECIALISTA

- Un (01) Profesional bachiller en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónico.
- Certificación vigente de seguridad a nivel experto, emitido por la marca de NGFW ofertada.
- Experiencia de 2 años como especialista de instalaciones de soluciones en redes.

4.3 GARANTÍA

Se requieren tres (03) años de garantía del contratista. La Oficina de Redes y Comunicaciones del Ministerio Público debe tener la capacidad de poder generar sus casos de soporte técnico directo con el contratista a través de llamada telefónica y/o correo electrónico el cual puede implicar cambio de equipo y/o reemplazo de partes en caso sea necesario en modalidad 7x24.

La garantía aplica a defectos de fabricación y a mal funcionamiento. El contratista deberá entregar una declaración jurada en su oferta, que sustente la garantía de los equipos, donde se evidencia que se dispondrá de reemplazos parcial o total de los equipos en caso de falla, donde los tiempos de respuesta como máximo para reemplazos de equipos son, de veinticuatro (24) horas para la sede de Lima.

El contratista debe proporcionar al Ministerio Publico el link de descarga y las credenciales correspondientes para realizar las actualizaciones de software y parches por temas de seguridad de los equipos ofertados, durante el tiempo que dure la garantía. En caso el contratista no responda los incidentes, se debe garantizar que la entidad tenga la capacidad de poder generar los requerimientos de cambio de equipo directo con el fabricante.

4.4 CAPACITACIÓN

Se debe realizar el dictado de un curso/taller de capacitación sobre la administración y configuración de la solución propuesta, la cual debe tener una duración de 06 horas. El curso/taller debe estar dirigido para 10 personas y puede ser brindado de manera virtual o presencial.

Al finalizar la capacitación se hará entrega de la constancia respectiva a cada participante. El curso deberá ser dictado por un capacitador que pueda tener cualquier nivel de certificación técnica en la marca de los productos ofertados, sustentado mediante copia simple del certificado que deberá presentarse para la suscripción del contrato. El curso deberá comprender entre otros los siguientes puntos:

- ✓ Deberá ser teórico y práctico con el desarrollo de laboratorios.
- ✓ Conceptos referidos a instalación, configuración y resolución de problemas.
- ✓ Administración de los equipos proporcionados

5. CONFIDENCIALIDAD

En caso de que el proveedor reciba por parte del Ministerio Publico información de carácter confidencial, ésta deberá ser utilizada sólo para los fines de ejecución de la prestación. Por ello, será obligación del contratista mantener confidencialidad respecto a los datos e información de cualquier clase, que el Ministerio Publico le proporcione, o bien, a la que tenga acceso, con motivo de la prestación.

Adicionalmente, el proveedor estará obligado a instruir a sus funcionarios o personal que será parte conformante del recurso humano que ejecutará la prestación, respecto a la obligación de mantener confidencialidad.

6. PROTOCOLOS SANITARIOS

Para entrega en almacén y atenciones por garantía presenciales, el proveedor será el responsable de garantiza que el personal asignado cumpla con los protocolos sanitarios conforme a lo dispuesto en el Decreto Supremo Nº 080-2020-PCM y la Resolución Ministerial Nº 972-2020-MINSA.

7. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes y servicios ofertados por un plazo de tres (03) años, contados a partir de otorgada la conformidad por parte de la Oficina de Redes y Comunicaciones.

8. **PENALIDADES**

La Penalidad de los bienes se aplicará de acuerdo a lo establecido en el artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

En caso de retraso injustificado del contratista 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 formula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto Vigente}}{F \times \text{Plazo vigente en días}}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F 0.40.
b) Para plazos mayores a sesenta (60) días:
   b.1) Para bienes, servicios en general y consultorías: F = 0.25
   b.2) Para obras: F = 0.15

9. LUGAR DE ENTREGA

La entrega de los bienes se realizará en el Almacén Central del Ministerio Publico. Av. Abancay cuadra 5 S/N – Cercado de Lima.

10. PLAZO DE ENTREGA

El plazo de entrega de los bienes y capacitación será de cuarenta y cinco (45) días calendarios contabilizados a partir del día siguiente de firmado el contrato.

11. CONFORMIDAD

La conformidad técnica de los bienes y capacitación se realizará mediante un Acta de Conformidad firmada por la Oficina de Redes y Comunicaciones, previa verificación y cumplimiento de lo requerido en las especificaciones técnicas.

12. FORMA Y PLAZO DE PAGO

El pago se realizará con la conformidad emitida por la Oficina Central de Tecnologías de la Información previo visto bueno de la Oficina de Redes y Comunicaciones. Se realizará el pago en un único pago. El pago se realizará de acuerdo con lo establecido en el artículo 171.1 del Reglamento de la Ley de Contrataciones del Estado.

13. REQUISITOS DE CALIFICACION

A	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 600,000.00 (Seiscientos Mil con 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:

- Equipos firewall de nueva generación.
- Equipos gestión de firewall.
- Servidores

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 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

[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".

	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 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.

C	**CAPACIDAD TÉCNICA Y PROFESIONAL**
C.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Jefe de Proyectos:** • Un (01) Profesional ingeniero en Ingeniería de Sistemas o Telecomunicaciones o Electrónico. • Experiencia de 3 años como Jefe de Proyectos de tecnologías de información y/o ciberseguridad. **Especialista:** • Un (01) Profesional bachiller en Ingeniería de Sistemas y/o Telecomunicaciones y/o Electrónico. • Experiencia de 2 años como especialista de instalaciones de ciberseguridad. 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.*