centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1216

Procedimiento de Empleo Seguro
Trend Vision One Endpoint Security

Julio 2026

Edita:

centro criptológico nacional

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 08:17:34 +02'00'

ÍNDICE

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

El servicio, **Trend Vision One Endpoint Security**, antes denominado Trend Micro Deep Security, es la solución de Trend Micro que permite proteger frente a amenazas, malware y cambios no autorizados en la nube, entornos físicos o entornos híbridos.

El servicio se divide en los siguientes componentes:

a) Trend Micro Deep Security Agent (DSA): o el "agente", es un componente software que se instala directamente en el ordenador o máquina que va a monitorizar y proteger. Supervisa el tráfico entrante y saliente en busca de amenazas por protocolo o en busca de señales de ataque, pudiendo intervenir y neutralizar la amenaza bloqueando o corrigiendo el tráfico.

b) Trend Micro Vision One Console: o la "consola", es una plataforma en la nube que combina ASRM y XDR en una sola consola gracias a las amenazas detectadas y datos enviados por el agente. ASRM ofrece una visibilidad centralizada de la superficie de ataque, puntuación de los riesgos detectados, activos que son vulnerables y tácticas recomendadas. Por su lado, XDR correlaciona datos entre múltiples capas de seguridad, incluyendo dispositivos finales (endpoint), servidores, correo electrónico, identidades de usuario, dispositivos móviles, cargas de trabajo en la nube y redes. Esta información proviene tanto de sensores nativos del sistema como de fuentes globales de inteligencia de amenazas y datos de terceros. Todo lo expuesto se presenta en una sola plataforma en la nube, la consola, que permite detectar, investigar y responder a comportamientos sospechosos, malware, ransomware, interrupciones y otros ataques críticos.

2 OBJETO Y ALCANCE

Este documento de Procedimiento de Empleo Seguro del servicio **Trend Vision One Endpoint Security** está orientado para los siguientes componentes:

- Trend Micro Deep Security Agent: 20.0.1.4540.
- Trend Micro Vision One Console: N/A.

El producto Trend Vision One Endpoint Security ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF22].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 1. En este apartado se recoge la descripción del servicio de forma general.

b) Apartado 2. Este apartado recoge el versionado, inclusión en CPSTIC e información de interés referente a la cualificación del servicio.

c) Apartado 3. Este apartado recoge la descripción de los apartados de Procedimiento de Empleo Seguro del servicio.

d) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del servicio.

e) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del servicio.

f) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del servicio, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

La consola, al estar desplegada en la nube íntegramente por Trend Micro, no requiere de entrega o instalación previa. El único requerimiento necesario es la adquisición de una licencia a través del formulario disponible en la página definida en la referencia REF2.

Para acceder a dicha página, se debe verificar que el protocolo es HTTPS y que el certificado SSL es válido, tal y como se aprecia en la Ilustración 1.

Ilustración 1. Certificado de la página.

La descarga del componente DSA debe realizarse a través de la página definida en la referencia REF3. El agente se ha evaluado en el sistema operativo Windows. También puede seguirse cualquiera de los despliegues mencionados en la guía definida en la referencia REF4

Todos los enlaces de descarga están acompañados de un hash SHA256 que permite validar que el fichero descargado no ha sido manipulado de forma no autorizada, como se aprecia en la Ilustración 2. El usuario autorizado que descargue e instale el DSA **debe realizar esta comprobación de la integridad** siguiendo la guía definida en la referencia REF5. REF5

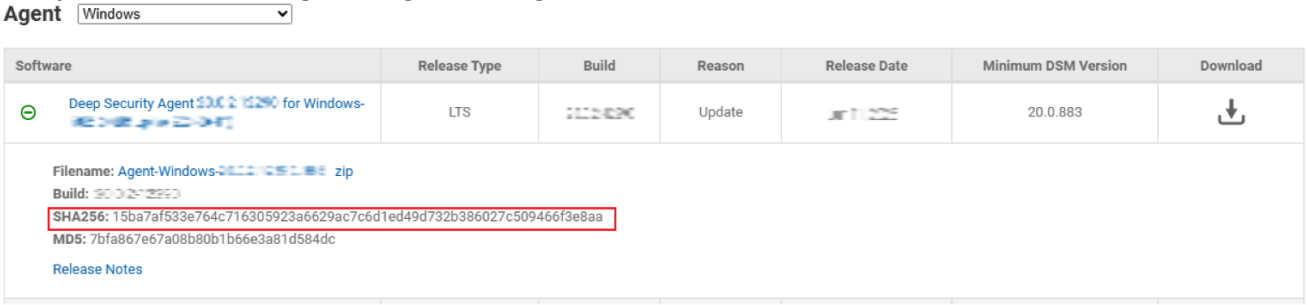

Ilustración 2. Verificación del agente.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Para este Procedimiento de Empleo Seguro no se considera la configuración de ningún entorno de instalación seguro para la consola, porque está desplegada por parte de Trend Micro en un entorno cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

Para el agente DSA, el entorno donde se instala (Windows) debe cumplir con las consideraciones previas mencionadas en la guía definida en la referencia REF6. Adicionalmente, deben seguirse los pasos descritos en la sección “Install the agent on Windows” de la guía.

4.3 REGISTRO Y LICENCIAS

Una vez adquirida la suscripción, el usuario administrador establecido para iniciar sesión por primera vez en Trend Vision One Console recibirá por correo electrónico la activación de la licencia de uso, que tendrá un formato parecido al que se muestra en la siguiente figura.

LICENSE CERTIFICATE

N° [redacted]

TREND MICRO

Page 1

LICENSEE INFORMATION

End User	Reseller	Distributor
[redacted]	[redacted]	NO DISTI INVOLVED SPAIN

Please register/activate your product here

LICENSE ENTITLEMENT

Ref	Solution	Registration Key	Activation Code	Cert No.	Volume	Start Date	End Date
1	Trend Vision One - Endpoint Security (Pro), New						

Ilustración 3. Ejemplo de licencia que se obtiene al adquirir la suscripción.

Tras pulsar sobre el texto en rojo “Please register/activate your product here” y activar correctamente el servicio, se debe iniciar sesión en la página web descrita en la referencia REF7, con sus credenciales de administrador, conformadas por usuario (proporcionado por Trend Micro) y contraseña (configurada por el propio usuario cuando accede por primera vez al servicio, como se define en la sección 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES).

4.4 CONSIDERACIONES PREVIAS

Las consideraciones previas para la instalación del DSA se encuentran en la guía referenciada en REF8.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El entorno de operación aplicable para este servicio contiene los siguientes componentes:

- Windows 10 Professional versión 10.0.19045 o superior, incluyendo Windows 11 Professional: Sistema operativo donde se instala el DSA y donde se ejecutan las funcionalidades del servicio aplicables para el agente.
- AWS: Plataforma en la nube donde Trend Micro despliega la consola.

5 FASE DE INSTALACIÓN

La consola no requiere de instalación para este Procedimiento de Empleo Seguro.

Para el DSA, se deben seguir los siguientes pasos para la instalación:

a) Iniciar sesión en la consola Trend Micro Vision One Console como usuario con rol "Master Administrator". Este mismo usuario es el que obtiene la licencia definida en el apartado 4.3 REGISTRO Y LICENCIAS.

b) Navegar hacia la sección "Endpoint Security > "Endpoint Inventory", y hacer clic sobre "Agent Installer".

c) En la ventana que se abre, seleccionar las siguientes opciones:

   i. Operating System: Windows

   ii. Full package

   iii. OS version: Microsoft Windows 10 (Sistema operativo usado durante el proceso de cualificación) o Microsoft Windows 11.

   iv. Protection Manager: Server and Workload Protection Manager - 846407779957

d) Descargar el paquete haciendo clic sobre el botón azul de descarga.

e) En el sistema operativo seleccionado, descomprimir el paquete.

f) Entrar a la ruta "packages > a4d5d1da-6838-4a92-808c-8bd400f58e76" e instalar "agent.msi".

g) Abrir CMD como usuario administrador del sistema operativo y navegar a la carpeta donde se ha instalado el agente (C:\Program Files\Trend Micro\Deep Security Agent) y ejecutar el siguiente comando para registrar el agente en la consola Trend Micro Vision One Console:

   i. dsa_control -a dsm://agents-020.workload.de-1.cloudone.trendmicro.com:443/ "tenantID:<ID_Tenant>" "token:<token>" "policyid:6"

   ii. Los valores <ID_Tenant> y <token> se obtienen desde la consola, en la sección "Support > Deployment Scripts". Tras seleccionar la plataforma de despliegue, se debe hacer clic en "Activate Agent automatically after installation", y en el script que aparece se localizan dichos valores.

h) Tras ejecutar el comando, se debe verificar en la consola Trend Micro Vision One Console que se ha activado correctamente, entrando en la sección "Security Endpoint > Endpoint Inventory", donde debe aparecer el agente recientemente instalado:

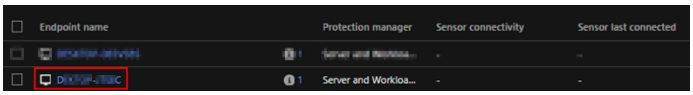

Ilustración 4. Ejemplo de agente instalado y activado en la consola.

Adicionalmente, el estado del agente debe ser "Managed (Online)" en la sección "Server & Workload Protection > Computers":

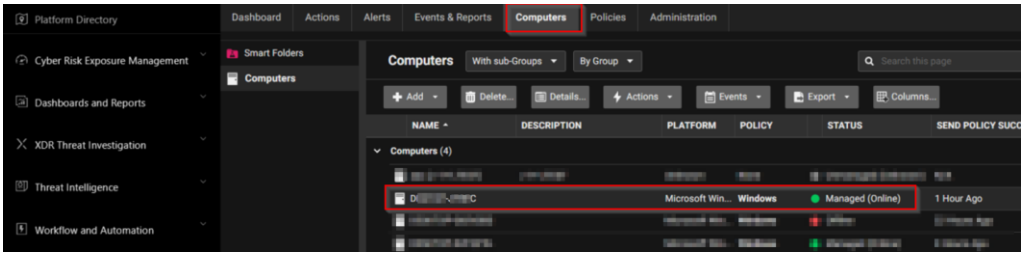

Ilustración 5. Ejemplo de agente en estado "Managed (Online)".

Una vez instalado y comprobado por primera vez, la máquina Windows debe reiniciarse. Una vez reiniciada, debe de hacerse la misma comprobación de nuevo. Si no aparece como "Managed (Online)", se debe reiniciar la máquina y esperar 24 horas para volver a hacer la comprobación.

También puede comprobarse que el DSA está correctamente activado haciendo clic sobre el icono en de la bandeja del sistema (o icono del área de notificación) en Windows, seleccionando la opción "Open Console":

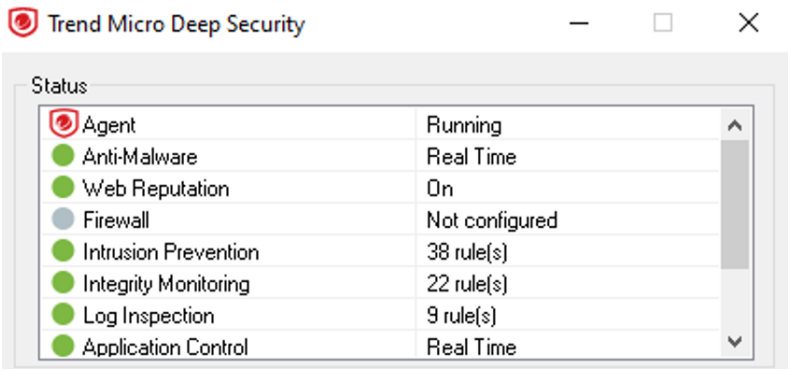

Ilustración 6. Verificación a través del icono del área de notificación.

Como método adicional para desplegar y activar agentes DSA, se puede realizar a través de *scripts* de automatización siguiendo la guía referenciada en REF9.

Nota: Esta alternativa no se ha ejecutado durante la cualificación del servicio.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para que el agente tenga todas las políticas de detección y mitigación configuradas, se deben activar desde la consola al agente. Para ello, se debe de navegar a la sección “Server & Workload Protection > Computers” y seleccionar la máquina destino listada, y posteriormente entrar al menú “Actions” y hacer clic sobre “Send Policy”.

Para comprobar que el DSA está configurado correctamente, se debe verificar que en la sección “Server & Workload Protection > Computers > <Máquina destino> > General” aparece como “On” las siguientes opciones:

a) Anti-Malware.

b) Web Reputation.

c) Device Control.

d) Application Control.

e) Intrusion Prevention.

f) Integrity Monitoring.

g) Log Inspection.

Si todo está en “On”, se debe comprobar la configuración del nivel de detección y prevención haciendo doble clic en la máquina que aparece en la Ilustración 5, entrando a la sección “Anti-Malware” y haciendo clic en “Edit” en la opción “Malware Scan Configuration”.

En caso de no estar todo en “On”, se debe repetir el paso especificado en el párrafo 0. En algunos casos, se debe reiniciar la máquina Windows donde se ha desplegado el agente y esperar 24 horas para volver a hacer la comprobación.

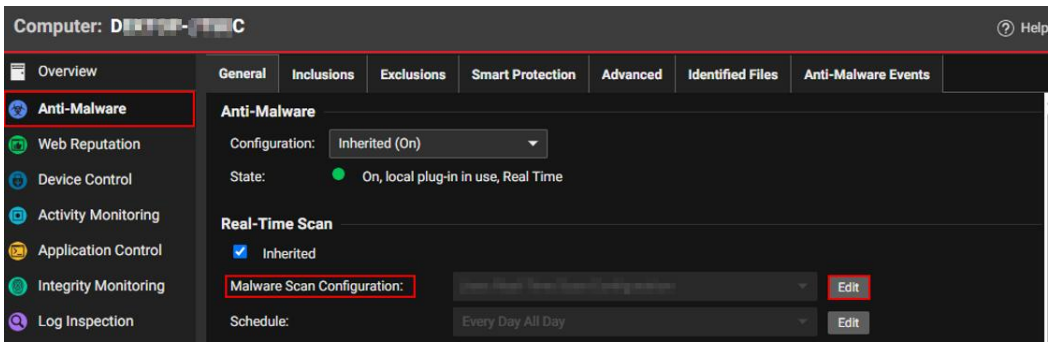

Ilustración 7. Configuración específica de nivel de detección y prevención.

Los campos *Detection Level* y *Prevention Level* debe estar establecido como “***3 – Aggressive***”:

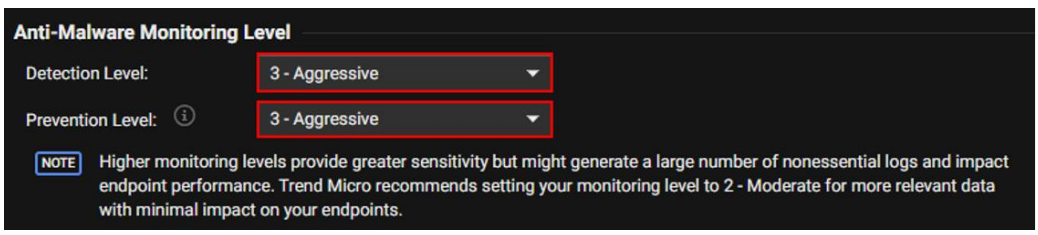

Ilustración 8. Nivel de detección y prevención.

La opción de "*Enable Trend Micro Smart Feedback (recommended)*" **debe ser desactivada** de la sección "Server & Workload Protection > Administration > System Settings > Smart Feedback".

Posteriormente, debe verificarse que la opción "Spyware/Grayware Pattern" y la opción "Spyware Active Monitoring Pattern" tienen las versiones 28.87 y 2.887.00 respectivamente. Para ello, se debe acceder al menú "Server & Workload Protection > Computers" y hacer clic en la máquina donde está instalado el DSA. Luego, se debe seleccionar el menú "Updates" y hacer clic en "Download Component Updates".

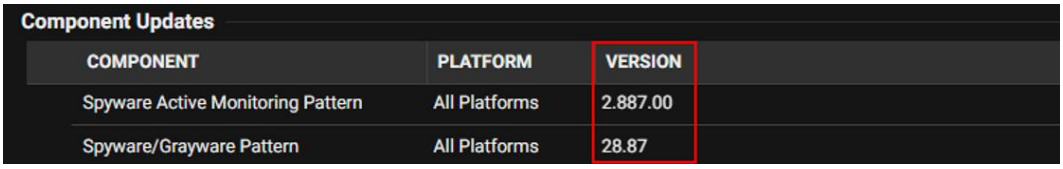

Ilustración 9. Configuración de "Spyware/Grayware Pattern" y "Spyware Active Monitoring Pattern".

Finalmente, se debe verificar que toda esta configuración se ha aplicado correctamente sobre el agente. En la máquina donde está instalado, se debe de hacer clic en el icono del área de notificaciones y seleccionar "Open Console". Si todo está correcto, las mismas opciones listadas en el párrafo 0 deben aparecer (tal y como se aprecia en la Ilustración 6).

6.2 AUTENTICACIÓN

Los mecanismos de autenticación usados por el servicio son los siguientes**:**

- **Usuarios administradores**: Credenciales locales (usuario y contraseña).
- **Autenticación entre componentes del servicio**: Mediante certificados X.509.V3

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración del servicio se realiza de forma remota a través del componente Trend Vision One Console (GUI).

NO deben permitirse protocolos **inseguros** para la administración, tales como:

- Versión TLS inferior a 1.2 (debe utilizarse TLSv1.2 o superior)

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Los roles activos en el servicio pueden encontrarse en la guía referenciada en REF10. No deben configurarse más roles personalizados o modificar los ya existentes.

Se deben tener en cuenta los siguientes aspectos para la configuración de usuarios administradores:

- **Configuración de la Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:
  - Longitud mínima de la contraseña: doce (12) caracteres.
  - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales.

- **Configuración de los parámetros de sesión.** Deberá cumplir con los siguientes requisitos mínimos:
  - Tiempo de inactividad de las sesiones: treinta (30) minutos, configurable siguiendo la guía referenciada en REF11.
  - Número de intentos fallidos de inicio de sesión: diez (10) intentos.
  - Tiempo de bloqueo tras los intentos fallidos: los diez (10) primeros intentos fallidos bloquean al usuario por cinco (5) segundos. A partir de cada diez (10) intentos fallidos adicionales, el tiempo de bloqueo se duplica.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

El DSA emplea unos puertos predefinidos para su operación:

a) Mensaje de estado periódico: 4120.

b) Propia operación del agente: 4118

Se recomienda no modificar los puertos por motivos de estandarización y estabilidad de la plataforma.

6.5 GESTIÓN DE CERTIFICADOS

Para este Procedimiento de Empleo Seguro, no se debe configurar o gestionar ningún tipo de certificado.

6.6 SERVIDORES DE AUTENTICACIÓN

Para este Procedimiento de Empleo Seguro, no se debe configurar o gestionar ningún servidor de autenticación externo.

6.7 SINCRONIZACIÓN

El DSA debe utilizar un servicio NTP de sincronización horaria, que deberá efectuarse a nivel de sistema operativo, por lo que este agente tomará la hora del sistema como referencia.

La consola debe utilizar un servicio NTP de sincronización horaria configurado íntegramente por Trend Micro.

6.8 ACTUALIZACIONES

Las actualizaciones de la consola son llevadas a cabo por el personal administrativo y técnico de Trend Micro. Por tanto, para este Procedimiento de Empleo Seguro, no se contempla la metodología de actualización para este componente.

Para actualizar el DSA, se deben seguir las consideraciones y pasos descritos en la guía referenciada en REF12.

a) Como consideraciones adicionales, la máquina donde se ha actualizado el DSA debe reiniciarse y esperar por 24 horas para completar la actualización.

b) Tras esperar ese tiempo, debe ejecutarse en el CMD con permisos de usuario administrador del sistema operativo el siguiente comando:

```
./dsa_control.cmd -r
```

c) Debe recibirse por CMD la respuesta “HTTP Status: 200 - OK”.

d) Posteriormente, debe ejecutarse el comando de activación registrado en el paso *g)* de la sección *5 FASE DE INSTALACIÓN* de este documento.

e) Tras repetir el paso de activación, se debe verificar el estado del DSA tal y como indica el paso *0* de la sección *5 FASE DE INSTALACIÓN* de este documento.

f) Una vez verificado el estado, se debe acceder al menú “Actions” de la misma sección en la consola, y hacer clic sobre “Send Policy”.

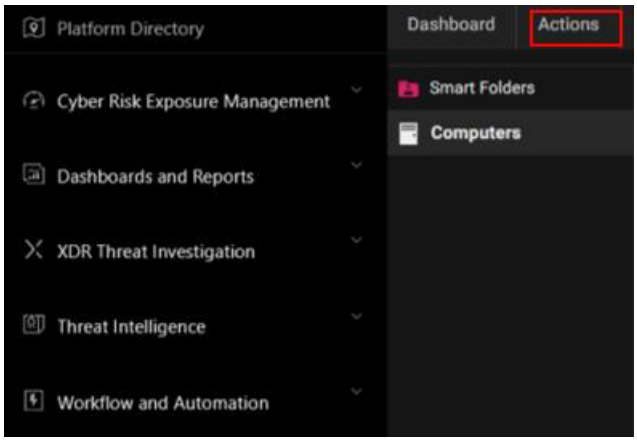

Ilustración 10. Menú “Actions”

6.9 AUTO-CHEQUEOS

El DSA, en la fase de arranque, efectúa los siguientes chequeos:

a) Verificación de integridad (*checksum*).

b) Conectividad con servicios de actualización.

c) Validez de los certificados empleados en la comunicación.

d) Disponibilidad del resto de nodos del grupo de balanceo de carga.

En el caso de que alguno de estos chequeos sea erróneo o inválido, se generará el correspondiente mensaje en el log del servidor de aplicaciones o en el log del sistema. **Se debe, por tanto, revisar y analizar la información de logs para detectar errores en los auto chequeos.**

Los auto chequeos y el monitoreo de integridad de la consola se gestionan de manera centralizada por Trend Micro, dado que este componente está desplegado en la nube. Este componente está diseñado para funcionar continuamente, con procesos automáticos que garantizan su rendimiento, integridad y disponibilidad sin necesidad de intervención directa por parte del usuario final.

6.10 ALTA DISPONIBILIDAD

El componente Trend Micro Vision One Console está diseñado para ofrecer alta disponibilidad mediante la implementación de arquitecturas en la nube redundantes, asegurando que los usuarios puedan acceder a los servicios de manera continua, sin interrupciones. La gestión de la alta disponibilidad es una responsabilidad directa de Trend Micro, que garantiza la operatividad de los servicios a través de diversas estrategias.

La combinación de redundancia geográfica, balanceo de carga y capacidades avanzadas de recuperación ante desastres asegura que los usuarios puedan confiar en que los servicios estarán disponibles en todo momento.

En caso de que se produzca una interrupción, Trend Micro gestiona el proceso de recuperación, asegurando que el servicio vuelva a estar operativo lo más rápido posible sin intervención del usuario final.

Por su parte, por la naturaleza del componente, no se considera aplicable el DSA como componente para desplegar en alta disponibilidad, ya que se instala un agente por máquina.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El servicio puede registrar tres (3) tipos de eventos:

a) **Eventos del sistema (*System Events*)**: Relativos a actividades relacionadas con el funcionamiento del servicio y tareas de auditoría (ej.: Acceso de usuarios, cambios de configuraciones en políticas, errores de actualización, etc). Eventos disponibles en la guía referenciada en REF13.

b) **Eventos de seguridad**: Relativos a actividades registradas en los módulos de seguridad proporcionados por el servicio (Antimalware (REF14), Web Reputation (REF15), Application Control (REF16), Log Inspection (REF17), Integrity Monitoring (REF18), Firewall (REF19) e IPS (REF20)). Ej.: Detección de malware por el módulo antimalware. Eventos disponibles en las guías marcadas.

c) **Alertas**: Generadas en base a un evento o error del sistema. Ej.: Problemas de comunicaciones con servicios de la nube de Trend Micro. Eventos disponibles en la guía referenciada en REF21.

6.11.2 ALMACENAMIENTO DE REGISTRO DE EVENTOS.

El servicio no cuenta con almacenamiento local de los eventos auditados, todo lo referido a auditoría está almacenado de forma remota por Trend Micro.

Para la evaluación bajo la metodología LINCE, tampoco se contempla la configuración de un servidor remoto por parte de los usuarios administradores.

6.12 BACKUP

La consola Trend Vision One Console está diseñada para almacenar información y tiene capacidades de respaldo de forma centralizada, gestionadas y configuradas íntegramente por Trend Micro.

Trend Micro gestiona la realización periódica de copias de seguridad.

7 REFERENCIAS

REF1	Trend Vision One Endpoint Security 20.0.1.4540
REF2	Solución de Endpoint Security - Trend Vision One™ | Trend Micro (ES)
REF3	Deep Security long term support Software | Deep Security
REF4	Get Deep Security Agent software | Deep Security
REF5	Check digital signatures on software packages | Deep Security
REF6	Install the agent | Deep Security
REF7	Trend Vision One™
REF8	Install the agent | Deep Security
REF9	Use deployment scripts to add and protect computers | Deep Security
REF10	Define roles for users | Deep Security
REF11	Console Settings | Trend Micro
REF12	Upgrade Deep Security Agent | Deep Security
REF13	System events | Deep Security
REF14	Anti-malware events | Deep Security
REF15	Web Reputation events | Deep Security
REF16	Application control events | Deep Security
REF17	Log inspection events | Deep Security
REF18	Integrity monitoring events | Deep Security
REF19	Firewall events | Deep Security
REF20	Intrusion prevention events | Deep Security
REF21	Predefined alerts | Deep Security
REF22	CPSTIC

8 ABREVIATURAS

ASMR	Attack Surface Risk Management
AWS	Amazon Web Service
CPSTIC	Catálogo de Productos y Servicios TIC
DSA	Deep Security Agent
ENS	Esquema Nacional de Seguridad.
HTTP	Hypertext Markup Language
HTTPS	HTTP Secure
TLS	Transport Layer Security
XDR	Extended Detection & Response