Guía de Seguridad de las TIC
CCN-STIC 1226

Procedimiento de Empleo Seguro
SentinelOne Singularity Complete

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.26 08:49:54 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 COMPONENTES DEL ENTORNO DE OPERACIÓN Y ENTORNO DE INSTALACIÓN SEGURO .. 6
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 10
6.1 MODO DE OPERACIÓN SEGURO 10
6.1.1 CONFIGURACIÓN DE LOS USUARIOS Y SESIONES 10
6.1.2 VISUALIZACIÓN DE AUDITORÍA DE LOS AGENTES. 10
6.1.3 CONFIGURACIÓN DE POLÍTICAS. 10
6.1.4 CONFIGURACIÓN DE CORREOS ELECTRÓNICOS. 11
6.2 AUTENTICACIÓN 11
6.3 ADMINISTRACIÓN DEL PRODUCTO 12
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 12
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 12
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 13
6.5 GESTIÓN DE CERTIFICADOS 13
6.6 SERVIDORES DE AUTENTICACIÓN 14
6.7 SINCRONIZACIÓN 14
6.8 ACTUALIZACIONES 14
6.9 AUTO-CHEQUEOS 14
6.10 ALTA DISPONIBILIDAD 15
6.11 AUDITORÍA 15
6.11.1 REGISTRO DE EVENTOS 15
6.11.2 ALMACENAMIENTO LOCAL 16
6.11.3 ALMACENAMIENTO REMOTO 16
6.12 BACKUP 17
7 REFERENCIAS 18
8 ABREVIATURAS 19

1 INTRODUCCIÓN

1. El servicio, **SentinelOne Singularity Complete**, representa un *Next Generation Endpoint Protection* (NGEP), que permite detectar y prevenir amenazas en *endpoints*. Las funcionalidades específicas se realizan a través de monitorización dinámica del comportamiento de los *endpoints* y a través del análisis y detección en tiempo real de vectores de ataque. El servicio incluye las siguientes características:

   a) Arquitectura flexible *multi-tenant* que ofrece sitios y agrupaciones personalizables para facilitar la administración empresarial.

   b) XDR que unifica y extiende la detección a través de diferentes capas de seguridad y permite la ingesta de datos de soluciones de terceros para conseguir máxima capacidad de respuesta y visibilidad mediante una vista única.

   c) Prevención con modelos con IA que permiten identificar archivos binarios y *ransomware* antes de que actúen.

   d) EDR activo para generar fácilmente contexto esencial para la detección y respuesta proactiva en tiempo real.

   e) Gestión de vulnerabilidades avanzada para aplicaciones y sistemas operativos.

   f) Amplio soporte de dispositivos (estación de trabajo, móvil, servidores) y sistemas operativos, así como entornos de nube privada, nube pública y contenedores.

2. El servicio está formado por los siguientes componentes principales:

   a) **Consola de gestión**. Representa el *dashboard* de gestión que utilizan los usuarios autorizados (administradores). Adicionalmente, actúa como la parte servidora en la solución, controlando y gestionando los agentes instalados en los *endpoints* y manteniendo la base de datos de las firmas o *signatures* de las amenazas empleada por los agentes. Además, este componente gestiona de forma centralizada los registros de auditoría del servicio.

   b) **Agente**. Es la parte instalable y que actúa como cliente en el servicio, monitorizando los ficheros y procesos en los *endpoints* para descubrir y remediar amenazas.

3. El flujo para la detección estática por parte del servicio es el siguiente:

   a) La Consola de gestión contiene, como ya se ha definido, la base de datos con la firma de las amenazas ya conocidas.

   b) Los Agentes, en caso de descubrir una potencial amenaza, calculan su firma para identificarla.

   c) Los Agentes hacen una petición a la Consola de gestión con la identificación realizada para consultar en la base de datos la firma, para ver si existe como amenaza conocida o no.

   d) La Consola de gestión responde tras analizar la amenaza, y los Agentes mantienen en una memoria volátil las últimas consultas realizadas para mantener el funcionamiento de forma eficiente.

4. Adicionalmente a este flujo, y como se ha mencionado con anterioridad, la solución también permite la detección y bloqueo de amenazas de forma dinámica, mediante el análisis de procesos, actividades sospechosas y comportamiento.

5. En la siguiente figura se muestra un diagrama con la estructura de la solución **SentinelOne Singularity Complete,** teniendo en cuenta la solución evaluada, en la que se establece una comunicación directa entre el agente de SentinelOne y la consola de gestión a través de Internet:

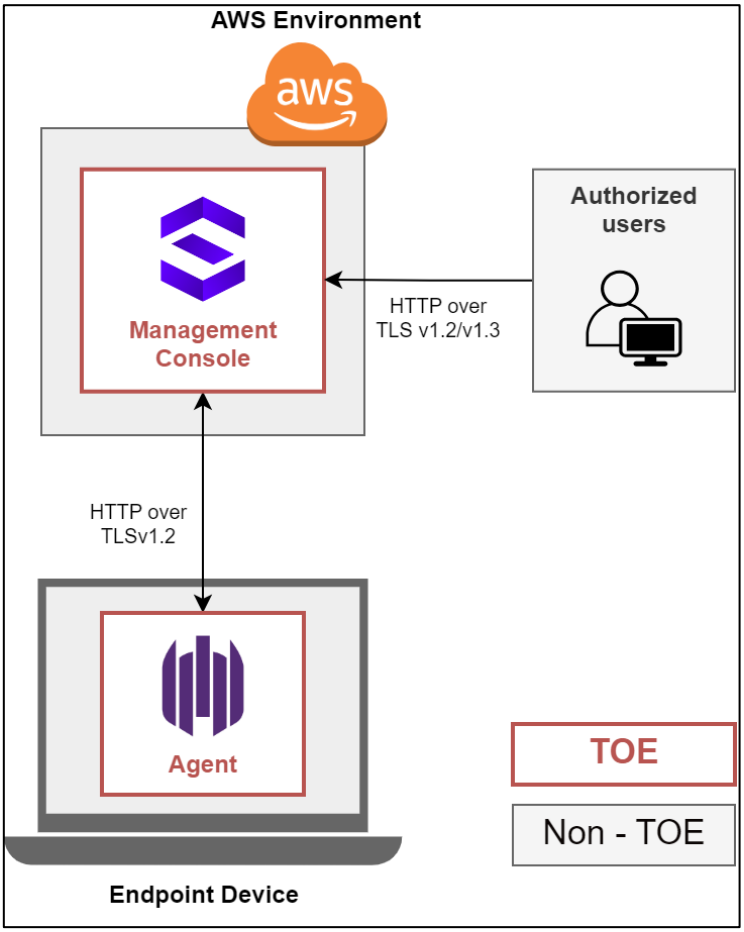

Ilustración 1 Estructura de SentinelOne Singularity Complete

6. En cualquier caso, también existiría la posibilidad de centralizar la gestión de los datos enviados a la consola de gestión a través de un servidor proxy, tal y como se define en la sección "Working with the Agent > Proxy Settings for Agents" de la guía [**REF1**].

2 OBJETO Y ALCANCE

7. El presente documento recoge el Procedimiento de Empleo Seguro (PES) de la solución **SentinelOne Singularity Complete**, incluyendo los siguientes componentes:

   a) Consola de gestión: Singularity Complete Management Console – versión 25.1.5.262.

   b) Agente: Windows Sentinel Agent – versión 24.2.3.471.

8. Esta solución ha sido incluida en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte **[REF4]**.

3 ORGANIZACIÓN DEL DOCUMENTO

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

b) Apartado 5. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración y operación del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. En primer lugar, se debe adquirir una suscripción del servicio para hacer uso de él, accediendo a la página web oficial de SentinelOne **[REF2]** y rellenando el formulario de contacto con el equipo comercial de SentinelOne.
10. Una vez adquirida la suscripción, SentinelOne proveerá una URL de acceso al punto de contacto facilitado, única para cada usuario, de forma que puedan iniciar sesión en la consola de gestión por primera vez. El usuario administrador, al acceder a la URL, definirá la contraseña que desee en base a las políticas de robustez establecidas.
11. Tras esto, el usuario autorizado dispondrá de acceso a la configuración del servicio y a la descarga e instalación de los agentes. En este caso, los agentes hacen uso de certificados para verificar la integridad y autenticidad del software descargado. Aunque esta verificación es realizada de forma automática, también es posible que el usuario del sistema operativo la realice de forma manual, por lo que se recomienda seguir los siguientes pasos:
    a) En Windows, hacer clic derecho sobre el agente descargado.
    b) Entrar al menú “Propiedades” y luego “Firmas digitales”.
    c) Seleccionar la firma digital y hacer clic sobre “Detalles”.
    d) El mensaje “La firma digital está OK”, o similares, junto con el nombre “SentinelOne Inc.” en el campo “Firmante” indican que la firma es válida.

4.2 COMPONENTES DEL ENTORNO DE OPERACIÓN Y ENTORNO DE INSTALACIÓN SEGURO

12. Para garantizar un entorno de instalación seguro de los componentes *on-premise* de la solución SentinelOne Singularity Complete (agentes) en equipos con sistema operativo Windows, es esencial seguir ciertas precauciones. Los componentes en la nube se encuentran alojados en la arquitectura de SentinelOne (AWS), por lo que el usuario final no necesita realizar ningún despliegue o configuración en este sentido.
13. Para la solución cualificada, el navegador web empleado para acceder a la consola de gestión será Microsoft Edge en su última versión disponible, el cual deberá estar instalado en una máquina Windows 10 Pro 64-bit 22H2, Windows 11 Pro 64-bit 24H2 o superior.
14. Por otro lado, el agente relativo a la solución cualificada deberá estar instalado en un sistema operativo Windows con soporte activo de seguridad y cuya versión figure entre las declaradas como compatibles por el fabricante en la sección “*Platform Requirements > System Requirements > Agent requirements on Windows*” de la guía [**REF1**]. Adicionalmente, las máquinas donde se instalen los agentes deberán de ser gestionadas por administradores del sistema que sean considerados confiables.

4.3 REGISTRO Y LICENCIAS

15. El procedimiento de **activación de licencias** para la solución SentinelOne Singularity Complete viene especificado en la sección "*Getting Started > SentinelOne Basics*" de las guías [**REF1**].

4.4 CONSIDERACIONES PREVIAS

16. Es preciso **configurar las cipher suites** de los canales de comunicación que establezcan los componentes *on-premise* con los componentes desplegados en la nube de la solución SentinelOne Singularity Complete. Se recomienda aplicar esta configuración a nivel de sistema operativo para garantizar el cumplimiento de las cipher suites aceptadas según la guía CCN-STIC-807 para la categoría ALTA del ENS:
    a) Acceder a la consola de administración de directivas de grupo (gpedit.msc).
    b) Acceder a "Configuración del Equipo > Plantillas Administrativas > Red > Configuración de SSL".
    c) Hacer doble clic en "Orden de cipher suites SSL" y clic en la opción "Habilitada"
    d) En el cuadro de texto de abajo, hacer clic derecho, eliminar las cipher suites existentes y añadir las siguientes cipher suites en el formato indicado:
        i. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    e) Adicionalmente, hacer clic derecho en el cuadro "Orden de Curvas ECC", habilitar la opción del orden y eliminar las curvas existentes y añadir las siguientes en el formato indicado (en diferentes líneas):
        a) curve25519
        b) secP256r1
        c) secP384r1
17. Por otro lado, para el acceso a la consola de gestión, el usuario administrador debe **configurar adicionalmente el navegador web** Microsoft Edge, para garantizar el cumplimiento de las cipher suites aceptadas según la guía CCN-STIC-807 para la categoría ALTA del ENS:
    a) En la máquina Windows, presionar la combinación de teclas "Windows" + "R".
    b) Escribir "regedit" en el cuadro de búsqueda que se abre:
    c) Acceder al menú "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge"
    d) Hacer clic derecho y seleccionar "Nuevo > Clave" con nombre "TLSCipherSuiteDenyList".
    e) Añadir los siguientes valores *string* (REG_SZ) de forma individual (numerados ordenadamente desde el 1 en adelante):
        i. 0xc013
        ii. 0xc014
        iii. 0xc009c

iv. 0xc009d

v. 0xc002f

vi. 0xc0035

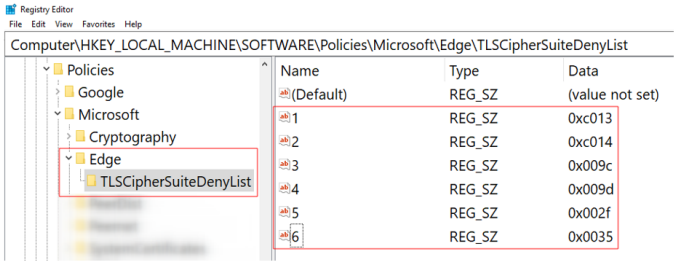

Ilustración 2. Ejemplo de cómo debe quedar TLSCipherSuiteDenyList.

f) Aplicar los cambios, guardar el registro y reiniciar Microsoft Edge.

g) Comprobar que la política se ha aplicado correctamente abriendo Microsoft Edge y navegando a “edge://policy”.

18. **Nota**: Para ambos procesos, se puede hacer uso de cualquier otra cipher suite o curva recomendada por la guía CCN-STIC-807.

19. Finalmente, y como consideración adicional, los equipos finales deberán tener conexión con la consola de gestión, las URLs y/o direcciones IP indicadas en **[REF3]**.

20. Es altamente recomendable aplicar de forma automatizada las configuraciones definidas en esta sección mediante políticas de grupo u otros mecanismos de administración centralizada de la organización, según corresponda en cada caso.

5 FASE DE INSTALACIÓN

21. En primer lugar, no existe un proceso de instalación o desinstalación de la Consola de Gestión asociado a la adquisición del TOE por parte de un cliente en particular, ya que la consola se encuentra desplegada en una infraestructura *cloud* gestionada por SentinelOne.
22. Respecto a la instalación del agente, se recomienda seguir los pasos definidos en la sección "*Getting Started > Deploying and Installing the Agent*" de la guía [**REF1**].
23. Específicamente, cabe destacar que la instalación del agente será posible de forma atendida y desatendida. En ambos casos, se requerirá de un token de instalación que identifica a la plataforma y a la organización que haga uso del servicio.
24. Este token, denominado por SentinelOne como **site token**, puede ser consultado en la consola de gestión dentro de la sección *Sentinels > Packages*.
25. Para instalar el agente descargado (el cual se recomienda que sea en formato ".msi"), se debe de ejecutar como administrador del sistema el instalador e introducir el token.
    a) Si se desea, también puede instalarse desde una CMD / Powershell con permisos de administración ejecutando el siguiente comando (en la carpeta donde se encuentre el instalador):

```
SentinelOneInstaller.exe -t <token>
```

    b) O, de forma desatendida:

```
SentinelOneInstaller.exe -t <token> -q
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

26. Para comenzar a hacer uso del servicio, la guía de "User Guide for Management Console" [**REF1**] debe seguirse. En específico, se recomienda seguir los pasos especificados en las siguientes subsecciones.
27. **Nota**: De forma general, para cualquier configuración realizada a través de la consola de gestión, siempre que se presente una ventana de confirmación al realizar cualquier modificación, se deberá hacer clic en "Yes" para confirmar los cambios.

6.1.1 CONFIGURACIÓN DE LOS USUARIOS Y SESIONES

28. En primer lugar, en caso de que cualquiera de los usuarios desee modificar la contraseña de su propia cuenta dentro de la consola de gestión o iniciar sesión por primera vez (en cuyo caso la propia consola lo requiere), deberá seguir la sección "*Setting Up The Management Console > Changing a User's Password*".
29. Adicionalmente, todos los usuarios que hagan uso de la consola de gestión requerirán configurar un doble factor de autenticación por defecto, de cara a acceder a la interfaz web de forma segura. Para ello se recomienda seguir la sección "*Setting Up The Management Console > Logging in with Two-Factor Authentication*".
30. Por último, para la solución cualificada, deberá configurarse un *timeout* automático de inactividad de 30 minutos que aplique a todos los usuarios autorizados de la consola de gestión. Para esta configuración, se debe seguir la sección "*Setting Up The Management Console > Configuring Session and Inactivity Timeout*".

6.1.2 VISUALIZACIÓN DE AUDITORÍA DE LOS AGENTES.

31. Para visualizar los registros de auditoría de los agentes, se recomienda seguir la sección "*Getting Started > Fetching Agent and Endpoint Logs*".
32. Cabe destacar que los logs de los agentes también pueden visualizarse de forma local, a través de la herramienta *Windows Event Viewer*, haciendo uso del siguiente fichero:

```
%SystemRoot%\System32\Winevt\Logs\SentinelOne%4Operational.evtx
```

6.1.3 CONFIGURACIÓN DE POLÍTICAS.

33. Se recomienda seguir la sección "*Singularity Endpoint Security > Policies & Modules > Policies*" de la guía de cara a adquirir los conocimientos necesarios para gestionar y actualizar políticas.
34. Específicamente, para la solución cualificada se deberán realizar las siguientes configuraciones a través de la consola de gestión, concretamente en la pestaña de "Sentinels" y la sección "Policy":
    a) Protection Mode:
        i. La opción de "Malicious Threat" debe establecerse en "Protect", con "Protect Level" configurado en "Kill & Quarantine, Remediate".

ii. La opción de "Suspicious Threat" debe establecerse en "Protect", con "Protect Level" configurado en "Kill & Quarantine, Remediate".

b) Detection Engines:

i. Todos los "Engines" deberán estar habilitados para esta opción, salvo "Drift Detection (Containers Only)".

c) Agent:

i. La opción de "Security Settings" debe estar habilitada.

ii. Dentro de la sección "Agent UI":

a. La opción "Show Agent UI & Tray icon on endpoints" debe estar habilitada.

b. La opción "Show pop-up notifications for" debe estar habilitada para los siguientes eventos:

i. Threats and Mitigation.

ii. Blocked Devices.

c. La opción "Show suspicious events in the UI" debe estar habilitada para los siguientes eventos:

i. Include Suspicious.

d. La opción "Show these menu ítems in the UI" debe estar habilitada para los siguientes eventos:

i. Quarantined Files.

ii. Contact Support.

d) La opción "Deep Visibility" debe estar deshabilitada.

e) Las opciones existentes en el menú "Applications > Policy > Scan Policy" y "Applications > Policy > Extensive Scan" deben activarse.

6.1.4 CONFIGURACIÓN DE CORREOS ELECTRÓNICOS.

35. Para configurar la notificación de las alertas generadas por los agentes por correo electrónico a los usuarios autorizados, se deben seguir los pasos especificados en la sección "*Setting Up the Management Console > Notifications and Data Forwarding > Configuring Email Notifications*" de la guía. Específicamente, se recomienda seleccionar recibir todas las notificaciones de "Malware" y "Mitigation".

6.2 AUTENTICACIÓN

36. SentinelOne Singularity Complete basa su administración en una consola web en la nube a la cual se puede acceder desde cualquier navegador. Una vez formalizada la compra de licencias, se recibirá la URL de la consola por correo electrónico junto con un enlace temporal para establecer la contraseña y doble factor de autenticación.

37. Tras este primer acceso, y tras la instalación y configuración de la solución, los mecanismos de autenticación usados por el servicio serán los siguientes:

a) **Usuarios administradores para la autenticación a la consola de gestión**: Mediante credenciales locales (usuario y contraseña) y doble factor de autenticación.

b) **Autenticación entre la consola de gestión y los agentes**: mediante certificados X.509.V3 y el uso del "Site Token" para el registro.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

38. La administración de la solución cualificada se realiza de forma remota en la consola web a través de la interfaz de administración. Esta comunicación se realiza a través de HTTPS (HTTP sobre TLS v1.2 o superior) haciendo uso de ciphersuites aceptadas por la guía CCN-STIC-807 para categoría ALTA de ENS.

39. La administración remota a través de esta consola permite a los usuarios autorizados ejercer las siguientes funcionalidades de seguridad:

    - Gestión de los dispositivos finales ("Sentinels"), incluyendo configuraciones de los agentes y políticas.
    - Gestión de incidentes.
    - Gestión de escaneos.
    - Gestión de configuraciones globales, entre las que se incluye la gestión de usuarios (creación, modificación y borrado) y la gestión del tiempo de inactividad.

40. Se deben considerar las recomendaciones de configuración a nivel de sistema operativo, definidas en la sección 4.4 CONSIDERACIONES PREVIAS, para limitar las ciphersuites a nivel de cliente y cumplir con las guías CCN.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

41. La solución SentinelOne Singularity Complete define roles de usuario para poder administrar las funcionalidades de seguridad que ofrece. Esta gestión viene definida en la sección "*Setting Up The Management Console > User Management > Management User Roles*" de [**REF1**].

42. A modo de resumen, los roles predefinidos y su descripción se muestran en la siguiente tabla.

Rol de usuario	Permisos
Viewer	Ver el contenido de la consola sin poder realizar acciones.
C-Level	Ver el contenido de la consola y obtener reportes.
Admin	Utilizar todas las funcionalidades de la consola.
IR Team	Responder a incidentes, investigaciones e IOCs.

IT	Editar exclusiones y lista negra. Configurar opciones como notificaciones, control de dispositivos y reglas de firewall.
SOC	Mitigar y remediar incidentes, aislar endpoints.

Tabla 1. Descripción de los roles de administración.

43. Se deben tener en cuenta los siguientes aspectos:

- **Configuración de la Política segura de contraseñas**. Por defecto, en la creación de la cuenta de un usuario, la contraseña que se solicita deberá cumplir con los siguientes requisitos mínimos:
  - Longitud mínima de la contraseña de doce caracteres.
  - Composición de la contraseña por al menos tres de los siguientes parámetros: letras mayúsculas, letras minúsculas, números y símbolos especiales.
  - Tiempo de validez máximo en días de las contraseñas tras el cual expiran de aproximadamente tres meses (90 días).
  - El usuario deberá también dar de alta un sistema de segundo factor de autenticación escaneando un código QR con alguna de las aplicaciones diseñadas para esta función.
- **Configuración de los parámetros de sesión**. Por defecto cumplirá con los siguientes requisitos mínimos:
  - Tiempo de inactividad de las sesiones: treinta minutos.
  - Número de intentos fallidos de inicio de sesión: tres intentos.
  - Tiempo de bloqueo tras los intentos fallidos: treinta minutos.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

44. Para acceder a la consola web, la comunicación se realizará a través del puerto 443 con la última versión de un navegador compatible.

45. Por defecto, los agentes instalados en los equipos finales se conectan a los componentes nube de SentinelOne Singularity Complete definidos en la sección 4.4 CONSIDERACIONES PREVIAS, específicamente, para la configuración cualificada únicamente será necesario permitir el tráfico TCP entrante y saliente por el puerto 443 del dominio "*euce1-<customer-id>.sentinelone.net*".

6.5 GESTIÓN DE CERTIFICADOS

46. Los usuarios finales que se beneficien del uso del servicio SentinelOne Singularity Complete no precisan de configuración de certificados digitales, ya que estos se encuentran preconfigurados y gestionados por defecto por SentinelOne para los distintos endpoints de la solución. Dichos certificados, firmados con claves **RSA de 3072 bits** o superiores, se emplean para la autenticación de los canales de comunicación a la consola de gestión para ejercer funcionalidades de seguridad entre componentes de la solución o con componentes del entorno operacional.

6.6 SERVIDORES DE AUTENTICACIÓN

47. La solución cualificada no hace uso de servidores externos de autenticación. La autenticación y autorización de usuarios la realiza el servicio de SentinelOne Singularity Complete a través de las credenciales de usuario y el doble factor de autenticación (2FA).

6.7 SINCRONIZACIÓN

48. Se recomienda que todos los equipos protegidos por los agentes de SentinelOne mantengan una sincronización precisa de fecha y hora del sistema operativo.

49. Una hora del sistema correctamente sincronizada es fundamental para el correcto funcionamiento de los registros de eventos, la correlación de alertas, la validez de certificados digitales y la trazabilidad de las acciones de seguridad. Por ello, se recomienda que los sistemas operativos donde se instalen los agentes de SentinelOne estén configurados para sincronizar su reloj mediante servicios NTP confiables, como los proporcionados por el sistema operativo o por servidores internos de la organización. Aunque el producto no implementa autenticación NTP propia, se sugiere, siempre que sea posible, utilizar servidores NTP que soporten autenticación para reforzar la integridad de la sincronización horaria.

6.8 ACTUALIZACIONES

50. Para la consola de gestión, las actualizaciones son llevadas a cabo por el personal administrativo y técnico de SentinelOne. Por tanto, para este Procedimiento de Empleo Seguro, no se contempla la metodología de actualización de este componente del servicio.

51. Por otro lado, es crucial mantener actualizado el agente para garantizar la detección y respuesta efectiva ante las amenazas más recientes, asegurando así la protección continua de los sistemas. Durante la fase de operación del servicio, los administradores deberán mantener los agentes de SentinelOne actualizados. Para ello, deben seguirse los pasos que se muestran a continuación:

    a) Actualización local: Se realiza mediante la descarga y ejecución de la nueva versión del agente, siguiendo los mismos pasos que para su instalación.

    b) Actualización remota: La actualización remota se realiza desde la consola de gestión. Los pasos que se deben realizar son los siguientes:

    c) Seleccionar el endpoint en la pestaña “Sentinels > Endpoints”.

    d) Desde Actions, seleccionar: “Agent version changes -> Update Software”.

    e) Seleccionar la nueva versión del agente y clicar “Update Agent”.

52. En este sentido, es recomendable seguir, de forma orientativa, un ciclo trimestral de actualización de los agentes.

6.9 AUTO-CHEQUEOS

53. Los auto chequeos y el monitoreo de integridad de la consola de gestión se gestionan de manera centralizada por SentinelOne, dado que este componente está desplegado en la nube.

54. A pesar de no contar con auto chequeos, los agentes de SentinelOne aplican medidas de seguridad que refuerzan su integridad y resistencia frente a manipulaciones. En particular, el agente no solicita la asignación de direcciones de memoria explícitas del sistema ni asigna memoria con permisos simultáneos de escritura y ejecución. Además, está configurado por defecto con permisos de archivo que impiden accesos no autorizados.

6.10 ALTA DISPONIBILIDAD

55. La consola de gestión está diseñada 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 SentinelOne, que garantiza la operatividad de los servicios a través de diversas estrategias.
56. 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.
57. En caso de que se produzca una interrupción, SentinelOne gestiona el proceso de recuperación, asegurando que el servicio vuelva a estar operativo lo más rápido posible sin intervención del usuario administrador / autorizado.
58. Para los agentes, no aplica la alta disponibilidad pues son exclusivamente instalados de forma individual en cada *endpoint* que se desee analizar.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

59. La plataforma de SentinelOne permite un registro de auditoría de las acciones llevadas a cabo por los componentes de la solución y sus servicios, además de los registros de inicio y cierre de sesión de los usuarios. La sección "*Getting Started > Using The Management UI > Using the Activity Log to filter and export activities*" [**REF1**] contiene información sobre estos registros de auditoría.
60. De forma específica, los eventos registrados por el servicio relacionados con la funcionalidad de seguridad cualificada se encuentran listados a continuación:

    a) **Inicio y cierre de sesión de usuarios autorizados,** así como **cambios en sus credenciales.**

    b) **Eventos generados por el agente**, incluyendo alertas, amenazas y malware detectado por las funcionalidades EPP/EDR.

    c) **Cambios en la configuración del servicio**:

        i. Eventos relacionados con la **gestión y operación de Sentinels Endpoints,** incluyendo acciones administrativas sobre agentes y dispositivos finales (reinicio, desinstalación o apagado), actualizaciones y cambios de versión, ejecución de escaneos y tareas de mantenimiento o resolución de problemas.

        ii. **Gestión de políticas, listas de bloqueo, exclusiones y políticas de actualización**, incluyendo acciones de creación, edición, modificación y eliminación.

iii. **Gestión de incidentes y amenazas**, incluyendo acciones como finalizar procesos, poner o liberar elementos en cuarentena, remediar amenazas, revertir cambios, desconectar el dispositivo final de la red o añadir amenazas a listas de bloqueo o exclusiones.

iv. **Gestión de aplicaciones** del dispositivo final, incluyendo el escaneo de vulnerabilidades en base al inventario de aplicaciones y la gestión de políticas asociadas a dicho escaneo.

v. **Configuración general de la consola,** incluyendo tiempo de inactividad y gestión de usuarios mediante acciones de creación, edición y eliminación, entre otros parámetros de configuración.

61. A efectos de garantizar su correcta trazabilidad, estos registros de eventos contienen, al menos, la fecha y hora, el tipo de evento identificado, el resultado del evento y, cuando aplique, el usuario que lo ha producido.

6.11.2 ALMACENAMIENTO LOCAL

62. Para la visualización de los registros de auditoría almacenados localmente por los agentes, se recomienda seguir la sección "*Getting Started > Fetching Agent and Endpoint Logs*".

63. Cabe destacar que logs de los agentes también puede visualizarse directamente forma local, a través de la herramienta *Windows Event Viewer*, haciendo uso del siguiente fichero:

```
%SystemRoot%\System32\Winevt\Logs\SentinelOne%4Operational.evtx
```

64. Este funcionamiento es configurado por defecto durante la instalación del agente, y, por tanto, no se requiere ninguna acción específica para garantizar la seguridad del almacenamiento de registros en los equipos protegidos. En este sentido, el periodo de retención de dichos registros dependerá de la configuración del sistema operativo Windows, en particular del tamaño máximo del registro y de la política de sobreescritura definida para el mismo.

6.11.3 ALMACENAMIENTO REMOTO

65. De forma adicional al almacenamiento local de los logs específicos de los agentes, la solución SentinelOne Singularity Complete almacena toda la información generada por estos agentes y la generada por la propia consola de forma centralizada en la infraestructura *cloud* de SentinelOne.

66. Esta arquitectura permite una gestión unificada, segura y resiliente de los registros, eliminando la necesidad de configuración adicional por parte del usuario. Por tanto, no se requiere ninguna acción específica para garantizar la seguridad del almacenamiento de registros en los equipos protegidos.

67. Adicionalmente, cabe destacar que, aunque la configuración evaluada no contempla el envío de logs a servicios externos, la solución permite su integración con servidores Syslog en caso de que resulte necesario. Para ello, se recomienda seguir la sección "*Setting Up The Management Console > Notifications and Data Forwarding > Integrating Syslog servers*" de la guía **[REF1]**.

6.12 BACKUP

68. En la solución SentinelOne Singularity Complete, las configuraciones, registros de actividad y otra información crítica generada por los agentes se almacenan de forma centralizada en la infraestructura *cloud* de SentinelOne. Esta infraestructura utiliza servicios de Amazon Web Services (AWS) como sistema de almacenamiento principal, con mecanismos de replicación automática que garantizan la disponibilidad y resiliencia de los datos.

69. Aunque el usuario final no necesita realizar configuraciones manuales de backup, se recomienda verificar periódicamente desde la consola de administración que los datos se están registrándose correctamente. La realización de copias de seguridad adicionales por parte del cliente no es necesaria, ya que el sistema está diseñado para garantizar la persistencia y recuperación de la información conforme a las buenas prácticas de seguridad en la nube.

7 REFERENCIAS

[REF1] User Guide for Management Console, Version Unity S-25.1. March 20, 2025.

[REF2] SentinelOne official website – Singularity Complete

[REF3] SentinelOne Community. Artículo 000004961

[REF4] CPSTIC

8 ABREVIATURAS

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AWS	Amazon Web Services
CMD	Command Prompt
CPSTIC	Catálogo de Productos y Servicios TIC
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie Hellman Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ENS	Esquema Nacional de Seguridad
EPP	Endpoint Protection Platform
GCM	Galois/Counter Mode
GUI	Graphic User Interface
HTTPS	HyperText Transfer Protocol Secure
IT	Information Technology
MSI	Microsoft Installer
NGEP	Next Generation Endpoint Protection
NIPO	Número de Identificación de Publicaciones Oficiales
NTP	Network Time Protocol
PES	Procedimiento de Empleo Seguro
QR	Quick Response Code
RSA	Rivest Shamir Adleman
SOC	Security Operations Center
SSL	Secure Sockets Layer
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
XDR	Extended Detection and Response