

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 1 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

ESPECIFICACIONES TÉCNICAS **ADQUISICIÓN DE SOFTWARE PARA LA COLECCIÓN DE EVENTOS Y** **DETECCIÓN DE AMENAZAS AVANZADAS DE LA RED PARA LA** **AUTORIDAD NACIONAL DEL AGUA**

CÓDIGO SIGA: 14.04.000.32821

1. FINALIDAD PÚBLICA:

La Dirección del Sistema Nacional de Información de Recursos Hídricos, como área técnica es la encargada de determinar las especificaciones técnicas de los bienes tecnológicos, con la finalidad de la operatividad de la infraestructura informática en la Autoridad Nacional del agua por lo que la presente adquisición tiene por finalidad contar con una solución que permita recolectar eventos y detección de amenaza avanzada de los servidores y equipamiento TIC, permitiendo garantizar la disponibilidad, confidencialidad e integridad de los servicios informáticos.

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 Autoridad Nacional del Agua (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.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 2 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

En ese marco, es necesario implementar a la Autoridad Nacional del Agua, una solución tecnológica la cual debe permitir la protección antimalware y contra software malicioso. La misma que debe ofrecer una seguridad integrada y proactiva que bloquee el malware y las amenazas de día cero y permita proteger los equipos dentro y fuera de la red, con una gestión centralizada basada en directivas y funciones de control, contribuyendo a proteger los equipos e información almacenada en los mismos.

3. JUSTIFICACIÓN:

El Reglamento de Organización y Funciones de la ANA, aprobado mediante Decreto Supremo N° 018-2017-MINAGRI, del 13 de diciembre del 2017, establece en su art. 44º diversas funciones a la Dirección del Sistema Nacional de Información de Recursos Hídricos, estableciéndose en el literal e): “Conducir, formular, implementar y realizar el seguimiento de políticas, planes y normas sobre tecnologías de la información, servicios informáticos, licenciamiento, uso de software, correo electrónico e internet; así como brindar atención y asesoría en cuanto a requerimientos, adquisición, soporte y mantenimiento de materiales, equipos computacionales, periféricos y de comunicación de la Autoridad Nacional del Agua”.

Que, para el cumplimiento de metas y objetivos institucionales resulta necesario la adquisición de una solución recolectora de eventos y detección de amenazas para la Autoridad Nacional del Agua, a fin de recolectar los registros de los servidores y equipamiento TIC, para analizar la infraestructura tecnológica del ANA y garantizar la disponibilidad, confidencialidad e integridad de los servicios informáticos, según lo programado dentro del Plan Operativo Institucional.

Asimismo, es necesario también disponer de una solución que nos permita la administración de eventos e información de seguridad. Esta solución de seguridad ayudará a la Autoridad Nacional del Agua – ANA a detectar y analizar amenazas y responder rápidamente antes de que afecten a las operaciones cotidianas de la entidad.

4. OBJETIVO:

La Autoridad Nacional del Agua a través de la Dirección del Sistema Nacional de Información de Recursos Hídricos – DSNIRH, requiere la adquisición de una solución recolectora de eventos y detección de amenazas avanzadas, con la finalidad de permitir dar visibilidad de las actividades de todos los equipos de la infraestructura TIC (Tecnologías de la Información y Comunicación, así como la de detectar y mitigar ataques informáticos.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 3 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

5. ESPECIFICACIONES TÉCNICAS MÍNIMAS:

SOLUCIÓN PARA LA COLECCIÓN DE EVENTOS DE RED	
ESPECIFICACIÓN	DETALLE
Generalidades de la Solución	<ul style="list-style-type: none"> La solución deberá ser enfocada totalmente en seguridad. No se aceptará soluciones que no se centren en seguridad o que la seguridad sea solo un módulo adicional y tampoco basadas en OpenSource a excepción de la base de datos de la solución, de la cual se aceptará que dicha solución cuente con una base de datos de código abierto siempre y cuando el proveedor garantice la seguridad de la misma a través de los controles de seguridad que proporcione la solución SIEM. La solución deberá estar preparada para soportar 1400 dispositivos entre equipos de cómputo y de infraestructura, tales como: PC's, Impresoras, switches, servidores, firewalls, entre otros. La solución deberá soportar desde un inicio 3000 EPS. La solución debe incluir licencias para 1,400 agentes o similar que permita: <ul style="list-style-type: none"> ✓ Recopilar registros de seguridad, aplicación y rendimiento de Windows ✓ Recopilar registros de DHCP/DNS, registros de sysmon ✓ Detectar cambios en el registro ✓ Detectar lectura, escritura y edición de archivos con el contexto del usuario para Windows o Linux ✓ Detectar inserción, eliminación, lectura y escritura de medios extraíbles Se debe considerar la creación de 20 casos de uso al inicio de la prestación y 20 casos de uso adicionales que se podrán implementar durante el periodo de la prestación. Las afinaciones de los casos de uso deben de estar contemplado dentro de la prestación sin costo adicional para entidad. La solución no debe tener Flash en ninguno de sus componentes críticos. Está demostrada ampliamente la falencia de seguridad de Flash. La solución deberá almacenar sus datos en una solución de Base de Datos como PostgreSQL o en solución de BigData o en Elasticsearch o ClickHouse, no se aceptará el uso de una única base de datos SQL. La solución deberá contar 200 licencias de UBA o UEBA que permita con algoritmos avanzados de Machine Learning incluidos en un módulo de User Behavior Analytics (UBA o UEBA) con el objetivo de monitorear el comportamiento de los usuarios de la red de la entidad y clasificarlos según el perfil de riesgo. El módulo/licencia de UBA o UEBA deberá trabajar en base a una integración con LDAP y/o Active Directory y/o detectar

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 4 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<p>usuario-grupo, de tal forma que se pueda relacionar las cuentas con identidades de usuario.</p> <ul style="list-style-type: none"> • El módulo/licencia de UBA o UEBA debe establecer patrones de comportamiento base de endpoint / servidor / usuario / granularidad de la hora, debe incluir disparadores incorporados y personalizables sobre anomalías de comportamiento. • El módulo/licencia de UBA o UEBA debe informar como mínimo los siguientes eventos de actividad del usuario: <ul style="list-style-type: none"> ✓ iniciar/cerrar sesión ✓ carga y descarga de archivos ✓ montaje y desmontaje de la unidad • La solución deberá soportar Feeds de Threat Intelligence del mismo fabricante, de tal forma que se pueda crear reglas de correlación para detectar y alertar algún evento o incidente que se suscite relacionado a indicadores de compromiso (IOC) maliciosos. • La solución debe ser capaz de ofrecerse en su totalidad como software, eso incluye, máquinas virtuales (*). • La solución deberá disponer de un sitio web en donde se pueda descargar casos de uso adicionales ya armados o que descargue automáticamente casos de uso directo del servicio de inteligencia de amenazas del fabricante. Estos casos de uso deben ser posible modificarlos a gusto. • Deberá tener una arquitectura modular, es decir con componentes dedicados para la colección y procesamiento de eventos independientes del motor de correlación (*). • La solución debe tener la capacidad de registrar actividades dentro de toda la red de datos de la entidad, sin discriminar la totalidad de segmentos preexistentes. Así mismo las actividades a registrar y/u ocurrencias deben ser: accesos a terminales de cómputo (estaciones y servidores), a nivel nacional (sede central y órganos desconcentrados) de uso de servicios de red (logueos a estaciones (dominio y red local), ejecución de impresiones (opcional), acceso a recursos compartidos entre estaciones, así como el acceso a toda información institucional) <p><i>(*) La Entidad (ANA) proporcionará de acuerdo con un criterio de optimización de recursos, las máquinas virtuales necesarias (ya sea en las sedes de Lima, en Ica o ambas) para que el proveedor pueda instalar el software, en caso así lo considere. Se precisa que la solución para la colección de eventos de red podrá ser on premise o en nube; sin embargo, como mínimo su colector deberá ser on premise.</i></p>
Modo de licenciamiento	<ul style="list-style-type: none"> • El licenciamiento deberá estar incluido en la prestación y soportar el crecimiento indicado.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 5 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> El licenciamiento deberá estar incluido en la prestación y de darse un crecimiento en la demanda de licencias de la Entidad, se procederá a hacer una adenda.¹
Destinos de colección	<ul style="list-style-type: none"> Los conectores que se encargan de la colección de eventos deberá enviarlos al motor de correlación para luego almacenarlos durante al menos 1 año en el componente específico que forme parte de la arquitectura de la solución SIEM.
Características de conectores o colectores	<ul style="list-style-type: none"> Deberá tener la capacidad de incorporar campos personalizados, además de los que ya trae la normalización, sin afectar considerablemente el storage. Los componentes que realizan la recolección de datos (conectores) deberán enviar los eventos hacia el SIEM a implementar, a través del protocolo de transporte TCP y con técnicas de cifrado y autenticación SSL (Secure Sockets Layer). No se permite el uso de protocolo Syslog/Syslog-ng TCP ni UDP para el envío de eventos de conectores hacia dicho SIEM. Opcionalmente, se permite el uso de protocolo Syslog/Syslog-ng TCP o UDP para el envío de eventos de conectores hacia dicho SIEM.² para el envío de eventos de conectores hacia dicho SIEM Los conectores de eventos remotos o distribuidos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia el SIEM, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos. Los conectores de eventos deberán enriquecer mediante categorías o parsear los eventos obtenidos en los componentes de recolección a fin de permitir la comprensión y el significado del evento, sin la necesidad de tener conocimiento previo de la bitácora. Opcionalmente, la solución de correlación debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes: <ul style="list-style-type: none"> ✓ Debe soportar Regex o XML para el parsing de eventos. ✓ Bases de datos relacionales por conexión ODBC o JDBC ✓ Traps de protocolo SNMP ✓ Eventos enviados por protocolo Syslog ✓ Neflow o archivos con formato XML La solución debe incluir un mecanismo para integrar las fuentes no soportadas en forma nativa, tales como los desarrollos hechos en casa, al menos, para los orígenes de datos más sencillos

¹ Modificado referida a la consulta 94 del postor SECURESOFT CORPORATION S.A.C

² Modificado referida a la consulta 98 del postor SECURESOFT CORPORATION S.A.C

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 6 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> • Los conjuntos de herramientas para definir la lógica para extraer, obtener, normalizar y categorizar los eventos a correlacionar por la solución deberán usar expresiones regulares o REGEX o XML para definir patrones de búsqueda de cadenas de texto. • Los componentes que realizan la recolección de eventos deberán realizar desde el origen la normalización completa de los eventos, es decir únicamente enviarán hacia el SIEM los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporte de los eventos. • No se acepta la normalización en un dispositivo que no esté encargado de recolectar • Los componentes que realizan la recolección de eventos podrán bajo demanda preservar el campo en crudo (raw data) o podrán realizar buffer de eventos, en adición al evento previamente normalizado. • La solución debe tener la capacidad de validar la integridad de los eventos a través del uso de algoritmos checksum o algoritmos criptográficos (opcional). • Los componentes que realizan la recolección de eventos deberán utilizar el protocolo TCP como medio de transporte hacia la solución de correlación, verificando constantemente el estado de la conexión por medio de un pulso o “Heartbeat” o verificación de salud. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache. • Los componentes que realizan la recolección de eventos podrán incluir atributos o agregar etiquetas en campos adicionales sobre los eventos con información proveniente de la configuración, tales como información de la red, unidad de negocio, que favorezca y optimice el proceso de correlación de eventos. • Los componentes que realizan la recolección y la correlación de eventos deberán estar en alta disponibilidad activo-pasivo o contar con un componente adicional para activar como contingencia en caso de falla del componente activo, de tal forma que se garantice la disponibilidad e integridad de los eventos almacenados. • La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación deberán utilizar mecanismos de compresión de datos. La agregación de datos no se considera similar a la compresión de los datos. • Opcionalmente, la solución debe permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados. Esto no debe ser realizado con tecnología VPN por ningún motivo.
--	--

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 7 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> La capacidad de filtrado es a nivel de colección, no de búsqueda (opcional). Los componentes que realizan la recolección de eventos tendrán la capacidad de administración y actualización remota, sin la necesidad de realizar cambios, ajustes o actualizaciones directamente en el componente. La solución deberá operar con los métodos nativos de auditoría, logs y eventos de cada plataforma/dispositivo/aplicación. Esta recolección debe ser no invasiva, y no debe implicar instalar agentes en todos los equipos (salvo excepciones como SO Windows). No se aceptará por ningún motivo la implementación únicamente de técnicas de interpretación de tráfico, debido a su conocido problema de pérdida de datos en reconstrucción de sesiones. El software de conectores deberá ser soportado para su instalación en plataformas Microsoft Windows, RedHat Enterprise Linux o Centos y podrán ser instalados en servidores físicos o virtuales Todos los conectores deben ser construidos por la misma marca que el resto de los productos, que incluyan normalización en la etapa de colección. Por ningún motivo se aceptará soluciones de recolección construidas bajo OpenSource, ni por comunidades de usuarios abiertas a clientes y otros usuarios que no sean de la marca." Todos los conectores deben trabajar con la normalización y categorización de los eventos recibidos. Ambos procesos deben ocurrir en la recolección, y no se aceptará interpretar etiquetas como si fuesen categorías. Los conectores deberán ser los encargados de realizar normalización antes de enviar los datos a otros componentes (pudiendo ser uno o más componentes desde un único conector) Las reglas de correlación deben poder construir en forma gráfica, en donde se puede seleccionar los campos obtenidos en la normalización y unirlos por medio de conectores lógicos. En ningún caso se interpretará búsquedas de datos a demanda como si fuesen reglas de correlación.
Formatos soportados	<ul style="list-style-type: none"> La solución de correlación de eventos ofrecida deberá ser integrable "fuera de la caja" (out-of-the-box) como mínimo con más de 270 dispositivos/aplicaciones lo cual evitará tener personal dedicado a la modificación de los formatos de logs, mediante componentes denominados conectores/colectores.

DETECCIÓN DE AMENAZAS AVANZADAS DE RED	
ESPECIFICACIÓN	DETALLE
Infraestructura	<ul style="list-style-type: none"> La solución deberá de presentarse en un esquema SaaS. La solución es administrada en su totalidad (agentes, políticas, reportes, etc.) mediante una única consola web (https).

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 8 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> • La solución deberá estar preparada para soportar 1400 dispositivos equipos de cómputo (computadoras y servidores). • La solución deberá de contar con un SLA de disponibilidad de la plataforma mínimo del 99.9%. • La solución deberá de poder soportar mecanismos que refuercen el acceso a la consola por medio de un segundo factor de autenticación (2FA). • La comunicación entre el sensor y la nube deberá de ejecutarse a través del uso de un puerto seguro y cifrado. • La solución deberá de contar con integración a sistemas de inteligencia, a través del uso de APIs. • La solución puede generar usuarios con privilegios limitados a su perfil de operación como lo pueden ser auditores, administradores de plataforma, usuarios de soporte técnico, etc. • La solución puede clasificar a los agentes/clientes basados en criterios internos como lo son sistema operativo, unidad de negocio o grupo, nombre o segmento de subred. • La información deberá de vivir en la nube por lo menos 90 días. • Las alertas o eventos deberán de tener un periodo de retención mínimo de 90 días. • La solución deberá contar con la capacidad de realizar acciones de seguridad (pudiendo ser mediante un sistema de inteligencia artificial y Machine Learning acompañado de expertos de seguridad en la nube, u otras acciones de seguridad) pensado por el fabricante, a fin de contar con una nube de Inteligencia que permita una interacción de colaboración de seguridad con los componentes de la solución, para poder hacer la detección de amenazas avanzadas. • La solución deberá de ser multiplataforma, soportando los siguientes sistemas operativos: <ul style="list-style-type: none"> ✓ Windows <ul style="list-style-type: none"> - Desktop: Windows 7/ Windows 8 (opcional) / Windows 8.1 (opcional) / Windows 10 / Windows 11. - Server: 2008 SP1 (opcional) / 2008 R2 SP2/ 2012 / 2012 R2/ 2016/ 2019/ 2022. ✓ Mac <ul style="list-style-type: none"> - macOS: 10.11 (opcional)/ 10.12 (opcional) / 10.14/ 10.15 / 12.2 / 12.4 / 13. ✓ Linux <ul style="list-style-type: none"> - RHEL/CentOS: 6.8 - 6.10 (opcionales) / 7.2 – 7.7 (opcionales)/ 7.8 - 7.9 / 8.0 – 8.5 - SUSE Linux: 12 SP5 / 15 (opcional) / 15 SP3 (opcional) - Open SUSE:15.2 (opcional) – 15.3 (opcional) - Ubuntu: 16.04 / 18.04 / 20.04 - Oracle Linux: 6.10 (opcional) / 7.7 – 7.8 (opcionales) / 7.9 (opcional) / 8.2 – 8.4 - Amazon Linux: 2" (opcional) • La solución propuesta debe permitir agregar automáticamente direcciones IP maliciosas detectadas en uno o más firewalls
--	---

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 9 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<p>remotos integrados, ya sea a través de API u otro método de integración.</p> <ul style="list-style-type: none"> • La solución debe tener la capacidad de creación de playbooks y/o Push Operations y/o plantillas de flujo de trabajo con el objetivo de automatizar las capacidades de detección y respuesta. • La solución propuesta debe tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria o "file operations" que permitan la realización de procesos forenses. • La solución propuesta debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos manteniendo la disponibilidad del dispositivo considerando que, también se aceptará la posibilidad de que la solución propuesta lo pueda realizar mediante la ejecución de escaneos de seguridad programados o en periodos específicos configurados por el administrador. • La instalación del agente deberá de poder hacerse a través de una invitación de correo electrónico. • La solución deberá de incluir la capacidad de descargar un paquete de instalación para los diferentes sistemas operativos con el fin de crear un paquete de instalación silenciosa. • La solución deberá de usar un sensor para administrar y proteger los equipos, pudiendo ser este a través del agente instalado en el end-point • La solución deberá de poder controlar la instalación del sensor a través de códigos o contraseña, de esta forma previniendo el abuso en la instalación de dispositivos no autorizados. • La desinstalación del agente deberá de requerir un código o contraseña para que no lo puedan desinstalar los usuarios. • La solución deberá de contener una bitácora con fines de auditar las actividades y cambios realizados en la consola. • La bitácora de auditoria no deberá poder ser modificada, incluso por administradores de la solución. • La bitácora de auditoría deberá de tener una retención de al menos 90 días.
Compatibilidad con vSphere	<ul style="list-style-type: none"> • La solución deberá de poder proteger servidores (Workloads). • La solución deberá de generar un inventario de forma automática. El inventario de todas las máquinas, indicando cuales equipos están protegidos y cuáles no. También se podrá aceptar mediante la muestra de todos los endpoint administrados y protegidos por la solución propuesta, ello dentro de la consola de administración. • La solución deberá de proporcionar visibilidad de las vulnerabilidades o comunicaciones de aplicaciones vulnerables en los servidores (Workloads) protegidos y/o la visualización de registros o eventos que muestren ataques o intentos de ataques sobre los endpoint protegidos. • La solución deberá de generar un tablero que indique el estado del agente de seguridad por cada máquina virtual.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 10 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> • La solución deberá tener la opción de permitir que los sensores en equipos Linux se comuniquen con la nube a través de un proxy, pudiendo este último ser parte de la solución a ofertarse • Protección contra amenazas (Aplica para Endpoints y servidores). • La solución puede ser configurada para que las políticas y/o reglas de seguridad apliquen a un grupo en particular de agentes/clientes (Granularidad). • La solución deberá de identificar actividades maliciosas en base en el análisis de comportamiento de los siguientes eventos: <ul style="list-style-type: none"> ✓ Carga de módulos o ejecución de ejecutables ✓ Modificación de archivos ✓ Modificación de llaves de registro ✓ Conexiones de red ✓ Procesos ✓ Metadata • La solución deberá de contar con un registro de los malware encontrados. • La solución deberá poder eliminar de manera automática el malware conocido detectado. • La solución deberá de contar con la capacidad de analizar archivos sospechosos por el fabricante, con el fin de determinar si son archivos maliciosos o no. • La solución deberá de ser capaz de identificar y bloquear adware. • La solución deberá de ser capaz de identificar y bloquear malware tradicional y malware desconocido (malware de día cero), ello mediante técnicas de Machine Learning y/o Sandboxing. • La solución deberá de ser capaz de identificar y bloquear ataques que no estén basados en archivos (fileless). • La solución deberá de poder generar listas blancas para archivos validos conocidos. • La solución deberá de poder generar listas negras de archivos maliciosos. • La solución deberá de poder poner en cuarentena equipos de forma remota y/o aislar dispositivos end-point. • La solución deberá de poder asignar un estado de bypass o desactivar la protección a los equipos y/o desactivar la protección de los equipos o módulos de seguridad específicos por el propio usuario • La solución deberá de reconocer comportamientos maliciosos y protección a los mismos son importar la ubicación del dispositivo. • La solución deberá de generar una vista grafica con el flujo del ataque, proporcionando así un análisis causa raíz con todos los eventos relacionados a actividades maliciosas. • La solución deberá de proveer un listado de todos los procesos, archivos y conexiones relacionadas a una alerta.
--	---

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 11 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> • La solución deberá de agregar inteligencia y contexto a las alertas para, poder revisar cada uno de los eventos asociados de manera secuencial. • La solución deberá de poder efectuar las siguientes tareas de respuesta a incidentes: <ul style="list-style-type: none"> ✓ Poner en cuarentena dispositivos de forma remota y/o aislar dispositivos end-point. ✓ Agregar proceso y archivos a listas blancas ✓ Agregar procesos y archivos a listas negras ✓ Eliminar aplicación o archivo de manera remota ✓ Solicitar una copia de la aplicación o archivo para su análisis ✓ Revisar la reputación de procesos y aplicaciones contra bases de datos de terceros como VirusTotal y/o con su propia nube de inteligencia de Amenazas. ✓ Capacidad de ejecutar comandos de manera remota y de manera segura. • La solución deberá de integrar la capacidad de hacer conexiones remotas a través de un canal cifrado para sistemas operativos Windows. • La solución deberá de poder controlar el comportamiento de diferentes aplicaciones, de tal manera que pueda negar la operación o terminar el proceso, de las siguientes actividades: <ul style="list-style-type: none"> ✓ Ejecución de la aplicación. ✓ Abrir comunicaciones sobre la red. ✓ Ejecutar código desde la memoria. ✓ Invocar procesos no confiables. ✓ Invocar interpretadores de comandos. ✓ Se comporten como Ransomware. ✓ Ejecutar fileless scripts. ✓ Inyectar código o modificar la memoria de otro proceso. • La solución deberá de tener la capacidad de configurar diferentes tipos de escaneos, así como de forma opcional contar con la funcionalidad de CDR (Content Disarm and Reconstruction) para la reconstrucción del contenido. • El sensor deberá de tener la capacidad de auto protegerse para que los usuarios no deshabiliten la protección. • La consola deberá de integrar un mecanismo a través del cual se puedan hacer búsquedas de eventos, independientemente si son clasificadas como maliciosos o no. Dentro de la información almacenada en la nube en base a los siguientes criterios: <ul style="list-style-type: none"> ✓ Periodo de tiempo (mínimo 90 días). ✓ Tipos de eventos. ✓ Procesos. ✓ Usuario. ✓ Dispositivos. • La solución deberá contar con acceso a reportes detallados de las últimas amenazas detectadas.
--	--

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 12 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<ul style="list-style-type: none"> La solución deberá poder exportar la siguiente información: <ul style="list-style-type: none"> ✓ Estado de los puntos finales. ✓ Ataques detenidos. ✓ Actividad sospechosa. ✓ Alertas detectadas en las diferentes etapas de un ataque. La solución deberá permitir la creación de notificaciones por correo electrónico en base a los siguientes eventos: <ul style="list-style-type: none"> ✓ Alertas que sean igual o superiores a una severidad definida. ✓ Alertas que sean igual o superiores a una severidad o condición o Threshold definido. ✓ En caso de que una política o violación de seguridad haya entrado en acción
Auditorias y análisis de vulnerabilidades.	<ul style="list-style-type: none"> La solución deberá de tener la capacidad de hacer evaluaciones a los equipos de forma programada o bajo demanda para sistemas Windows, Mac y Linux. La solución deberá de tener la capacidad de dar visibilidad a la siguiente información: <ul style="list-style-type: none"> Equipos Windows <ul style="list-style-type: none"> ✓ Inventario de parches o CVE. ✓ Información del sistema operativo. ✓ Información del dispositivo. ✓ usuarios conectados o nombre del dispositivo analizado ✓ Listado de procesos en ejecución o nombre de la aplicación vulnerable. Equipos Mac <ul style="list-style-type: none"> ✓ Usuarios conectados o nombre del dispositivo analizado. ✓ Información del dispositivo. ✓ Información del sistema operativo. Equipos Linux <ul style="list-style-type: none"> ✓ Usuarios conectados o nombre del dispositivo analizado ✓ Información del sistema operativo ✓ Información del dispositivo La solución deberá de permitir crear evaluaciones o escaneos personalizados. La solución deberá de realizar análisis de vulnerabilidades o comunicaciones de aplicaciones vulnerables de forma automática o bajo demanda. La solución deberá de contener un tablero (dashboard) que clasifique las vulnerabilidades encontradas basadas en su nivel de riesgo. La solución deberá de poder proveer una descripción de las vulnerabilidades encontradas; mostrando a través del módulo forense desde la consola (web u on premise) o reporte, las siguientes acciones: Impacto o Información del incidente, archivos exfiltrados o cifrados del incidente, detalle de la línea de tiempo del incidente para determinar si es una infección u ataque y que el reporte y/o detalle forense proporcionado

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 13 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<p>incluya información del mapa o la matriz, del Framework MITRE ATT&CK; el cual mostrará las tácticas y técnicas de compromiso que fueron ejecutadas por el atacante.</p> <ul style="list-style-type: none"> La solución deberá de incluir una calificación que indique el nivel de riesgo que representa la vulnerabilidad.
Caza de Amenazas.	<ul style="list-style-type: none"> Debe licenciar o habilitar la funcionalidad de Threat Hunting o Caza de Amenazas con herramientas que permitan buscar en toda la organización si hay un malware existe en otro endpoint. Se aceptará que opcionalmente, la solución permita realizar consultas que filtren eventos de actividad maliciosa y realizar la prevención de Phishing de día cero, haciendo similitud de URL con original, si posee únicamente imágenes, similitud general con sitio original y que los mensajes de alerta o bloqueo al usuario final sean configurables. La solución deberá de generar un diagrama de flujo de los procesos donde se muestre los diferentes eventos y dependencias relacionadas, sin importar si los eventos son maliciosos o no. La solución deberá permitir la creación de indicadores de compromiso (IoCs) de forma personalizada. La solución deberá realizar la protección utilizando indicadores de compromiso preconfigurados o brindados por el servicio de inteligencia de amenazas del fabricante.

6. GARANTÍA Y SOPORTE DEL BIEN:

- El postor deberá ofrecer 36 meses de garantía por mal funcionamiento, a partir de la puesta en operación de la solución contratada. El postor deberá incluir 36 meses de soporte de licencias de los módulos ofertados.
- Debe cubrir todo defecto que se pudiera presentar en los componentes o software que forman parte del bien ofertado, como consecuencia del mal diseño, manufactura, materiales o vicios ocultos; debiéndose corregir o reparar (de ser el caso), el fallo del software defectuoso a la brevedad.
- ~~La solución SIEM propuesta de forma obligatoria, deberá estar presente en el cuadrante mágico de Gartner mínimamente en 03 de las últimas 04 evaluaciones, el cual, deberá acreditarse a la presentación de la propuesta mediante links de la página oficial de Gartner e imágenes de los cuadrantes mágicos de Gartner, en los cuales se evidencie lo solicitado en el presente apartado.~~
- ³La solución SIEM propuesta de forma obligatoria, deberá estar presente en el cuadrante mágico de Gartner, mínimamente en 03 de las últimas 04 evaluaciones (considerado desde los años 2019, 2020, 2021, 2022). La información que se aceptará, será de la siguiente forma:
El último reporte de la consultora Gartner de Security Información and Event Management - SIEM (2022) se puedan sustentar mediante links de la página oficial de Gartner y los otros reportes de años anteriores se podrán sustentar con imágenes de los cuadrantes en los cuales se evidencia lo solicitado, con los links de donde fue obtenida dicha información (La información

³ Modificado referida a la consulta 4 del postor SSG PERU SAC

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 14 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

presentada deberá estar traducido al idioma español, según lo establecido por la Ley de Contrataciones del Estado y su Reglamento).⁴⁵⁶⁷⁸⁹

- ~~La solución EDR propuesta, deberá estar presente en el cuadrante mágico de Gartner mínimamente en 03 de las últimas 04 evaluaciones y/o, el fabricante de la solución ofertada deberá tener un resultado igual o superior al 94% de efectividad en Cobertura Analítica (Analytic Coverage) y Visibilidad (Visibility) sobre los entornos Windows y Linux, para la última evaluación de técnicas y tácticas de ciberseguridad realizada por MITRE ATT&CK (Wizard Spider + Sandworm) del año 2022. Se precisa que, respecto al requerimiento solicitado referente al cuadrante de Gartner, éste deberá acreditarse a la presentación de la propuesta mediante links de la página oficial de Gartner e imágenes de los cuadrantes mágicos de Gartner, en los cuales se evidencie lo solicitado en el presente apartado. Concerniente al requerimiento solicitado referente a la última evaluación de técnicas y tácticas de ciberseguridad realizada por MITRE ATT&CK, éste deberá acreditarse a la presentación de la propuesta mediante links de la página oficial del MITRE, y capturas de pantalla o documentos emitidos por el MITRE, en los cuales se evidencie lo solicitado en el presente apartado.~~
- 10La solución EDR propuesta, deberá estar presente en el cuadrante mágico de Gartner Magic Quadrant for Endpoint Protection Platforms mínimamente en 03 de las últimas 04 evaluaciones (considerado desde los años 2019, 2020, 2021, 2022) y/o, el fabricante de la solución ofertada deberá tener un resultado igual o superior al 94% de efectividad en Cobertura Analítica (Analytic Coverage) y Visibilidad (Visibility) sobre los entornos Windows y Linux, para la última evaluación de técnicas y tácticas de ciberseguridad realizada por MITRE ATT&CK (Wizard Spider + Sandworm) del año 2022. Se precisa que, respecto al requerimiento solicitado referente al cuadrante de Gartner, éste deberá acreditarse a la presentación de la propuesta mediante links de la página oficial de Gartner e imágenes de los cuadrantes mágicos de Gartner y/o reporte oficial de la marca ofertada donde se aprecie imágenes de los cuadrantes mágicos de Gartner y/o imágenes de los cuadrantes mágicos de Gartner con los links de donde fue obtenida dicha información y/o documentos emitidos por Gartner; en los cuales se evidencie lo solicitado en el presente apartado. Concerniente al requerimiento solicitado referente a la última evaluación de técnicas y tácticas de ciberseguridad realizada por MITRE ATT&CK, éste deberá acreditarse a la presentación de la propuesta mediante links de la página oficial del MITRE e imágenes de dicha evaluación; o imágenes de dicha evaluación con los links de donde fue obtenida dicha información o documentos emitidos por el MITRE, en los cuales se evidencie lo solicitado en el presente apartado (La información presentada deberá estar traducido

⁴ Modificado referida a la consulta 12 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

⁵ Modificado referida a la observación 13 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

⁶ Modificado referida a la consulta 35 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

⁷ Modificado referida a la consulta 91 del postor SECURESOFT CORPORATION S.A.C

⁸ Modificado referida a la consulta 92 del postor SECURESOFT CORPORATION S.A.C

⁹ Modificado referida a la consulta 69 del postor AI INVERSIONES PALO ALTO II S.A.C.

¹⁰ Modificado referido a la consulta 5, 6 y 7 del postor SSG PERU SAC

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 15 de 34
		CUT : 103630-2023

al idioma español, según lo establecido por la Ley de Contrataciones del Estado y su Reglamento)¹¹¹²¹³¹⁴

- El postor debe contar con un Data Center (propio o hospedado) certificado TIER III. El postor a la ~~presentación de la oferta~~ [firma del contrato](#)¹⁵¹⁶¹⁷¹⁸¹⁹²⁰, presentará una declaración jurada de contar con un Data Center (propio o hospedado) certificado TIER III.
- La garantía iniciará desde la puesta en operación del producto ofertado, refrendado por la suscripción del Acta de Cumplimiento de implementación del bien.
- El contratista, a la suscripción del Acta de Cumplimiento de implementación del bien, deberá informar a la entidad sobre los canales de atención para las atenciones de soporte técnico.
- El contratista en su Informe técnico sobre las actividades realizadas durante la Implementación del bien, deberá entregar una Carta de Garantía de la solución, la cual debe coberturar y contemplar los alcances solicitados en las presentes especificaciones técnicas.

7. CONSIDERACIONES GENERALES:

7.1. DE LA PRESTACIÓN PRINCIPAL:

- A partir del día siguiente de suscrito el contrato y hasta el plazo máximo de tres (03) días calendarios, el contratista deberá remitir al área usuaria vía correo electrónico (infraestructura_dsnirh@ana.gob.pe) el plan de trabajo de la prestación principal.
- El contratista deberá entregar y realizar la implementación (que incluye: instalación, configuración y capacitación) del producto ofertado de acuerdo a lo solicitado en el numeral 5 de las presentes especificaciones técnicas, en un plazo no mayor de 60 días calendario contabilizados a partir del día siguiente de suscrito el contrato. La puesta en operatividad del bien empezará cuando la entidad de la plena satisfacción del bien entregado, instalado y configurado, a través de la supervisión del personal designado por la Dirección del Sistema Nacional de Información de Recursos Hídricos - DSNIRH, para cuyo efecto ambas partes suscribirán un Acta de Cumplimiento de implementación del bien, la cual será redactada en dos ejemplares de igual redacción y valor, y estará firmada por personal designado por la DSNIRH.

¹¹ Modificado referido a la consulta 10 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

¹² Modificado referido a la observación 14 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

¹³ Modificado referida a la consulta 70 del postor AI INVERSIONES PALO ALTO II S.A.C.

¹⁴ Modificado referida a la consulta 93 del postor SECURESOFT CORPORATION S.A.C.

¹⁵ Modificado referida a la consulta 15 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

¹⁶ Modificado referida a la observación 45 del postor CYBER SECURITY ENTERPRISE S.A.C.

¹⁷ Modificado referida a la observación 50 del postor IB TECHNOLOGY GROUP S.A.C.

¹⁸ Modificado referida a la consulta 56 del postor AI INVERSIONES PALO ALTO II S.A.C.

¹⁹ Modificado referida a la consulta 65 del postor AI INVERSIONES PALO ALTO II S.A.C.

²⁰ Modificado referida a la consulta 86 del postor SECURESOFT CORPORATION S.A.C.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 16 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

- De igual forma, la entrega de las licencias de los bienes, tendrá un plazo no mayor de 30 días calendarios contabilizados a partir del día siguiente de suscrito el contrato, para lo cual, ambas partes suscribirán un Acta de entrega de bien, la cual será redactada en dos ejemplares de igual redacción y valor, y estará firmada por personal designado por la DSNIRH.
- Para el caso de la solución EDR, se debe incluir como mínimo 05 días calendarios de servicios profesionales brindados directamente por el área especializada del mismo fabricante, contabilizados dentro del periodo de instalación y configuración de la solución.
- La vigencia del producto ofertado deberá ser por un periodo de 03 años, contabilizado a partir del Acta de Cumplimiento de implementación del bien.
- El producto ofertado deberá contar con 03 años de mantenimiento y actualizaciones sin que genere costo adicional para la entidad, contabilizado a partir del Acta de Cumplimiento de implementación del bien.
- El contratista evidenciará a la entrega del bien ofertado, la documentación que garantice el origen o su procedencia legal del mismo.
- El bien ofertado por el postor debe cumplir en su totalidad las especificaciones técnicas solicitadas, conforme a lo señalado en las presentes especificaciones técnicas.
- Hasta sesenta (60) días calendarios contabilizados a partir del día siguiente de suscrito el contrato, el Contratista hará entrega de un Informe técnico sobre las actividades realizadas durante la Implementación del bien, el cual debe contener como mínimo lo siguiente:
 - ✓ Acciones y configuraciones realizadas.
 - ✓ Imágenes.
 - ✓ Manuales.
 - ✓ Carta de Garantía de la solución, la cual debe coberturar y contemplar los alcances solicitados en las presentes especificaciones técnicas.
- Teniendo en cuenta que dentro de la adquisición se llevará a cabo la capacitación sobre el bien ofertado, y en caso de realizarse trabajos de manera presencial:
 - ✓ El Contratista deberá dar cumplimiento a lo normado por la entidad aplicables a las actividades que desarrolle como Proveedores, 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.
- La entidad se reserva el derecho de comprobar la veracidad, originalidad y cumplimiento de toda la información incluida en la propuesta del contratista, a fin de aceptar o desestimar su propuesta.

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 17 de 34
		CUT : 103630-2023

7.2. DE LA PRESTACIÓN ACCESORIA:

Asimismo, y como parte de la adquisición, se incluirá la siguiente prestación accesoria:

a. CAPACITACIÓN

El contratista deberá brindar una capacitación de 12 horas para un mínimo de 03 personas, en las soluciones SIEM y EDR, la cual se realizará como máximo hasta los cincuenta (50) días calendarios contabilizados a partir del día siguiente de suscrito el contrato, en las oficinas de la entidad durante el periodo de instalación y configuración del bien ofertado. La capacitación solicitada podrá ser brindada de manera remota por medio de herramientas de capacitación. Deberán cubrir los siguientes temas: instalación, configuración, administración, diagnóstico de problemas y generación de reportes de la solución ofertada, para lo cual se hará entrega de una constancia de participación por cada uno de los asistentes.

b. OPERACIÓN

Como parte de la “Adquisición de software para la colección de eventos y detección de amenazas avanzadas de la red para la Autoridad Nacional Del Agua”, el Contratista ejecutará cotidianamente durante el periodo de tres (03) años contabilizados a partir del Acta de Cumplimiento de implementación del bien, acciones proactivas y reactivas en las plataformas contratadas con el objetivo de disminuir el riesgo y mantener o elevar el nivel de seguridad de la red de la Autoridad Nacional del Agua - ANA.

El contratista cumplirá labores cotidianas de atención y maniobras sobre las plataformas contratadas por la Autoridad Nacional del Agua - ANA. Durante la prestación accesoria, el Contratista realizará acciones técnicas a cargo de especialistas y actuarán en base a metodologías probadas y seguras.

Como resultado de dichas labores y de forma anual, deberá presentar un Informe de las atenciones y acciones proactivas y reactivas realizadas, por el periodo ejecutado de la prestación accesoria.

c. OBJETIVOS DE LA PRESTACIÓN ACCESORIA

El objetivo principal de la presente prestación accesoria es que las maniobras cotidianas y a demanda ejecutadas durante los tres (03) años de duración de la prestación, sean técnicamente eficientes y se apoyen en un estudio periódico y visión proactiva, de tal forma que se busque la mejora continua en el nivel de seguridad y la consecuente minimización del riesgo.

Los objetivos secundarios durante los tres (03) años de duración de la prestación accesoria son:

- Optimizar la arquitectura de seguridad actual y el modelo de supervisión, aplicando las mejores prácticas recomendadas por los fabricantes de Ciberseguridad.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 18 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

- Gestionar las plataformas contratadas y tomar acción oportuna ante amenazas externas e internas, minimizando los tiempos de afectación de los recursos operativos.
- Realizar un análisis de riesgo continuo, con el objetivo de buscar periódicamente la mejora continua y así hacer más eficientes y seguras las plataformas administradas.
- Establecer un modelo de mejora continua basado en indicadores periódicos.

d. MODALIDAD DE LA PRESTACIÓN

La presente prestación accesoria se brindará en la modalidad On-Site y On-line con las siguientes facilidades:

- Operador de la solución – On-Site (Presencial en la sede central de la institución), que actuará en el horario de oficina de la Autoridad Nacional del Agua - ANA.
- Equipo CyberSOC – On-Line, que actuará en el horario de oficina de la Autoridad Nacional del Agua - ANA.
- Equipo CyberSOC - On-Line, que actuará fuera del horario de oficina de la Autoridad Nacional del Agua - ANA
- La solución no se deberá ver afectada en caso de inasistencias del personal.
- El personal se deberá integrar a los procesos y cultura de la Autoridad Nacional del Agua - ANA.

e. METODOLOGÍA DE TRABAJO

La metodología de la prestación accesoria consistirá en seguir los fundamentos de un Sistema de Gestión de Seguridad Informática, que ayudará a implementar y mantener total o parcialmente los requisitos, líneas guía y técnicas necesarias en los sistemas de seguridad.

Las normativas nacionales e internacionales relacionadas a la operación de las soluciones de seguridad deben estar alineadas a:

- ISO/IEC 27001:2013. Lineamientos guía y principios generales para iniciar, implementar, mantener un sistema de gestión de la seguridad de la información en una organización.
- ISO/IEC 27002:2013. Mejores prácticas para los controles de seguridad de la información.
- ISO/IEC 31000:2009. Principios y lineamientos guía de la gestión de riesgos.

Adicionalmente a las mencionadas, las prácticas relacionadas al análisis de riesgo contemplarán marcos metodológicos como NIST 800-39 / 800-37 / 800-30, ISO 27005 y FAIR.

f. ÁMBITO DE LA PRESTACIÓN

El ámbito de la presente prestación accesoria está circunscrito a la plataforma y componentes adquiridos a través de la prestación principal, siendo que la prestación accesoria se brindará por un periodo de tres (03) años contabilizados a partir del Acta de

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 19 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

Cumplimiento de implementación del bien.

TECNOLOGÍA	Prestación Principal
Software de Solución para colección de eventos de red	1 SIEM que incluye: - Soporte hasta para 1400 dispositivos y 3000 EPS. - Licencia para 1400 agentes avanzados - 200 licencias de UBA o UEBA.
Software de Detección de amenazas avanzadas de red	1400 licencias EDR para detección de amenazas avanzadas

g. ACTIVIDADES A DESARROLLARSE DURANTE LA PRESTACIÓN

Las actividades que forman parte de esta prestación accesoria serán las siguientes:

I. Actividades a desarrollar:

- Administración de la configuración idónea de los sistemas contratados.
- Revisión cotidiana de la plataforma a cargo de un operador de la solución.
- Reporte de actualizaciones, cobertura y de cumplimiento de estándares de la plataforma.
- Supervisión de licenciamiento y suscripciones.
- Gestión de perfiles y accesos de supervisión a plataforma operada.

II. Cambios, configuraciones y maniobras:

Durante el desarrollo de esta prestación accesoria, el Contratista recibirá, evaluará, aprobará e implementará las solicitudes de cambio y configuración para las plataformas adquiridas mediante procedimientos establecidos. Estas solicitudes serán registradas, documentadas y supervisadas hasta su resolución y reporte, mediante procedimientos preestablecidos.

III. Soporte técnico:

Tendrá por objetivo absolver consultas técnicas y dar soporte a incidentes. Los incidentes o solicitudes serán recibidos y procesados hasta su completa resolución. Los incidentes atendidos serán registrados, tendrán seguimiento y a su finalización generarán el informe técnico respectivo. Incluirá maniobras en la modalidad On-site y Off-Site.

IV. Copias de respaldo de los sistemas de gestión:

Consistirá en obtener periódicamente y almacenar de forma encriptada el respaldo de la configuración y de las políticas de seguridad de los sistemas contratados, a través de procedimientos aprobados de obtención, almacenamiento y restauración. De esta forma la plataforma estará preparada para recuperarse ante un posible desastre. [\(el repositorio en donde se guardarán las copias de respaldo serán brindadas por](#)

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 20 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

la entidad). ²¹

V. Gestión de las actualizaciones y mejoras:

Se trata de la evaluación, planificación e instalación de mejoras y/o de nuevas versiones de los componentes de los sistemas administrados. Para este fin se evaluarán las últimas versiones y parches que sean publicadas por el fabricante. Además, se evaluarán las versiones actuales, la oportunidad de mejora y los tiempos de fin de vida y de fin de soporte de cada una de ellas. De esta forma la entidad mantendrá su sistema siempre actualizado y protegido.

VI. Planificación de la seguridad:

Se realizarán la siguiente actividad de evaluación y planificación que permitan lograr efectividad y mejora continua en los mecanismos de seguridad implantados y administrados:

VII. Comité de la Seguridad mensual:

- Reportar indicadores.
- Reportar incidentes.
- Seguimiento de las iniciativas de seguridad.
- Tablero de mejora continua de seguridad.

h. REQUERIMIENTOS DE CONECTIVIDAD

La prestación accesoria deberá incluir un acceso remoto a la plataforma a ser gestionada, desde el CyberSOC del contratista, ya sea a través de un acceso de administración remoto por internet seguro o por canal VPN.

Niveles de la prestación accesoria ofrecidos

ACUERDO DE NIVEL		
Prestación Accesoria	SLA	Productos
Gestor de la solución	<ul style="list-style-type: none"> • Supervisión cotidiana. • Asistencia a comités de seguridad mensuales. 	
Operador de la solución	<ul style="list-style-type: none"> • Operación cotidiana a cargo del Operador de la solución y supervisado por el Gestor de la solución, en horario de oficina en modalidad presencial; y el Equipo CyberSOC – On Line (En horario 24x7) 	<ul style="list-style-type: none"> • Informe de actividad técnica semanal. • Informe de actividad técnica mensual.
Cambios, Configuraciones y Maniobras	<ul style="list-style-type: none"> • Número de solicitudes: Ilimitado • Horario: 24x7 • SLA: P2, P3 o P4. 	<ul style="list-style-type: none"> • Solicitud/resolución individual.

²¹ Modificado referida a la consulta 84 del postor SECURESOFTE CORPORATION S.A.C

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 21 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

Soporte técnico	<ul style="list-style-type: none"> Número de solicitudes: Ilimitado Horario: 24x7 SLA: P1, P2, P3 o P4. 	<ul style="list-style-type: none"> Solicitud/resolución individual.
Copias de respaldo	<ul style="list-style-type: none"> Periodicidad: Semanal. SLA: 99.8% de cumplimiento 	<ul style="list-style-type: none"> Informe técnico.
Actualizaciones y mejoras	<ul style="list-style-type: none"> Periodicidad: De acuerdo con el plan de mejoras. SLA: 99.8% de cumplimiento 	<ul style="list-style-type: none"> Informe técnico.

ACUERDO DE NIVEL				
TIEMPOS DE ATENCIÓN PARA CAMBIOS, CONFIGURACIONES, MANIOBRAS Y SOPORTE				
P5	P4	P3	P2	P1
Nivel Informacional	Nivel bajo o rutina	Nivel medio/moderado	Nivel alto	Nivel crítico o de emergencia
TIEMPO DE EJECUCIÓN PARA CAMBIOS Y CONFIGURACIONES				
72 horas	48 horas	24 horas	12 horas	6 horas
TIEMPO DE RESOLUCIÓN ESPERADA PARA INCIDENTES				
72 horas	24 horas	6 horas	4 horas	2 horas
<ul style="list-style-type: none"> Los tiempos SLA se contabilizan en horas desde el ingreso de la solicitud. Algunas labores de cambios y configuraciones complejas requieren acciones de planificación, validación o pruebas complementarias y que incluso pueden depender de proveedores terceros. 				

CANALES DE ATENCION DISPONIBLES
<ul style="list-style-type: none"> Telefónico. - Se brindará a través de medios de telefonía fija o móvil, se debe entregar una cartilla trimestral de atención de contacto. E-mail y Chat. - Se brindará a través de comunicación electrónica como e-mail y chat (mensajería instantánea). Para el caso de e-mail, se recibirán nuestras consultas o solicitudes de soporte en la dirección de correo que se establezca. Atención Remota (control remoto). - Se ejecutará mediante procedimientos especiales de conexión remota, el cual es un método rápido y seguro. La conexión remota puede ser establecida mediante conexión VPN o conexión a escritorio remoto mediante software cliente certificado.

8. CONSIDERACIONES ESPECÍFICAS:

8.1. DE LA EXPERIENCIA DEL PROVEEDOR EN LA ESPECIALIDAD

El postor debe acreditar, un monto facturado acumulado equivalente a cinco millones cuatrocientos mil (5'400,000 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.

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 22 de 34
		CUT : 103630-2023

Se consideran bienes similares a los siguientes:

- ✓ Venta o Servicios de Seguridad de red interna y perimetral (²²Referido a Adquisición de una solución recolectora de eventos y detección de amenazas avanzadas, con la finalidad de permitir y dar visibilidad de las actividades de todos los equipos de la infraestructura TIC (Tecnologías de la Información y Comunicación) así como la de detectar y mitigar ataques informáticos)
- ✓ Venta o mantenimiento o renovación de licencias de sistemas de control y seguridad de puntos finales.
- ✓ Venta o mantenimiento o renovación de licencias de software de tipo detección y respuesta – EDR.
- ✓ Venta o mantenimiento o renovación de sistemas de correlación de eventos o SIEM.

8.2. DEL PERSONAL

Para la ejecución de las prestaciones principal y accesorio, se requerirá del siguiente personal clave: (la experiencia será contabilizada de manera independiente al grado de bachiller o título universitario del personal).²³

8.2.1. DE LA PRESTACIÓN PRINCIPAL:

- **Especialista en Gestión de Proyectos**

Actividades a desarrollar:

- ✓ Realizar el seguimiento del progreso de la implementación de la prestación principal.
- ✓ Realizar informes y/o entregables requeridos por la entidad.
- ✓ Gestionar los posibles riesgos en la implementación de la prestación y resolver los problemas que se presenten.
- ✓ Gestionar los plazos y tiempos de la implementación de la prestación.
- ✓ Coordinar con el área usuaria los diferentes permisos o accesos que se requieran durante la implementación de la prestación.
- ✓ Sostener reuniones y/o comunicación que se requiera con el área usuaria, durante la implementación de la prestación.
- ✓ Velar por el cumplimiento de los alcances del requerimiento de la prestación principal.

Perfil Mínimo del personal:

- ✓ Bachiller o Ingeniero en: Ingeniería de Sistemas y/o Informática y/o Electrónica y/o Cómputo y/o Industrial y/o Computación y Sistemas y/o Sistemas Empresariales y/o Industrial y de Sistemas y/o Sistemas de Información, y/o

²² Modificado referida a la consulta 3 del postor SSG PERU S.A.C.

²³ Modificado referida a la consulta 71 del postor AI INVERSIONES PALO ALTO II S.A.C.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 23 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

Sistemas y cómputo y/o Telecomunicaciones y/o
Sistemas e Informática y/o Informático y de Sistemas.²⁴²⁵

- **Especialista de la solución a Implementar**

Actividades a desarrollar:

- ✓ Realizar las implementaciones y personalizaciones que se requieran de la solución, durante la etapa de implementación.
- ✓ Proponer mejoras o cambios en la implementación y/o configuración de la solución, a partir de su experiencia obtenida en proyectos de implementación similares.
- ✓ Verificar las configuraciones realizadas.
- ✓ Reportar posibles problemas encontrados en la solución y ejecutar la solución al mismo.

Perfil Mínimo del personal:

- ✓ Bachiller o Ingeniero en: Ingeniería de Sistemas y/o Informática y/o Electrónica y/o Cómputo y/o Industrial y/o Computación y Sistemas y/o Sistemas Empresariales y/o Industrial y de Sistemas y/o Sistemas de Información y/o **Sistemas y cómputo y/o Telecomunicaciones y/o Sistemas e Informática y/o Informático y de Sistemas**²⁶.

8.2.2. DE LA PRESTACIÓN ACCESORIA: (El personal puede ser el mismo de la prestación principal, siempre y cuando cumpla el perfil)²⁷

- **Gestor de la solución**

Actividades a desarrollar:

- ✓ Supervisión cotidiana.
- ✓ Asistencia a comités de seguridad mensuales.

Perfil Mínimo del personal:

- ~~✓ Bachiller o Ingeniero en: Computación, o Computación y Sistemas, o Informática, o Sistemas, o Sistemas y Cómputo o Sistemas e Informática.~~
- ✓ **Bachiller o Ingeniero en: Computación y/o Computación y Sistemas y/o Informática y/o Sistemas y/o Sistemas y Cómputo y/o Sistemas e Informática y/o Electrónica y/o Cómputo y/o Industrial y/o Sistemas Empresariales y/o Industrial y de Sistemas y/o Sistemas de Información y/o Telecomunicaciones.**²⁸²⁹³⁰

²⁴ Modificado referida a la consulta 61 del postor AI INVERSIONES PALO ALTO II S.A.C.

²⁵ Modificado referida a la consulta 87 del postor SECURESOFTE CORPORATION S.A.C.

²⁶ Modificado referida a la consulta 61 del postor AI INVERSIONES PALO ALTO II S.A.C.

²⁷ Modificado referida a la consulta 53 del postor AI INVERSIONES PALO ALTO II S.A.C.

²⁸ Modificado referida a la observación 36 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

²⁹ Modificado referida a la consulta 62 del postor AI INVERSIONES PALO ALTO II S.A.C.

³⁰ Modificado referida a la consulta 88 del postor SECURESOFTE CORPORATION S.A.C.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 24 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

- **Operador de la solución**

Actividades a desarrollar:

- ✓ Responsable de la operación cotidiana de la solución, en horario de oficina.
- ✓ Responsable de la elaboración de Informes de actividad técnica semanal.
- ✓ Responsable de la elaboración de Informes de actividad técnica mensual.

Perfil Mínimo del personal:

- ✓ ~~Bachiller o Ingeniero en: Computación, o Computación y Sistemas, o Informática, o Sistemas, o Sistemas y Cómputo o Sistemas e Informática.~~
- ✓ Bachiller o Ingeniero en: Computación y/o Computación y Sistemas y/o Informática y/o Sistemas y/o Sistemas y Cómputo y/o Sistemas e Informática y/o Electrónica y/o Cómputo y/o Industrial y/o Sistemas Empresariales y/o Industrial y de Sistemas y/o Sistemas de Información y/o Telecomunicaciones y/o Redes y Comunicaciones y/o Electrónica y Telecomunicaciones³¹³²³³

NOTA: El perfil mínimo del personal tanto de la prestación principal como de la prestación accesoria, se acreditará con copia simple del título profesional o copia simple del grado de bachiller, según sea el caso, a la firma del contrato.

El Grado de Bachiller o Título profesional 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/>.

9. ENTREGABLES:

El contratista hará entrega de lo siguiente:

9.1. DE LA PRESTACIÓN PRINCIPAL:

Primer entregable:

- Acta de entrega de Licencias: hasta treinta (30) días calendarios, contabilizado a partir del día siguiente de suscrito el contrato.

Segundo entregable:

- Informe de Instalación y configuración de la solución implementada: hasta sesenta (60) días calendarios, contabilizado a partir del día

³¹ Modificado referida a la observación 37 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

³² Modificado referida a la consulta 62 del postor AI INVERSIONES PALO ALTO II S.A.C.

³³ Modificado referida a la consulta 89 del postor SECURESOFTECH CORPORATION S.A.C.

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 25 de 34
		CUT : 103630-2023

siguiente de suscrito el contrato, el cual debe contener como mínimo lo siguiente:

- ✓ Acciones y configuraciones realizadas.
- ✓ Imágenes de instalación.
- ✓ Manuales
- ✓ Carta de Garantía de la solución, la cual debe coberturar y contemplar todos los alcances solicitados en las presentes especificaciones técnicas.

9.2. DE LA PRESTACIÓN ACCESORIA:

Primer entregable:

- Constancias de participación en la capacitación: hasta cincuenta (50) días calendarios, contabilizado a partir del día siguiente de suscrito el contrato

Segundo entregable:

- Informe de las atenciones y acciones proactivas y reactivas realizadas: a presentarse desde los 365 días calendarios contabilizados a partir del Acta de Cumplimiento de implementación del bien, hasta por un plazo máximo de 15 días calendarios.

Tercero entregable:

- Informe de las atenciones y acciones proactivas y reactivas realizadas: a presentarse desde los 730 días calendarios contabilizados a partir del Acta de Cumplimiento de implementación del bien, hasta por un plazo máximo de 15 días calendarios.

Cuarto entregable:

- Informe de las atenciones y acciones proactivas y reactivas realizadas: a presentarse desde los 1095 días calendarios contabilizados a partir del Acta de Cumplimiento de implementación del bien, hasta por un plazo máximo de 15 días calendarios.

Los entregables deberán 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 ventanilla de mesa de partes virtual ubicada en la página web de la institución: www.ana.gob.pe en el link trámite virtual.

10. PLAZO Y LUGAR DE ENTREGA:

10.1. PLAZO DE ENTREGA DE LA PRESTACIÓN PRINCIPAL

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

Actividad	Inicio	Fin
-----------	--------	-----

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 26 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

Acta de entrega de bien	✓ A partir del día siguiente de suscrito el contrato	✓ Hasta el plazo máximo de treinta (30) días calendarios.
Instalación, configuración de la solución y entrega del Informe de Instalación y configuración de la solución	✓ A partir del día siguiente de suscrito el contrato	✓ Hasta el plazo máximo de sesenta (60) días calendarios.

10.2. PLAZO DE LA PRESTACIÓN ACCESORIA

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

Actividad	Inicio	Fin
Capacitación	✓ A partir del día siguiente de suscrito el contrato	✓ Hasta el plazo máximo de cincuenta (50) días calendarios.
Atenciones y acciones proactivas y reactivas	✓ A partir del Acta de Cumplimiento de implementación del bien.	✓ Hasta el plazo máximo de trescientos sesenta y cinco (365) días calendarios.
Atenciones y acciones proactivas y reactivas	✓ A partir del Acta de Cumplimiento de implementación del bien.	✓ Hasta el plazo máximo de setecientos treinta (730) días calendarios.
Atenciones y acciones proactivas y reactivas	✓ A partir del Acta de Cumplimiento de implementación del bien.	✓ Hasta el plazo máximo de mil noventa y cinco (1095) días calendarios.

10.3. LUGAR DE ENTREGA DE LA PRESTACIÓN PRINCIPAL Y ACCESORIA

La entrega e implementación de la solución (prestación principal), así como de las atenciones y acciones proactivas y reactivas (prestación accesoria), será en las instalaciones de la Sede Central de la Autoridad Nacional del Agua, sito en calle Diecisiete N° 355, Urb. El Palomar, San Isidro – Lima.

11. SISTEMA DE CONTRATACIÓN:

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

12. MODALIDAD DE EJECUCIÓN CONTRACTUAL:

Contrato Llave en Mano.

13. ADELANTOS:

No corresponde

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 27 de 34
		CUT : 103630-2023

14. SUPERVISION Y CONFORMIDAD DE LA CONTRATACIÓN:

- La supervisión de la implementación estará a cargo del personal de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la Autoridad Nacional del Agua.
- La conformidad será otorgada por la Dirección del Sistema Nacional de Información de Recursos Hídricos de la Autoridad Nacional del Agua, en un plazo no mayor a siete (07) días calendarios, desde la presentación de los respectivos entregables tanto para la prestación principal, como para la accesoria.

15. FORMA DE PAGO:

a) PARA LA PRESTACIÓN PRINCIPAL:

El pago por la prestación principal se realizará en dos (02) armadas, previa conformidad otorgada por parte de la Dirección del Sistema Nacional de Información de Recursos Hídricos de los siguientes entregables:

Entregable	MONTO DE PAGO
PRIMER ENTREGABLE: Acta de entrega de bien	1ra ARMADA: 55% del monto de la prestación principal
SEGUNDO ENTREGABLE: Informe de Instalación y configuración de la solución implementada.	2da ARMADA: 45% del monto de la prestación principal

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.

b) PARA LA PRESTACIÓN ACCESORIA:

El pago por la prestación accesoria se realizará en una (01) armada por la capacitación y tres (03) armadas por las atenciones y acciones proactivas y reactivas, previa conformidad otorgada por parte de la Dirección del Sistema Nacional de Información de Recursos Hídricos de los siguientes entregables:

i. CAPACITACIÓN:

Entregable	MONTO DE PAGO
PRIMER ENTREGABLE: Constancias de participación en la capacitación.	1ra ARMADA: 100% del monto por capacitación, de la prestación accesoria.

ii. ATENCIONES Y ACCIONES PROACTIVAS Y REACTIVAS:

SEGUNDO ENTREGABLE: Informe de las atenciones y acciones	1ra ARMADA: 30% del monto por las atenciones y acciones proactivas
---	---

	FORMATO	Código : SGC-F-006
	ESPECIFICACIONES TECNICAS	Versión : 00
		Aprobado por : DSNIRH
		Fecha : Octubre 2023
		Página : 28 de 34
		CUT : 103630-2023

proactivas y reactivas realizadas	y reactivas, de la prestación accesoria.
TERCER ENTREGABLE: Informe de las atenciones y acciones proactivas y reactivas realizadas	2da ARMADA: 35% del monto por las atenciones y acciones proactivas y reactivas, de la prestación accesoria.
CUARTO ENTREGABLE: Informe de las atenciones y acciones proactivas y reactivas realizadas	3ra ARMADA: 35% del monto por las atenciones y acciones proactivas y reactivas, de la prestación accesoria.

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.

16. 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:

- a) Plazos menores o iguales a sesenta (60) días: F = 0.40
- b) 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.

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 tres (03) años, contado a partir del Acta de Cumplimiento de implementación del bien.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 29 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

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, **teniendo en cuenta cuando la obligación de confidencialidad no aplicará a la información que:**

1. Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.
2. Haya sido publicada con anterioridad a la fecha de la firma de contrato.
3. Se encuentre en poder de la Parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.
4. Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
5. Sea independientemente desarrollada por la Parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.
6. Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden.³⁴

19. PROPIEDAD INTELECTUAL:

El proveedor cede a favor del ANA, cualquier tipo de derechos generados como consecuencia de la elaboración de los informes, opiniones, documentos generados, que son materia de la presente adquisición, 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 del mismo, sin que medie autorización escrita otorgada por ANA.

20. CESIÓN DE DERECHOS:

Por medio de la presente cláusula, el proveedor 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

³⁴ Modificado referida a la observación 38 del postor TELEFÓNICA CYBERSECURITY & CLOUD TECH PERÚ S.A.C.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 30 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

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 proveedor 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 Autoridad Nacional del Agua 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 proveedores 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 proveedor de la prestación 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 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 proveedor 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
	ESPECIFICACIONES TECNICAS	Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 31 de 34 CUT : 103630-2023

REQUISITOS DE CALIFICACIÓN

A	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar, un monto facturado acumulado equivalente a cinco millones cuatrocientos mil (5'400,000 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 o Servicios de Seguridad de red interna y perimetral ((³⁵Referido a Adquisición de una solución recolectora de eventos y detección de amenazas avanzadas, con la finalidad de permitir y dar visibilidad de las actividades de todos los equipos de la infraestructura TIC (Tecnologías de la Información y Comunicación) así como la de detectar y mitigar ataques informáticos) ✓ Venta o mantenimiento o renovación de licencias de sistemas de control y seguridad de puntos finales. ✓ Venta o mantenimiento o renovación de licencias de software de tipo detección y respuesta – EDR. ✓ Venta o mantenimiento o renovación de sistemas de correlación de eventos o SIEM. <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 pago³⁶, 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</p>

³⁵ Modificado referida a la consulta 3 del postor SSG PERU S.A.C.

³⁶ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

“... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”

(...)

“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 32 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

	<p>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> <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 Proveedores en Consorcio en las Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</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 Proveedores en Consorcio en las Contrataciones del Estado”.</i></p> </div>
A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p>❖ <u>DE LA PRESTACIÓN PRINCIPAL:</u></p> <ul style="list-style-type: none"> - <u>Especialista en Gestión de Proyectos</u> <p><u>Requisitos:</u> Cuatro (04) años de experiencia mínima profesional como jefe o gerente o</p>

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 33 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

líder o coordinador o responsable de proyecto o gestor de proyectos similares al objeto de la contratación.

- **Especialista de la solución a Implementar**

Requisitos:

Cuatro (04) años de experiencia profesional ejecutando implementaciones similares al objeto de la contratación.

❖ **DE LA PRESTACIÓN ACCESORIA:**

- **Gestor de la solución**

Requisitos:

Tres (03) años de experiencia profesional en la gestión de plataformas de ciberseguridad o de Seguridad de red interna y perimetral o similares al objeto de la contratación.

- **Operador de la solución**

Requisitos:

Dos (02) años de experiencia profesional en la gestión de plataformas de ciberseguridad o de Seguridad de red interna y perimetral o similares al objeto de la contratación.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

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.*

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha : Octubre 2023 Página : 34 de 34 CUT : 103630-2023
	ESPECIFICACIONES TECNICAS	

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.*