

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 1 de 30 Año : 2024

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA LA AUTORIDAD NACIONAL DEL AGUA

1. FINALIDAD PÚBLICA

La presente contratación busca contar con una solución de seguridad perimetral para la Autoridad Nacional del Agua, administrada por la Dirección del Sistema Nacional de Información de Recursos Hídricos (DSNIRH), con la finalidad de brindar seguridad en el perímetro que permita la continuidad operativa en el borde de la infraestructura tecnológica que soporta los diversos servicios y sistemas institucionales.

La Autoridad Nacional del Agua es el órgano superior del sistema nacional de control y tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental. Para ello, aplica las Tecnologías de la Información para optimizar sus procesos de gestión institucional y brindar un mejor servicio. Dentro de este contexto, la solución de seguridad perimetral protege toda la infraestructura tecnológica que aloja documentos con valor legal.

2. ANTECEDENTES

La Autoridad Nacional de Agua (en adelante ANA) fue creada al amparo de la primera Disposición Complementaria Final de la Ley de Organización y Funciones del Ministerio de Agricultura, aprobada con Decreto Legislativo N° 997, como organismo público adscrito al Ministerio de Agricultura responsable de dictar las normas y establecer los procedimientos para la gestión integrada sostenible de los recursos hídricos. Tiene personería jurídica de derecho público interno y constituye un pliego presupuestal.

La ANA, Organismo Técnico Especializado adscrito al Ministerio de Agricultura y Riego, creado por la Primera Disposición Complementaria Final del Decreto Legislativo N° 997 del 13 marzo 2008, es el ente rector del Sistema Nacional de Recursos Hídricos, el cual es parte del Sistema Nacional de Gestión Ambiental, por lo que se constituye en la máxima autoridad técnico - normativa en materia de recursos hídricos y los bienes asociados a estos.

El literal f) del Artículo N° 5 de la Ley N° 27658 – Ley Marco de Modernización del Estado señala que el proceso de modernización de la gestión del Estado se sustenta, entre otros, en la institucionalización de la evaluación de la gestión por resultados a través del uso de modernos recursos tecnológicos, la planificación estratégica y concertada, la rendición pública y periódica de cuentas y la transparencia, a fin de garantizar canales que permitan el control de las acciones del Estado.

Para el cumplimiento de metas y objetivos institucionales, la Dirección del Sistema Nacional de Información de Recursos Hídricos (en adelante DSNIRH) requiere contar con una solución de seguridad perimetral para la ANA, con la finalidad de mantener la seguridad para el correcto funcionamiento de toda la plataforma tecnológica que soporta la totalidad de los servicios de red y sistemas institucionales.

3. JUSTIFICACIÓN

La ANA, a través de la DSNIRH, requiere contar con la adquisición de una solución de seguridad perimetral, de forma que se permita la continuidad de operación asegurando el correcto funcionamiento de la plataforma tecnológica instalada, la cual soporta los servicios de red y las aplicaciones institucionales.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 2 de 30 Año : 2024

4. OBJETIVO

Contar con la adquisición de una solución de seguridad perimetral para la ANA, con la finalidad de asegurar su operación, continuidad, crecimiento y disponibilidad, permitiendo la seguridad para el correcto funcionamiento de la plataforma tecnológica instalada y que soporta los servicios de red y las aplicaciones institucionales.

5. ALCANCES Y DESCRIPCIÓN DEL REQUERIMIENTO

En el presente numeral se describen las características técnicas mínimas de los bienes y servicios requeridos que deben ser considerados por los participantes como parte de su propuesta técnica:

Ítem Paquete	Prestación	Descripción	Cantidad	Unidad de medida
Único	Principal	Gestores del perímetro	4	Unidad
		Gestores centralizados	4	Unidad
		Gestores de eventos y reportes	2	Unidad
	Accesorio	Mantenimiento preventivo y correctivo por 1095 días	1	Servicio

PRESTACIÓN PRINCIPAL

El Contratista debe garantizar que todos los bienes suministrados en virtud del Contrato son de la versión más reciente e incorporan todas las últimas mejoras en cuanto a funcionalidad y prestaciones.

A. Cuatro (04) gestores del perímetro (Código SIGA: 952278320001):

A.1. Características generales:

- Cuatro (04) equipos de propósito específico de firewall de siguiente generación, implementados en alta disponibilidad.
- Los gestores del perímetro deben ser instalados y configurados dos (02) para el Centro de procesamiento de datos principal (CPDP) y dos (02) para el Centro de procesamiento de datos secundario (CPDS).
- El fabricante del NGFW debe ser miembro activo de la organización CTA (Cyber Threat Alliance) permitiendo el intercambio eficiente de inteligencia de amenazas entre terceros.
- La marca del firewall propuesto debe contar con certificación USGv6- r1 en Firewall.
- Estar licenciado como mínimo tres (03) años y habilitado en simultaneo las funcionalidades de: Firewall, IPS, Antivirus de red, Control de aplicaciones, identificación de usuarios a través de directorio activo, prevención de Bots y Sandboxing Cloud.
- La solución perimetral ofertada debe brindar funcionalidades de Firewall e IPS en IPv4 e IPv6.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 3 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	


- Protección para protocolos y tráfico anómalos, y debe tener habilitado mínimamente los siguientes protocolos: RIP, BGP, OSPF v2 y v3, IGMP v2 y v3, PIMSM, PIM-DM.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT) y Capa 2 (Transparente y/o Sniffer), precisándose que será opcional que la operación de ambos modos trabaje de forma simultánea o no.
- Debe soportar redundancia a enlaces. La solución podrá incluir capacidades de SD-WAN habilitadas durante la vigencia del contrato.
- Debe ser capaz de inspeccionar el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- Reconocer por lo menos 4500 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.
- Soporte de rutas estáticas, PBR (policy-based routing) o PBF (Policy-based Forwarding).

A.2. Capacidad:

- Tener un rendimiento Threat Prevention (cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware) de 15 Gbps mínimo, medido en condiciones de prueba o mixtura empresariales o en transacciones HTTP de 64KB.
- El equipo debe soportar como mínimo 10 millones de sesiones concurrentes en TCP o HTTP.
- El equipo debe soportar 400 mil nuevas sesiones por segundo en TCP o HTTP.
- Debe contar con fuente de poder redundante con capacidad de cambio en caliente.
- El Gateway debe soportar mínimo las siguientes interfaces: 04 interfaces 10/100/1000Mbps RJ-45, 08 interfaces de 10GbE (incluido como mínimo 06 transceiver de 10Gbps), 02 interfaces de 40GbE (incluido los 02 transceiver de 40Gbps), 01 puerto dedicado para HA o sincronización de clúster y 01 puerto dedicado para gestión.
- Se debe incluir transceivers para fibra multimodo para las interfaces SFP+ y QSFP y cualquier otro componente que permita la operatividad de las interfaces solicitadas.
- Incluir capacidad de trabajar con firewalls virtualizados dentro del mismo equipo, al menos 10 sistemas virtuales. Esta funcionalidad debe estar licenciada.
- Altura máxima de 2RU.

A.3. VPN:

- La plataforma debe tener la capacidad de soportar al menos 500 conexiones VPN SSL concurrentes desde dispositivos endpoint y móviles, usando agente y sin agente.
- El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e iOS. Incluye el licenciamiento necesario para permitir esta capacidad.
- El agente de VPN client-to-site debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red.
- Se deberá incluir doble factor de autenticación para 1800 usuarios (mínimo). Además, se solicita que el segundo factor de autenticación deba ser mediante una contraseña de un solo uso (OTP) mediante SMS y/o aplicativo móvil y/o Email; y soporte de: Radius y/o TACAC's.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 4 de 30 Año : 2024

A.4. Identificación de Usuarios:

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local.
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad/controles basados en usuarios y grupos de usuarios.
- Debe permitir el control de navegación sin necesidad de instalación de software de cliente, a través del uso portal cautivo.

A.5. QoS Traffic Shaping:

- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad y/o pesos.

A.6. Filtro de Datos:

- Debe permitir realizar la detección y bloqueo de archivos por su extensión.
- Soportar la identificación de archivos comprimidos.
- Soportar la identificación de archivos cifrados y/o tipos de archivos relacionados con ASC, KEY, P12 o PFX.

A.7. Prevención de amenazas:

- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets).
- Opcionalmente, las características de IPS y antivirus podrán funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
- Identificar y bloquear la comunicación con redes de botnet.
- Debe incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca.
- Soportar Threat Feeds mediante cualquier de los siguientes métodos: STIX, servicios web, archivos o texto; o en su defecto, que soporte como mínimo los siguientes formatos: CSV, SNORT o STIX XML.
- Soportar, proteger contra ataques de día cero y/o phishing (conocido y desconocido) y/o malware (conocido y desconocido) a través de un servicio de sandboxing en la nube del fabricante por el periodo del contrato.
- Opcionalmente, debe contar con protección que al hacer una descarga por HTTP/HTTPS, debe soportar modificar archivos (reconstruido durante su análisis) eliminando componentes riesgosos (código, link).

A.8. Filtro Web

- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 5 de 30 Año : 2024

- Debe tener capacidad de actualizar la base de datos de URLs y categorías desde el servicio de inteligencia del fabricante.
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL.
- Tener por lo menos 70 categorías de URL.
- Permitir el bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

B. Cuatro (04) gestores centralizados (Código SIGA:952278320027):

B.1. Características generales:

- Se requiere la gestión de los firewalls sea dedicada, es decir que cumpla únicamente la gestión centralizada de los Firewalls.
- Los gestores centralizados deben ser instalados y configurados, dos (02) para el Centro de procesamiento de datos principal (CPDP) y dos (02) para el Centro de procesamiento de datos secundario (CPDS).
- La gestión de los firewalls debe realizarse desde una solución en appliance provista por el mismo fabricante de los firewalls. No se aceptarán soluciones en software o máquinas virtuales montadas sobre servidores o hipervisores.
- Debe tener una capacidad de almacenamiento mínima de 4 TB utilizables después de configurar el RAID 0 o 1.
- El appliance debe contar con al menos dos interfaces GE RJ45.
- El equipo deberá tener una altura no superior a 2RU y deberá poder ser montado en un rack de 19".
- La solución debe tener la capacidad y contar con el licenciamiento para gestionar al menos 10 dispositivos o instancias virtuales.
- La administración de las políticas de seguridad debe realizarse sobre hardware dedicado para dicho propósito y provisto por el mismo fabricante de los firewalls.
- La solución debe permitir realizar todos los cambios en los firewalls de manera centralizada.
- El postor deberá garantizar compatibilidad con las versiones nuevas del fabricante de Firmware durante el periodo del contrato; en caso de no soportar las nuevas versiones, el postor deberá reemplazar la solución por un equipo que garantice la compatibilidad.
- La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación, IPS, antivirus, y filtro de URL.
- Permitir buscar cuáles reglas un objeto está siendo utilizado.
- La solución debe permitir importar los cambios realizados directamente en los firewalls para sincronizarlos con la configuración existente en la plataforma de gestión.
- La caída o falla de la plataforma de gestión no debe impedir el acceso a los firewalls para realizar cambios en la configuración.
- La solución debe contar con la capacidad de asignar un perfil de administración basado en roles (RBAC) que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
- Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, como el administrador que la realizó, su IP y el horario de la alteración;
- Generar alertas automáticas vía email, SNMP y Syslog.
- La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en JSON o XML.
- La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 6 de 30 Año : 2024

- Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador, o también, la creación de flujos podrá realizarse a través del bloqueo de la configuración que evite que otros administradores cambien la configuración actual hasta que se termine de realizar el cambio de otro administrador (con la finalidad de no realizar cambios conflictivos en la misma configuración).
- Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware.
- Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración.
- Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos.
- Tener histórico de los scripts ejecutados en los dispositivos gestionados por la solución de gestión; o en su defecto, la solución deberá contar con el historial de todas las modificaciones realizadas en la política de seguridad configurada.
- Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos.
- Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada.

C. Dos (02) gestores de eventos y reportes (Código SIGA: 740892000226):

C.1. Características generales:

- Se requiere que la generación de reportes de los firewalls sea dedicada, es decir que cumpla únicamente la función de generar reportes y monitoreo de eventos de los firewalls.
- Los gestores de eventos y reportes deben ser instalados y configurados, uno (01) para el Centro de procesamiento de datos principal (CPDP) y uno (01) para el Centro de procesamiento de datos secundario (CPDS).
- Con la finalidad de no degradar el performance del procesamiento de red y seguridad del NGFW, se requiere un (01) appliance dedicado. No se aceptarán soluciones conformadas por software instalado sobre hardware o servidores genéricos.
- Una consola centralizada para el almacenamiento de logs (registros), correlación de eventos de seguridad y reportes, con capacidad de hasta 10 Firewalls.
- La plataforma de recolección de logs y generación de reportes debe ser de mismo fabricante de los equipos de seguridad perimetral.
- Debe recibir como mínimo 3000 logs/segundo.
- Debe tener una capacidad de almacenamiento mínima de 4 TB utilizables después de configurar el RAID 0 o 1.
- Debe contar con al menos dos (02) puertos o interfaces de red RJ45.
- Dimensiones del equipo de 1RU
- Debe soportar acceso vía SSH, WEB (HTTPS) y/o GUI para la gestión de la solución.
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
- Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3
- Autenticación de usuarios de acceso a la plataforma vía LDAP y Radius.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 7 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña de este.
- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora de este.
- Debe permitir visualizar en tiempo real los logs recibidos.
- Contar con mecanismos de borrado automático de logs antiguos.
- Debe permitir exportar los logs en formato CSV o algún formato similar legible.
- Debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- Debe contar con la capacidad de crear informes en formato HTML o PDF.
- Debe contar con la capacidad de crear informes en formato XML o CSV.
- La solución debe contar con reportes predefinidos.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto y/o imágenes, alineación y/o saltos de página, entre otros.
- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- Debe incluir dashboard para monitorear las principales amenazas de seguridad para su red
- Debe incluir dashboard para monitorear el tráfico en su red.
- Debe incluir dashboard para monitorear el tráfico de aplicaciones y sitios web en su red
- Debe incluir dashboard para monitorear actividad VPN en su red.
- Debe permitir generar alertas de eventos a partir de logs recibidos
- Debe contar como mínimo con los siguientes reportes (crear o personalizar los reportes señalados):
 - Reporte de utilización de aplicaciones SaaS.
 - Reporte de VPN.
 - Reporte de Sistema de prevención de intrusos (IPS).
 - Reporte de análisis de seguridad de usuario.
 - Reporte de análisis de amenaza cibernética.
 - Reporte de breve resumen diario de eventos e incidentes de seguridad.
 - Reporte de Top 10 de Aplicaciones utilizadas en la red.
 - Reporte de Top 10 de Websites utilizadas en la red.
 - Reporte de uso de redes sociales.
 - Reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal, o Reporte detallado sobre las amenazas y/o vulnerabilidades encontradas a nivel del tráfico inspeccionado.
 - Reporte de seguridad en aplicaciones web.

Instalación, configuración y migración de la solución de seguridad perimetral

- La solución de seguridad perimetral debe ser instalada, configurada, migrada en sus respectivos centros de procesamiento de datos.
- El Contratista propondrá a la DSNIRH un “Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral” que será ejecutado de acuerdo con las factibilidades de la ANA, las mismas que podrían variar por causas no imputables al Contratista.
- En dicho plan establece plazos para el cumplimiento de las tareas: discriminando las que debe cumplir la ANA, las que debe cumplir el Contratista, y las que deben cumplir en forma compartida.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 8 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- En dicho plan se debe contemplar entre otras, pruebas de diagnóstico, pruebas de funcionamiento, operación, integración, de seguridad, y lo que corresponda de la solución de seguridad perimetral.
- Será de total y exclusiva responsabilidad del Contratista efectuar las tareas necesarias para la puesta en marcha de la solución de seguridad perimetral.
- La solución de seguridad perimetral debe ser instalada adecuadamente como parte de la LAN del CPDP y CPDS. El Contratista debe suministrar todos los componentes de hardware y software necesarios para la correcta operación de la solución de seguridad perimetral dentro de la LAN y SAN de cada CPD.
- Los servicios solicitados deben ser realizados por personal técnico calificado para todas las instalaciones requeridas, de acuerdo con lo indicado en el perfil del personal solicitado.
- El Contratista instalará y contemplará todos los servicios, componentes y accesorios que sean necesarios para el correcto funcionamiento de la solución ofertada en los equipos en producción.
- Para efectos de la migración hay que considerar que el equipamiento actual es de la marca Check Point modelo 15400 – NGTX para ambos CPD.

Capacitación y/o entrenamiento oficial

- El postor como parte del “Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral” requerido, debe diseñar y presentar un plan de capacitación de nivel técnico para el personal que se encargará tanto del diseño, la administración como de la operación de la solución, el mismo que debe ser presentado junto con el plan de trabajo. El postor bajo cuenta, costo y riesgo se hará cargo de todo lo necesario para llevar a cabo la capacitación.
- La capacitación debe realizarse como mínimo para tres (03) participantes.
- El objetivo de las capacitaciones es permitir el correcto diseño, administración de la infraestructura tecnológica y la operación, monitoreo y soporte de las herramientas puestas en producción. Hay que considerar que el curso oficial debe tener un mínimo de 40 horas. Se requiere que el Contratista incorpore en el Plan de Capacitación los siguientes cursos, tres (03) cursos oficiales:
 - Administración de los gestores del perímetro (firewall), curso oficial del fabricante.
 - Administración de los gestores centralizados, curso oficial del fabricante.
 - Administración de los gestores de eventos y reportes, curso oficial del fabricante.
- Opcionalmente, en el caso de los dos últimos cursos (Administración de los gestores centralizados y Administración de los gestores de eventos y reportes), el curso puede estar embebido en el otro en la medida que cubra ambos temarios (ej.: curso oficial de Administración de los gestores centralizados, eventos y reportes.). Para este caso el Plan de Capacitación contendría dos (02) cursos oficiales.
- El curso oficial debe ser de la marca ofertada, propuesto por el fabricante o por un centro autorizado del fabricante.
- Se espera que el contenido mínimo del Plan de Capacitación abarque los siguientes aspectos:
 - Plan de los cursos
 - Objetivos de los cursos.
 - Contenido de los cursos.
 - Duración.
 - Lugar.
 - Perfil requerido de los participantes.
 - Material Didáctico y recursos pedagógicos y modalidades de entrega física y especificar medios digitales.
 - Equipos, Manuales, certificados y/o constancias de participación

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 9 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- El contenido de los cursos y el material didáctico debe referirse a la versión de la solución propuesta según currículo oficial del fabricante. Al momento de la presentación de la propuesta, de no existir el curso requerido en la versión de la solución, se podrá presentar como parte de la propuesta el curso similar vigente y/o de una versión anterior de la solución propuesta, la misma que será validada con: la lista de cursos oficiales que se encuentre publicada en la página web del fabricante (link) y/o con documentación oficial del fabricante que muestre la lista de cursos oficiales vigentes, a ser presentado obligatoriamente por el postor como parte de su propuesta.
- Al momento de la presentación de propuestas, de no existir un curso oficial requerido en la versión de la solución o, curso similar vigente y/o de una versión anterior de la solución propuesta; éste podrá ser dictado en modalidad de Curso Taller (No Oficial) ejecutado por el fabricante de la solución ofertada y con un instructor autorizado por el fabricante; el cual deberá ser brindado por un valor no menor de 12 horas lectivas por Curso Taller que se realice (Administración de los gestores del perímetro (firewall) y/o Administración de los gestores centralizados y/o Administración de los gestores de eventos y reportes). Se deberá entregar certificado por cada Curso Taller, el cual, como mínimo debe ser a nivel de asistencia.
- El instructor de cada curso debe estar certificado por el fabricante.
- El Contratista proporcionará el espacio físico y todos los componentes necesarios para la capacitación.
- En caso la capacitación sea impartida en laboratorio remoto y/o virtual, el Contratista deberá garantizar capacidad de procesamiento, almacenamiento y tiempo de respuesta similares a un entorno local.
- Será aceptado como laboratorio de las capacitaciones, entornos remotos que poseen las mismas funcionalidades con diferente configuración.
- El Contratista proporcionará equipos, medios, herramientas, programas y material didáctico para el desarrollo de la capacitación.
- El curso se dictará en idioma español, o en su defecto en inglés con traducción simultánea.
- Si el dictado de la capacitación debería darse al interior o fuera del país el Contratista incluirá, como parte de la solución, los costos de traslado, hospedaje y viáticos para el personal solicitado.
- Se debe entregar certificado (de participación) por cada curso, otorgado por el fabricante.

Entregada la solución de seguridad perimetral se suscribe el Acta de recepción de la solución de seguridad perimetral, previa validación técnica por parte de la DSNIRH.

Posteriormente, concluida la instalación, configuración, migración y capacitación se suscribe el Acta de inicio del servicio de la solución de seguridad perimetral, previa validación técnica por parte de la DSNIRH (para dar inicio al servicio de mantenimiento preventivo y correctivo, computado desde el día siguiente de firmada la presente acta).

Finalmente, el Contratista presentará un Informe Técnico a la DSNIRH, incluyendo ambas actas. El informe técnico detalla las tareas realizadas en los CPDP y CPDS. Debe contener i) Adecuaciones del centro de datos: Descripción, diagrama de ubicación, reporte fotográfico que incluya leyenda, ii) Configuración de red data: diseño inicial vs diseño final de las conexiones físicas y lógicas (incluyen diagramas), iii) Configuración del equipamiento: distribución de equipos en el rack de comunicaciones, cableado de energía, descripción de equipos adquiridos, credenciales de acceso hacia la interface web de gestión, tabla de IP de gestión del hardware, estado de cada componente de la solución de seguridad perimetral y cualquier otro que solicite la entidad en el marco de la implementación de la solución de seguridad perimetral, iv) duración de todos los componentes de la solución de seguridad perimetral (incluye licencias) y v) nivel de escalamiento para las atenciones (incluye celulares y correos electrónicos).

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 10 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

PRESTACIÓN ACCESORIA

Mantenimiento preventivo y correctivo (Código SIGA: 602000010362):

A. Mantenimiento preventivo

- La revisión periódica de los equipos y los cambios de elementos que así lo requieran se efectuarán de acuerdo con las recomendaciones del fabricante y previa coordinación con la DSNIRH, mediante correos electrónicos y/o llamadas telefónicas, de tal manera que dichas tareas no interfieran en el desarrollo de las actividades de la ANA.
- Deberá realizarse un total de tres (03) mantenimientos preventivos, con una frecuencia anual (una revisión periódica por cada 365 días calendario), contados a partir del día siguiente de suscrita el Acta de inicio del servicio de seguridad perimetral, debiendo considerarse el mantenimiento físico y lógico de la solución de seguridad perimetral ofertada, durante el periodo de tiempo que dure la prestación accesoria. El Contratista deberá proporcionar como parte de su "Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral" un Cronograma de fechas para la realización del mantenimiento preventivo de la solución de seguridad perimetral ofertada, de acuerdo con lo solicitado; sin embargo, durante el periodo de la prestación accesoria quedará a discrecionalidad de la institución la posibilidad de reprogramación de las fechas establecidas en dicho cronograma y que será oportunamente coordinado con el Contratista que se otorgue la buena pro. La revisión de la solución de seguridad perimetral ofertada deberá realizarse en el lugar donde se encuentren instalados.
- En caso de encontrar algún desperfecto en el equipo revisado, el Contratista deberá tomar las acciones correctivas o realizar los cambios de los componentes que así lo requieran para solucionar el desperfecto, sin costo alguno para la Entidad contratante.
- Cada vez que el Contratista realice una revisión periódica a los equipos, deberá pegar una etiqueta que identifique el número de revisión y fecha en la cual se realizó.
- En caso de ser necesario trasladar el equipo para la revisión, los costos del envío/retorno y otros serán por cuenta del Contratista.
- Asimismo, deberá remitir a la DSNIRH, mediante correo electrónico y a través de la mesa de partes de la Autoridad Nacional del Agua, el resumen detallado de las revisiones periódicas programadas, considerando como mínimo los datos indicados en el Reporte de Servicio Técnico.

Monitoreo y respuesta avanzada a incidentes

El Contratista deberá monitorear proactivamente de acuerdo a una disponibilidad de 24x7 es decir, de lunes a domingo (incluidos feriados) durante las 24 horas del día, en el periodo de vigencia del contrato, la solución de seguridad perimetral propuesta para una detección oportuna de amenazas que puedan atentar contra la seguridad de la institución.

Las alertas de eventos producto del monitoreo realizado e identificación de un comportamiento anómalo, deberán ser comunicados según la Matriz de Niveles de Criticidad establecido, al área usuaria (DSNIRH) vía correo electrónico a la siguiente dirección: infraestructura_dsnirh@ana.gob.pe de manera inmediata y/o reportadas vía llamada celular al personal de la DSNIRH que se tenga registrado como personal autorizado previa información; indicando recomendaciones a seguir y brindar asesoría de mitigación de incidentes puntuales o de gran escala mediante respuesta avanzada a incidentes. De igual forma, se utilizará el mencionado correo electrónico para el envío de los reportes diarios y los reportes consolidados mensuales.

La respuesta avanzada a incidentes consistirá en la atención de alerta de eventos causados por amenazas de seguridad como ataques, comportamiento malicioso, tráfico anómalo, entre otros en la solución de seguridad perimetral propuesta. Se encargarán de analizar e

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 11 de 30 Año : 2024

investigar el hecho con sus expertos y plantearán las acciones de corrección, mitigación, contención o remediación recomendadas para cada incidente en coordinación con el área usuaria (DSNIRH).

La respuesta avanzada a incidentes responderá metódicamente y seguirá un ciclo de acción: utilizando herramientas y/o librerías como la normatividad NIST SP 800-61 y/o ISO 27032 y/o ISO 27001 y/o Membresía FIRST, entre otras que apliquen.

La respuesta avanzada a incidentes podrá ser activada en los siguientes casos:

- ✓ Por un incidente en la solución de seguridad perimetral propuesta de tipo Crítico, Alto o Medio.
- ✓ A solicitud del área usuaria.
- ✓ Acciones de iniciativa propia del contratista (por ejemplo, producto del monitoreo y análisis de riesgo).

El tiempo máximo de atención inicial de la respuesta avanzada a incidentes activados deberá ser de quince (15) minutos.

Para el cumplimiento de lo estipulado en el punto anterior, se entenderá como Tiempo Máximo de atención inicial de la respuesta avanzada a incidentes activados, al tiempo transcurrido entre la comunicación al Contratista de la existencia de un incidente que demanda la respuesta avanzada a incidentes activados, realizada por parte de la Entidad (llamada telefónica de servicio y/o correo electrónico), y la respuesta de inicio de acciones de la respuesta avanzada a incidentes activados.

De igual forma, el Contratista realizará el monitoreo de estado de salud de la plataforma de seguridad propuesta a través de su solución de monitoreo para lo cual incluirá la evaluación de la performance, disponibilidad, uso de interfaces, estatus de procesamiento de la solución (estado de salud), entre otros; el cual como mínimo debe cumplir lo siguiente:

- Compatible con la marca de la solución de seguridad propuesta para el monitoreo de sus componentes y características.
- Monitorear la performance de la solución.
- Monitorear el uso de interfaces de la solución.
- Monitorear la cantidad de sesiones concurrentes.
- Monitoreo del uso de Internet e identificación de violaciones de reglas establecidas en la solución de seguridad propuesta.
- Supervisión de seguridad de la red y gestión de cumplimiento.
- Monitoreo de cambios efectuados en la configuración del firewall.
- Monitoreo en tiempo real de conexiones (por ejemplo: VPN's).
- Monitoreo y gestión de las reglas del firewall.
- Monitoreo y análisis completo de tráfico de red, ancho de banda y URL's.
- Almacenamiento de datos históricos de la solución de seguridad propuesta por lo menos de 3 meses.
- Investigaciones forenses y análisis de registros de la solución de seguridad propuesta.

La solución de seguridad perimetral deberá ser monitoreada por el NSOC o NOC o SOC del Postor y brindar reporte de alerta del estatus de seguridad de la entidad de manera mensual, que permita tomar decisiones de los riesgos cibernéticos a los cuales se puedan estar expuesto. Deberá detallar mínimamente información de tráfico, amenazas, vulnerabilidades, uso de aplicaciones por usuarios, performance de la solución de seguridad perimetral, sesiones de conexión VPN y tiempo de actividad, actividad de los usuarios y conexiones URL, dentro del reporte mensual.


	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 12 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

ACCIÓN	SLA	REPORTES
Monitoreo de salud de la plataforma	Disponibilidad diaria 24x7 de lunes a domingo (incluidos feriados), en el periodo de vigencia del contrato.	<ul style="list-style-type: none"> - Reportes diarios vía correo electrónico. - Reporte consolidado mensual, vía correo electrónico.
Monitoreo en tiempo real y Alerta de eventos	Disponibilidad diaria 24x7 de lunes a domingo (incluidos feriados), en el periodo de vigencia del contrato.	<ul style="list-style-type: none"> - Reportes diarios vía correo electrónico. - Reporte consolidado mensual, vía correo electrónico. - Envío de alertas a través de los medios de comunicación establecidos para con el área usuaria y de acuerdo con la Matriz de Niveles de Criticidad.

MATRIZ DE NIVELES DE CRITICIDAD		
Son categorizaciones para casos enmarcados dentro del monitoreo y respuesta avanzada a incidentes.		
Nivel Crítico	<ul style="list-style-type: none"> - Situación: La entidad o servicios críticos de la entidad han sido afectados. 	Comunicación: ✓ Vía correo electrónico y, ✓ Vía llamada celular al personal de la DSNIRH autorizado.
Nivel Alto	<ul style="list-style-type: none"> - Situación: Servicios no críticos han sido afectados. Problema ha sido controlado temporalmente por la DSNIRH. Probabilidad que se afecte sistemas críticos de la entidad en el corto plazo. 	Comunicación: ✓ Vía correo electrónico y, ✓ Vía llamada celular al personal de la DSNIRH autorizado.
Nivel Medio	<ul style="list-style-type: none"> - Situación: Se necesita más información para determinar posible impacto. Existen incongruencias en la solución. 	Comunicación: ✓ Vía correo electrónico
Nivel Bajo	<ul style="list-style-type: none"> - Situación: Alertas o incidentes sobre acciones o actividades de bajo riesgo a la seguridad. 	Comunicación: ✓ Vía correo electrónico
Nivel Informacional	<ul style="list-style-type: none"> - Situación: actividades de intercambio de información donde no se requiere ninguna acción. 	Comunicación: ✓ Vía correo electrónico

B. Mantenimiento correctivo:

- En caso se presenten fallas en la operatividad de los componentes de la solución, la DSNIRH realizará llamadas telefónicas y/o correos electrónicos solicitando la atención del incidente, dicha atención se brindará en la modalidad de disponibilidad de 24x7, es decir de lunes a domingo (incluidos feriados) durante las 24 horas del día, en el periodo de vigencia del contrato. Además del Contratista, las atenciones de soporte técnico deberán ser brindadas directamente por el fabricante en la modalidad 24x7 por el tiempo que dure el contrato.
- El tiempo máximo de respuesta inicial para la solución de incidentes reportados deberá ser de una (01) hora.
- La reparación de los equipos debe ser ejecutado a satisfacción de la Entidad, en el lugar donde estos se encuentren instalados y tomando en cuenta que el Tiempo Máximo de

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 13 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

Reparación será de cuarenta y ocho (48) horas. Se aceptará como forma de reparación, una reparación de tipo provisional en la cual, el Contratista proponga la instalación de equipos en la modalidad de “reemplazo temporal” siempre que estos sean de iguales características o superiores a los adquiridos y en las mismas condiciones de garantía y demás solicitados en las presentes especificaciones técnicas, lo cual será validado por la entidad. Cabe señalar que dichos equipos en la modalidad de “reemplazo temporal” serán reemplazados posterior a la reparación definitiva, previa coordinación con la DSNIRH a fin de no afectar la normalidad de las operaciones institucionales. Hay que considerar que, luego de notificado mediante correo electrónico el reemplazo por parte del fabricante aprobando las reparaciones se contabilizará las 48 horas como tiempo máximo.

- Para el cumplimiento de lo estipulado en el punto anterior, se entenderá como Tiempo Máximo de Reparación al tiempo transcurrido entre la comunicación al Contratista de la existencia del mal funcionamiento del/(los) equipo/(s) por parte de la Entidad beneficiaria (llamada telefónica de servicio y/o correo electrónico) y la reparación y puesta en funcionamiento del/(los) mismo(s) a satisfacción de la Entidad.
- El servicio de reparación será a satisfacción de la Entidad y en el lugar donde los equipos se encuentren instalados.
- El servicio de reparación incluirá: el reemplazo de las partes o componentes con desperfectos de fábrica por repuestos originales de fábrica o reemplazo del equipo por uno nuevo de iguales características a los solicitados en la presente especificación técnica. No incluye los desperfectos por uso inadecuado del equipo (golpes o derrame de sustancias líquidas), que se determinará en el diagnóstico realizado por los técnicos del Contratista.
- El Contratista no debe alegar inconvenientes con el fabricante para la obtención de los servicios mencionados, debiendo garantizar la posibilidad de escalamiento de los eventos en cualquier circunstancia.
- El Contratista brindará el servicio de reparación de los equipos con personal especializado del fabricante de los equipos ofertados, o en su defecto con su propio personal calificado que se encuentre debidamente certificado por el fabricante.
- A la suscripción del contrato, el Contratista deberá presentar el documento donde consigne los datos de la persona (Nombres y Apellidos, Teléfono y Correo Electrónico) con la cual realizará todas las coordinaciones administrativas, con la finalidad de llevar el control sobre la calidad del servicio brindado.
- A efectos de velar por el fiel cumplimiento del servicio de mantenimiento preventivo y correctivo, la DSNIRH revisará la información brindada por el Contratista y emitirá el informe de periodicidad anual donde se señale el control de llamada por servicios que tengan naturaleza de mantenimiento correctivo, cuantificando las horas de exceso en la atención. La cuantificación de los valores y las reglas serán de acuerdo con lo establecido en las especificaciones técnicas y de ser el caso se aplicarán las penalidades correspondientes.
- El Contratista deberá contar con un centro de atención de llamadas de reparación o asistencia técnica instalado, de tal manera que le asegure a la Entidad que se encuentra en condiciones de cumplir con lo estipulado.
- El servicio incluye la permanente actualización del software provisto, incluyendo el suministro de nuevas versiones (releases) y reparaciones (en general denominadas comercialmente como patches, temporary fixes, etc.).
- Ante cada notificación el Contratista debe realizar y presentar a la Entidad un correo electrónico conteniendo como mínimo la siguiente información:
 - Descripción detallada del problema, su causa y solución propuesta.
 - Personal que se asignó para la solución de este.
 - Problemas que se presentaron durante la solución.
 - Documentación adjunta de los cambios hechos.
 - Recomendaciones.
 - Fecha y hora de solución.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 14 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- Durante el periodo de la prestación accesoria, la entidad podrá solicitar al Contratista realizar cambios a las configuraciones de la solución adquirida bajo requerimiento, de forma ilimitada, durante el periodo establecido para la prestación accesoria (1095 días), en horario de disponibilidad de 24x7, es decir de lunes a domingo (incluidos feriados) durante las 24 horas del día, en el periodo de vigencia del contrato.
- El tiempo máximo de respuesta inicial para la atención de cambios a las configuraciones requeridas será de una (01) hora.
- La realización de cambios a las configuraciones requeridas de los equipos debe ser ejecutado a satisfacción de la Entidad, tomando en cuenta que el Tiempo Máximo de ejecución de cambios a las configuraciones requeridas que se establezca dependerá de la complejidad que requiera la atención del cambio requerido, el cual deberá ser informado previamente por el Contratista mediante correo electrónico y aprobado su Tiempo Máximo de ejecución por la DSNIRH para su ejecución, a fin de que dichas tareas no interfieran en el desarrollo de las actividades de la ANA.

6. CONSIDERACIONES GENERALES:

- ✓ El postor debe contar con un Network and Security Operation Center (NSOC) o similar (NOC o SOC), ubicado en Perú, desde donde se realizará el monitoreo a las soluciones propuestas. Se acreditará mediante una constancia firmada por el representante legal de la empresa y/o cliente donde se evidencie el servicio prestado. Se deberá presentar en la propuesta.
- ✓ A la suscripción del contrato, el Contratista deberá presentar un documento donde consigne los niveles de escalamiento de atención requeridos en la presente especificación técnica y/o los datos de las personas de contacto para todo caso de atención, con el contratista y/o la marca: Nombres y Apellidos (de corresponder), Teléfonos o Celulares y Correos Electrónicos; a fin de realizar todas las coordinaciones administrativas o técnicas, con la finalidad de llevar gestión sobre la calidad y atención de los requerimientos solicitados.
- ✓ El postor deberá presentar a la firma del contrato, una Carta dirigida a la Autoridad Nacional del Agua sustentada de forma adjunta con algún documento oficial o link de la página oficial del fabricante, en el que señale que el postor es Partner de la marca; el que lo autoriza a ofrecer lo detallado en las presentes especificaciones técnicas.
- ✓ Asimismo, el postor deberá presentar a la firma del contrato del presente requerimiento, una Declaración Jurada dirigida a la Autoridad Nacional del Agua, en el que señale que el personal propuesto cuenta con el conocimiento especializado necesario para el manejo y operación de la solución de seguridad perimetral ofertada detalladas en la presente EE.TT.
- ✓ Para el caso de renovación de equipamiento, cambio de equipos en desperfecto o RMA (Return Merchandise Authorization) sólo dicha actividad se realizará de forma presencial y por parte del Contratista, en la sede que se presente el desperfecto; para ello, a la firma del contrato, el Contratista deberá presentar una Carta de Compromiso donde garantiza que:
 - El Contratista dará cumplimiento a lo normado por la entidad aplicable a las actividades que desarrolle como Contratista, siendo el “Protocolo de seguridad, prevención de riesgos de contagio por COVID 19 y atención de salud de los servidores civiles de la entidad que retornan a laborar luego de culminada la emergencia nacional” (y sus posteriores adecuaciones) y lo normado por la Ley de Seguridad y Salud en el Trabajo.
 - El personal asignado por el Contratista, así como su personal clave, cuando asista a las instalaciones de la Autoridad Nacional del Agua, contará con el Seguro Complementario de Trabajo de Riesgo – SCTR actualizado, el cual deberá presentar previamente para su autorización de ingreso a las instalaciones, ante el personal designado por la DSNIRH para la supervisión del servicio.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 15 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- Contará durante las labores de servicio con los respectivos EPP'S.
 - El contratista cubrirá con todos los gastos y/o obligaciones del personal asignado al servicio que sufriera algún accidente producto de la ejecución de este. Esto último, en caso de asistir a las instalaciones de la Autoridad Nacional del Agua.
- ✓ Todos los equipos ofertados deben ser nuevos de fábrica, de primer uso, estar en perfectas condiciones de uso, no remanufacturados. En ningún caso, el postor podrá presentar soluciones con equipos que estén en la etapa de obsolescencia o que hayan anunciado su "end-of-life" o "end-of-sale" o "end-of-support" (fin de vida o fin de ventas o fin de soporte), o dejen de ser fabricados, comercializados y/o soportados durante los 4 años siguientes a la instalación de la solución de seguridad perimetral ofertada. Se deberá acreditar con carta de fabricante al momento de presentar la propuesta.
- ✓ Lo ofertado por el postor debe cumplir en su totalidad las especificaciones técnicas, conforme a lo señalado en el presente documento. Para ello, de manera obligatoria a la presentación de su propuesta, deberá incluir al lado derecho de cada especificación técnica solicitada, la captura de pantalla y el respectivo link del fabricante, donde se demuestre que cumple con cada especificación técnica solicitada en los apartados A, B y C de la Prestación Principal. El link del fabricante se refiere a toda información y/o publicación del fabricante a través de su página web, tales como catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales. Es de vital importancia para la institución constatar que el postor tiene pleno conocimiento de la oferta técnica que proponga, por lo que se obliga a documentar y sustentar cada una de las especificaciones técnicas solicitadas.
- ✓ La Autoridad Nacional del Agua se reserva el derecho de comprobar la veracidad, originalidad y cumplimiento, de toda la información incluida en la propuesta del Postor, a fin de aceptar o desestimar su propuesta.


DE LA PRESTACIÓN PRINCIPAL

De la solución de seguridad perimetral:

- Considerar el Centro de procesamiento de datos principal (CPDP) en la Calle Los Petirrojos 355 - San Isidro, Lima. De la misma forma, hay que considerar que el Centro de procesamiento de datos secundario es en la Calle Salaverry s/n, Cdra. 4, Cercado de Ica, Ica.
- La solución de infraestructura tecnológica estará debidamente licenciada contando con todos los feature habilitados.
- Recibida la solución de infraestructura tecnológica en sus centros de procesamiento de datos respectivamente, se procederá a realizar la validación técnica para la recepción correspondiente. De estar conforme, se suscribirá el Acta de recepción de la solución de seguridad perimetral. La cual será suscrita por el especialista por parte del Contratista y por el especialista por parte de la DSNIRH. Previa presentación de las guías de remisión, licencias y/o cualquier otro documento que certifique la entrega de la solución de infraestructura tecnológica.
- Posteriormente, el Contratista realizará la instalación, configuración, migración y capacitación de la solución de seguridad perimetral actual, cuyo objetivo traerá que el servicio se desarrolle de manera transparente. De estar conforme, se suscribirá el Acta de inicio del servicio de la solución de seguridad perimetral. La cual será suscrita por el especialista por parte del Contratista y el especialista por parte de la DSNIRH. Previa validación de la puesta en marcha y que los servicios tecnológicos operan de manera transparente para el usuario final.

DE LA PRESTACIÓN ACCESORIA

Mantenimiento preventivo y correctivo:

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 16 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- El servicio de mantenimiento preventivo y correctivo se computa desde el día siguiente de firmada el Acta de inicio del servicio de la solución de seguridad perimetral, cuyo servicio tiene una duración de 1095 días.

7. CONSIDERACIONES ESPECÍFICAS

7.1. DE LA EXPERIENCIA DEL CONTRATISTA EN LA ESPECIALIDAD

Requisitos. -

El postor debe acreditar un monto facturado acumulado equivalente a S/ 6' 000,000.00 (seis millones y 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) 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:

- Venta de equipamiento de firewall de última generación.
- Venta de equipamiento de seguridad perimetral.
- Venta de solución de seguridad perimetral
- Venta de licenciamiento para firewalls de seguridad informática.
- Venta de Firewall de seguridad perimetral.
- Venta de hardware de seguridad perimetral informática.
- Venta de implementación y soporte de firewalls de seguridad.
- Venta de soporte y/o licenciamiento de equipos de seguridad informática.
- Venta de renovación de soporte del equipo de seguridad perimetral - Firewall.
- Venta de soporte para los equipos de seguridad informática perimetral.
- Venta de solución de respuesta, automatización y orquestación de la seguridad.

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, 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 N° 8 referido a la Experiencia del Postor en la Especialidad.

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

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 17 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

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 contratistas 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 de 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 de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

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

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

7.2. DEL PERSONAL

Para la ejecución de la prestación principal, se requerirá del siguiente personal clave:

a. UN (01) JEFE DE PROYECTOS

i. Actividades:

Responsable de la gestión de la adquisición en general. Es el responsable de facilitar las coordinaciones entre el personal de la Entidad y el personal del Contratista, en merito a los trabajos de la adquisición, instalación, configuración, migración, capacitación de la solución de seguridad perimetral.

ii. Perfil:

▪ Formación Académica:

Ingeniero colegiado y habilitado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Computación y Sistemas o Ingeniería en Telecomunicaciones

Debe contar con certificación PMP e ITIL. Última versión y vigente.

Para la validación del presente requerimiento, a la firma del contrato, el postor deberá presentar la copia del diploma y certificaciones respectivas a fin de acreditar la formación académica requerida.

El Título profesional de Ingeniero será verificado 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/>.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 18 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

- Experiencia:
Experiencia mínima de cinco (05) años como: jefe y/o gerente y/o director y/o líder y/o coordinador y/o responsable, de proyectos de TI y que haya gestionado proyectos de tecnología de información.

La experiencia se computará desde la fecha de emisión del grado de bachiller.

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.

b. UN (01) ESPECIALISTA EN SEGURIDAD PERIMETRAL INFORMÁTICA

- Actividades:
Responsable de todas las actividades técnicas que correspondan al proceso de instalación, configuración, migración y mantenimiento de la solución de seguridad perimetral. Asimismo, será responsable de las actividades técnicas detalladas como parte del Mantenimiento preventivo y correctivo.

- Perfil:

- Formación Académica:
Ingeniero colegiado y habilitado en: Redes y Comunicación de Datos, o Computación, o Computación y Sistemas, o Informática, o Electrónica, o Telecomunicaciones, o Sistemas, o Sistemas y Cómputo.
Debe contar con certificación nivel profesional o ingeniero o experto, de la marca de los equipos a ser ofertados.
Debe contar con un curso o certificación ITIL. Última versión y vigente.
Debe contar con certificado en Lead CyberSecurity Professional Certification.

Para la validación del presente requerimiento, a la firma del contrato, el postor deberá presentar la copia del diploma y las certificaciones respectivas a fin de acreditar la formación académica requerida.

El Título profesional de Ingeniero será verificado 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: <https://titulosinstitutos.minedu.gob.pe/>, según corresponda.

- Experiencia:
Experiencia mínima de cinco (05) años en diseño de redes a nivel de seguridad perimetral y/o servicios de implementación y/o servicios de instalación similares al objeto de la contratación.

La experiencia se computará desde la fecha de emisión del grado de bachiller.

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 19 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

c. UN (01) ANALISTA EN OPERACIONES DE SEGURIDAD INFORMÁTICA

iii. Actividades:

Responsable de brindar asistencia técnica de apoyo a las actividades que correspondan al proceso de instalación, configuración, migración y mantenimiento de la solución de seguridad perimetral. Asimismo, será responsable de brindar asistencia técnica de apoyo a las actividades técnicas detalladas como parte del Mantenimiento preventivo y correctivo.

iv. Perfil:

▪ Formación Académica:

Técnico y/o bachiller y/o título profesional en: Redes y Comunicación de Datos, o Computación, o Computación y Sistemas, o Informática, o Electrónica, o Telecomunicaciones, o Sistemas, o Sistemas y Cómputo o Computación e informática.

Debe contar con certificación nivel profesional o ingeniero o experto, de la marca de los equipos a ser ofertados.

Debe contar con un curso o certificación ITIL. Última versión y vigente.

Opcionalmente, debe contar con un curso o certificación en ciberseguridad.

Para la validación del presente requerimiento, a la firma del contrato, el postor deberá presentar la copia del diploma y certificaciones respectivas a fin de acreditar la formación académica requerida.

El técnico y/o bachiller y/o título profesional de Ingeniero será verificado 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: <https://titulosinstitutos.minedu.gob.pe/>, según corresponda.

▪ Experiencia:

Experiencia mínima de dos (02) años en administración y/o servicios de implementación y/o servicios de instalación similares al objeto de la contratación.

La experiencia se computará desde la fecha de emisión del grado de bachiller o fecha de emisión del Título Técnico.

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.

8. ENTREGABLES

El contratista hará entrega de lo siguiente:

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 20 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

Prestación	Entregable
Principal	Entregable 1: A los cinco (05) días calendario, contados a partir del día siguiente de la suscripción del contrato. Consiste en la presentación del: Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral.
	Entregable 2: A los diez (10) días calendario, contados a partir del día siguiente de la suscripción del Acta de inicio del servicio de la solución de seguridad perimetral. Consiste en la presentación de: Informe técnico (en el cual deberá abordar mínimamente los puntos requeridos en el apartado que lo describe en las presentes EE.TT.), el Acta de recepción de la solución de seguridad perimetral y el Acta de inicio del servicio de la solución de seguridad perimetral.
Accesoría	Entregable 3: A partir de los 365 días calendario, previa conformidad de la DSNIRH. El entregable debe incluir el reporte del mantenimiento preventivo y correctivo (incluye las atenciones e incidentes, precisándose los tiempos y demás que permitan deslindar posibles penalidades).
	Entregable 4: A partir de los 730 días calendario, previa conformidad de la DSNIRH. El entregable debe incluir el reporte del mantenimiento preventivo y correctivo (incluye las atenciones e incidentes, precisándose los tiempos y demás que permitan deslindar posibles penalidades).
	Entregable 5: A partir de los 1095 días calendario, previa conformidad de la DSNIRH. El entregable debe incluir el reporte del mantenimiento preventivo y correctivo (incluye las atenciones e incidentes, precisándose los tiempos y demás que permitan deslindar posibles penalidades).

Los entregables deben ser presentados, dentro de los plazos establecidos, en la ventanilla de mesa de partes de la Autoridad Nacional del Agua, sito en la Calle Diecisiete N° 355 de la Urbanización el Palomar del distrito de San Isidro del departamento de Lima, o a través de la página web: www.ana.gob.pe en el link trámite virtual.

9. PLAZO Y LUGAR DE ENTREGA

9.1. PLAZO DE ENTREGA DE LA PRESTACIÓN PRINCIPAL

El plazo de la prestación principal será realizado según el siguiente cuadro:

Prestación principal	Cantidad	Plazo de entrega	Lugar de entrega	Plazo de revisión	Supervisión y Conformidad Técnica
Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral	1	5 días calendario, contabilizados desde el día siguiente de suscrito el contrato	CPDP	10 días calendario	Estará a cargo de la DSNIRH
Gestores del perímetro	4	45 días calendario, contabilizados	CPDP y CPDS		

	FORMATO		Código : SGC-F-006
	ESPECIFICACIONES TÉCNICAS		Versión : 00
			Aprobado por : DSNIRH
			Fecha aprob. : Julio 2024
			Página : 21 de 30
			Año : 2024

Gestores centralizados	4	desde el día siguiente de suscrito el contrato.			
Gestores de eventos y reportes	2				
Instalación y configuración de la solución de seguridad perimetral	1	30 días calendario, contabilizados desde el día siguiente de firmada el Acta de recepción de la solución de seguridad perimetral	Lugar designado por el Contratista en su propuesta técnica		
Capacitación	1				

9.2. PLAZO DE LA PRESTACIÓN ACCESORIA

El plazo de la prestación accesoria será realizado según el siguiente cuadro:

Prestación accesoria	Cantidad	Plazo de entrega	Lugar de entrega	Plazo de revisión	Supervisión y Conformidad Técnica
Mantenimiento preventivo y correctivo	1	1095 días calendarios, contabilizados desde el día siguiente de firmada el Acta de inicio del servicio de la solución de seguridad perimetral	CPDP y CPDS	10 días calendario	Estará a cargo de la DSNIRH

9.3. LUGAR DE ENTREGA DE LA PRESTACIÓN PRINCIPAL Y ACCESORIA

La entrega de la solución de seguridad perimetral (prestación principal), se realizará en las instalaciones de: i) el Centro de Procesamiento de Datos Principal (CPDP), sito en calle Diecisiete N° 355, Urb. El Palomar, San Isidro – Lima, al área usuaria (DSNIRH), ii) Centro de Procesamiento de Datos Secundario (CPDS), sito en Calle Salaverry s/n – Ica y iii) las licencias serán entregadas al área usuaria (DSNIRH) vía correo electrónico a la siguiente dirección: infraestructura_dsnirh@ana.gob.pe

El mantenimiento preventivo y correctivo (prestación accesoria), será de forma remota al Centro de Procesamiento de Datos Principal (CPDP) ubicado en Calle Diecisiete N° 355, Urb. El Palomar, San Isidro - Lima, Perú y al Centro de Procesamiento de Datos Secundario (CPDS) ubicado en Calle Salaverry s/n – Ica; con la excepción del cambio de equipos en desperfecto o RMA (Return Merchandise Authorization) dicha actividad se realizará de forma presencial y por parte del Contratista en la sede que se presente el desperfecto que son:

- Dirección del Sistema Nacional de Información de Recursos Hídricos de la Autoridad Nacional del Agua, sito Calle Diecisiete N° 355, Urb. El Palomar, San

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 22 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

Isidro - Lima, Perú, sede del Centro de Procesamiento de Datos Principal (CPDP)

- Dirección del Sistema Nacional de Información de Recursos Hídricos de la Autoridad Nacional del Agua, sito Calle Salaverry s/n – Ica, sede del Centro de Procesamiento de Datos Secundario (CPDS)

10. SISTEMA DE CONTRATACIÓN

El sistema de contratación tanto para la prestación principal como para la prestación accesoria será a Suma Alzada.

11. MODALIDAD DE EJECUCIÓN CONTRACTUAL

Contrato Llave en Mano.

12. ADELANTOS

No corresponde

13. SUPERVISIÓN Y CONFORMIDAD DE LA CONTRATACION

- La supervisión de la ejecución del servicio estará a cargo del personal profesional de la Dirección del Sistema Nacional de Información de Recursos Hídricos (DSNIRH) de la ANA.
- La conformidad será otorgada por la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión.

La DSNIRH otorgará la conformidad dentro de un plazo no mayor a diez (10) días, después de presentados los respectivos entregables que correspondan.

14. FORMA DE PAGO

Prestación	Pago	Monto de pago	
Principal	Pago 1	<u>El 70% del monto total del contrato.</u>	Pago 1: Posterior a la presentación del Entregable N° 02 que incluye el Informe Técnico, Acta de recepción de la solución de seguridad perimetral y el Acta de inicio del servicio de la solución de seguridad perimetral.
Accesoria	Pago 2	<u>El 10% del monto total del contrato.</u>	Pago 2: Posterior a la presentación del Entregable N° 03 que incluye el informe técnico del servicio mantenimiento. A partir de los 365 días calendarios, previa conformidad de la DSNIRH.
	Pago 3	<u>El 10% del monto total del contrato.</u>	Pago 3: A la presentación del Entregable N° 04 que aborda el servicio de mantenimiento. A partir de los 730 días calendarios, previa conformidad de la DSNIRH
	Pago 4	<u>El 10% del monto total del contrato.</u>	Pago 4: A la presentación del Entregable N° 05 que aborda el servicio de mantenimiento. A partir de los 1095 días calendarios, previa conformidad de la DSNIRH

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 23 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

Asimismo, y a efectos de que la Entidad pueda realizar el pago de la contraprestación pactada a favor del contratista, previa conformidad de los entregables otorgado por parte de la Dirección del Sistema Nacional de Información de Recursos Hídricos, el contratista deberá presentar las facturas respectivas.

15. PENALIDAD

Si el contratista incurre en retraso injustificado en los plazos establecidos de las prestaciones principales y/o accesorias objeto del contrato, la Autoridad Nacional del Agua le aplicará en cada caso de retraso, una penalidad por cada día calendario de retraso, hasta por un máximo equivalente al diez por ciento (10%) del monto de la compra, la penalidad se aplicará automáticamente y se calculará 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 tiene los siguientes valores:

Plazos menores o iguales a sesenta (60) días: F = 0.40
Para plazos mayores a sesenta (60) días: F = 0.25

Cuando se llegue a cubrir el monto máximo de la penalidad la Autoridad Nacional del Agua, podrá resolver el contrato parcial o totalmente por incumplimiento mediante carta notarial.

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.

16. OTRAS PENALIDADES:

La ANA aplicará otras penalidades, distintas a la penalidad por mora, cuando el Contratista se encuentre inmerso en cualquiera de los siguientes supuestos:

SUPUESTOS DE APLICACIÓN	PENALIDAD	PROCEDIMIENTO
Por no presentar el “Plan de instalación, configuración, migración, capacitación y mantenimiento de la solución de seguridad perimetral”, dentro de los plazos establecidos.	<div>P = 0.2 x UIT x D</div> <p>Donde: P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. D: Cantidad de Días de atraso.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.
Por exceder el tiempo máximo de atención inicial de la respuesta avanzada a incidentes activados, respecto a lo señalado en el apartado de Monitoreo y respuesta avanzada a incidentes. La penalidad se aplicará en cada caso de incumplimiento.	<div>P = 0.1 x UIT x M</div> <p>Donde: P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. M: Cantidad de Minutos atrasados.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 24 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

		ejecutar la penalidad correspondiente.
Por incumplimiento de los SLA de disponibilidad, respecto a lo señalado en los apartados de mantenimiento preventivo y correctivo. La penalidad se aplicará en cada caso de incumplimiento.	$P = 1.0 \times UIT \times D$ <p><u>Donde:</u> P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. D: Cantidad de Días de atraso.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.
Por exceder el tiempo máximo de respuesta inicial para la solución de incidentes reportados, respecto a lo señalado en el apartado de mantenimiento correctivo. La penalidad se aplicará en cada caso de incumplimiento.	$P = 0.1 \times UIT \times H$ <p><u>Donde:</u> P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. H: Cantidad de Horas de atraso.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.
Por exceder el tiempo máximo de reparación, respecto a lo señalado en el apartado de mantenimiento correctivo. La penalidad se aplicará en cada caso de incumplimiento.	$P = 0.3 \times UIT \times H$ <p><u>Donde:</u> P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. H: Cantidad de Horas de atraso.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.
Por exceder el tiempo máximo de respuesta inicial para la atención de cambios a las configuraciones requeridas, respecto a lo señalado en el apartado de mantenimiento correctivo. La penalidad se aplicará en cada caso de incumplimiento.	$P = 0.1 \times UIT \times H$ <p><u>Donde:</u> P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento. H: Cantidad de Horas de atraso.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.
Por utilizar y/o difundir, de manera indebida y sin autorización, a terceros la información relativa al presente requerimiento. La penalidad se aplicará en cada caso de incumplimiento.	$P = 0.2 \times UIT$ <p><u>Donde:</u> P: Penalidad UIT: Unidad Impositiva Tributaria en la fecha en que suscitó el incumplimiento.</p>	El área usuaria remitirá un informe indicando el evento ocurrido a la Oficina de Administración – Unidad de abastecimiento y patrimonio a fin de ejecutar la penalidad correspondiente.

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra el monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (02) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 25 de 30 Año : 2024

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso; la ANA puede resolver el contrato por incumplimiento.

17. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por vicios ocultos del bien ofertado por el plazo de un (01) año, contado a partir de la conformidad otorgada por LA ENTIDAD.

18. CONFIDENCIALIDAD:

El Contratista está obligado a mantener la confidencialidad de la información recibida a raíz de la presente relación contractual y/o toda la información, análisis y conclusiones contenidas en sus informes u otros documentos, durante el plazo de ejecución contractual y hasta dentro del plazo de cuatro (04) años desde la recepción de la conformidad final del bien, a menos que cuente con un pronunciamiento escrito de la ANA en sentido contrario.

19. PROPIEDAD INTELECTUAL:

El Contratista cede a favor del ANA, cualquier tipo de derechos generados como consecuencia de la elaboración de los informes, opiniones, documentos generados, que son materia del presente termino de referencia, en el marco de la Ley N° 822, Ley sobre derecho de autor. Asimismo, se compromete a no utilizarlos para fines distintos a los de la prestación realizada, ni durante su ejecución ni después de la recepción de este, sin que medie autorización escrita otorgada por ANA.


20. CESIÓN DE DERECHOS:

Por medio de la presente clausula, el Contratista cede los derechos patrimoniales de los cuales sea titular sobre el programa de ordenador o software producido o desarrollo en ejecución del presente contrato, para su explotación no exclusiva, ilimitada, perpetua y con alcance mundial, para cualquier uso, pretendiendo actualmente y en el futuro a favor de la Autoridad Nacional del Agua - ANA. Esta cesión de derechos comprende, mas no se limita, a los derechos de reproducción, comunicación al público, distribución, traducción, modificación, u otra transformación, importación al territorio nacional de copias por cualquier medio incluyendo la transmisión, así como cualquier otra forma de utilización que no estén contempladas en la ley de la materia como excepción al derecho patrimonial y, en general, para cualquier tipo de utilización y explotación, que la entidad estime pertinentes, pudiendo ponerlo a disposición por medio de autorizaciones o licencias a favor del público en general. Sin perjuicio de otras obligaciones a su cargo, el Contratista deberá entregar una versión final del software incluyendo el código fuente, código objeto, documentación técnica y manuales, sin ninguna medida tecnológica efectiva ni sistema de autotutela, sin contraseña ni restricción. Lo dispuesto en relación con los programas de ordenador o software no se aplicará cuando la entidad pública sea solo licenciataria del software.”

21. COMPROMISO ANTICORRUPCIÓN

Se le informa por medio del presente que la ANA en cumplimiento con la norma NTP-ISO 37001:2017 ha implementado y mantiene un Sistema de Gestión Antisoborno, que prohíbe el soborno mediante el establecimiento de procedimientos y directivas que guían el comportamiento de todos colaboradores y Contratistas que tengan relación contractual con la ANA.

Por lo expuesto y en cumplimiento del Decreto Supremo N° 092-2017-PCM que aprueba la Política Nacional de Integridad y Lucha contra la Corrupción, el Contratista del servicio se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad, cumplir con los lineamientos del Sistema de Gestión de Antisoborno de

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 26 de 30 Año : 2024

ANA y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de los socios, accionistas, integrantes de los Órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

La ANA dispone de un canal de denuncias que permite al Contratista reportar el intento, sospecha o comisión de un acto de soborno o cualquier incumplimiento del Sistema de Gestión Antisoborno, asimismo se garantiza la confidencialidad de las denuncias y comunicaciones recibidas, así como la protección de cualquier tipo de amenaza o coacciones mediante la aplicación de la normativa vigente sobre defensa al denunciante, todo ello con respecto a los derechos de legítima defensa.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024
	ESPECIFICACIONES TÉCNICAS	Página : 27 de 30 Año : 2024

REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 6' 000,000.00 (seis millones 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.</p> <p>Se consideran bienes similares a los siguientes:</p> <ul style="list-style-type: none"> ▪ Venta de equipamiento de firewall de última generación. ▪ Venta de equipamiento de seguridad perimetral. ▪ Venta de solución de seguridad perimetral ▪ Venta de licenciamiento para firewalls de seguridad informática. ▪ Venta de Firewall de seguridad perimetral. ▪ Venta de hardware de seguridad perimetral informática. ▪ Venta de implementación y soporte de firewalls de seguridad. ▪ Venta de soporte y/o licenciamiento de equipos de seguridad informática. ▪ Venta de renovación de soporte del equipo de seguridad perimetral - Firewall. ▪ Venta de soporte para los equipos de seguridad informática perimetral. ▪ Venta de solución de respuesta, automatización y orquestación de la seguridad. <p><u>Acreditación:</u></p> <p>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 pago¹, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>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.</p> <p>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.</p>

¹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 28 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

	<p>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 Contratistas 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 de que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>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.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <div> <p>Importante</p> <p><i>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 Contratistas en Consorcio en las Contrataciones del Estado”.</i></p> </div>
--	--

“... 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”.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 29 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

C	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p>➤ <u>UN (01) JEFE DE PROYECTOS</u></p> <p><u>Requisitos:</u> Experiencia mínima de cinco (05) años como: jefe y/o gerente y/o director y/o líder y/o coordinador y/o responsable, de proyectos de TI y que haya gestionado proyectos de tecnología de información.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>La experiencia se computará desde la fecha de emisión del grado de bachiller.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p>➤ <u>UN (01) ESPECIALISTA EN SEGURIDAD PERIMETRAL INFORMÁTICA</u></p> <p><u>Requisitos:</u> Experiencia mínima de cinco (05) años en el diseño de redes a nivel de seguridad perimetral y/o servicios de implementación y/o servicios de instalación similares al objeto de la contratación.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>La experiencia se computará desde la fecha de emisión del grado de bachiller.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p>➤ <u>UN (01) ANALISTA EN OPERACIONES DE SEGURIDAD INFORMÁTICA</u></p> <p><u>Requisitos:</u> Experiencia mínima de dos (02) años en administración y/o servicios de implementación y/o servicios de instalación similares al objeto de la contratación.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>La experiencia se computará desde la fecha de emisión del grado de bachiller o fecha de emisión del Título Técnico.</p>

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : Julio 2024 Página : 30 de 30 Año : 2024
	ESPECIFICACIONES TÉCNICAS	

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

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

- *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.*