INFORME TÉCNICO PREVIO EVALUACIÓN DE SOFTWARE N° 002-2023-ANA-DSNIRH

SOFTWARE DE DETECCIÓN DE AMENAZAS AVANZADAS DE LA RED (EDR)

1. NOMBRE DEL ÁREA

Dirección del Sistema Nacional de Información de Recursos Hídricos

2. RESPONSABLE DE LA EVALUACIÓN

Ing. Javier Eduardo Suarez Niño
Director de la Dirección del Sistema Nacional de Información de Recursos Hídricos

Ing. Junior David Morocho Torres
Coordinador de Infraestructura y Comunicaciones

3. FECHA

14 de junio de 2023

4. JUSTIFICACIÓN

En el marco DS N° 103-2022-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública al 2030, la misma que plantea cuatros (04) objetivos prioritarios y veintidós (22) lineamientos. Los Objetivos Prioritarios "Mejorar la gestión interna en las entidades públicas" y "Fortalecer la mejora continua en el estado", están vinculados al Planeamiento Estratégico y Operativo.

El Decreto Legislativo N° 1088, Ley del Sistema Nacional de Planeamiento Estratégico y del Centro Nacional de Planeamiento Estratégico, se creó el Sistema Nacional de Planeamiento Estratégico como conjunto articulado e integrado de órganos, subsistemas y relaciones funcionales cuya finalidad es coordinar y viabilizar el proceso de planeamiento estratégico nacional para promover y orientar el desarrollo armónico y sostenido del país. Entre sus diferentes etapas establece que el seguimiento es un proceso continuo, oportuno y sistemático donde se analiza el avance en el cumplimiento de las políticas nacionales y planes, asimismo comprende la recopilación periódica de información, su registro sistematizado y un análisis descriptivo donde se compara lo obtenido respecto a lo esperado.

Por ello, la Autoridad Nacional del Agua, requiere evaluar softwares de detección de amenazas avanzadas de la red (EDR); a fin de optimizar la capa de seguridad en razón de que actualmente, la entidad cuenta con una infraestructura de alta criticidad para las operaciones institucionales la cual, brinda servicios de red, internet y acceso a otros servicios que permiten la ejecución de actividades institucionales por parte de los colaboradores en la sede central y en órganos

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

desconcentrados nivel nacional, y que por medio de las estaciones de trabajo procesan la información.

En tal sentido, cabe señalar que, la internet es un medio inseguro donde se producen diversos tipos de ataques informáticos con la finalidad de vulnerar la seguridad de las redes de las entidades y cometer delitos informáticos, como es acceso ilícito, fraude informático, suplantación de identidad y sustracción o robo de información reservada. Una de las principales amenazas que enfrentan las computadoras conectadas a la Internet, son los malware del tipo "ransomware".

Las amenazas tipo ransomware tienen por objetivo inutilizar la información del equipo infectado, capturando la información del equipo y encriptándola con una llave digital específica a la cual solo tiene acceso el atacante.

Para recuperar la información, usualmente el atacante pide una recompensa económica, normalmente a través de una criptomoneda, sin embargo, no hay ninguna garantía de que el atacante pueda liberar la información encriptada, aun realizando el pago.

Una vez capturada y encriptada la información, no existe software de seguridad actual que permita liberar la información para ser recuperada, es por ello la gravedad de este tipo de malware, con mayor riesgo cuando se refiere a las computadoras de la Autoridad Nacional del Agua que se encuentran con acceso a la Internet, y que adicionalmente, al poder infectarse e inutilizar la información del profesional; existe el riesgo de que esta amenaza, también pueda ser diseminada por la red a los servidores de la institución, ya que algunos de los profesionales acceden a los servidores de archivos de manera remota para el cumplimiento de sus labores.

En el caso de los ransomware, pueden encontrarse alojados en un sitio web o servidor externo infectado que contiene la amenaza, y que una vez accedido, este es descargado a las computadoras sin ser detectado por la víctima, aun cuando ésta tenga un antimalware "tradicional" (ya sea antivirus u otro) actualizado a la fecha. Existen además otros tipos de amenazas, que son cada vez más sofisticados y difíciles de identificar, tales como el phishing.

Estas amenazas generalmente emplean como foco de ataque el correo electrónico, a través del cual envían comunicaciones que inducen a los usuarios a ingresar a enlaces de internet de sitios web fraudulentos, haciéndose pasar por canales oficiales o formales de comunicación. Una vez ingresado a los enlaces donde se aloja la amenaza, el atacante puede robar información personal, que va desde credenciales de accesos, contraseñas, número de tarjeta bancaria, entre otros.

Si bien actualmente, la Autoridad Nacional del Agua a través de la Dirección del Sistema Nacional de Información de Recursos Hídricos, ha implementado

herramientas perimetrales para la prevención de SPAM y Antimalware en el canal de correo electrónico, es cada vez más común a nivel mundial ver como las amenazas de phishing atraviesan los filtros perimetrales sin ser detectados y llegan a los equipos de las víctimas. Además, el phishing podría llegar por otros canales de correo que no son gestionados por la institución, como son los correos de dominios públicos (Ej. Gmail, Hotmail, entre otros) a los cuales se tiene acceso desde los equipos de la institución.

Por lo tanto, es en esta instancia (estaciones de usuarios) donde se debe proteger y mitigar la amenaza, para que el ciclo del ataque no sea efectivo, aun cuando atraviesen los controles actuales.

Si bien existen mecanismos preventivos ya establecidos en los equipos de la institución, estos no resultan suficientes y tienen que ser complementados con la capacidad de identificación y respuesta de amenazas, componentes que resultan necesario ante amenazas más sofisticadas que tienen técnicas evasivas, o en los casos donde se requiere control a nivel de aplicación, contraste con indicadores de compromiso (IoC) externos, o información detallada de la amenaza para poder contenerla (fuente origen de la amenaza, nivel de impacto y alcance de los dispositivos comprometidos).

Estas nuevas técnicas de seguridad y respuesta ante amenazas, se utilizan mediante el uso de un software EDR (Endpoint Detection and Response), que ayudan a tener una mayor visibilidad y cobertura de detección de las amenazas no conocidas, ya que incorporan nuevas tecnologías basadas en emulación de malware (sandbox), identificación amenazas basadas en comportamiento e información forense para acciones de remediación y respuesta ante incidentes.

Los softwares EDR brindan capacidades de identificación detalla de las amenazas detectadas, indicando puntos de entrada, acciones de remediación, impacto o alcance de la amenaza, tipo de ataque, ejecución de procesos y reputación de archivos, todo ellos integrados en una consola de gestión, con la finalidad de poder tomar acción rápida para la respuesta ante amenazas. Este tipo de software es muy importante, ya que reduce considerablemente el tiempo empleado en la identificación y contención.

En síntesis, las medidas de seguridad informática empleadas por la Autoridad Nacional del Agua son adecuadas y han permitido la continuidad de los servicios y operaciones diarias. Sin embargo, estas requieren ser fortalecidas dada la identificación de nuevas amenazas globales más complejas que pueden no lograr ser detectadas por las versiones actuales de herramientas de seguridad informáticas, tanto en la parte perimetral, como en las estaciones de los profesionales de la ANA que se conectan a través de Internet.

Por lo expuesto y en el marco de la Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública" se procede a evaluar herramientas de software de detección de amenazas avanzadas de la red (EDR) que permitan responder de manera oportuna ante un evento de seguridad informática, permitiendo con ello la mejora de la seguridad informática con que cuenta la Autoridad Nacional del Agua.

5. ALTERNATIVAS DE EVALUACIÓN

En base a la experiencia del personal de la Dirección del Sistema Nacional de Información de Recursos Hídricos, las investigaciones realizadas a través de Internet y en el mercado local, se ha realizado la selección de tres (03) alternativas de productos que consoliden la seguridad institucional de manera oportuna ante un evento de seguridad informática, a través de herramientas de software de detección de amenazas avanzadas de la red (EDR), que cumplan con los requerimientos expuestos y dispongan de soporte local, siendo los encontrados los siguientes:

- ✓ FortiEDR
- ✓ CARBONBLACK
- ✓ CORTEX

6. ANÁLISIS COMPARATIVO TÉCNICO

El informe se ha realizado utilizando los parámetros establecidos en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

6.1. Propósito de Evaluación

Validar que las alternativas seleccionadas sean las más convenientes para cubrir las necesidades de la Autoridad Nacional del Agua, de forma que permita agenciar de un software de detección de amenazas avanzadas de la red (EDR) que fortalezca y optimice la capa de seguridad informática con que cuenta la institución, brindando capacidades de identificación detalla de las amenazas detectadas, indicando puntos de entrada, acciones de remediación, impacto o alcance de la amenaza, tipo de ataque, ejecución de procesos y reputación de archivos; con la finalidad de poder tomar acción rápida para la respuesta ante amenazas. El propósito es poder determinar los atributos y/o características mínimas para el producto a adquirir.

6.2. Identificar el tipo de producto

- ✓ Software de detección de amenazas avanzadas de la red (EDR).

6.3. Identificación del Modelo de Calidad

Para la evaluación técnica del software de detección de amenazas avanzadas de la red (EDR), se va utilizar la guía de evaluación de software aprobado por Resolución Ministerial Nº 139-2004-PCM.

6.4. Selección de métricas

Las métricas fueron seleccionadas en base a las necesidades de implementación de la institución, los criterios técnicos del personal de la Dirección del Sistema Nacional de Información de Recursos Hídricos, el análisis de las características de productos de software de detección de amenazas avanzadas de la red (EDR), el propósito de la adquisición de la solución y a la información técnica de los productos señalados en el punto 5 del presente informe (alternativas).

En el Anexo Nº 01 se presenta las características técnicas que debe cumplir la solución y sus respectivas métricas.

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

(Ver Anexo Nº 02)

8. COTIZACIONES

(Ver Anexo Nº 03)

9. CONCLUSIÓN

Se determinaron los atributos y/o características técnicas mínimas para la solución de Software de detección de amenazas avanzadas de la red (EDR) requerido, así como el análisis de costo – beneficio para la Autoridad Nacional del Agua por lo cual; se concluye que la mejor alternativa para Software de colección de detección de amenazas avanzadas de la red (EDR) es el software FortiEDR, al obtener el mayor puntaje de la evaluación.

10. FIRMAS

FIRMADO DIGITALMENTE ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B° **JAVIER EDUARDO SUAREZ NIÑO** DIRECTOR DIRECCIÓN DEL SISTEMA NACIONAL DE INFORMACIÓN DE RECURSOS HÍDRICOS AUTORIDAD NACIONAL DEL AGUA	**FIRMADO DIGITALMENTE** ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B° **JUNIOR DAVID MOROCHO TORRES** PROFESIONAL DIRECCION DEL SISTEMA NACIONAL DE INFORMACION DE RECURSOS HIDRICOS AUTORIDAD NACIONAL DEL AGUA

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

ANEXO N° 01

ANÁLISIS COMPARATIVO TÉCNICO

1. ESTABLECIMIENTO DE LAS MÉTRICAS

1.1. Atributos y Calidad de Uso

Atributos internos/externos			Puntajes	
Ítem	**Características**	**Descripción**	**Max**	**Min**
1	Funcionalidad	Análisis de comportamiento e inteligencia artificial (sin depender de firmas), entrenada por los expertos en seguridad cibernética de la marca, detectando todas las amenazas conocidas y desconocidas. El aprendizaje automático debe mejorar las detecciones al reconocer nuevas tácticas, técnicas y procedimientos emergentes con lanzamientos de procesos asociados, conexiones de red y tipos de aplicaciones.	4	1
2		Proteger contra amenazas avanzadas, actividad sospechosa de red y actividad maliciosa	4	1
3		La solución deberá permitir la creación de indicadores de compromiso (IoCs) de forma personalizada.	4	1
4		Catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.	4	1
5		El cliente EDR debe tener un agente que le permita ser administrado desde una consola centralizada "on premise o en nube. Este agente debe reportar el estado de todas las soluciones instaladas en la dependencia.	4	1
6		Consola de gestión 100% web y de acceso seguro vía HTTPS y con doble factor de autenticación donde se deberá gestionar entre otras cosas: ✓ El análisis de causa raíz de la detección. ✓ El listado de equipos, así como el inventario de aplicaciones utilizadas en cada uno de los EDR. ✓ El análisis detallado de la detección con el listado de direcciones de archivos, procesos, URLS, eventos y demás acciones que ha realizado la detección. ✓ Integración con motores de análisis de malware en tiempo real para la verificación automática de firmas de archivos en dicha plataforma.	4	1

		✓ Permitir correlacionar los eventos detectados. ✓ Listar todas las detecciones similares presentes en otros EDR con el fin de tomar acciones de corrección. ✓ Permitir realizar el aislamiento de los equipos afectados. ✓ Permitir filtrar las amenazas de acuerdo con el grado de riesgo, éstos deben ser configurables por lo menos en (03) niveles.		
7		El servidor de administración remota debe estar en idioma español o inglés y deberá ser compatible al menos con los siguientes sistemas operativos: ✓ Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019 ✓ Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit.	4	1
8		Las alertas o eventos deberán de tener un periodo de retención mínimo de 90 días.	4	1
9		Contar con protección especializada contra ataques de ramsonware y exploits de tipo Día Zero.	4	1
10		Generación de reportes avanzados en modo gráfico, que permitan identificar: ✓ Intentos de infección más repetidos y recientes en la red. ✓ Host con mayor número de infección. ✓ Dispositivos de almacenamiento externos bloqueados por usuario. ✓ Cantidad de estaciones/servidores con o sin EDR. ✓ Última conexión de los hosts a la consola. ✓ Última actualización de los hosts y la versión del agente instalado.	4	1
11		Reconocer un incidente y ser enviado al fabricante desde la misma consola para su análisis e investigación de la amenaza con el fin de contar con mayor detalle de esta, así como recibir información para su reconocimiento y posterior respuesta frente a incidentes iguales o similares.	4	1
12		El EDR usará la automatización de procesos para detener y contener las amenazas inmediatamente. También deberá proporcionar una visualización del ataque con todos los puntos finales afectados, y una guía sobre cómo aislar y remediar la amenaza.	4	1
13		Capacidad de escanear y ejecutar los archivos recopilados, en un ambiente aislado para un	4	1

		análisis profundo basado tecnología sandbox opcionalmente de análisis local, utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red.		
14		Sistema de reportes de EDR el cual deberá permitir configurar lo siguiente: ✓ El envío de reportes diarios, semanales o mensuales de la detección de amenazas. ✓ Programar el envío automático de alertas por correo frente a la detección de una amenaza.	4	1
15	Eficiencia	Instalación de agentes livianos desplegados en las versiones de los Sistemas Operativos de las estaciones de trabajo, laptops y servidores de TI.	4	1
16		Detecta, detiene, bloquea y evita la instalación, propagación e infección de amenazas avanzadas desconocidas.	4	1
17	Capacidad de Mantenimiento	La desinstalación del agente deberá de requerir un código o contraseña para que no lo puedan desinstalar los usuarios.	4	1
18		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.	4	1
19	Portabilidad	Instalarse en su última versión, sobre las plataformas Windows Server 2003, Windows 7, Windows 8, Windows 8.1, Windows 10, Vmware, Hyper-V. Contar con soporte para plataformas de 32 y 64 bits. Sobre las plataformas Linux de 32 y 64 bits, en distribuciones basadas en Ubuntu y RedHat tales como: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit	4	1
20		La consola de acceso al servidor deberá ser 100% web, siendo compatible mínimamente con los navegadores: Chrome y Mozilla Firefox.	4	1
		Total (A):	80	20

Métricas de calidad de uso			**Puntajes**	
Ítem	**Características**	**Descripción**	**Max**	**Min**
21	Eficacia	Detecta y brinda contra amenazas: a) Antes de su ejecución, b) En ejecución, c) Después de su ejecución.	4	1
22		La solución antimalware debe permitir un análisis forense de lo ocurrido en los equipos, permitiendo realizar una correlación de eventos que brinde visibilidad detallada de las amenazas presentadas.	4	1

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

23	Productividad	La solución debe tener la capacidad de analizar cualquier tipo de amenaza en laboratorio de inteligencia del fabricante con el objetivo de recategorizar cualquier tipo de evento.	4	1
24		La consola de administración debe desplegar las actualizaciones a los agentes clientes de forma automática y de la manera óptima en relación de seguridad y performance.	4	1
25	Seguridad	Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Antimalware.	4	1
Total (B):			20	5
TOTAL (A)+(B):			100	25

Cuadro 01.- Determinación de métricas y atributos, acorde con los requerimientos técnicos de la Entidad, así como su asignación de puntajes máximos y mínimos, conforme a las recomendaciones realizadas en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

2. COMPARACIÓN DE PRODUCTOS VS MÉTRICAS

Métricas de Calidad del Producto (Atributos internos/externos)			Puntajes		FortiEDR	CARBON BLACK	CORTEX
Ítem	Características	Descripción	Max	Min			
1	Funcionalidad	Análisis de comportamiento e inteligencia artificial (sin depender de firmas), entrenada por los expertos en seguridad cibernética de la marca, detectando todas las amenazas conocidas y desconocidas. El aprendizaje automático debe mejorar las detecciones al reconocer nuevas tácticas, técnicas y procedimientos emergentes con lanzamientos de procesos asociados, conexiones de red y tipos de aplicaciones.	4	1	4	4	4
2		Proteger contra amenazas avanzadas, actividad sospechosa de red y actividad maliciosa	4	1	4	4	4
3		La solución deberá permitir la creación de indicadores de compromiso (IoCs) de forma personalizada.	4	1	4	3	3
4		Catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.	4	1	4	4	3
5		El cliente EDR debe tener un agente que le permita ser administrado desde una consola centralizada "on premise o en nube. Este agente debe reportar el estado de todas las soluciones instaladas en la dependencia.	4	1	4	4	4
6		Consola de gestión 100% web y de acceso seguro vía HTTPS y con doble factor de autenticación donde se deberá gestionar entre otras cosas: ✓ El análisis de causa raíz de la detección. ✓ El listado de equipos, así como el inventario de aplicaciones utilizadas en cada uno de los EDR. ✓ El análisis detallado de la detección con el listado de direcciones de archivos, procesos, URLS, eventos y demás acciones que ha realizado la detección. ✓ Integración con motores de análisis de malware en tiempo real para la verificación automática de firmas de archivos en dicha plataforma. ✓ Permitir correlacionar los eventos detectados.	4	1	4	4	4

		✓ Listar todas las detecciones similares presentes en otros EDR con el fin de tomar acciones de corrección. ✓ Permitir realizar el aislamiento de los equipos afectados. Permitir filtrar las amenazas de acuerdo con el grado de riesgo, éstos deben ser configurables por lo menos en (03) niveles.					
7		El servidor de administración remota debe estar en idioma español o inglés y deberá ser compatible al menos con los siguientes sistemas operativos: ✓ Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019 Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit.	4	1	4	4	4
8		Las alertas o eventos deberán de tener un periodo de retención mínimo de 90 días.	4	1	4	3	3
9		Contar con protección especializada contra ataques de ramsonware y exploits de tipo Día Zero.	4	1	4	4	4
10		Generación de reportes avanzados en modo gráfico, que permitan identificar: ✓ Intentos de infección más repetidos y recientes en la red. ✓ Host con mayor número de infección. ✓ Dispositivos de almacenamiento externos bloqueados por usuario. ✓ Cantidad de estaciones/servidores con o sin EDR. ✓ Última conexión de los hosts a la consola. Última actualización de los hosts y la versión del agente instalado.	4	1	4	4	3
11		Reconocer un incidente y ser enviado al fabricante desde la misma consola para su análisis e investigación de la amenaza con el fin de contar con mayor detalle de esta, así como recibir información para su reconocimiento y posterior respuesta frente a incidentes iguales o similares.	4	1	4	4	4
12		El EDR usará la automatización de procesos para detener y contener las amenazas inmediatamente. También deberá proporcionar una visualización del ataque con todos los puntos finales afectados.	4	1	4	4	3
13		Capacidad de escanear y ejecutar los archivos recopilados, en un ambiente	4	1	4	4	4

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

		aislado para un análisis profundo basado tecnología sandbox opcionalmente de análisis local, utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red.					
14		Sistema de reportes de EDR el cual deberá permitir configurar lo siguiente: ✓ El envío de reportes diarios, semanales o mensuales de la detección de amenazas. Programar el envío automático de alertas por correo frente a la detección de una amenaza.	4	1	4	4	3
15	Eficiencia	Instalación de agentes livianos desplegados en las versiones de los Sistemas Operativos de las estaciones de trabajo, laptops y servidores de TI.	4	1	4	4	3
16		Detecta, detiene, bloquea y evita la instalación, propagación e infección de amenazas avanzadas desconocidas.	4	1	4	4	4
17	Capacidad de Mantenimiento	La desinstalación del agente deberá de requerir un código o contraseña para que no lo puedan desinstalar los usuarios.	4	1	4	4	4
18		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.	4	1	4	4	4
19	Portabilidad	Instalarse en su última versión, sobre las plataformas Windows Server 2003, Windows 7, Windows 8, Windows 8.1, Windows 10, Vmware, Hyper-V. Contar con soporte para plataformas de 32 y 64 bits. Sobre las plataformas Linux de 32 y 64 bits, en distribuciones basadas en Ubuntu y RedHat tales como: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit	4	1	4	4	4
20		La consola de acceso al servidor deberá ser 100% web, siendo compatible mínimamente con los navegadores: Chrome y Mozilla Firefox.	4	1	4	4	4
		Total (A):	80	20	**80**	**78**	**73**

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

Métricas de calidad de uso			Puntajes		FortiEDR	CARBON BLACK	CORTEX
Ítem	Características	Descripción	Max	Min			
21	Eficacia	Detecta y brinda protección contra amenazas: a) Antes de su ejecución, b) En ejecución, c) Después de su ejecución.	4	1	4	3	3
22		La solución antimalware debe permitir un análisis forense de lo ocurrido en los equipos, permitiendo realizar una correlación de eventos que brinde visibilidad detallada de las amenazas presentadas.	4	1	4	4	4
23	Productividad	La solución debe tener la capacidad de analizar cualquier tipo de amenaza en laboratorio de inteligencia del fabricante con el objetivo de recategorizar cualquier tipo de evento.	4	1	4	4	4
24		La consola de administración debe desplegar las actualizaciones a los agentes clientes de forma automática y de la manera óptima en relación de seguridad y performance.	4	1	4	4	4
25	Seguridad	Permitir bloquear y/o desactivar mediante políticas el acceso a las opciones de configuración del Antimalware.	4	1	4	4	4
		Total (B):	20	5	**20**	**19**	**19**
TOTAL (A)+(B):			100	25	**100**	**97**	**92**

Cuadro 02.- Determinación de puntajes a los productos FortiEDR, CARBONBLACK y CORTEX, en función a su acercamiento con los atributos y métricas previamente establecidas en el cuadro 01.

3. RESUMEN DEL ANÁLISIS COMPARATIVO TÉCNICO

MÉTRICAS	PRODUCTO 1	PRODUCTO 2	PRODUCTO 3
	FortiEDR	CARBONBLACK	CORTEX
Total de Métricas de Calidad del Producto	80	78	73
Total de Métricas de Calidad de Uso	20	19	19
Total	**100**	**97**	**92**

Cuadro 03.- Resumen de los resultados obtenidos en el cuadro 02.

Se puede observar producto del análisis comparativo técnico realizado, que el mayor puntaje obtenido es del software de detección de amenazas avanzadas de la red (EDR) **FortiEDR** al obtener 100 puntos producto de la evaluación, seguido de los softwares de detección de amenazas avanzadas de la red (EDR) **CARBONBLACK y CORTEX,** con 97 y 92 puntos respectivamente.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

ANEXO N° 02

ANÁLISIS COMPARATIVO COSTO – BENEFICIO

1) ANÁLISIS COSTO – BENEFICIO

Para efectuar el análisis de Costo - Beneficio se tiene en cuenta lo expresado en los siguientes cuadros:

VALORACIÓN DEL PRODUCTO TOTAL = METRICA DE CALIDAD DEL PRODUCTO + METRICA DE CALIDAD DE USO / 2			
VALORACIÓN:	**FortiEDR**	**CARBONBLACK**	**CORTEX**
Total Métricas de Calidad del Producto	80	78	73
Total Métricas de Calidad de Uso	20	19	19
RESULTADO VALORACIÓN DEL PRODUCTO	**50**	**48.5**	**46**

Cuadro 04.- Cálculo de la valoración de los productos, en base a la información obtenida en el cuadro 03.

a) VALORACIÓN DEL COSTO DE LICENCIAMIENTO

Costo	Puntaje
Alto Costo	1
Costo Medio	2
Costo Bajo	3

Cuadro 05.- Escala de puntaje a asignarse, de la valoración del costo.

b) VALORACIÓN DE REFERENCIA DEL MERCADO

Producto	Costo de la adquisición (*)	Puntaje
FortiEDR	S/. 550,019.20	2
CARBONBLACK	S/. 708,000.00	1
CORTEX	S/. 542,800.00	3

(*) Precios referenciales de la estimación de mercado, incluyen IGV.

Cuadro 06.- Asignación de puntajes en función del costo estimado de mercado para la adquisición del software de detección de amenazas avanzadas de la red (EDR), por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

c) VALORACIÓN DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO

Producto	Análisis	Puntaje
FortiEDR	El costo del hardware para el funcionamiento del software de detección de amenazas avanzadas de la red (EDR) es cero soles (S/. 0.00), porque no se necesita hardware adicional para la implementación de la solución. La institución cuenta con todo lo necesario.	3
CARBONBLACK		3
CORTEX		3

Cuadro 07.- Asignación de puntajes en función del costo de hardware necesario para el funcionamiento, por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

d) VALORACIÓN DEL COSTO DE SOPORTE Y/O MANTENIMIENTO Y/O IMPLEMENTACIÓN Y/O MIGRACIÓN EXTERNO

Producto	Costo por 3 años (*)	Puntaje
FortiEDR	S/. 44,980.80	3
CARBONBLACK	S/. 70,800.00	2
CORTEX	S/. 118,000.00	1

(*) Precios referenciales de la estimación de mercado, incluyen IGV.

Cuadro 08.- Asignación de puntajes en función del costo estimado de mercado para el soporte y/o mantenimiento y/o implementación y/o migración por tres (03) años, por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

e) VALORACIÓN DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO

Producto	Análisis	Puntaje
FortiEDR	El costo de personal y mantenimiento interno para el funcionamiento del software de detección de amenazas avanzadas de la red (EDR) es cero soles (S/. 0.00), ya que no será necesaria la contratación de un personal adicional, puesto que la institución cuenta con el personal CAS (Ing. Junior Morocho Torres) designado por la Dirección del Sistema Nacional de Información de Recursos Hídricos, para la operación y administración del software requerido.	3
CARBONBLACK		3
CORTEX		3

Cuadro 09.- Asignación de puntajes en función del costo de personal y mantenimiento interno necesario para el funcionamiento, por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

f) VALORACIÓN DEL COSTO DE CAPACITACIÓN

Producto	Costo de capacitación	Puntaje
FortiEDR	S/. 5,000.00	3
CARBONBLACK	S/. 35,400.00	2
CORTEX	S/. 59,000.00	1

Cuadro 10.- Asignación de puntajes en función del costo de capacitación necesario para el funcionamiento, por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

g) VALORACIÓN DEL IMPACTO CON EL CAMBIO DE PRODUCTO Y/O ADQUISICIÓN DE NUEVO PRODUCTO

Producto	Análisis	Puntaje
FortiEDR	Si bien, en el caso del software, el área usuaria no se encuentra familiarizada con la interfaz gráfica del software, se incluye en la adquisición una capacitación en la solución a adquirirse, lo que permitirá una adquisición de conocimiento y manejo de experiencias con la solución, de forma progresiva.	2
CARBONBLACK		2
CORTEX		2

Cuadro 11.- Asignación de puntajes en función del impacto en el caso de un posible cambio de producto y/o adquisición de nuevo producto, por cada producto analizado, conforme a los puntajes señalados en el cuadro 05.

h) VALORACIÓN DEL COSTO TOTAL

Costos	FortiEDR	CARBON BLACK	CORTEX
VALORACION DE REFERENCIA DEL MERCADO **(ver cuadro 06)**	2	1	3
VALORACION DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO **(ver cuadro 07)**	3	3	3
VALORACION DEL COSTO DE SOPORTE Y/O MANTENIMIENTO Y/O IMPLEMENTACIÓN Y/O MIGRACIÓN EXTERNO **(ver cuadro 08)**	3	2	1
VALORACIÓN DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO **(ver cuadro 09)**	3	3	3
VALORACIÓN DEL COSTO DE CAPACITACIÓN **(ver cuadro 10)**	3	2	1
VALORACIÓN DEL IMPACTO CON EL CAMBIO DE PRODUCTO Y/O ADQUISICIÓN DE NUEVO PRODUCTO **(ver cuadro 11)**	2	2	2
VALORACIÓN DEL COSTO PARCIAL	**16**	**13**	**13**

Cuadro 12.- Suma de los puntajes a las valoraciones realizadas, conforme a la información generada en los cuadros 06,07,08, 09, 10 y 11.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

i) VALORACIÓN TOTAL

TOTAL = VALORACIÓN DEL PRODUCTO + VALORACIÓN DEL COSTO PARCIAL 2			
VALORACIÓN	**FortiEDR**	**CARBON BLACK**	**CORTEX**
VALORACIÓN DEL PRODUCTO **(ver cuadro 04)**	50	48.5	46
VALORACIÓN DEL COSTO PARCIAL **(ver cuadro 12)**	16	13	13
VALORACIÓN TOTAL	**33**	**30.75**	**29.5**

Cuadro 13.- Valoración total de cada producto, calculada en base a los resultados obtenidos en los cuadros 04 y 12.

2) RESUMEN DE EVALUACIÓN COMPARATIVA COSTO - BENEFICIO

MÉTRICAS	PRODUCTO 1	PRODUCTO 2	PRODUCTO 3
SOFTWARE DE COLECCIÓN DE EVENTOS (SIEM)	**FortiEDR**	**CARBON BLACK**	**CORTEX**
VALORACIÓN DEL PRODUCTO	50	48.5	46
VALORACIÓN DEL COSTO PARCIAL	16	13	13
VALORACION TOTAL	**33**	**30.75**	**29.5**

Cuadro 14.- Resumen de los resultados obtenidos en el cuadro 13.

Se puede observar producto de la Evaluación Comparativa Costo - Beneficio, que el mayor puntaje obtenido es el software de detección de amenazas avanzadas de la red (EDR) **FortiEDR** al obtener 33 puntos, producto de la evaluación realizada, seguido de los softwares de detección de amenazas avanzadas de la red (EDR) **CARBONBLACK y CORTEX,** con 30.75 y 29.5 puntos respectivamente.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

ANEXO N° 03

COTIZACIONES

Cotización Software de amenazas avanzadas de la red (EDR) – FortiEDR

BAFING

SOLUCIÓN PARA LA DETECCIÓN DE AMENAZAS AVANZADAS DE LA RED PARA LA AUTORIDAD NACIONAL DEL AGUA

Empresa	AUTORIDAD NACIONAL DEL AGUA - ANA
Validez de la Cotizacion	30 días calendario.
Impuestos	Los precios están expresados en Soles e incluyen el 18% del IGV.

Item	Descripción	Cant.	Valor Total Soles
PRESTACION PRINCIPAL			
1	**SOLUCION DE DETECCION DE AMENAZAS AVANZADAS DE LA RED** ✓ Fortinet - FortiEDR Discover, Protect & Respond - 1400 devices. ✓ Fortinet - FortiCare Premium Support for Software FortiEDR – 3 years.	1	S/ 550,019.20
2	**SERVICIOS PROFESIONALES** ✓ Instalación y configuración de la solución FortiEDR.	1	S/ 15,000.00
3	**CAPACITACION** ✓ Capacitación virtual de 08 horas para 03 personas, en la solución FortiEDR.	1	S/ 5,000.00
	Sub Total (A)		S/ 550,019.20
PRESTACION ACCESORIA			
4	**SERVICIOS** Servicio de Operación de la solución de detección de amenazas avanzadas FortiEDR por 36 meses con los siguientes alcances: ✓ Administración de la configuración idónea de los sistemas contratados. ✓ Revisión cotidiana de la plataforma a cargo de un operador del servicio. ✓ 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. ✓ Cambios, configuraciones y maniobras. ✓ Soporte técnico 24x7. ✓ Copias de respaldo de los sistemas de gestión ✓ Gestión de las actualizaciones y mejoras, planificación de la seguridad, comité de la Seguridad mensual.	1	S/ 29,980.80
	Sub Total (B)		S/ 550,019.20
	TOTAL (A+B)		S/ 600,000.00

Bafing S.A.C. / Telef +51-12259900
RUC: 20199144961
Av. Del Parque Sur 560 – San Borja – Lima 41 - PERU
http://www.bafing.com

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

Cotización Software de amenazas avanzadas de la red (EDR) - CARBONBLACK

Propuesta Económica

Descripción	P.U. en Soles	Valor Total Soles
EDR Carbon Black 1.400 licencias con soporte por 36 meses.	600.000	600.000
Instalación, configuración y soporte de acuerdo con alcance y SLAs establecidos.	60.000	60.000
Capacitación EDR para 3 personas. Curso práctico virtual	30.000	30.000
	Total Soles sin IGV	690.000
	Total Soles incluido IGV	814.200

- El precio se encuentra en Nuevos Soles Peruanos - PEN
- ANA deberá pagar el 30% del total del proyecto de EDR como anticipo contra Orden de Servicio y firma de contrato y el 70% dentro de las condiciones de presentaciónón principal y presentación accesoria.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°

Cotización Software de amenazas avanzadas de la red (EDR) - CORTEX

CyberServices Corporation

SOLUCIÓN DE END POINT DETECTION AND RESPONSE CORTEX EDR CON CAPACIDADES DE DETECCIÓN Y RESPUESTA EXTENDIDA XDR

Propuesta Económica

Item	Descripción	Cantidad	Valor Total Soles (PEN)
1	Licencias Cortex XDR Pro for 1.400 End Points. Incluye retención por 30 días. Incluye Soporte de Fabricante por 3 años.	1.400	460,000.00
2	Host Insigths addon for Cortex XDR	1.400	
3	Soporte 7x24 sobre la solución EDR por 3 años: Gestión de incidentes 7x24 (ilimitado) Gestión de cambios/configuraciones sobre EDR Backup de configuración Escalación de tickets con fabricante	1	S/ 100,000.00
4	Capacitación EDR & XDR 20 horas	1	S/ 50,000.00
IGV (18%)			S/ 109,800.00
Total incluido IGV			S/ 719,800.00

Condiciones Generales

- Precios mostrados en Nuevos Soles (PEN).
- Incluye impuestos locales (IGV)
- Incluye implementación
- La facturación y contrato estará a cargo Cyber Services Corp.
- Todos los precios son limitados al alcance del programa definido en esta propuesta.
- Todos los precios son sujetos de un acuerdo mutuo bajo las condiciones del contrato a celebrar entre las partes y en relación con el propósito de la presente Propuesta.

ANA Firmado digitalmente por SUAREZ NIÑO Javier Eduardo FAU 20520711865 hard Motivo: Doy V° B°

ANA Firmado digitalmente por MOROCHO TORRES Junior David FAU 20520711865 hard Motivo: Doy V° B°