Departamento de Informática

Informe Técnico de Estandarización de solución de protección, monitoreo y análisis continuo de Endpoint

N° 002-2022-07.06

SERVICIOS RELACIONADOS A SOLUCION ANTIMALWARE WITHSECURE ELEMENTS ENDPOINT PREMIUM O EQUIVALENTES

Agosto de 2022

ÍNDICE

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática

1. PROPÓSITO

El presente documento tiene por objetivo presentar el sustento técnico que demuestre la necesidad de estandarizar los servicios relacionadas a la solución Antimalware WithSecure, antes conocida como Fsecure, la cual se encuentra implementada, desplegada e instalada en todas PC de escritorio, estaciones de trabajo portátiles (laptops) y equipos móviles (celulares) del SENCICO.

Los servicios requeridos permitirán al SENCICO no perder el valor agregado que con el tiempo se ha ido incluyendo a la solución implementada, así como evitar realizar esfuerzos en un nuevo despliegue y configuraciones a una consola de administración. Asimismo, permitirán al Dpto. de Informática proporcionará la continuidad operativa de la seguridad ante amenazas a los equipos del SENCICO.

2. ANTECEDENTES Y MARCO LEGAL

El SENCICO es un Organismo Público Descentralizado adscrito al Sector Vivienda, Construcción y Saneamiento, cuyas funciones son la formación de los trabajadores del sector construcción, la educación superior no universitaria, el desarrollo de investigaciones vinculadas a la problemática de la vivienda y edificación, así como a la propuesta de normas técnicas de aplicación nacional.

Desde el año 2019, el SENCICO cuenta con el servicio de suscripción de licencias WithSecure, anteriormente conocidas como Fsecure, la cual brinda a la Entidad seguridad con inteligencia y aprendizaje automático ante las amenazas actuales (virus, malware, spyware), incluido el ransomware y los ataques de día cero a todas las PC de escritorio, estaciones de trabajo portátiles (laptops) y equipos móviles (celulares).

Por otra parte, el numeral 8.4 del artículo 8° del Reglamento de la Ley de Contrataciones del Estado, aprobado con Decreto Supremo Nº 350-2015-EF, modificado por Decreto Supremo N° 056-2017-EF, establece: “En la definición del requerimiento no se hace referencia a fabricación o procedencia, procedimiento de fabricación, marcas, patentes o tipos, origen o producción determinados, ni descripción que oriente la contratación hacia ellos, salvo que la Entidad haya implementado el correspondiente proceso de estandarización debidamente autorizado por su Titular, en cuyo caso deben agregarse las palabras “o equivalente” a continuación de dicha referencia”.

En el Anexo Único del Reglamento de la Ley de Contrataciones del Estado se define Estandarización como: “El Proceso de racionalización consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos preexistentes”.

Asimismo, en el numeral 7.1 del Ítem VII de la Directiva Nº 004-2016-OSCE/CD “Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular”, aprobada por Resolución Nº 011-2016-OSCE/PRE, se indica que:

“La Estandarización debe responder a criterios técnicos y objetivos que la sustenten, debiendo ser necesaria para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente de la Entidad. En tal sentido, el área usuaria de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones,

canaliza los requerimientos formulados por otras dependencias, debe elaborar un informe técnico sustentando la necesidad de realizar la estandarización".

En tal sentido, el Departamento de Informática define y sustenta en el presente informe la necesidad de mantener renovada la suscripción de estas licencias, así como contar con el soporte del fabricante, y contratar servicios adicionales los cuales permitan mejorar la protección de los Endpoint del SENCICO.

3. DESCRIPCION DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

El SENCICO en el año 2019, realizó la implementación de la Solución Antimalware de Fsecure, la cual con el tiempo cambió al nombre de WithSecure.

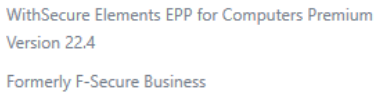

Imagen N° 01 – Actualización de nombre del producto

Con esta implementación se contrató el servicio de suscripción de las siguientes licencias:

- 2800 licencias para estaciones de trabajo WithSecure™ (antes Fsecure)
- 80 licencias para servidores WithSecure™.
- 80 licencias para móviles WithSecure™.

El servicio de suscripción permite al SENCICO contar con actualizaciones constantes para la Solución, permitiendo hasta la fecha contar con nuevas funcionalidades liberadas por el fabricante que han mejorado la seguridad de los endpoint de la Institución.

Como parte de esta implementación se segmentó y se configuró, para cada una de las Sedes del SENCICO, diferentes políticas según sus necesidades, permitiendo que la administración de los endpoints sea más óptima. Asimismo, como parte de la implementación del servicio, se realizaron capacitaciones para la gestión de estas consolas al personal informático del SENCICO a nivel nacional.

Adicional a ello, también se contrató el servicio de soporte técnico, el cual ha permitido a la Entidad actualizar y mejorar las configuraciones de seguridad con el transcurso del tiempo; así como la creación de políticas según las necesidades de cada Sede y/o usuario especifico.

En tal sentido, se dispone del siguiente equipamiento y/o infraestructura preexistente:

Ítem	Equipamiento o Infraestructura Preexistentes		Fabricante
	Descripción	Cantidad	
01	Solución WithSecure desplegada en todos los equipos del SENCICO.	01	WithSecure™ (antes Fsecure)

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática

02	Consola de administración con la siguiente configuración por Sede y/o usuario específico: • Control de aplicaciones. • DataGuard. • Reglas. • Tareas automatizadas. • Control de dispositivo. • Actualización de software. • Protección de navegación. • Entre otras configuraciones.	01	

Cuadro 01 – Equipamiento o Infraestructura Preexistentes

Cabe precisar que estas configuraciones han ido evolucionando con el tiempo en función a las necesidades de cada Sede y de las amenazas detectadas.

4. DESCRIPCION DEL BIEN O SERVICIO REQUERIDO

El SENCICO requiere contar con los siguientes servicios con la finalidad de mantener la operativa de la solución previamente implementada:

Ítem	Descripción del servicio requerido	Fabricante
01	Servicio de Suscripción de licencias WithSecure Element Endpoint Premium o equivalente, el cual incluya el mantenimiento de licencias.	WithSecure™ (antes Fsecure)
02	Servicio de Suscripción de licencias Endpoint Detection and response o equivalente.	
02	Servicio de Suscripción de módulos adicionales WithSecure o equivalentes.	
03	Servicio de Soporte Técnico a solución WithSecure o equivalente.	

Cuadro 02 – Descripción del bien o servicio requerido

Cabe precisar que es necesario que todas las licencias requeridas se administren desde la consola ya configurada por el SENCICO, con la finalidad de facilitar la gestión de protección de los equipos.

5. USO O APLICACIÓN DEL BIEN REQUERIDO

Los servicios requeridos serán usados para:

- Servicio de Suscripción de licencias WithSecure Element Endpoint Premium o equivalente, el cual incluya el mantenimiento de licencias.
    - Identificar y bloquear malware sofisticado en tiempo real en los endpoints del SENCICO.
    - Gestionar parches y mantener todos los softwares instalados actualizados en los endpoint.

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática

- Brinda protección contra ransomware, evitando la destrucción y manipulación de datos.
- Detectar características, patrones y tendencias maliciosas.
- Bloquear el acceso a sitios maliciosos y de phishing, lo que limita la exposición a contenido dañino.
- Bloquear la ejecución de aplicaciones y scripts.
- Mantener la solución actualizada y contar con nuevas funcionalidades que libere el fabricante.

- Servicio de Suscripción de licencias Endpoint Detection and response o equivalente
  - Mejorar la visibilidad del estado y la seguridad de los endpoint del SENCICO.
  - Detectar fácilmente comportamiento de malwares.
  - Detectar rápidamente ataques dirigidos gracias a alertas inmediatas.
  - Buscar y explorar los datos de eventos recopilados de los endpoints.
- Servicio de Suscripción de módulos adicionales WithSecure o equivalentes.
  - Permitir contar con una mejor protección en atención a los nuevos tipos de amenazas que se generen con el tiempo.
- Servicio de Soporte Técnico a solución WithSecure o equivalente.
  - Solicitar la atención de incidentes y requerimientos relacionadas con el uso de la solución y ataques recibos al SENCICO.
  - Solicitar información actualizada y capacitaciones de las nuevas funcionalidades que libere el fabricante.

6. JUSTIFICACION DE LA ESTANDARIZACIÓN

6.1 ASPECTOS TÉCNICOS

Las razones técnicas que justifican la estandarización del software son las siguientes:

6.1.1. Se realizó una evaluación técnica (Informe Técnico Previo de Evaluación de Software N° 003-2022-07.06) de soluciones similares en la cual se concluyó que la opción más favorable para la Entidad, según las circunstancias actuales, es mantener la solución antimalware de WithSecure.

6.1.2. La solución de WithSecure posee las herramientas necesarias que el Dpto. de Informatica requiere para brindar protección ante amenazas a los endpoint del SENCICO.

6.1.3. Actualmente se cuenta con una consola de administración configurada según las particularidades y necesidades de cada una de las Sedes y usuarios del SENCICO.

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática

6.1.4. El personal de SENCICO ha adquirido conocimientos y habilidades operativas en la administración de la solución WithSecure, por lo que cambiar a una Solución alternativo implicará el uso de mayores recursos y tiempo, resultando en mayores costos para el SENCICO.

6.2 VERIFICACIÓN DE PRESUPUESTOS PARA ESTANDARIZACIÓN

En esta sección deben verificarse los presupuestos indicados en el numeral 7.2 de la Directiva Nº 004-2016-OSCE/CD aprobada por la Resolución Nº 011-2016-OSCE/PRE, que son los siguientes:

6.2.1. La Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados:

- El SENCICO cuenta con el equipamiento e infraestructura precisados en el numeral 3 del presente documento.

6.2.2. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura:

- Los servicios listados en el numeral 4 del presente documento son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles debido que:
  - Garantizan la funcionalidad y operativa de la Solución de protección Antimalware implementada.
  - Garantizan el valor económico (costos, tiempo, entre otros) invertido en la configuración de la consola de administración y el despliegue de la solución.
  - Garantizan la protección antes amenazas a todos los endpoint del SENCICO.

6.3 INCIDENCIA ECONÓMICA DE LA ADQUISICIÓN

- Las ventajas técnicas ya mencionadas se ven ampliadas en lo económico con el aprovechamiento del nuevo servicio requerido de Suscripción de licencias Endpoint Detection and response o equivalente, dado que permitirá dar una mejor visibilidad del estado y la seguridad de los endpoint del SENCICO, permitiendo prevenir ataques que puedan generar perjuicio económico a la Entidad.
- La Solución WithSecure, ha demostrado con el tiempo la inclusión de nuevas funcionalidades que han sido liberadas por el fabricante como parte del licenciamiento vigente. En el caso de la mayoría de otras soluciones estas funcionalidades requieren un costo adicional para su uso.

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática

Por lo expuesto, para prevenir y mantener la protección ante amenazas es necesario estandarizar los servicios relacionados a la Solución WithSecure implementada en el SENCICO.

7. VIGENCIA

El presente Informe Técnico tiene 3 (tres) años de vigencia o en caso quede sin efecto o varíe alguna de las condiciones que determinaron la estandarización requerida, descrita en el punto (4).

8. DATOS DEL RESPONSABLE DE LA EVALUACIÓN

Nombres	Sello y Firma
Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Firmado digitalmente por VERA DAMIAN Dante Vladimir FAU 20131377810 soft Motivo: Soy el autor del documento Fecha: 10.08.2022 17:00:01 -05:00

Nombres	Sello y Firma
Ing. Hector Varas Graus Asesor en Sistemas e Informática	Firmado digitalmente por VARAS GRAUS Roger Hector FAU 20131377810 soft Motivo: Doy V° B° Fecha: 11.08.2022 14:19:26 -05:00

Fecha de Elaboración	Responsable de Evaluación	Departamento de Informática:
10/08/2022		
	Dante Vladimir Vera Damian Especialista en Redes y Comunicaciones	Ing. Hector Varas Graus Asesor en Sistemas e Informática