INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 00015-2023-OSINFOR/05.1

SOFTWARE PARA ANÁLISIS DE VULNERABILIDADES A REDES Y EQUIPOS DE CÓMPUTO

1. NOMBRE DEL ÁREA

Oficina de Tecnologías de la Información

2. RESPONSABLES DE LA EVALUACIÓN

Ing. Gustavo Artica Cuyubamba - Director de la Oficina de Tecnologías de la Información
Juan Praelli Bueno – Especialista en Infraestructura y Plataformas Digitales

3. FECHA

20 de noviembre del 2023

4. JUSTIFICACIÓN

El Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre lleva a cabo el procesamiento y difusión de información para el cumplimiento de sus objetivos estratégicos a través de sus plataformas tecnológicas y sistemas de información, los cuales deben ser protegidos conforme a la normatividad y controles del Sistema de Gestión de Seguridad de la Información y la NTP-ISO/IEC 27001:2014, uno de cuyos objetivos de control, **A.12.6,** es la **Gestión de vulnerabilidades técnicas**. Por ello, con el fin de proteger y preservar la información digital de la Entidad almacenada en medios electrónicos es necesario contar con herramientas que permitan gestionar las vulnerabilidades digitales de manera permanente, conforme a las recomendaciones del Centro Nacional de Seguridad Digital de la PCM.

La solución debe permitir el análisis y gestión de vulnerabilidades técnicas y el cumplimiento de buenas prácticas de seguridad para al menos 100 equipos, considerando tanto infraestructura de red, de virtualización, servidores, almacenamiento, física y de seguridad, como las bases de datos, aplicaciones y sistemas de información implementados en esta infraestructura. La solución debe cumplir con las siguientes especificaciones técnicas mínimas:

Características y condiciones	**SOFTWARE (INC. LICENCIA) PARA ANÁLISIS DE VULNERABILIDADES A REDES Y EQUIPOS DE CÓMPUTO** ▪ La licencia de la solución propuesta deberá permitir el análisis y detección de vulnerabilidades de al menos **100** equipos, con vigencia mínima de **01 año** contabilizado a partir del día siguiente de culminada la implementación y configuración de la solución. ▪ Deberá realizar escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Los resultados de estos deberán estar consolidados en un único sistema de gestión.

	▪ Deberá colectar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y/o agentes. Además, deberá contar con motores de escaneo públicos para escanear ambientes publicados a Internet. ▪ Deberá auto-clasificar los hallazgos y vulnerabilidades encontradas en base a su criticidad, así como permitir modificar la criticidad asignada. ▪ Deberá ser capaz de ofrecer la característica de gestión o verificación de cumplimiento ("compliance"); es decir, deberá ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y marcos de trabajo ("frameworks") de seguridad tales como NIST, PCI, entre otros, para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, bases de satos, aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Se requiere esta capacidad sin límites de licenciamiento. ▪ La solución deberá proponer automáticamente planes de remediación con actividades recomendadas concretas y estimaciones sobre cuál será el impacto en la reducción de riesgo previo a su ejecución. Esta capacidad deberá ser global y permitirá aplicar filtros por grupo de activos específico. ▪ Deberá permitir la configuración y almacenamiento seguro de credenciales de usuario para escanear mediante cuentas locales y de dominio Windows, cuentas ssh para sistemas Unix/Linux y dispositivos de red, entre otras. ▪ Deberá contar con escaneos que auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas). ▪ Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición. Además, se deberá contar con una vista de vulnerabilidades remediadas. ▪ La solución deberá ser capaz de identificar sistemas comprometidos por malware y otros códigos maliciosos. También deberá ser capaz de identificar la ejecución y nivel de firmas del sistema de antimalware presente en el dispositivo. ▪ Deberá reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de "exploit" (si aplica), documentar de qué forma se explota (malware, acceso remoto, con o sin credenciales), si el "exploit" está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras. ▪ Deberá proporcionar control de acceso basado en roles y perfiles con suficiente granularidad para controlar a los usuarios el acceso a determinados conjuntos de datos y la funcionalidad que está disponible para los usuarios tales como ejecutar escaneos, cambiar configuraciones, acceder a los resultados, generar reportes, aceptar riesgos y otros casos de uso. Debe contar con roles predefinidos y permitir crear nuevos roles. ▪ La solución debe permitir configurar características de desempeño de red para impedir que produzca excesos de tráfico en redes de bajo ancho de banda disponible. También deberá permitir configurar la simultaneidad de sistemas escaneados y la cantidad de chequeos por escaneo. Aun teniendo estas medidas el sistema deberá incluir la capacidad de programar ventanas horarias que automáticamente detengan la ejecución de todos los escaneos y luego los reanuden. ▪ Deberá presentar paneles de control predefinidos y personalizables que contengan datos estadísticos, gráficos de tendencias, información relevante mediante filtros, índices de riesgos y otros datos importantes. ▪ La solución deberá ser capaz de identificar activos mediante escaneos de descubrimiento y escaneos pasivos. Además, deberá detectar el sistema

	operativo, los servicios que se ejecutan, el software instalado y datos que permitan identificarlo tales como IP, MAC Address, hostname/DNS Name. Deberá permitir aplicar etiquetas que designen criterios de clasificación tales como criticidad, área o departamento, dueño, ubicación física, ambiente. Estas etiquetas deberán ser completamente personalizables y permitir crear reglas que las apliquen automáticamente. También deberá registrar el día y hora que se vio al activo por primera y última vez y la última vez que fue escaneado con credenciales. ▪ Deberá permitir realizar escaneos del tipo auditoría de configuración para determinar el cumplimiento de los controles de seguridad y mejores prácticas contra estándares de industria (CIS, NIST, etc), recomendaciones de fabricantes y políticas internas personalizadas. Estas auditorías deberán alcanzar a sistemas operativos, incluyendo los de los dispositivos de red, aplicaciones, motores de bases de datos, hipervisores, cuentas cloud (AWS, Azure, Google Cloud Platform, entre otros) y otros componentes de infraestructura y deberá permitir ser ejecutado con escáner de red o con agente ▪ Deberá contar también con mecanismos para detectar información sensible y ser capaz de auditar la ejecución y estado de actualización de los paquetes antivirus instalados. ▪ Garantía comercial: Se requiere una garantía mínima de un (01) año ante averías o fallas de funcionamiento, en cuyo caso el contratista deberá brindar la asistencia para la reinstalación del software y/o la gestión de nuevos enlaces de descarga y/o claves de acceso de ser necesario. La garantía rige a partir del día siguiente de emitida la conformidad de la prestación.

5. ALTERNATIVAS

Se han evaluado los siguientes productos:

a) Tenable Vulnerability Management
b) SecPod SanerNow
c) OWASP ZAP

6. ANÁLISIS COMPARATIVO TÉCNICO

6.1. Descripción de métricas

Nº	Atributo	Descripción	Escala
	ATRIBUTOS INTERNOS		
1	Escaneo de vulnerabilidades	Escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Resultados consolidados en un único sistema de gestión. Recolección de datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y/o agentes. Motores de escaneo públicos para escanear ambientes publicados a Internet. Deberá reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de “exploit” (si aplica), documentar de qué forma se explota (malware, acceso remoto, con o sin credenciales), si el “exploit” está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.	20
2	Gestión de cumplimiento	Auditar configuraciones y compararlas contra las mejores	15

		prácticas y marcos de trabajo (“frameworks”) de seguridad tales como NIST, PCI, entre otros, para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, bases de satos, aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización.	
3	Gestión de remediación	La solución deberá proponer automáticamente planes de remediación con actividades recomendadas concretas y estimaciones sobre cuál será el impacto en la reducción de riesgo previo a su ejecución. Esta capacidad deberá ser global y permitirá aplicar filtros por grupo de activos específico.	10
4	Gestión de parches de seguridad	Deberá contar con escaneos que auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas).	10
5	Control de acceso	Control de acceso basado en roles y perfiles con suficiente granularidad para controlar a los usuarios el acceso a determinados conjuntos de datos y la funcionalidad que está disponible para los usuarios tales como ejecutar escaneos, cambiar configuraciones, acceder a los resultados, generar reportes, aceptar riesgos y otros casos de uso. Debe contar con roles predefinidos y permitir crear nuevos roles.	5
	ATRIBUTOS EXTERNOS		
6	Implementación	Simplicidad para la instalación y/o configuración de la consola de administración central. En caso de requerir agentes, el despliegue a los clientes debe poder realizarse remotamente y en segundo plano.	10
7	Administración	Administración, implementación, actualización y monitoreo desde una consola de administración central. Interfaz gráfica rápida, atractiva y amigable.	10
	ATRIBUTOS DE USO		
8	Alertas y reportes	La solución deberá generar reportes configurables, automatizados y gráficos.	5
9	Estabilidad y escalabilidad	La solución mantiene un buen rendimiento con un alcance de 100 a 500 equipos	5
10	Productividad	La solución debe tener el menor impacto sobre los recursos de sistema y red, de modo que se asegure una velocidad normal de procesamiento en los equipos.	10
		TOTAL	**100**

6.2. Puntajes

Nº	**Atributo**	**Tenable Vulnerability Manager**	**SecPod SanerNow**	**OWASP ZAP**
	ATRIBUTOS INTERNOS			
1	Escaneo de vulnerabilidades	20	20	20
2	Gestión de cumplimiento	14	14	12
3	Gestión de remediación	10	10	9
4	Gestión de parches de seguridad	9	9	7
5	Control de acceso	5	5	3
	ATRIBUTOS EXTERNOS			
6	Implementación	10	10	8

7	Administración	10	10	8
	ATRIBUTOS DE USO			
8	Alertas y reportes	5	5	4
9	Estabilidad y escalabilidad	5	5	4
10	Productividad	9	9	8
	TOTAL	**97**	**97**	**83**

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

- Producto: **Tenable Vulnerability Management**. Costo estimado: **S/ 22,931.18** (licencia anual para 100 activos, sobre la base de la oferta de BAFING SAC, **Anexo 1,** considerando tipo de cambio S/ 3.80)

- Producto: **SecPod SanerNow**. Costo estimado: **S/ 38,468** (licencia anual para 2000 activos; sobre la base de la oferta de INNOVA TECNOLOGIA CORP S.A.C., **Anexo 2**)

- Producto: **OWASP ZAP**. Costo estimado: **Software gratuito** (soporte por medio de consultas en foros en línea de usuarios)

8. CONCLUSIONES

- Se determina que los productos evaluados son adecuados para la gestión de vulnerabilidades digitales, en particular Tenable Vulnerability Management, y SecPod SanerNow. Dado que las prestaciones son similares, sería recomendable adquirir la solución cuyas condiciones de contratación sean las más favorables para la entidad.

9. FIRMAS

Firmado digitalmente por
Juan Praelli Bueno
Especialista en Infraestructura y Plataformas Digitales
Oficina de Tecnologías de la Información

OSINFOR
Firmado digitalmente por: PRAELLI BUENO Juan Antonio FAU 20522224783 soft
Motivo: Soy el autor del documento
Fecha: 20/11/2023 17:44:50-0500

Firmado digitalmente por
Ing. Gustavo Artica Cuyubamba
Director
Oficina de Tecnologías de la Información

OSINFOR
Firmado digitalmente por: ARTICA CUYUBAMBA Gustavo FAU 20522224783 soft
Motivo: En señal de conformidad
Fecha: 20/11/2023 17:55:17-0500

Anexo 1

BAFING

PROPUESTA ECONÓMICA

Tenable io				
Ítem	**Descripción**	**Precio Unit.**	**Cant.**	**Precio Total**
1	**Tenable io** ✓ Tenable.io Vulnerability Management Part: TIOVMHV Term: 12 Months	**$ 43.10**	**100**	**$ 4,314.00**
2	**Capacitación** ✓ 02 Horas de capacitación de uso y manejo de la plataforma Tenable Io (4 personas)	**$ 0 .00**		**$ 0 .00**
3	**Servicios – Implementación** ✓ Instalación de agentes, configuración de políticas y sincronización en nube Tenable ✓ Servicio de Soporte Técnico On-Line telefónico / e-mail (8x5). - Incidencias	**$ 800.00**	**1**	**$ 800.00**
			TOTAL	**$ 5,114.00**

COBERTURA DE LA PROPUESTA

Los precios están expresados en dólares americanos
Los precios NO incluyen el 18% del IGV
Forma de pago: Al contado
Plazo de entrega: La licencia de software entrega en 05 días calendario.
Vigencia de la propuesta: La presente propuesta tiene una vigencia de 30 días
Presentación del producto: Licencia corporativa de software, múltiples idiomas disponibles.

+51 1 225 9900
info@bafing.com
www.bafing.com
@BafingSAC
Av. Del Parque Sur 560, San Borja, Lima, Perú

Ciberseguridad
Smart Buildings
eHealth

Anexo 2

27 de Set. de 23

INNOVA ciberdefensa

e. Cierre de registro en OWL Security

PROPUESTA ECONOMICA

ÍTEM	DESCRIPCIÓN DEL BIEN O SERVICIO	SUSC	CANT	P.U.	COSTOS
01	SanerNow Platform SaaS, incluye: - SanerNow IT Asset Exposure - SanerNow Posture Anomaly Management - SanerNow Vulnerability Management - SanerNow Compliance Management - SanerNow Patch Management - SanerNow Security Controls, Beyond Patching	1 AÑO	100	S./326.00	S./32,600.00
02	Servicios - Despliegue - Configuración de alertas - Capacitación con certificación - Ejercicios de remediación 5 casos - Soporte técnico a incidentes 24x7x365		NA	S./0.00	S./0.00
				SUBTOTAL	S./32,600.00
				IGV	S./ 5,868.00
				TOTAL	S./38,468.00

(*) Los precios están expresados en soles
(*) Los costos incluyen IGV
(*) Forma de pago: Previa conformidad

DATOS DEL PROVEEDOR

- Razón Social : INNOVA TECNOLOGIA CORP S.A.C.
- RUC : 20601100593
- Dirección : Av. Los Constructores 1125, urb. santa patricia, La Molina
- Contacto : Jimmy Jauregui
- E-mail : administracion@innovatc.com
- Teléfonos : +51 348 0842 | # +51 987 303 162

CUENTAS BANCARIAS

- Banco de Crédito del Perú – BCP **Cuenta en dolares**
  Cta. Cte. BCP USD : N° 193-2460888-1-62
  Cod. BCP Interbancario dólares : N° 002-19300246088816219

- Banco de Crédito del Perú – BCP **Cuenta en soles**
  Cta. Cte. BCP SOLES : N° 193-2472760-0-72
  Cod. BCP Interbancario soles : N° 002-19300247276007218

- Sujeto a detracción del 12%
  Cta. Cte. Banco de la Nación : Nº 00-066-092593

INNOVA TC S.A.C.
ventas@innovatc.com | soporte@innovatc.com
+ 511 348-0842
Av. Los Constructores 1125, Urb. Santa Patricia La Molina
https://innovatc.com/