

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 1 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

ESPECIFICACIONES TÉCNICAS DE SOFTWARE ANTIVIRUS (SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMÁTICOS) PARA LA SEDE CENTRAL Y ÓRGANOS DESCONCENTRADOS DE LA AUTORIDAD NACIONAL DEL AGUA

CODIGO SIGA: 14.04.0003.0076

1. FINALIDAD PUBLICA:

El presente proceso busca salvaguardar la información alojada en la infraestructura informática de la Autoridad Nacional del Agua; mediante la implementación de una solución contra ataques de virus informáticos, que proteja y que mitigue a la red de datos, aplicativos, bases de datos y servicios informáticos, de programas como los virus troyanos, macros virus, adware, spyware, gusanos, rootkits, exploits y todo tipo de programa malicioso (malware); garantizando así, el adecuado desarrollo de las actividades de los profesionales al público interno y externo.

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.

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. 44° 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”.

3. JUSTIFICACIÓN:

Que, para el cumplimiento de metas y objetivos institucionales resulta necesario la adquisición de 01 solución de protección de virus informáticos (Software Antivirus para Endpoint) para la Sede central y Órganos Desconcentrados de la Autoridad Nacional del Agua, cuya finalidad es la de proteger y mitigar

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 2 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

los principales riesgos de seguridad de la información; de tal forma que intente entre otras cubrir las principales formas de ataque a los dispositivos informáticos, ya sea un servidor, ordenador o smartphone, teniendo en cuenta que al navegar por Internet o copiando archivos a tu dispositivo, la información esta propensa a una infección y por ende a la pérdida de la información, principal activo de la institución.

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 01 Solución de protección de virus informáticos para la Sede central y Órganos Desconcentrados de la Autoridad Nacional del Agua (para 2170 nodos y por el periodo de 3 años), la cual mitigue los principales riesgos de seguridad de la información como son los virus informáticos y amenazas persistentes (APTs) como RANSOMWARE, minimizando así las interrupciones por caídas del servicio y pérdida de datos.

5. ESPECIFICACIONES TÉCNICAS MÍNIMAS:

La solución debe cumplir como mínimo con las siguientes especificaciones técnicas:

5.1	SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMÁTICOS PARA LA SEDE CENTRAL Y ÓRGANOS DESCONCENTRADOS DE LA AUTORIDAD NACIONAL DEL AGUA	
	5.1.1	PLATAFORMA ANTIMALWARE (2170 Licencias)
	5.1.1.1	GESTIÓN CENTRALIZADA
		Todos los componentes que forman parte de la plataforma antimalware deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes a fin de no sobrecargar los recursos de los sistemas.
		La consola de monitoreo y configuración deberá ser a través de una central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos.
		La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional.
		La consola debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM.
		Este mecanismo de comunicación vía API deberá obtener los eventos y alertas asociados a la consola en al menos, los siguientes formatos: json, cef, or keyvalue.
		Este mecanismo de comunicación vía API deberá obtener la información correspondiente sin eliminarla ni borrarla de la consola primaria de administración.
		La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
		Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
		Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.
		La instalación debe poder realizarse de forma manual obtenido a través del cliente descargado de la consola central o también vía correo electrónico. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.
		Debe proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.

	FORMATO		Código : SGC-F-006
	ESPECIFICACIONES TECNICAS		Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 3 de 23 CUT : 163312-2023

		Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
		La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros.
		Debe permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador.
		Debe utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
		Debe presentar mensajes generados por el agente en el idioma español o permitir su edición.
		Debe permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
		Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
		Debe contar con la posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
		Debe tener la capacidad de generación de informes, estadísticas o gráficos, tales como: Detalle cuáles usuarios están activos, inactivos o desprotegidos, así como detalles de estos; Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
		La comunicación debe permitir limitar el ancho de banda utilizado por los agentes.
		La solución deberá permitir la selección de la versión del software de preferencia, permitiendo así la prueba de la actualización sobre un grupo de PC's piloto antes de implementarlo para toda la red. También debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.
		La plataforma de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
		La plataforma de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.
		Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.
		Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.
		Una vez que se identifique un problema, debe permitir corregir los problemas de forma remota, con al menos las siguientes opciones:
		Proteger el dispositivo con la opción de inicio de una exploración;
		Forzar una actualización en ese momento;
		Ver los detalles de los eventos ocurridos;
		Ejecutar la comprobación completa del sistema;
		Forzar el cumplimiento de una nueva política de seguridad;
		Mover el equipo a otro grupo;
		Borrar el equipo de la lista;
		Aislarlo a demanda de la red corporativa.
		Ejecutar una interfaz de línea de comando sobre el dispositivo.
		Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro manual

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 4 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		o automáticamente;
		Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses.
		Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF.
		Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints.
		Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF
		Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.
		Deberá tener la posibilidad de instalar un servidor para reenvío de eventos en caso de que el agente no pueda comunicarse con la consola en la nube.
	5.1.1.2	AGENTE DE PROTECCIÓN ANTIMALWARE
		Debe permitir la detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
		Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
		Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).
		Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
		Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
		Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA).
		Debe poseer la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
		Debe permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
		Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
		Debe ser capaz de aplicar un análisis adicional, inspeccionando el comportamiento del código durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
		Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
	5.1.1.3	AGENTE DE DETECCIÓN, MITIGACIÓN Y RECUPERACIÓN PROACTIVA DE RECONOCIMIENTO DE NUEVAS AMENAZAS
		Debe integrar protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
		Debe incluir funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep Learning.
		Debe tener la capacidad de detección, y bloqueo proactivo de malware no conocido (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
		Debe tener la capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 5 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		Debe detectar el malware en pre-ejecución un tiempo aproximado de no más de 20 milisegundos.
		Debe contar con la capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
		Debe integrar la funcionalidad de análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
		Debe integrar el bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
		Debe poder configurar excepciones ante falsos positivos.
		La solución debe tener capacidad de protección AMSI contra scripts maliciosos
		La solución debe poseer un IPS Snort de Host.
	5.1.1.4	AGENTE DE PREVENCIÓN Y PROTECCIÓN CONTRA ATAQUES DE TIPO RANSOMWARE
		Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.
		Disponer de capacidad de remediación de la acción de encriptación maliciosa de los ransomwares.
		Debe poseer protección anti-ransomware para el sector de booteo.
		De restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
		Protección contra Vulnerabilidades y técnicas de explotación
		<p>Debe brindar detección y protección de al menos las siguientes técnicas de explotación:</p> <ul style="list-style-type: none"> • Enforce Data Execution Prevention • Mandatory Address Space Layout Randomization • Bottom-up ASLR • Null Page (Null Deference Protection) • Heap Spray Allocation • Dynamic Heap Spray • Stack Pivot • Stack Exec (MemProt) • EStack-based ROP Mitigations (Caller) • Branch-based ROP Mitigations (Hardware Assisted) • Structured Exception Handler Overwrite (SEHOP); Import Address Table Filtering (IAF) • Load Library • Reflective DLL Injection • Shellcode • VBScript God Mode • Wow64 • Syscall • Hollow Process • DLL Hijacking • Squiblydoo Applocker Bypass • APC Protection (Double Pulsar / AtomBombing)
		Debe integrar funcionalidad que mitiguen la inyección de códigos en procesos.
		Debe integrar protección contra robo de credenciales
		Debe integrar protección contra malware escondido en aplicaciones legítimas (code cave)

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 6 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		Debe evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
		Debe evitar obtener escalada de privilegios y acceso elevado a recursos.
		Debe evitar la modificación de las claves de registro para la ejecución de código arbitrario
	5.1.2	PLATAFORMA DE EVALUACIÓN Y GESTIÓN DE SUPERFICIE DE ATAQUE PARA SERVIDORES CRITICOS
		La plataforma deberá poder desplegarse sobre treinta (30) servidores más críticos de la institución, lo cual permitirá evaluar el nivel de exposición al riesgo; tomando así, acciones de remediación crítica sobre los activos más vulnerables de la red.
		La plataforma; como resultado de la evaluación de exposición de riesgo inicial, deberá poder implementar un proceso de gestión de riesgo cibernético sobre treinta (30) servidores más críticos de la institución, monitoreando en tiempo real la postura de seguridad y el impacto de las actividades de remediación que se realicen durante tres años.
		La plataforma de evaluación de superficie de ataque deberá poder gobernar de forma integral el proceso de gestión de riesgos para los servidores seleccionados como críticos en la institución.
		La plataforma de evaluación de superficie de ataque deberá estar basada en solución 100% cloud y provista en modo de software as a Service (SaaS) a fin de no demandar ningún recurso adicional de infraestructura.
		La plataforma de evaluación de superficie de ataque deberá poder desplegar el agente de múltiples formas, desde la plataforma, desde el directorio activo o desde herramienta de distribución.
		La plataforma de evaluación de superficie de ataque deberá poder implementar un proceso de gestión de riesgos desde la identificación, priorización, presentación y remediación de riesgos a través del gobierno de activos de TI mediante un único agente ligero que permita administrar los módulos de vulnerabilidades, cumplimiento, anomalías, control de terminal y gestión de parches.
		La plataforma podrá crear usuarios de gestión basado en roles de gestión, administrador, técnico y auditor.
		La plataforma deberá poder habilitar un nivel de acceso modular a cada tipo de usuario creado, permitiendo que solo determinados usuarios tengan acceso a funciones de identificación y priorización de amenazas y otro grupo con accesos a funciones de remediación y ejecución de políticas.
		La plataforma de evaluación de superficie de ataque deberá integrar mínimamente módulos de análisis avanzado de vulnerabilidades, mapeo de vectores de ataque basados en malware, kits de explotación, cumplimiento normativo de la NITS, anomalías basadas en actividad de procesos, configuración de servicios, privilegios asignados, actividades de red, actividad de disco, integridad de archivos, actividad de puertos de comunicación, gestión integral de parches, aplicación de firmware y un panel de herramientas que permitan reiniciar servicios, desinstalar programas, instalar programas, parar procesos, quitar entradas en registro entre otros.
		La plataforma de evaluación de superficie de ataque deberá presentar un dashboard de priorización de riesgo, para ayudar a priorizar las vulnerabilidades.
		El dashboard de priorización de riesgo deberá estar implementado sobre el marco CISA SVCC (Stakeholder Specific Vulnerability Categorization).
		El dashboard deberá presentar un panel unificado que grafique una imagen clara y concisa de la postura de riesgo de seguridad de su organización, cubriendo Visibilidad, Detección, Priorización y Remediación, todo en una sola consola siendo interactivo.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 7 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		La plataforma de evaluación de superficie de ataque deberá presentar un Cyber Hygiene Score (CHS), una perspectiva para la puntuación de riesgos la cual deberá cuantificar los riesgos existentes con un puntaje de higiene proporcionando un plan de acción basado en un conjunto de mejores prácticas que puede seguir para remediar los riesgos y aumentar el puntaje de higiene cibernética en la red.
		La plataforma de evaluación de superficie de ataque deberá poder escanear la red a través de escaneos autenticados contra dispositivos de red de destino proporcionando credenciales para realizar escaneos autenticados en los dispositivos de red para descubrir vulnerabilidades a profundidad.
		La plataforma de evaluación de superficie de ataque deberá monitorear en tiempo real el consumo de RAM, CPU, actividad de red y actividad de disco a fin de poder brindarle al administrador evidencia sobre alguna posible anomalía.
		La plataforma de evaluación de superficie de ataque deberá presentar un sistema de puntuación de riesgo de errores de configuración (CCEs) basándose en el sistema de puntuación de configuración común (CCSS). Cada puntaje de CCE se calculará según el algoritmo CCSS y poder clasificarse como crítico, alto, medio y bajo.
		La plataforma de gestión de superficie de ataque deberá contar con una consola de administración centralizada que incluya todos los criterios de seguridad de acceso como factor de doble autenticación; además de estar diseñada y acondicionada para el gobierno remoto en tiempo real, de equipos dentro y fuera de la red de la entidad.
		La plataforma de gestión de superficie de ataque deberá integrar un inicio de sesión único (SSO) para una autenticación segura y sin problemas en base a SAML V2, admitiendo la integración con todos los proveedores de identidad compatibles con SAML v2, incluidos PingID, PingFederate, AWS, Azure, Auth0 y Okta.
		La plataforma de gestión de superficie de ataque deberá ser compatible con proveedores adicionales de autenticación multifactor (MFA) como ID de ping, Okta y Aplicaciones TOTP Authenticator.
		La plataforma de gestión de superficie de ataque deberá poder habilitar el acceso a usuarios basados en roles, administrador con acceso total, supervisor con posibilidad de solo ver el desempeño de la solución con posibilidad de generar informes y usuarios con privilegios restringidos a determinados módulos.
		La plataforma de gestión de superficie de ataque deberá poder integrarse al directorio activo a fin de descubrir, desplegar e integrar el sistema a la red de la entidad.
		La plataforma de gestión de superficie de ataque debe poder enviar alertas que se envíen automáticamente al correo electrónico cuando: Se detecte una vulnerabilidad con calificación crítica y/o alta y/o media y/o baja. Se determine la viabilidad de determinado ataque o malware reconocido. Se detecte una configuración débil o errónea se presente. Se presente un indicador de compromiso, la alerta deberá asociarse al ataque o malware específico. Se presente un indicador de ataque y cuando una determinada acción de respuesta no logre mitigar un ataque.
		La plataforma de gestión de superficie de ataque deberá poder lanzar tareas de escaneo de red desde los nodos que cuenten con el agente de gestión.
		La plataforma de gestión de superficie de ataque deberá incluir sistema de gestión de riesgos y usuarios desde donde se pueda habilitar perfiles de acceso con privilegios para ver, ver y editar configuraciones y ver, editar y lanzar tareas de remediación.
		La plataforma de gestión de superficie de ataque debe contar con un sistema de auditoría que identifique mediante código determinado Jobs ejecutado, fecha y hora de ejecución, además del usuario responsable de la ejecución.
		La plataforma de gestión de superficie de ataque debe presentar un panel de resumen de la

	FORMATO		Código : SGC-F-006
	ESPECIFICACIONES TECNICAS		Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 8 de 23 CUT : 163312-2023

		actividad de los activos donde se pueda apreciar mínimamente: Nombre del host, IP, Dirección MAC, Sistema Operativo, Versión y/o detalle técnico del agente que lo gobierna, Grupo al que pertenece, Status de actividad del servicio, Consumo en tiempo real del CPU, Consumo en tiempo real de la memoria RAM, Consumo en tiempo real de la red, Consumo en tiempo real de la actividad del disco.
		La plataforma de gestión de superficie de ataque debe ser compatible con los siguientes sistemas operativos Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 18.10, Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.10, Debian 7, Debian 8, Debian 9, Debian 10, Amazon Linux, Amazon Linux 2, Redhat Enterprise Linux 5, Redhat Enterprise Linux 6, Redhat Enterprise Linux 7, Redhat Enterprise Linux 8, CentOS 5, CentOS 6, CentOS 7, CentOS 8, Oracle Linux 5, Oracle Linux 6, Oracle Linux 7, Oracle Linux 8, Fedora 27, Fedora 28, Fedora 29, Fedora 31, Fedora 32.
		La plataforma de gestión de superficie de ataque debe integrar componentes de ciberseguridad que contribuyan a la gestión transversal de un proceso de ciberseguridad para estaciones de trabajo y servidores independiente del sistema operativo.
		La plataforma de gestión de superficie de ataque debe gestionar servidores y estaciones de trabajo multiplataforma a través de la ejecución de un agente ligero instalado en cada activo, el agente debe ser de un tamaño máximo de 16 MB.
		La plataforma de gestión de superficie de ataque debe garantizar que la instalación del agente no demande reinicios ni impacte en el consumo recursos durante su etapa de diagnóstico.
		La plataforma de gestión de superficie de ataque debe integrar su propia fuente de inteligencia de vulnerabilidades la cual deberá realizar mínimamente 150,000 comprobaciones.
		La plataforma de gestión de superficie de ataque deberá poder realizar escaneos rápidos de 5 a 7 minutos para detectar vulnerabilidades y riesgos automatizando todas las tareas desde una sola consola.
		La plataforma de gestión de superficie de ataque deberá poder instalar agentes en puntos finales heterogéneos y realizar todas las tareas que se les asignan sin consumir ancho de banda ni recursos del sistema excesivos.
		La plataforma de gestión de superficie de ataque deberá poder supervisar y administrar los dispositivos distribuidos desde una consola centralizada logrando incorporar nuevos dispositivos con facilidad y escalar a cualquier número de dispositivos.
		La plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de vulnerabilidades capaz de detener infracciones de seguridad identificando automáticamente las vulnerabilidades críticas, evaluando los riesgos y el potencial de explotación, priorizando las vulnerabilidades cruciales en función de su gravedad y corrigiéndolas instantáneamente mediante parches.
		La plataforma de gestión de superficie de ataque deberá detectar el Common Vulnerability Scoring System (CVSS), que determina la gravedad de la vulnerabilidad en función de las características principales que se traducen en una puntuación numérica.
		La plataforma de gestión de superficie de ataque deberá priorizar vulnerabilidades considerando factores internos y externos influyen en el panorama de amenazas en vivo en toda la organización llevando más allá de las herramientas que solo muestran puntajes CVSS considerando la actividad de explotación, el tiempo y la importancia de los sistemas afectados presentando mínimamente esta clasificación: Vulnerabilidades de movimiento lateral refiriéndose a vulnerabilidades que se extienden a la red a medida que la amenaza se mueve de un dispositivo a otro y de un activo a otro, permitiendo que los atacantes recopilen datos

	FORMATO		Código : SGC-F-006
	ESPECIFICACIONES TECNICAS		Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 9 de 23 CUT : 163312-2023

		valiosos. Vulnerabilidades fácilmente explotables que refieren a vulnerabilidades que son conocidas en el dominio público, lo que hace que un exploit se configure fácilmente. Vulnerabilidades de explotación pública disponible que hace referencia a vulnerabilidades para las cuales las explotaciones están disponibles públicamente y que se han producido en el pasado. Vulnerabilidades explotables en la red que refieren a vulnerabilidades que pueden explotarse con acceso a la red, a menudo de forma remota. El camino del atacante es a través de la capa de red.
		La plataforma de gestión de superficie de ataque deberá poder generar informes que enumeren los detalles de las vulnerabilidades según los grupos de dispositivos y dispositivos específicos, el reporte debe incluir las instancias de vulnerabilidades para cada activo vulnerable y una descripción de cada vulnerabilidad.
		La plataforma de gestión de superficie de ataque deberá poder reconocer las vulnerabilidades de cada grupo y host para posteriormente clasificar por gravedad, la gravedad de las vulnerabilidades se representa mediante códigos de color Rojo – Crítico, Naranja – Alto, Amarillo – Medio, Verde – Bajo.
		La plataforma de gestión de superficie de ataque deberá poder agrupar de forma gráfica los hosts, los activos implicados y las vulnerabilidades debidamente clasificadas con el correspondiente status del servicio.
		La plataforma de gestión de superficie de ataque deberá poder organizar de forma sencilla graficas de host más afectados a fin de tomar atención y priorizar las tareas de remediación.
		La plataforma de gestión de superficie de ataque deberá incluir una descripción detallada de las tareas de remediación o FIX por cada vulnerabilidad detectada y ponderarla.
		La plataforma de gestión de superficie de ataque deberá poder mostrar un panel que agrupe las vulnerabilidades por los kits de explotación que se pueden utilizar para explotar la debilidad como por ejemplo Zyklon Backdoor, ZombieLoad, VegaLocker Ransomware, Underminer Exploit Kit, ThreadKit Exploit Kit, Sundown-Pirate Exploit Kit. Esto permitiría priorizar las tareas de remediación.
		La plataforma de gestión de superficie de ataque deberá permitir implementar políticas de exclusión de vulnerabilidades de los informes, logrando excluir/eliminar vulnerabilidades de los informes después de aceptar los criterios de riesgo de exclusión. La política de exclusión se puede aplicar para una sola vulnerabilidad, varias vulnerabilidades o todas las vulnerabilidades de un activo.
		La plataforma de gestión de superficie de ataque deberá permitir implementar políticas de exclusión de parches de ser considerado para un trabajo de aplicación de parches o una regla logrando configurar una política para toda la cuenta para excluir el parche de la lista mientras crea un trabajo de aplicación de parches o una regla. Si no se aprueba un parche o si desea evitar las actualizaciones del sistema operativo o del paquete de servicio, o si hay herramientas de desarrollo que no desea actualizar, se puede aplicar una política de exclusión.
		La plataforma de gestión de superficie de ataque deberá automatizar el proceso de gestión de vulnerabilidades.
		La plataforma de gestión de superficie de ataque integrará un módulo de gestión de cumplimiento capaz de reforzar las configuraciones del sistema para reducir la exposición a amenazas, a través del cumplimiento de estándares regulatorios populares de la industria, como HIPAA, PCI, ISO y NIST.
		La plataforma de gestión de superficie de ataque deberá poder escanear de forma remota cualquier punto final vulnerable o desviado para remediar el riesgo de manera proactiva.
		La plataforma de gestión de superficie de ataque deberá poder presentar gráficos de cumplimiento por plataforma evaluada.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 10 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		La plataforma de gestión de superficie de ataque deberá poder crear plantillas personalizadas de auditoría de cumplimiento, definiendo y automatizando la validación de condiciones específicas de cumplimiento.
		La plataforma de gestión de superficie de ataque deberá poder validar como mínimo 3 aspectos de cumplimiento: Cumplimiento predeterminado, brindando la capacidad de que cada sistema operativo tenga reglas individuales de forma predeterminada, la solución deberá asignar los valores. Cumplimiento genérico, diseñado para corresponder a los diferentes sistemas operativos y configuraciones de seguridad, como la política de bloqueo de cuentas, las plantillas administrativas, los tipos de autenticación, etc. Cumplimiento normativo define estándares, como los estándares PCI, HIPAA y NIST.
		La plataforma de gestión de superficie de ataque deberá poder presentar de forma gráfica la cantidad y el detalle de las configuraciones de seguridad no habilitadas en cada host evaluado.
		<p>La plataforma de gestión de superficie de ataque debe cubrir mínimamente la siguiente lista de puntos de referencia para su módulo de cumplimiento:</p> <ul style="list-style-type: none"> • Tiempo mínimo de la contraseña • Permitir estados de espera cuando el equipo o servidor inicio sesión. • Requerir una contraseña cuando una computadora se activa. • Criptografía del sistema para el forzado de una fuerte protección de claves para las claves de usuario almacenadas en la computadora. • La clave debe cumplir los requerimientos de complejidad • Desactivar la prevención de ejecución de datos para el ejecutable de ayuda HTML • Requerir contraseña al conectarse. • Habilitar la autenticación del cliente del asignador de extremos de RPC • Requerir autenticación de usuario para conexiones remotas mediante autenticación de nivel de red • Requerir el uso de inicio rápido • Desactivar la prevención de ejecución de datos para Explorer • Hacer cumplir el historial de contraseñas • Seguridad de la red: nivel de autenticación de LAN Manager • Control del comportamiento del Registro de eventos cuando el archivo de registro alcanza su tamaño máximo (Seguridad) • Inicio de sesión interactivo: límite de inactividad de la máquina • Desactiva las notificaciones de aplicaciones en la pantalla de bloqueo • Permitir el acceso remoto a la interfaz Plug and Play • No procesar la lista de ejecutar una vez para la configuración del equipo • Restablecer contador de bloqueo de cuenta después • No enumerar usuarios conectados en equipos unidos a un dominio • Umbral de bloqueo de cuenta • Seguridad de red: seguridad de sesión mínima para clientes basados en NTLM SSP (incluido RPC seguro) • Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM • No procesar la lista de ejecución heredada para la configuración del equipo • Impedir la instalación de dispositivos extraíbles • Longitud mínima de la contraseña • Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash

FORMATO

Código : SGC-F-006
Versión : 00
Aprobado por : DSNIRH
Fecha aprob. : 13/09/2023
Página : 11 de 23
CUT : 163312-2023

ESPECIFICACIONES TECNICAS

		<p>y la firma</p> <ul style="list-style-type: none"> Control de cuentas de usuario: eleve solo las aplicaciones de UIAccess que están instaladas en ubicaciones seguras Acceso a la red: rutas y subrutas de registro accesibles de forma remota Miembro del dominio: cifre o firme digitalmente los datos del canal seguro (siempre) Control de cuentas de usuario: Comportamiento del aviso de elevación para usuarios estándar Control de cuentas de usuario: detecte instalaciones de aplicaciones y solicite la elevación Cuentas: estado de la cuenta de invitado Acceso a la red: restrinja el acceso anónimo a canalizaciones con nombre y recursos compartidos Acceso a la red: no permitir la enumeración anónima de cuentas SAM Acceso a la red: permite que los permisos de Todos se apliquen a usuarios anónimos Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador Control de cuentas de usuario: eleve solo los ejecutables que estén firmados y validados
		La plataforma de gestión de superficie de ataque debe auditar el cumplimiento a través de rutinas para presentar y/o evidenciar siempre una foto del momento, permitiendo evaluar estadísticamente el fortalecimiento de las configuraciones.
		La plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de activos para inventariar el hardware y el software relacionado al activo con información detallada de IP, MAC, Plataforma de Sistema Operativo, Detalles de Discos, Detalle de Componentes, fabricantes y el estado del activo.
		La plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de activos que presente gráficamente la distribución de dispositivos.
		La plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de activos que clasifique los inventarios en tiempo real en tipos de dispositivos, por fabricante, por riesgo asociado, por licencias, por aplicaciones, por violaciones a las políticas de uso, por uso de aplicaciones inscritas como lista negra, como lista blanca y aplicaciones poco utilizadas.
		La plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de activos que integre alertas y genere informes automáticos de forma centralizada.
		La plataforma de gestión de superficie de ataque debe integrar un módulo que proporcione una visibilidad total sobre los puntos finales gestionados.
		La plataforma de gestión de superficie de ataque debe integrar un módulo que ejecute acciones integradas que ayuden a que los terminales cumplan con las normas y estén actualizados con parches de software y hardware.
		<p>La plataforma de gestión de superficie de ataque debe integrar un módulo que ejecute acciones para alinear políticas de uso de los activos tales como:</p> <ul style="list-style-type: none"> Bloquear una aplicación por determinado tiempo. Permitir la ejecución de aplicaciones en determinados intervalos de tiempo. Bloquear y determinar el acceso a dispositivos por determinado intervalo de tiempo. Enviar un script Gestionar un proceso Gestionar un servicio Gestionar un registro

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 12 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		<ul style="list-style-type: none"> • Instalar o desinstalar una aplicación • Evaluar la red • Evaluar la transferencia de archivos • Validar que programas inician sesión • Borrar un archivo • Mover un archivo a cuarentena
		La plataforma de gestión de superficie de ataque debe integrar un módulo de consultas y respuestas que detecten ataques actuales y en curso incluyendo comandos para responder a las amenazas.
		La plataforma de gestión de superficie de ataque debe ser compatible con las fuentes STIX/TAXII, OpenIOC y Yara y use inteligencia de amenazas de otras fuentes para detectar indicadores de compromiso (IoC).
		La plataforma de gestión de superficie de ataque debe contar con su propia fuente de amenazas, los feeds de amenazas deben estar en formato JSON y se deberá poder realizar comprobaciones de registros y archivos y comprobaciones md5sum para fuentes de amenazas.
		La plataforma de gestión de superficie de ataque debe agregar y administrar diferentes fuentes de amenazas las cuales deben estar en constante actualización.
		La plataforma de gestión de superficie de ataque debe poder ejecutar consultas basadas en síntomas de ataque para investigar comportamientos anormales o detectar un ataque en curso en la red.
		<p>La plataforma de gestión de superficie de ataque debe reconocer mínimamente los siguientes indicadores de ataque (IoA):</p> <ul style="list-style-type: none"> • Notificación de AntiVirus Security Center deshabilitada • Anomalías en la creación de cuentas de computadora • Cortafuegos deshabilitados • Notificación del centro de seguridad del cortafuego deshabilitada • Procesos Altamente Sospechosos • Ejecutable de Svchost altamente sospechoso • Detección de ataques ICMP DoS • Detección de ataques de reproducción de Kerberos • Acceso al registro deshabilitado • Anomalías de tareas programadas • Explorador sospechoso • Proceso sospechoso llamado operación de servicio de sistema privilegiado • Anomalías de instalación de servicio sospechosas • Inicio de sesión de grupo especial sospechoso • Registro sospechoso de auditoría de seguridad de Windows borrado • Sistema ASLR deshabilitado • Sistema DEP siempre apagado • Sistema ExecShield deshabilitado • GateKeeper del sistema deshabilitado • Sistema NX DX deshabilitado • UAC del sistema desactivado • Administrador de tareas deshabilitado • Notificación del centro de seguridad de UAC deshabilitado

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 13 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		<ul style="list-style-type: none"> • Aplicación no autorizada que accede al puerto LPC • Actualizaciones Notificación del centro de seguridad deshabilitada • Anomalías en la creación de cuentas de usuario • Cuenta de usuario bloqueada o desbloqueada • Anomalías fallidas en el inicio de sesión de la cuenta de usuario • Cuenta de usuario o computadora creada o eliminada • Uso de CPU o RAM de Windows Más del 95 Porcentaje • Filtrado de Windows Bloqueado Conexión de paquetes sospechosos • Firewall de Windows no se pudo inicializar o iniciar
		La plataforma de gestión de superficie de ataque debe poder crear su propio grupo de consultas y respuestas especificando un nombre de paquete, la cantidad de veces que desea ejecutar la consulta y los intervalos en los que desea ejecutarla.
		La plataforma de gestión de superficie de ataque debe poder personalizar la ejecución de consultas inmediatamente, diariamente, semanalmente, mensualmente o en una fecha específica, especificando la hora y los días correspondientes de la semana, mes o fecha determinando la gravedad la cual puede ser baja, media, alta o crítica de la consulta.
		plataforma de gestión de superficie de ataque debe integrar un módulo de gestión de parches el cual permita relacionar sus actividades con los demás servicios requeridos.
		La plataforma de gestión de superficie de ataque debe permitir aplicar parches de seguridad que tengan por objetivo principal eliminar vulnerabilidades en el software por lo que sus gráficas y reportes estarán alineados a medir el impacto en términos de seguridad.
		La plataforma de gestión de superficie de ataque debe integrar un sistema de parchado, que automatice las tareas de parcheo de extremo a extremo, desde el escaneo hasta la implementación, para reducir la superficie de ataque y mejorar la postura de seguridad de manera efectiva.
		La plataforma de gestión de superficie de ataque debe incluir parches para todos los principales sistemas operativos, como Windows, Mac, Linux, firmware y muchas aplicaciones de terceros.
		La plataforma de gestión de superficie de ataque deberá poder relacionar los parches que se aplican con las vulnerabilidades latentes y llevar un control estadístico de la aplicación e impacto de estos.
		La plataforma de gestión de superficie de ataque deberá poder controlar el proceso de parchado considerando mínimamente: <ul style="list-style-type: none"> • Control sobre el reinicio • Remediación final o definitiva de una vulnerabilidad • Notificar la aplicación del parche • Lanzar un script de remediación antes y después de la aplicación del parche • Testear y desplegar
		La plataforma de gestión de superficie de ataque deberá cubrir la aplicación de parches software de terceros.
		La plataforma de gestión de superficie de ataque deberá poder escanear vulnerabilidades a dispositivos de red, páginas web y URLs específicos desde cualquier equipo o servidor con el agente.
		La plataforma de gestión de superficie de ataque deberá incluir rutinas de troubleshooting para ejecutarse remotamente.
		La plataforma de gestión de superficie de ataque deberá poder actualizar cualquier firma de antivirus de forma centralizada permitiendo corregir debilidades en las configuraciones.
		La plataforma de gestión de superficie de ataque deberá poder mapear amenazas de real-time

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 14 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

		threat hunting.
		<p>La plataforma deberá generar y exportar los siguientes reportes detallados sobre los mil (1000) activos expuestos durante la evaluación:</p> <ul style="list-style-type: none"> • Reporte ejecutivo de riesgos cibernéticos. • Informe de exposición de activos incluyendo Hostos físicos, virtuales, aplicaciones y servicios. • Informe de anomalía de postura. • Informe de vulnerabilidades y vectores de infección. • Informe de resultados. • Informe de evaluación de riesgos. • Informe de impacto del parche. • Informe de parches con detalle y referencia de aplicación. • Informe de gestión de terminales

6. INSTALACIÓN E IMPLEMENTACIÓN:

6.1. Alcances para la instalación e implementación

El Postor que se adjudique la Buena Pro, deberá realizar el proceso de instalación, configuración y puesta en marcha de políticas y operaciones de despliegue.

El Contratista deberá realizar el UPGRADE de versión del software instalado asegurándose que se utilice la última versión disponible.

El Contratista deberá entregar una guía de usuario en español que permita al administrador de la solución implementar todas las funcionalidades disponibles.

El Contratista deberá brindar una capacitación avanzada la cual deberá tener una duración mínima de ocho (08) horas.

El Contratista deberá organizar los activos reconocidos por ubicación (Según sedes).

El Contratista debe presentar un informe técnico con 3 capítulos bien detallados:

- Informe Técnico Capítulo N°1
Detalle de la exposición a riesgo cibernético sobre la totalidad de servidores en la institución en función a las vulnerabilidades, vectores de ataque conocidos, configuraciones débiles y anomalías a nivel de procesos, puertos, usuarios, servicios, eventos y actividad de red describiendo un plan de acción concreto para reducir la superficie de ataque en la institución.
- Informe Técnico Capítulo N°2
Detalle de implementación de la plataforma de gestión de riesgos sobre los treinta (30) activos más críticos después de la evaluación inicial realizada, se deberá adjuntar certificado de suscripción por el periodo de tres (03) años para continuar con las tareas de remediación en el tiempo.
- Informe Técnico Capítulo N°3
Informe de despliegue de la solución antimalware en estaciones y servidores de la red.

Los servicios de instalación e implementación deben ser realizados por:

- **Un (01) Especialista en Gestión de Proyectos**
 - ❖ Ingeniero titulado en la especialidad de Electricidad y/o Electrónica, sistemas, informática, redes, telecomunicaciones, computación o afines.
 - ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma antimalware ofertada con referencia al presente proceso, donde acredite que cuenta con certificación en identificación de amenazas, peligros y vulnerabilidades cibernéticas.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 15 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

- ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma de evaluación de superficie de ataque cibernético ofertado con referencia al presente proceso, donde acredite que cuenta con certificación en análisis y gestión de amenazas, peligros y vulnerabilidades cibernéticas.
- ❖ Tres (03) años de experiencia mínima como Jefe de Proyectos en Soluciones de Seguridad TI, ciberseguridad y/o similar.
Se debe acreditar para la presentación de la propuesta con la copia simple de título, constancia, certificado, u otro (según corresponda).
Actividades: Diseñar, Planificar y Auditar las actividades para la implementación de la solución ofertada.

○ **Un (01) Especialista en Seguridad TI**

- ❖ Ingeniero titulado en la especialidad de Electricidad y/o Electrónica, sistemas, informática, redes, telecomunicaciones, computación o afines.
- ❖ Curso, taller o diplomado de CIBERSEGURIDAD: ATAQUES Y CONTRAMEDIDAS con una duración mínima de veinte y cuatro (24) horas.
- ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma antimalware ofertada con referencia al presente proceso, donde acredite que cuenta con certificación en instalación, configuración y soporte de antimalware.
- ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma de evaluación de superficie de ataque cibernético ofertado con referencia al presente proceso, donde acredite que cuenta con certificación en instalación, configuración y soporte de plataforma de evaluación de superficie de ataque cibernético.
- ❖ Tres (03) años de experiencia mínima como especialista en seguridad TI, en Soluciones de Seguridad TI.
Se debe acreditar para la presentación de la propuesta con la copia simple de título, constancia, certificado, u otro (según corresponda).
Actividades: Ejecutar las actividades para la implementación y despliegue de la plataforma requerida.

○ **Un (01) Especialista de Apoyo, Soporte TI y Capacitaciones**

- ❖ Ingeniero titulado en la especialidad de Electricidad y/o Electrónica, sistemas, informática, redes, telecomunicaciones, computación o afines.
- ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma antimalware ofertada con referencia al presente proceso, donde acredite que cuenta con certificación en soporte y resolución de problemas de antimalware.
- ❖ Constancia emitida por la subsidiaria del fabricante en Perú de la plataforma de evaluación de superficie de ataque cibernético ofertado con referencia al presente proceso, donde acredite que cuenta con certificación en soporte y remediación de vulnerabilidades de plataforma de evaluación de superficie de ataque cibernético.
- ❖ Tres (03) años de experiencia mínima como especialista en soporte TI, en Soluciones de Seguridad TI.
Se debe acreditar para la presentación de la propuesta con la copia simple de título, constancia, certificado, u otro (según corresponda).

	<p style="text-align: center;">FORMATO</p>	<p>Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 16 de 23 CUT : 163312-2023</p>
	<p style="text-align: center;">ESPECIFICACIONES TECNICAS</p>	

Actividades: Ejecutar las actividades para la implementación, despliegue y soporte técnico de la plataforma requerida por el tiempo de la suscripción.

6.2. Alcances para el traslado de conocimiento

- El Contratista deberá incluir como parte de la adquisición, acceso a cursos oficiales de las plataformas y/o tecnologías ofertadas, lo cual permitirán el eficiente uso y administración de las plataformas solicitadas:
 - o Acceso a Curso Online con Certificación Técnica Oficial en el Portal del Fabricante de la plataforma ANTIMALWARE ofertada. Deberá cubrir el acceso a cuatro (04) técnicos y/o profesionales de la institución. El curso deberá desarrollar técnicas de despliegue, configuraciones ideales para cada entorno de red y troubleshooting.
 - o Acceso a Curso Online con Certificación Técnica Oficial en el Portal del Fabricante o Subsidiaria de la PLATAFORMA DE EVALUACIÓN Y GESTIÓN DE SUPERFICIE DE ATAQUE ofertada. Deberá cubrir el acceso a cuatro (04) técnicos y/o profesionales de la institución.

El curso deberá ponerse a disposición a través de una plataforma de e-learning interactiva que contenga video cursos, talleres live-online y aprendizaje GAMIFICADO con puntos, retos, badges y ranking, para fomentar la sana competencia entre los participantes.

Los temas que se desarrollarán en la plataforma de e-learning deberán cubrir mínimamente:

- o Criptografía
- o Reversing
- o Ransomware
- o Seguridad en redes
- o Gestión de identidades
- o Exploiting
- o Programación segura
- o Hacking Forense
- o Respuesta a incidentes
- o OWASP
- o Red Team
- o Blue Team
- o Pentesting
- o Riesgos en Ti
- o OSINT

Cada tema deberá desarrollarse en modalidades de básico, intermedio y avanzado.

- El Contratista deberá realizar una capacitación teórica - práctica sobre la protección antimalware que se proponga para un mínimo de cuatro (04) personas designadas por la Dirección del Sistema Nacional de Información de Recursos Hídricos de la Autoridad Nacional del Agua, con un mínimo de 04 horas, pudiendo ser en forma virtual o presencial, cumpliendo los protocolos de ley por la emergencia sanitaria. Al final de la capacitación se hará entrega de un certificado, para cada uno de los participantes; la misma que lo deberá realizar dentro de los 10 días calendario, contados a partir del día siguiente de la firma del contrato, se redactará un Acta de Capacitación en señal de conformidad. La capacitación deberá ser realizada por personal técnico certificado, se debe acreditar para la suscripción del contrato con la copia simple de la certificación oficial o carta emitida por el fabricante de la solución ofertada con referencia al presente proceso de selección que

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 17 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

acredite que el personal técnico certificado cumple las condiciones para realizar la capacitación.

- El contratista deberá implementar una base de conocimiento de las plataformas desplegadas las cuales describirá mínimamente:
 - o Procedimiento de instalación antimalware
 - o Procedimiento para mitigar ransomware y APTs
 - o Procedimientos para restablecer configuraciones del antivirus
 - o Procedimientos para reportar incidencias
 - o Procedimientos para validar reconocimiento de malware
 - o Procedimiento de gestión de riesgos cibernético en servidores identificando, priorizando, presentando y remediando vulnerabilidades, configuraciones débiles y anomalías basadas en indicadores de ataque (IoA) e indicadores de compromiso (IoC) sobre servidores.

7. **PRESENTACION OBLIGATORIA DENTRO DE LA PROPUESTA:**

El Postor dentro de su propuesta, deberá incluir al lado derecho de cada especificación técnica solicitada, de la captura de pantalla y el respectivo link del fabricante, donde se demuestre que cumple con cada especificación técnica solicitada. 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.

El Postor dentro de su propuesta deberá incluir carta de la subsidiaria del fabricante en Perú con referencia al presente proceso, que acredite que los componentes que forman parte de la plataforma antimalware son de la misma marca (donde se deberá indicar marca, modelo y de ser el caso el número de parte correspondiente).

8. **DURACION DE LA EJECUCION DEL CONTRATO:**

El plazo de la ejecución del contrato es por el periodo de (tres) 03 años contado a partir del día siguiente de suscrito el acta de implementación de toda la solución en la Autoridad Nacional del Agua.

9. **PRESTACIONES ACCESORIAS:**

SOPORTE TECNICO:

- La solución ofertada debe contar con 3 años de soporte, 24x7. Se debe acreditar para la presentación de la propuesta con una declaración jurada.
- El postor deberá considerar 3 años de soporte técnico vía telefónica, correo electrónico y presencial de forma ilimitada.
- A fin de asegurar un adecuado servicio post venta, el postor deberá contar con un sistema de gestión de tickets online; el cual permita el registro y seguimiento de cada incidencia reportada, así como el acceso a una base de conocimientos que reúna las buenas prácticas y todo el Now How requerido para gestionar la solución. Se debe presentar en la propuesta una declaración de jurada indicando los datos de contacto y alcances solicitados.
- El contratista deberá incluir una bolsa de horas de soporte técnico ilimitada 24x7x365 la cual se presentará en dos niveles:
 - Nivel 1: Soporte local responsable de implementaciones, migraciones, reinstalaciones, seguimiento para mantenimiento y capacitación técnica certificada.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 18 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

- Nivel 2: Bolsa de 180 minutos de soporte técnico directo con el fabricante, para brindar soluciones integrales a casos de emergencias relacionadas a problemas específicos.

10. CONDICIONES GENERALES:

- Las licencias ofertadas deben ser en su última versión publicada por el fabricante.
- 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.

11. LUGAR DE ENTREGA DEL SOFTWARE

En la Sede Central de La Autoridad Nacional del Agua, Calle Diecisiete N° 355, Urb. El Palomar – San Isidro.

12. PLAZO DE ENTREGA

12.1. PARA LA PRESTACION PRINCIPAL

El plazo máximo de entrega, instalación e implementación es de 20 días calendario (incluido el traslado de conocimiento y entrega de los certificados), contados a partir del día siguiente de la firma del contrato.

12.2. PARA LA ACTIVACIÓN DEL LICENCIAMIENTO

La fecha de activación del licenciamiento objeto del presente proceso de selección, iniciará el 21 de diciembre del 2023.

12.3. PARA LA PRESTACION ACCESORIA

El soporte técnico será durante los tres (3) años 24x7, contados a partir del día siguiente de la activación del licenciamiento. Anualmente se brindará una conformidad sobre el servicio brindado.

13. SISTEMA DE CONTRATACIÓN

Suma Alzada

14. MODALIDAD DE EJECUCIÓN CONTRACTUAL

Llave en mano

15. ADELANTOS

No corresponde

16. SUPERVISION Y CONFORMIDAD

La supervisión estará a cargo del personal de la Dirección del Sistema Nacional de Información de Recursos Hídricos – DSNIRH de la Autoridad Nacional del Agua y la conformidad a cargo del director de la DSNIRH.

En señal de conformidad se presentará un acta para otorgar conformidad a la adquisición del bien, dentro del plazo de 07 días calendarios.

17. FORMA DE PAGO

Para efectos del pago de las contraprestaciones ejecutadas por el postor ganador, la entidad deberá realizar el pago de la contraprestación pactada a favor del contratista en dos formas de pago sobre las

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 19 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

prestaciones equivalentes por la duración del contrato, siendo:

Armadas	Formas de Pago de Prestación Principal	
	Descripción	Forma de Pago
Única Armada:	Después de ejecutado la instalación e implementación, capacitación y entrega de los certificados y emitido la conformidad.	100% del monto total de la Prestación Principal según contrato.

Armadas	Formas de Pago Prestaciones Accesorias	
	Descripción	Forma de Pago
Primera Armada:	- <u>Soporte Técnico</u> ; después de los trescientos sesenta y cinco (365) días calendario de la conformidad de la prestación principal; previa Acta de Conformidad del Soporte Técnico.	40% del monto total ofertado por brindar el servicio de Soporte Técnico según contrato.
Segunda Armada:	- <u>Soporte Técnico</u> ; después de los setecientos treinta (730) días calendario de la conformidad de la prestación principal; previa Acta de Conformidad del Soporte Técnico.	30% del monto total ofertado por brindar el servicio de Soporte Técnico según contrato.
Tercera Armada:	- <u>Soporte Técnico</u> ; después de los un mil noventa y cinco (1095) días calendario de la conformidad de la prestación principal; previa Acta de Conformidad del Soporte Técnico.	30% del monto total ofertado por brindar el servicio de Soporte Técnico según contrato.

18. PENALIDAD

Si el proveedor incurre en retraso injustificado en la ejecución de las prestaciones objeto del requerimiento, LA ENTIDAD le aplicará una penalidad por cada día de atraso, hasta por un monto máximo equivalente de hasta el diez por ciento (10%) del monto de la orden de compra o del monto del ítem que debió ejecutarse.

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

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

$$\text{PENALIDAD DIARIA} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Esta penalidad será deducida de los pagos periódicos, de los pagos parciales o pago final.

19. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por vicios ocultos del bien ofertado por un plazo de tres (03) años, contado a partir de la conformidad otorgada por la Entidad.

20. CONFIDENCIALIDAD:

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 20 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

El proveedor 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 servicio, a menos que cuente con un pronunciamiento escrito de la ANA en sentido contrario.

21. 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 del presente servicio, en el marco de la Ley N° 822, Ley sobre derecho de autor. Asimismo, se compromete a no utilizarlos para fines distintos a los del servicio realizado, ni durante su ejecución ni después de la recepción del mismo, sin que medie autorización escrita otorgada por ANA.

22. CESION DE DERECHOS:

Por medio de la presente clausula, 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 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.”

23. 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 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 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 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 21 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

REQUISITOS DE CALIFICACION:

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
B.1	FACTURACIÓN
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none"> - El postor debe acreditar un monto facturado acumulado equivalente a S/1,000,000.00 (Un millón con 00/100 soles) por la venta de bienes similares al objeto de la convocatoria y/o en la actividad, durante un periodo de ocho (08) años a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: Ventas y/o renovación de Software Antivirus <p><u>Acreditación:</u></p> <p>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 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° 7 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</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>

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 22 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

	<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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>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.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 7 referido a la Experiencia del Postor en la Especialidad.</p> <p><u>IMPORTANTE</u> En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto materia de la convocatoria, previamente ponderada, conforme a la Directiva N° 002-2016-OSCE/CD "Participación de Proveedores en Consorcio en las Contrataciones del Estado"</p>
C	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Un (01) Especialista en Gestión de Proyectos</p> <ul style="list-style-type: none"> - Tres (03) años de experiencia mínima como Jefe de Proyectos en Soluciones de Seguridad TI, ciberseguridad y/o similar. <p>Un (01) Especialista en Seguridad TI</p> <ul style="list-style-type: none"> - Tres (03) años de experiencia mínima como especialista en seguridad TI, en Soluciones de Seguridad TI. <p>Un (01) Especialista de Apoyo, Soporte TI y Capacitaciones</p> <ul style="list-style-type: none"> - Tres (03) años de experiencia mínima como especialista en soporte TI, en Soluciones de Seguridad TI. <p><u>Acreditación:</u> La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos:</p> <ul style="list-style-type: none"> (i) Copia simple de contratos y su respectiva conformidad, o; (ii) Constancias o certificados, o; (iii) Cualquier otra documentación que de manera fehaciente demuestre la experiencia del personal propuesto.

	FORMATO	Código : SGC-F-006 Versión : 00 Aprobado por : DSNIRH Fecha aprob. : 13/09/2023 Página : 23 de 23 CUT : 163312-2023
	ESPECIFICACIONES TECNICAS	

	<p>Importante</p> <ul style="list-style-type: none"> • <i>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.</i> • <i>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.</i> • <i>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.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i>
--	---

	<p>Importante</p> <ul style="list-style-type: none"> • <i>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.</i> • <i>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.</i> • <i>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.</i>
--	--