INFORME TÉCNICO PREVIO EVALUACIÓN DE SOFTWARE N° 001-2023-ANA-DSNIRH

SOFTWARE DE COLECCIÓN DE EVENTOS (SIEM)

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 colección de eventos (SIEM); 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 y acceso a otros servicios que permiten la ejecución de actividades institucionales por parte de los colaboradores en la sede central y en órganos desconcentrados nivel nacional, y que por medio de las estaciones de trabajo procesan la información.

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°

Por otra parte, 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 organizaciones y cometer delitos informáticos, como es acceso ilícito, fraude informático, suplantación de identidad y sustracción o robo de información reservada.

La Autoridad Nacional del Agua cuenta con sistemas internos que son usadas por el personal de la institución para cumplir con sus funciones que igualmente presentar riesgos informáticos. Para contrarrestar dichas amenazas, la Dirección del Sistema Nacional de Información de Recursos Hídricos ha implementado controles técnicos de seguridad informática, con la finalidad de mitigar las vulnerabilidades y amenazas de dichos servicios, así como de la infraestructura tecnológica con la que cuenta la institución.

Si bien, ante intentos de ataques o explotación de vulnerabilidades, los administradores de red acceden a los registros de cada una de las herramientas, resulta complejo contar con una respuesta temprana y preventiva, debido principalmente al alto número de registros que produce cada una de las herramientas de seguridad informática con que se cuenta, las cuales deben ser analizadas en simultáneo cuando se detecta una amenaza.

Asimismo, la complejidad del análisis se incrementa con nuevas amenazas informáticas, las cuales son más sofisticadas y, por lo cual, su identificación se enfoca más en un comportamiento de ataque que en un análisis basado en un patrón o firmas de ataque, las cuales requieren una rápida evaluación de distintas fuentes (herramientas de seguridad informática, servicios y aplicaciones web) para su detección oportuna.

Por esta razón, la Autoridad Nacional del Agua requiere de un software de colección de eventos (SIEM) que permita realizar el almacenamiento, consolidación, correlación y, finalmente, el análisis de estos registros y eventos de seguridad, de manera que puedan ser explotados, permitiendo un análisis en tiempo real y brinde una visión rápida sobre el estado de alguna amenaza o vulnerabilidad en curso y poder responder de manera oportuna a dicho evento, permitiendo mejorar la seguridad a la información.

Un software de colección de eventos (SIEM - Security Information and Event Management) por sus siglas en inglés, es una categoría de software que tiene como objetivo otorgar a las instituciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Proveen patrones de tendencia y permiten identificar comportamientos anómalos en un contexto donde se cuentan con diversas fuentes y miles de registros de eventos de seguridad, los cuales fueron previamente indexados y correlacionados.

La implementación de un software de colección de eventos (SIEM) en la Autoridad Nacional del Agua brindará el soporte para lograr los siguientes objetivos:

- ✓ Cumplimiento y monitoreo básico en tiempo real de controles de seguridad seleccionados.

- ✓ Detección avanzada de amenazas: Monitoreo y notificación en tiempo real de la actividad del usuario, acceso a datos y actividad de aplicaciones, incorporación de inteligencia de amenazas de acuerdo al contexto, en combinación con capacidad de consulta ad-hoc personalizadas.

- ✓ Análisis Forense y Respuesta a Incidentes: Elaboración de tableros de alertas y capacidades de visualización, así como, soporte de flujos de trabajo y documentación, que permitan una identificación efectiva de incidentes, investigación y respuesta.

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 colección de eventos (SIEM) que permitan responder de manera oportuna ante un evento de seguridad informática, permitiendo con ello la mejora de los servicios informáticos 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 colección de eventos (SIEM), que cumplan con los requerimientos expuestos y dispongan de soporte local, siendo los encontrados los siguientes:

- ✓ Splunk Enterprise
- ✓ SIEM Netwitness
- ✓ FortiSIEM

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 colección de eventos que permita realizar el

almacenamiento, consolidación, correlación y, finalmente, el análisis de registros y eventos de seguridad, para que puedan ser explotados permitiendo un análisis en tiempo real y brinde una visión rápida sobre el estado de alguna amenaza o vulnerabilidad en curso y poder responder de manera oportuna a dicho evento, permitiendo mejorar la seguridad a la información de la institución. 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 colección de eventos (SIEM).

6.3. Identificación del Modelo de Calidad

Para la evaluación técnica del software de colección de eventos (SIEM), 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 colección de eventos (SIEM), 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 colección de eventos (SIEM) 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 eventos (SIEM) es el software FortiSIEM, al obtener el mayor puntaje de la evaluación.

10. FIRMAS

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°

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 comportamientos	5	1
2		Análisis forenses	4	1
3		Creación de informes de conformidad	4	1
4		Gestión de puntos de terminación	5	1
5		Gestión de registros	6	1
6		Inteligencia de amenazas	7	1
7		Seguridad de aplicaciones	3	1
8		Supervisión de actividad de usuarios	4	1
9		Supervisión de la integridad de archivos	3	1
10		Supervisión de redes	3	1
11		Supervisión en tiempo real	7	1
12	Fiabilidad	Se encuentra en el cuadrante mágico de Gartner 2022	6	1
13		Alto rendimiento para realizar el análisis (velocidad de procesamiento)	6	1
14		Sistema basado en la reputación de sitios web	6	1
15	Usabilidad	Fácil uso	6	1
		Total (A):	75	15
Métricas de calidad de uso			**Puntajes**	
Ítem	**Características**	**Descripción**	**Max**	**Min**
16	Productividad	Alerta frente a ataques sofisticados	5	1
17		La solución actualiza su firma constantemente	5	1
18	Satisfacción	Permitir tomar distintas acciones	5	1
19		Emite informes en tiempo real	5	1
20	Seguridad	Conexión segura a la consola de administración	5	1
		Total (B):	25	5
		TOTAL (A)+(B):	100	20

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		Splunk Enterprise	SIEM Netwitness	FortiSIEM
Ítem	Características	Descripción	Max	Min			
1	Funcionalidad	Análisis de comportamientos	5	1	5	5	5
2		Análisis forenses	4	1	4	4	4
3		Creación de informes de conformidad	4	1	3	3	4
4		Gestión de puntos de terminación	5	1	5	5	5
5		Gestión de registros	6	1	5	5	6
6		Inteligencia de amenazas	7	1	7	7	7
7		Seguridad de aplicaciones	3	1	3	3	3
8		Supervisión de actividad de usuarios	4	1	4	4	4
9		Supervisión de la integridad de archivos	3	1	3	2	3
10		Supervisión de redes	3	1	3	2	3
11		Supervisión en tiempo real	7	1	7	7	7
12	Fiabilidad	Se encuentra en el cuadrante mágico de Gartner 2022	6	1	6	6	6
13		Alto rendimiento para realizar el análisis (velocidad de procesamiento)	6	1	6	6	6
14		Sistema basado en la reputación de sitios web	6	1	6	6	6
15	Usabilidad	Fácil uso	6	1	5	5	6
		Total (A):	75	15	**72**	**70**	**75**

Métricas de calidad de uso			Puntajes		Splunk Enterprise	SIEM Netwitness	FortiSIEM
Ítem	Características	Descripción	Max	Min			
16	Productividad	Alerta frente a ataques sofisticados	5	1	5	5	5
17		La solución actualiza su firma constantemente	5	1	5	5	5
18	Satisfacción	Permitir tomar distintas acciones	5	1	5	5	5
19		Emite informes en tiempo real	5	1	5	5	5
20	Seguridad	Conexión segura a la consola de administración	5	1	5	5	5
Total (B):			25	5	**25**	**25**	**25**
TOTAL (A)+(B):			100	20	**97**	**95**	**100**

Cuadro 02.- Determinación de puntajes a los productos Splunk Enterprise, SIEM Netwitness y FortiSIEM, 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
	Splunk Enterprise	SIEM Netwitness	FortiSIEM
Total de Métricas de Calidad del Producto	72	70	75
Total de Métricas de Calidad de Uso	25	25	25
Total	**97**	**95**	**100**

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 colección de eventos (SIEM) **FortiSIEM** al obtener 100 puntos producto de la evaluación, seguido de los softwares de colección de eventos (SIEM) **Splunk Enterprise y SIEM Netwitness,** con 97 y 95 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:	**Splunk Enterprise**	**SIEM Netwitness**	**FortiSIEM**
Total Métricas de Calidad del Producto	72	70	75
Total Métricas de Calidad de Uso	25	25	25
RESULTADO VALORACIÓN DEL PRODUCTO	**48.5**	**47.5**	**50**

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
Splunk Enterprise	S/. 1'357,000.00	2
SIEM Netwitness	S/. 1'534,000.00	1
FortiSIEM	S/. 1'285,044.80	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 colección de eventos (SIEM), 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
Splunk Enterprise	El costo del hardware para el funcionamiento del software de colección de eventos (SIEM) 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
SIEM Netwitness		3
FortiSIEM		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
Splunk Enterprise	S/. 236,000.00	2
SIEM Netwitness	S/. 318,600.00	1
FortiSIEM	S/. 109,955.20	3

(*) 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
Splunk Enterprise	El costo de personal y mantenimiento interno para el funcionamiento del software de colección de eventos (SIEM) 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
SIEM Netwitness		3
FortiSIEM		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
Splunk Enterprise	S/. 106,200.00	1
SIEM Netwitness	S/. 35,400.00	2
FortiSIEM	S/. 5,000.00	3

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
Splunk Enterprise	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
SIEM Netwitness		2
FortiSIEM		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	Splunk Enterprise	SIEM Netwitness	FortiSIEM
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)**	2	1	3
VALORACIÓN DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO **(ver cuadro 09)**	3	3	3
VALORACIÓN DEL COSTO DE CAPACITACIÓN **(ver cuadro 10)**	1	2	3
VALORACIÓN DEL IMPACTO CON EL CAMBIO DE PRODUCTO Y/O ADQUISICIÓN DE NUEVO PRODUCTO **(ver cuadro 11)**	2	2	2
VALORACIÓN DEL COSTO PARCIAL	**13**	**12**	**17**

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	**Splunk Enterprise**	**SIEM Netwitness**	**FortiSIEM**
VALORACIÓN DEL PRODUCTO **(ver cuadro 04)**	48.5	47.5	50
VALORACIÓN DEL COSTO PARCIAL **(ver cuadro 12)**	13	12	17
VALORACIÓN TOTAL	**30.75**	**29.75**	**33.5**

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)	**Splunk Enterprise**	**SIEM Netwitness**	**FortiSIEM**
VALORACIÓN DEL PRODUCTO	48.5	47.5	50
VALORACIÓN DEL COSTO PARCIAL	13	12	17
VALORACION TOTAL	**30.75**	**29.75**	**33.5**

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 colección de eventos (SIEM) **FortiSIEM** al obtener 33.5 puntos, producto de la evaluación realizada, seguido de los softwares de colección de eventos (SIEM) **Splunk Enterprise y SIEM Netwitness,** con 30.75 y 29.75 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 colección de eventos (SIEM) – Splunk Enterprise

CyberServices Corporation

SOLUCIÓN PARA LA GESTIÓN Y CORRELACIÓN DE EVENTOS SIEM

Propuesta Económica

Item	Descripción	Cantidad	Valor Total Soles (PEN)
1	Splunk Enterprise. Licencia para virtualización con alcance de hasta 3.000 EPS. Soporte de fabricante por 3 años.	1	1'150,000.00
2	Servicio de Instalación, configuración, soporte para SIEM por 36 meses. Soporte 7x24 sobre la solución SIEM por 3 años con servicios de operación: - Gestión de incidentes 7x24 (ilimitado) - Gestión de la plataforma bajo analista - Gestión de cambios/configuraciones sobre SIEM - Backup de configuración Escalación de tickets con fabricante	1	200.000
3	Capacitación oficial de fabricante SIEM para 4 personas.	1	90.000
Subtotal			S/ 1'440,000.00
IGV (18%)			S/ 259,200.00
Total incluido IGV			S/ 1'699,200.00

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°

Cotización Software de colección de eventos (SIEM) – SIEM Netwitness

SOLERATEC

Propuesta Económica

Descipción	P.U. en Soles	Valor Total Soles
SIEM Netwitness hasta 3.000 Eventos por segundo – EPS. Licenciamiento y soporte por 36 meses.	1'300.000	1'300.000
Instalación, configuración y soporte de acuerdo con alcance y SLAs detallados en la propuesta.	270.000	270.000
Capacitación SIEM para 3 personas. Curso práctico virtual	30.000	30.000
	Total Soles sin IGV	1'600.000
	Total Soles incluido IGV	1'888.000

- 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.

Consideraciones Comerciales - Servicios

Condiciones Generales:

- El precio se encuentra en dólares americanos.
- BBV deberá pagar el 30% del total del proyecto de SOC como anticipo contra Orden de Servicio y firma de contrato y el 70% dentro de la presentación principal y accesoria.
- SOLERATEC procederá a realizar la instalación contra recepción de la OC siempre y cuando se haya iniciado el proceso de revisión del contrato por parte del área legal de ANA y este no deberá sobre pasar 30 días naturales para su firma.
- **Forma de Pago:** Pago mensual con plazo a 30 días según fecha de factura, efectivamente radicada
- Los costos **NO** incluyen **IGV**

  La información contenida, costos y tiempos de dedicación son válidos por un periodo de 30 días
- Tiempo de Implementación del Servicio de SOC entre 4 y 6 semanas.

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 colección de eventos (SIEM) – FortiSIEM

BAFING

SOLUCIÓN PARA LA COLECCIÓN DE EVENTOS 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
PRESTACIÓN PRINCIPAL			
1	**SOLUCIÓN PARA LA COLECCIÓN DE EVENTOS DE RED** ✓ Fortinet - FortiSIEM All-In-One License - 1400 devices & 3000 EPS. ✓ Fortinet – FortiSIEM Advanced Agents - Log & FIM license. ✓ Fortinet - FortiCare Premium Support for Software FortiSIEM – 3 years.	1	S/ 1'285,044.80
2	**SERVICIOS PROFESIONALES** ✓ Instalación y configuración de la solución FortiSIEM.	1	S/ 40,000.00
3	**CAPACITACIÓN** ✓ Capacitación virtual de 08 horas para 03 personas, en la solución FortiSIEM.	1	S/ 5,000.00
	Sub Total (A)		S/ 1'330,044.80
PRESTACIÓN ACCESORIA			
4	**SERVICIOS** Servicio de Operación de la solución de colección de eventos FortiSIEM 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/ 69,955.20
	Sub Total (B)		S/ 69,955.20
	TOTAL (A+B)		S/ 1'400,000.00

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°