INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 003-2021-ANA-DSNIRH

SOFTWARE DE ANALISIS, DETECCIÓN Y RESPUESTA ANTE AMENAZAS CIBERNETICAS (EDR)

1. NOMBRE DEL ÁREA

Dirección del Sistema Nacional de Información de Recursos Hídricos

2. RESPONSABLES DE LA EVALUACIÓN

Lic. Edwin Dante Quispe Soto
Director
Dirección del Sistema Nacional de Información de Recursos Hídricos

Nombre: Tec. Pablo Demetrio Carrión Méndez
Cargo: Coordinador de Soporte Técnico

3. FECHA

12 de agosto de 2021

4. JUSTIFICACIÓN

La Autoridad Nacional del Agua – ANA; como parte del cumplimiento de sus funciones, genera gran cantidad de información digital de vital importancia respecto a los recursos hídricos, la cual es alojada en la plataforma de servidores dentro de los Centros de Procesamiento de Datos que cuenta la institución por lo cual, en prevención y viendo el constante cambio y evolución en que se dan las ciberamenazas a nivel mundial y a la par del avance tecnológico, es necesario proteger la producción de información digital, fortaleciendo la plataforma de seguridad tecnológica con la que actualmente cuenta la institución, con soluciones de seguridad que no solo se limiten a la detección de la amenaza, sino que sean capaces de adelantarse a ella.

AUTORIDAD NACIONAL DEL AGUA V°B° Lic. Edwin Dante Quispe Soto Director Dirección del Sistema Nacional de Información de Recursos Hídricos

Por esta razón, la ANA requiere contar con una solución EDR que coadyuve así a la protección de la información crítica con la que se cuenta dada la necesidad del monitoreo, análisis, anticipación y solución de las amenazas que puedan poner en riesgo la red interna y dispositivos que utiliza el personal de la ANA en sus labores; además de garantizar la confidencialidad, integridad y disponibilidad de la misma.

AUTORIDAD NACIONAL DEL AGUA V°B° Téc. Pablo D. Carrión Méndez Coordinador Dirección del Sistema Nacional de Información de Recursos Hídricos

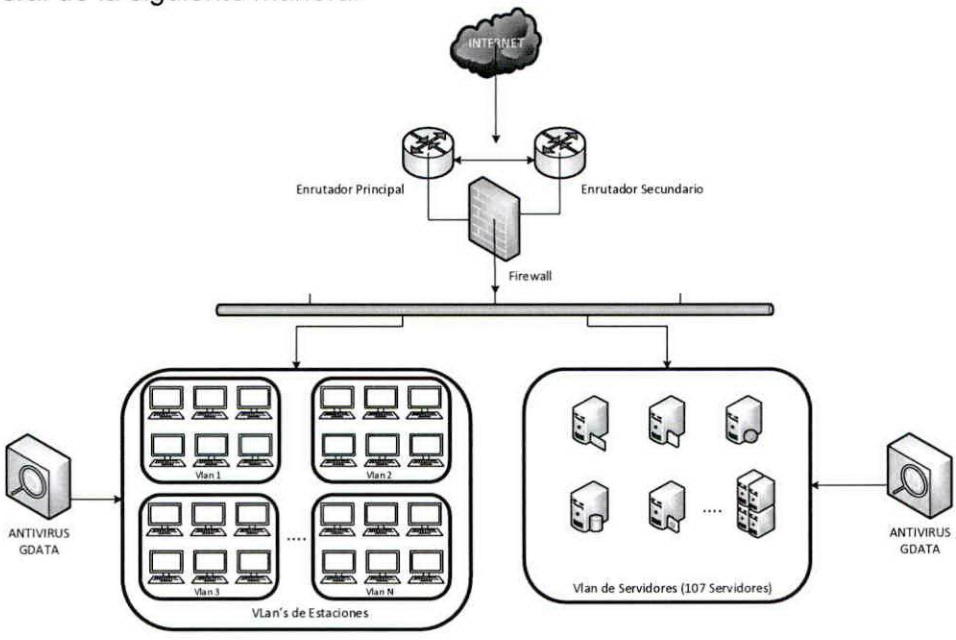
Un EDR es un sistema de protección y monitoreo de la red interna y de equipos endpoint (aquellos dispositivos desde los que se conecta el personal de la institución en forma remota, que van desde ordenadores a smartphones y/o tablets). Las siglas EDR que significan "Endpoint Detection Response" (detección y respuesta de punto final), refieren a una solución de seguridad que combina diferentes herramientas para monitorizar, analizar, anticiparse y solucionar las

amenazas que puedan poner en riesgo la red interna y los dispositivos endpoint que utiliza en sus labores el personal.

Cabe señalar que solo durante el 2020, aproximadamente 6 de cada 10 organizaciones (59%) a nivel mundial fueron víctimas de algún incidente significativo o grave de ciberseguridad en los últimos 12 meses[1], de acuerdo a los datos entregados por la última Encuesta Global de Seguridad de la Información 2019-2020 de EY GISS. En consecuencia, contar con el software EDR tiene como objetivo en la ANA, reforzar la seguridad endpoint de la misma, así como mantener segura la red interna, configurándose como una solución proactiva, capaz de detectar riesgos y amenazas que puedan sobrepasar la actual línea defensa, conformada por: equipos de seguridad perimetral distribuidas en los dos Centros de Datos con que cuentan la institución, AppDefense-VMware, así como el software antivirus instalados en los equipos de cómputo (estaciones de trabajo y servidores de la institución).

Por otro lado, los softwares antivirus convencionales (también llamados EPP - Endpoint Protection Plataform) actúan como parte de la primera línea de defensa de protección perimetral antes que el EDR, filtrando los ataques de ciberseguridad. Los EDR (Endpoint Detection and Response) actúan como un segundo nivel de protección de las amenazas que consigan penetrar la primera línea de defensa, permitiendo que el personal de infraestructura tecnológica de la institución, observe y tome acción ante aquello que fue omitido por las barreras de detección de malware y amenazas conocidas, corrigiendo brechas de seguridad de manera proactiva y oportuna, anticipando a las amenazas y lograr proteger la entidad.

La actual arquitectura de seguridad de la ANA, se encuentra graficada de forma general de la siguiente manera:



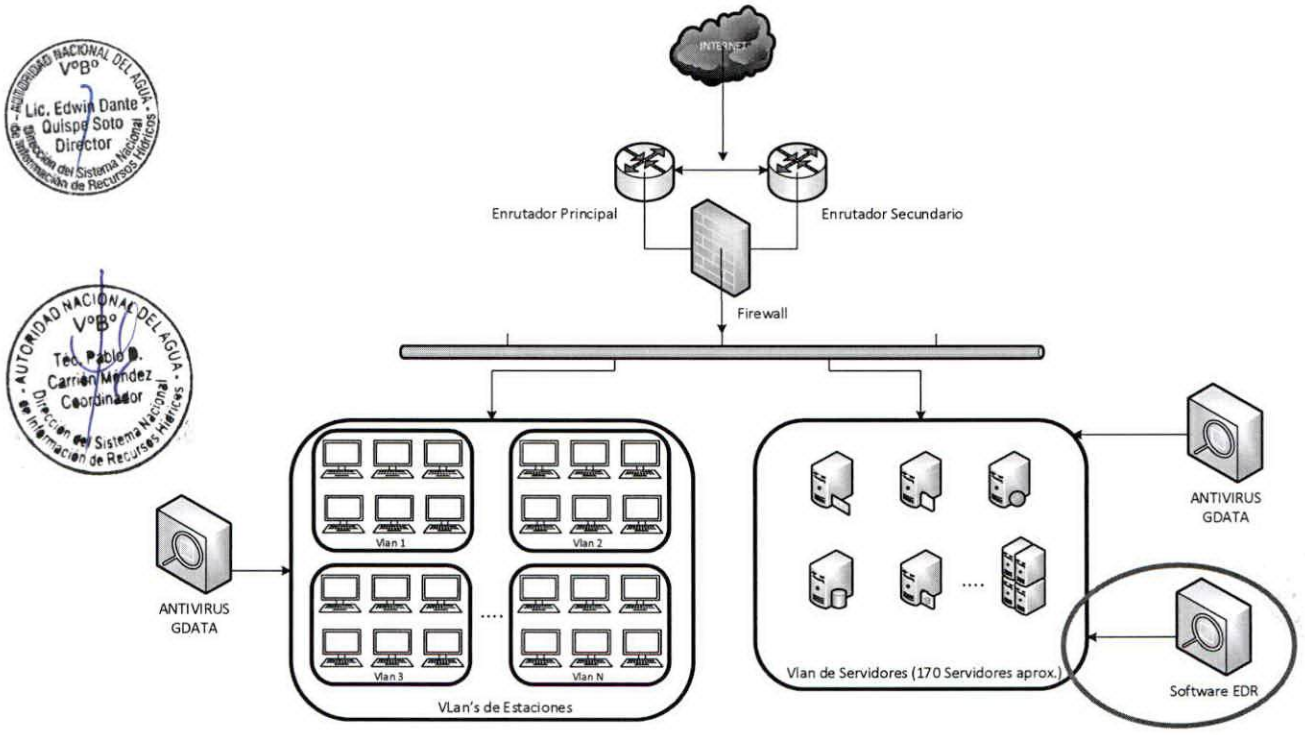
Centro de Procesamiento de Datos Principal (Lima) y Secundario (Ica)

[1] Fuente: https://assets.ey.com/content/dam/ey-sites/ey-com/es_pe/topics/cybersecurity/ey-giss-como-pasar-seguridad-aislada-integrada.pdf

Las ventajas que representa la adquisición de una solución EDR para la ANA se tiene:

- ✓ Crea una segunda línea defensa para frenar las amenazas que logren traspasar una primera solución de seguridad, como puede ser el antivirus.
- ✓ Puesto que monitoriza todo el sistema en tiempo real (o prácticamente en tiempo real), incrementa las cualidades de anticipación frente a ataques cibernéticos dirigidos contra la institución.
- ✓ Reducción del tiempo de exposición a los incidentes de seguridad.
- ✓ Al recopilar y almacenar información de forma automática, tanto de dispositivos endpoint como de la propia red, es capaz de crear sus propios patrones de detección automatizados, lo que ayuda en el propio proceso de detección de las amenazas.
- ✓ Recoge en un solo punto toda la información relativa a incidentes o eventos o acciones sospechosas, lo que permite llevar a cabo una investigación más rápida.
- ✓ Concentración de la información a través de un panel administrativo para análisis.
- ✓ Cobertura extensa de endpoints soportados y simplicidad de despliegue.

Posterior a la implementación, se tiene que la arquitectura de seguridad de la ANA, se vería reforzada de la siguiente manera:



Centro de Procesamiento de Datos Principal (Lima) y Secundario (Ica)

La ANA a través de su área de Infraestructura tecnológica, considera como cualidades principales de seguridad tecnológica que debe contar una solución de software EDR para sumarse a su actual esquema de seguridad, en concordancia con las necesidades a cubrir en materia de seguridad como son monitorizar, analizar, anticiparse y solucionar las amenazas que puedan poner en riesgo la red interna y los dispositivos endpoint que utiliza en sus labores el personal de la ANA; las siguientes:

- ✓ Contar con una solución de tipo Software as a Service (SaaS) que se hospede en la nube, con capacidad de integrar mecanismos de seguridad avanzada para el acceso y almacenamiento de datos en la institución.
- ✓ Monitorear e identificar cambios realizados en archivos críticos, cambios en la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor, esto, a través de reglas de monitoreo de integridad realizadas e identificadas automáticamente.
- ✓ Capacidad de detectar y bloquear software no autorizado, de forma automática, tanto en servidores Windows como en servidores Linux.
- ✓ Inspeccionar las bitácoras de los sistemas operativos y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos.
- ✓ Permitir corregir vulnerabilidades de forma integral a través de gestión de parches y ejecución de scripts de forma centralizada.
- ✓ Permitir realizar despliegue y configuración de agentes de protección en los servidores, sin cortes de servicio.

Por lo expuesto y en el marco de la ley 28612 "Ley que norma el uso, adquisición y adecuación del software de la Administración Pública", se procede a evaluar el Software EDR que cubre las necesidades de la institución.

5. ALTERNATIVAS DE EVALUACIÓN:

AUTORIDAD NACIONAL DEL AGUA V°B° Lic. Edwin Dante Quispe Soto Director Dirección del Sistema Nacional de Información de Recursos Hídricos

Teniendo como base las necesidades expuestas en el numeral anterior, se ha considerado evaluar software con soporte local, que cuenten además con características y requerimientos de implementación semejantes; por lo cual se ha considerado como alternativas de solución a:

Producto evaluado
Symantec
SecPod

AUTORIDAD NACIONAL DEL AGUA V°B° Téc. Pablo D. Carrión Méndez Coordinador Dirección del Sistema Nacional de Información de Recursos Hídricos

Para la determinación de estas soluciones, así como la evaluación técnica y elaboración de los términos de referencia, se ha tomado información disponible en las páginas web de los fabricantes de cada uno de los productos a evaluar.

6. ANÁLISIS COMPARATIVO TÉCNICO.

El análisis técnico ha sido realizado en conformidad con la metodología de la "Guía Técnica sobre evaluación de software en la administración pública" (R.M.N° 139-2004-PCM) tal como se exige en el reglamento de la Ley N.° 28612.

6.1. Propósito de Evaluación

Validar que las alternativas seleccionadas sean las más convenientes para cubrir las necesidades de la Autoridad Nacional del Agua. El propósito es determinar los atributos o características para el producto final.

6.2. Identificar el Tipo de Producto

Software EDR que permita la protección de la información alojada en los servidores de la ANA.

6.3. Identificación del Modelo de Calidad

Para la evaluación técnica del Software EDR se aplicará el modelo de calidad descrito en la parte I de la Guía de evaluación de software aprobada por R.M. Nº 139-2014-PCM y la Ley Nº 28612 – "Ley que norma el uso, adquisición y adecuación del software en la administración pública".

6.4. Selección de Métricas

Las métricas establecidas fueron consideradas de acuerdo a las necesidades de la ANA en contraste con las principales características de los fabricantes de software EDR evaluados, siendo el resultado el siguiente:

CUADRO 1
METRICAS: ATRIBUTOS

N°	ATRIBUTO	PUNTAJE MAXIMO	PUNTAJE MINIMO	SYMANTEC	SECPOD
1	La solución es tipo Software as a Service (SaaS) hospedada en la nube del fabricante, la misma que integra mecanismos de seguridad avanzada para el acceso y almacenamiento de datos de la institución.	5	0	3	5
2	Monitoreo de integridad. Identifica los cambios en archivos críticos, cambios a la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor, esto, a través de reglas de monitoreo de integridad realizadas e identificadas automáticamente.	5	0	5	5
3	Módulo de control de aplicaciones multiplataforma. Detecta y bloquea software no autorizado, de forma automática, tanto en servidores Windows como en servidores Linux.	5	0	5	5
4	Módulo de bitácoras. Inspecciona las bitácoras del sistema operativo y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos.	5	0	5	5
5	Funcionalidad de respuesta avanzadas. Permitiendo corregir vulnerabilidades de forma integral a través de la gestión de parches y ejecución de scripts de forma centralizada.	5	0	5	5
6	Administración centralizada con mínimo impacto. Permite realizar el despliegue y configuración de los agentes de protección, en los servidores sin cortes de servicio.	5	0	5	5
TOTAL				28	30

AUTORIDAD NACIONAL DEL AGUA V°B° Lic. Edwin Danae Quispe Soto Director Dirección del Sistema Nacional de Información de Recursos Hídricos

AUTORIDAD NACIONAL DEL AGUA V°B° (Téc. Pablo D. Carrión Méndez Coordinador Dirección del Sistema Nacional de Información de Recursos Hídricos

METRICAS: ATRIBUTOS DE USO						
N°	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	SYMANTEC	SECPOD
1	Capacitación	Se dispone con cursos estándares con evaluación y certificación técnica emitida por el fabricante	5	0	5	5
2	Soporte	Se dispone de especialistas calificados por el fabricante, para la instalación y configuración	5	0	5	5
3	Facilidad de uso	El usuario interactúa con familiaridad sobre la plataforma	5	0	5	5
4	Acceso seguro	Mecanismos de seguridad avanzada para la administración segura de la consola	5	0	0	5
				SUBTOTAL	15	20
				TOTAL	43	50

ESCALA	DESCRIPCIÓN
1	Deficiente: La tecnología empleada no funciona correctamente y existen reportes de problemas por los usuarios
2	Regular: Tecnología con algunas limitaciones en las características
3	Bueno: Tecnología con algunas limitaciones en desempeño y funcionalidad
4	Muy Bueno: Tecnología con buen desempeño y funcionalidad
5	Excelente: Tecnología de gran desempeño y funcionalidad aprobada a nivel mundial

Del CUADRO N°1, se muestra los resultados de evaluación de los productos considerados para la adquisición de software EDR, en la que SecPod resulta el más adecuado para los fines de la institución.

6.5. Análisis Comparativo Técnico/Funcional

El análisis se realizó acorde al alcance y características generales que los fabricantes de software EDR evaluados deben brindar:

AUTORIDAD NACIONAL DEL AGUA - V°B° - Lic. Edwin Dante Quispe Soto - Director - Dirección del Sistema Nacional de Información de Recursos Hídricos

AUTORIDAD NACIONAL DEL AGUA - V°B° - Téc. Pablo D. Carrión Méndez - Coordinador - Dirección del Sistema Nacional de Información de Recursos Hídricos

ATRIBUTOS/CARACTERITICAS	SYMANTEC	SECPOD
Alerta en tiempo real (por correo electrónico o syslog) cuando una modificación ha sido detectada en carpetas, archivos o llaves de registro del sistema operativo y aplicaciones.	SI	SI
Crea reglas personalizadas para el monitoreo de modificaciones en archivos críticos, carpetas y llaves de registro.	SI	SI
Permite ayudar a capturar amenazas que todavía no tienen Firma, incluyendo las amenazas de día cero.	SI	SI
Cuenta con la capacidad de aislar de la red equipo infectados	SI	SI
Integra servicios de reputación para mejorar la protección contra amenazas.	SI	SI
Cuenta con un servicio análisis de cumplimiento de estándares de seguridad integrado.	SI	SI

La consola cuenta con la capacidad de envío de alertas por correo electrónico y generación de roles personalizados	SI	SI
La consola de administración cuenta con reportes predefinidos, los cuales brindan información de los eventos detectados.	SI	SI

Se ha observado que en la evaluación las 2 soluciones cumplen con los requerimientos técnico funcional que se requiere en la Entidad, aunque el software SECPOD presenta mayor granularidad y detalle en las configuraciones de seguridad.

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO.

Análisis Costo – Beneficio de licencias, implementación, actualización, soporte y mantenimiento por 3 años para 114 servidores, tomado a través de proveedores locales:

SOFTWARE	COSTO	VALORACIÓN
Symantec	S/ 620,000.00 inc. IGV	1
Secpod	S./350,000.00 inc. IGV	2

VALORACION DEL COSTO DE LICENCIAMIENTO:

COSTO	PUNTAJE
Alto Costo	1
Bajo Costo	2

NOTA: Las cotizaciones de referencia se adjuntan al presente en los Anexos

8. CONCLUSIONES

De acuerdo a la evaluación realizada, se recomienda la adquisición de software EDR.

Acorde al presente documento, se determinaron los atributos y/o características mínimas que deben ser considerados para la evaluación del software EDR que cubra las necesidades de la Autoridad Nacional del Agua, donde se demuestra que la mejor alternativa para la institución es SecPod; sin embargo, esto no excluye a participar del proceso de selección al software Symantec.

9. FIRMAS

Nombre	Cargo	Firma
Lic. Edwin Dante Quispe Soto	Director de la Dirección del Sistema Nacional de Información de Recursos Hídricos.	
Tec. Pablo Demetrio Carrión Méndez	Coordinador de Soporte Técnico	

10. ANEXOS

- ✓ Anexo 1: Cotización de Symantec
- ✓ Anexo 2: Cotización de SecPod

PERÚ | Ministerio de Agricultura y Riego

ANA
Autoridad Nacional del Agua

ANEXO 1

Cotización de Symantec

SIP | SISTEMAS INFORMÁTICOS DEL PERÚ

CLIENTE: AUTORIDAD NACIONAL DEL AGUA
ATENCIÓN: SR. PABLO CARRIÓN
FECHA: 02 de Julio 2021

Item	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
		Workstations			
1	Licencias EDR	Symantec Endpoint Detection and Response (EDR) por 3 años, para 114 servidores	1	S/ 620,000.00	S/ 620,000.00
				[illegible]	[illegible]
				IGV	[illegible]
				TOTAL	[illegible]

Observaciones:
Symantec es la solución Nº 1 en EDR

Condiciones Comerciales:

Tiempo de Entrega:	10 días
Precios:	Expresados en soles e incluyen el IGV
Condición de Pago:	Comercial
Validez de la Oferta:	60 días

Nuestra Información:

Ruc:	20472908309
Razón Social:	Sistemas Informáticos del Perú EIRL
Dirección:	Av Benavides 5483 Oficina 201 Santiago de Surco Lima Perú Cesar Vallejo 441 Huanchaco - Trujillo
Cuenta Corriente dólares:	Banco de Crédito del Perú 194-1351551-1-39 CCI: 002-194-001351551139-95
Teléfono:	51 1 6373232

Giancarlo Corzo
Sistemas Informáticos del Perú
Mail: giancarlo.corzo@sip.pe
Cel. 51 [illegible]
Telf. 51 [illegible]
web: www.sip.pe

PERÚ | Ministerio de Agricultura y Riego

ANA
Autoridad Nacional del Agua

ANEXO 2

Cotización de SecPod

TECNOLOGÍA Y CREATIVIDAD

TECNOLOGIA Y CREATIVIDAD S.A.C.
Av. República de Panamá 3563, oficina 101, San Isidro
Central: 644-9400 anexo 209
http://www.tcrealividad.com

San Isidro, 01 de Julio 2021

Señores,
Autoridad Nacional del Agua
Ing. Pablo Carrión

Atención:

Presentamos nuestra empresa TECNOLOGIA Y CREATIVIDAD SAC con más de Quince años de experiencia en el sector de Tecnología de la Información y Comunicaciones (TIC), comercializando diferentes productos, servicios y software que en su conjunto configuran soluciones de tecnología para las diferentes empresas del Perú.

Hacemos llegar nuestra oferta comercial para el proyecto de suscripción de EDR para su organización.

Ítem	Descripción	Cantidad	P.U.	Total
1	114 Licencias por 3 años de SecPod Saner Now For Server	1	S/ 350,000.00	S/ 350,000.00
			Subtotal	S/ 296,610.17
			IGV	S/ 53,389.83
			Total	S/ 350,000.00

(*) Los precios están expresados en soles
(*) Los precios impuestos de ley
(*) Forma de pago. - Comercial
(*) Oferta valida solo hasta el 31 de agosto de 2021

Atentamente,
Susana Rodríguez Caprille
TECNOLOGIA Y CREATIVIDAD SAC
Av. Rep. Panamá 3563 of.101 San Isidro
Tel Fijo: 644-9400 Ext.209
Celular: 998-984266
srodriguez@tcreatividad.com