Guía de Seguridad de las TIC
CCN-STIC 1247

Procedimiento de Empleo Seguro
Symantec Endpoint Security Complete

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:25:38 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. La plataforma Symantec Endpoint Security Complete es una herramienta 'Antivirus' ofreciendo funcionalidades de EPP (Endpoint Protection Platform) y EDR (Endpoint Detection and Response). Esta herramienta está diseñada para la prevención, detección y desinfección de Malware, siendo también capaz de detectar y bloquear Malware no conocido.
2. Esta solución integral combina múltiples tecnologías de protección en una única plataforma. Proporciona defensa multicapa frente a malware, ransomware, exploits, ataques sin archivos y amenazas avanzadas, utilizando análisis de comportamiento, aprendizaje automático e inteligencia global de amenazas. Es compatible con análisis de entornos Windows, macOS y Linux, tanto en estaciones de trabajo como en servidores, gracias a sus agentes.
3. Symantec Endpoint Security Complete permite investigar incidentes, analizar el origen y el alcance de un ataque y responder de forma rápida y centralizada. Para ello, la solución ofrece una consola unificada para la gestión de políticas, monitorización en tiempo real y análisis de seguridad, facilitando la visibilidad completa del estado de los endpoints y ayudando a reducir la superficie de ataque y mejorar la postura de seguridad de la organización.
4. Los componentes de la plataforma son los siguientes:
    a) Symantec Agent: Agente instalado en el endpoint del usuario final. Se encargan de recopilar información y enviarla hacia los endpoints de análisis de antivirus.
    b) Symantec Integrated Cyber Defense Manager (ICDm): Consola de gestión centralizada de todos los agentes desplegados y los endpoints donde están desplegados. En el caso de que se detecte alguna anomalía por parte de los endpoints antivirus, se mostrará una alerta en la consola. Está formado por los siguientes dominios:
        a. sep.eu.securitycloud.symantec.com
        b. accounts.security.com
        c. api.saas.broadcomcloud.com
        d. access.broadcom.com
    c) Symantec malware domains: Dominios donde se aloja el motor de análisis y detección de malware. Recibirá toda la información de los agentes y será el encargado de ofrecer un veredicto. Este está formado por los siguientes endpoints:
        a. eu.spoc.securitycloud.symantec.com
        b. liveupdate.symantec.com
        c. ent-shasta-rrs.symantec.com

2 OBJETO Y ALCANCE

5. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación seguras de Symantec Endpoint Security Complete de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad de acuerdo con el ENS. Esta guía aplica a las siguientes versiones del servicio:

    a) Symantec Integrated Cyber Defense Manager: Servicio Cloud

    b) Symantec Agent v14.3 RU10/14.3.12154.10000

    c) Symantec malware domains: Servicio Cloud

6. El producto Symantec Endpoint Security Complete ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC). Para conocer el listado, categoría o nivel y familia de éste, consulte: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic .

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 a tener en cuenta durante la fase de instalación del producto.

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Primeramente, será necesario contactar al equipo de Broadcom solicitando las credenciales de acceso al ICDm, el cual es ofrecido como servicio Cloud. Por otro lado, los dominios de detección de malware también son gestionados por el equipo de Broadcom, ofrecidos como servicios Cloud.
8. Al mismo tiempo, el instalador del Symantec Agent se descarga accediendo al ICDm en su sección *Ajustes -> Paquete de Instalación*. Se deberá de seleccionar la versión correspondiente y, tras hacer clic en el elegido, se descargará el paquete correspondiente desde los repositorios de descarga gestionados por el equipo de Broadcom, considerados como repositorios confiables.
9. Una vez recibido el paquete del Symantec Agent, se deberá de atender a la sección 5 de este documento para seguir su instalación correcta. Posteriormente, se deberá de atender a la sección 6 para la correcta configuración de cada componente.

4.2 REGISTRO Y LICENCIAS

10. Para poder hacer uso de Symantec Endpoint Security Complete se requiere de una suscripción válida. Para gestionar las suscripciones al servicio se debe de acceder a la sección *Ajustes -> Suscripciones* de la consola de ICDm.
11. En la guía oficial de Suscripciones y Licencias de Symantec Endpoint Security [REF1] se indica con más detalle la gestión de la suscripción.

4.3 CONSIDERACIONES PREVIAS

12. De acuerdo con la configuración del servicio cualificada, será necesario integrar un servicio de gestión de identidades externo para poder gestionar los usuarios del servicio. El proveedor de identidad elegido dependerá de la decisión de los administradores, pero se recomienda el uso de IDP cualificados por CPSTIC, incluidos en la guía CCN-STIC-105 [REF3].
13. Para ello, se deberá acceder al portar de soporte de Broadcom [REF15]. Será necesario crear un ticket indicando la información básica acerca del IDP que se desee integrar y el equipo técnico del fabricante gestionará la integración. Durante este proceso el equipo técnico solicitará más información concreta sobre el IDP, como el nombre y dirección de correo del dominio.
14. Cuando el equipo de Broadcom cierre el ticket e indique que toda la configuración ya ha finalizado por su parte, será necesario deshabilitar todas las cuentas de usuario por defecto en el servicio. Para ello, se deberá de acceder a la consola de gestión, ICDm, y acceder a la sección *Configuración de cuenta -> Administradores* y desactivar todas las cuentas. Después de esta última gestión, toda la configuración de usuarios se realizará a través el IDP integrado.
15. Por último, de cara a llevar a cabo un uso correcto del servicio el fabricante ofrece una guía oficial de Buenas Prácticas para Symantec Endpoint Security Complete [REF13].

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. Para el correcto funcionamiento del producto, este establece distintas comunicaciones con los siguientes componentes en su entorno de operación, tal y como se muestra en el siguiente diagrama:

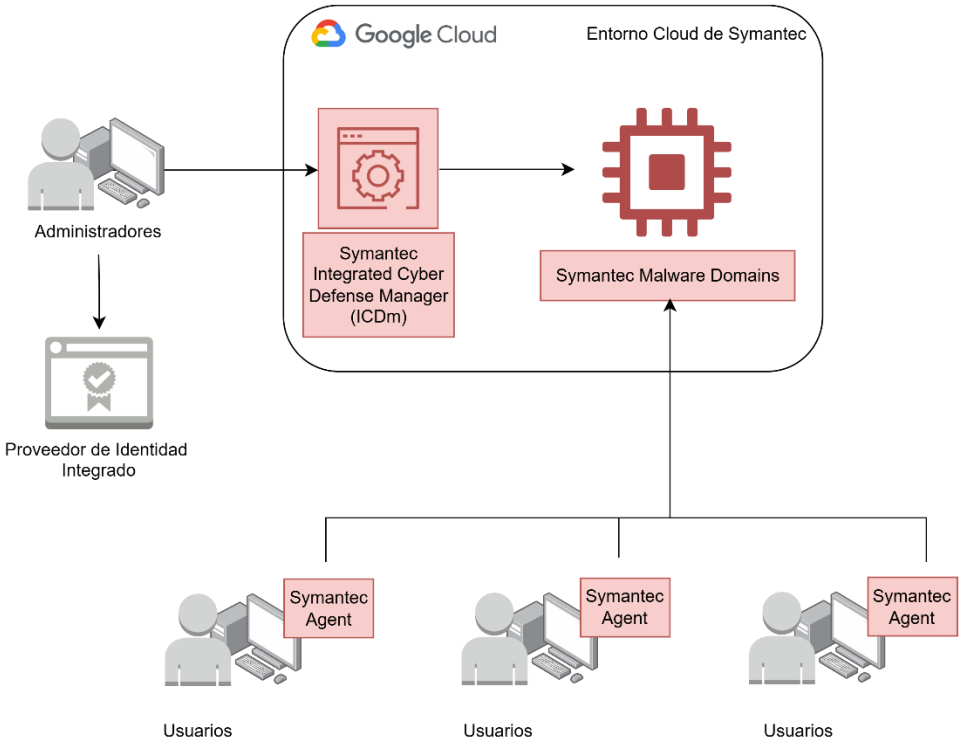

Figura 1: Componentes del entorno operacional

17. A continuación, se describe cada uno de los componentes en el entorno:

    a) Usuarios: Refieren a los usuarios monitorizados por el agente de Symantec, junto a sus equipos que actuarán como endpoint, el cual será analizado gracias a los agentes instalados en sus equipos. Los Sistemas Operativos que admite Symantec Endpoint son los siguientes:

        i. Windows. Windows 11 x64 será la opción recomendada al ser el SO cualificado.
        ii. Linux
        iii. MacOS
        iv. Android
        v. iOS

    b) Administradores: Personal autorizado para acceder a la consola de ICDm. Estos serán los usuarios encargados de la monitorización de los endpoints y, en general, de realizar una gestión centralizada de todo el despliegue. Para acceder a la consola de ICDm se recomienda utilizar un navegador web Microsoft Edge versión 136 o superior.

    c) Proveedor de Identidad Integrado: Este es el servicio responsable de la autenticación e identificación de los Administradores, ya que son los usuarios que se comunican

directamente con la interfaz de gestión. Este componente, que debe de ser gestionado de forma propia, se limita a devolver un token de sesión para los administradores. Este token será presentado ante ICDm para autenticar así a todos los usuarios. Mediante este despliegue, no habrá comunicación directa entre este IDP y la propia consola de gestión.

d) Entorno Cloud de Symantec: Con este componente se quiere referenciar el propio entorno sobre el que están desplegados los componentes cloud de Symantec Endpoint Security Complete. Para el caso de este servicio, los componentes cloud están desplegados sobre la Plataforma de Google Cloud.

5 FASE DE INSTALACIÓN

18. El despliegue cualificado de Symantec Endpoint Security Complete consta de los servicios Cloud de Symantec Integrated Cyber Defense Manager (ICDm) y los Symantec Malware Endpoints, además de los Symantec Agent desplegados en cada endpoint. El acceso a estos servicios cloud y al paquete de instalación de los agentes deberá de ser proporcionado por el fabricante según lo especificado en la sección *4.1 ENTREGA SEGURA DEL PRODUCTO* de este documento.
19. Tal y como se ha comentado en la sección anteriormente referenciada, una vez se haya solicitado la cuenta de acceso a la consola de gestión, ICDm, se deberá de descargar el paquete de instalación de los agentes. Dada su naturaleza, estos serán desplegados sobre los endpoints a monitorizar según sea necesario, de forma que se gestionen todos los equipos Windows necesarios, de acuerdo con el despliegue evaluado. En la guía oficial de Instalación de los Agentes Symantec [REF2] se podrá encontrar más información respecto a los agentes. Además de ello, se recomienda atender a la guía oficial de requisitos de red para la correcta instalación del producto [REF7].
20. Una vez instalados los agentes, se recomienda comprobar su versión. Para ello, se deberá de acceder al programa del agente y acceder a la sección *Ayuda -> Acerca de*.
21. Por otro lado, si se desea comprobar la versión del componente ICDm en el despliegue cloud, se deberá de acceder a esta misma consola en la sección *Estado del Sistema -> Soporte*.

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

22. Para el acceso a la consola de gestión, el servicio requiere de la identificación y autenticación de cada administrador. Según la configuración evaluada, y tal y como se ha comentado en las secciones anteriores de este documento, será necesario integrar un IDP.
23. De esta forma, las funciones de autenticación e identificación quedan delegadas en esta integración, y no se permitirá realizar ninguna función de administración hasta que este componente externo ofrezca un token de autenticación válido para el acceso a ICDm.
24. Para más información acerca de los IDP cualificados por el CPSTIC, se deberá de atender a la guía CCN STIC 105 [REF3].

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN REMOTA

25. El componente Symantec Integrated Cyber Defense Manager es el encargado de ofrecer de forma integral y centralizada la gestión de la plataforma cloud y de todos los agentes desplegados. Para ello, este componente ofrece una interfaz web accesible a través de un navegador web.
26. Mediante este navegador se establecerá una comunicación HTTPS hacia el entorno cloud donde está desplegada la consola, y una vez comprobado el token de identificación, se accederán a las funciones de administración de forma remota.
27. Se recomienda el uso de Microsoft Edge en su versión 136 o superior, ya que este ha sido el navegador utilizado para la evaluación de este servicio.

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

28. Para hacer una configuración correcta de los administradores y sus roles asociados se recomienda atender a las siguientes guías, atendiendo a los principios de separación de roles y funciones de seguridad establecidos en el ENS:
    a) Creación de una cuenta de usuario administrador: [REF4]
    b) Roles por defecto en ICDm: [REF5]
    c) Configuración de administradores y roles: [REF6]

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

29. Como ya se ha indicado a lo largo de este documento, los agentes Symantec están indicados para ser instalados en equipos Windows 11, de acuerdo con el entorno evaluado, de los cuales se recogerá información para que ésta sea analizada en busca de problemas de seguridad.
30. Para que los agentes establezcan una comunicación segura con los endpoints de análisis de malware se deberá de configurar el propio sistema operativo sobre el que se instala el agente. Para ello, se deberán de seguir los siguientes pasos:

a) Pulsar las teclas *Win+R* en el SO donde el agente se ha instalado.

b) Sobre el panel de búsqueda que aparece, se deberá de buscar el siguiente texto: *gpedit.msc*.

c) Esto accederá a configuraciones internas del SO. Para acceder a la configuración criptográfica del SO se deberá de acceder a la sección *Configuración de Ordenador > Plantillas de Administración > Red > Ajustes de Configuración SSL.*

d) En el lado derecho de la ventana aparecerán dos secciones, primeramente, se deberá de acceder la sección de *Orden de Sitios de Cifrado SSL*, se deberá de habilitar y, por último, en la sección de *Sitios de Cifrado* se deberá de indicar el siguiente texto:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_CCM,
TLS_ECDHE_ECDSA_WITH_AES_128_CCM.

e) En la sección *Orden de Curvas ECC* esta se deberá de habilitar, y se deberán de indicar los siguientes parámetros: "*NistP256,NistP384,NistP521*".

f) Finalmente se deberán de guardar los cambios y, para que estos se apliquen, se deberá de acceder a una línea de comandos y se deberá ejecutar el siguiente comando: *gpupdate /force*.

31. Gracias a esta configuración la comunicación HTTP sobre TLS establecida entre los Symantec Agent y los Endpoints de Análisis de Malware quedará securizada.

32. Para poder gestionar esta configuración de una forma centralizada a un gran número de endpoints, se recomienda desplegar esta política mediante GPO de dominio, en aquellos sistemas que lo soporten.

6.4 GESTIÓN DE CERTIFICADOS

33. Los certificados utilizados en las comunicaciones establecidas entre los componentes de Symantec Endpoint Security Complete son gestionados por parte del equipo técnico de Broadcom, por lo que los administradores no necesitan realizar ninguna configuración.

34. Este equipo se encargará de realizar un tratamiento adecuado de estos certificados, manteniendo actualizados y en validez todos los certificados ofrecidos en los endpoints del entorno cloud de Symantec Endpoint Security Complete.

6.5 SERVIDORES DE AUTENTICACIÓN

35. Tal y como se ha comentado anteriormente en este documento, el producto delega sus funciones de identificación y autenticación de usuarios en un IDP externo.

36. Para una configuración segura de este servicio, se recomienda establecer los siguientes parámetros para las cuentas de los administradores:

a) La contraseña debe configurarse con una longitud mínima o igual a 12 caracteres.

b) La contraseña deberá de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"].

c) Se deben implementar mecanismos que impidan ataques de autenticación de fuerza bruta.

d) Se deberá de implementar un cierre de sesión de los usuarios después de un máximo de 30 minutos de inactividad del usuario, como valor recomendado.

e) En el caso de que se ofrezcan contraseñas por defecto junto a las credenciales de los administradores, se deberá de obligar al cambio de estas tras su primer uso, utilizando la política de contraseñas mencionadas anteriormente.

f) Se establecerá una política de caducidad de las contraseñas, siendo necesaria la renovación periódica.

37. Para más información acerca de los IDP cualificados por el CPSTIC, se deberá de atender a la guía CCN STIC 105 [REF3].

6.6 ACTUALIZACIONES

38. En el caso de este servicio tan solo los Agentes podrán ser actualizados por parte de los administradores. El resto de los componentes tienen naturaleza cloud, por lo que el mantenimiento de estos componentes se realizará por parte del fabricante.

39. Para poder realizar el proceso de actualización de los agentes correctamente y de una forma segura se recomienda atender a la guía oficial de Actualización de los Symantec Agent [REF7].

6.7 AUDITORÍA

6.7.1 REGISTRO DE EVENTOS

40. La funcionalidad principal de Symantec Endpoint Security Complete es la de generar una alerta en el momento en que se detecte un comportamiento anómalo en alguno de los endpoints monitorizados.

41. Principalmente, se destacan los siguientes registros generados:

a) Virus o Malware detectado en alguno de los endpoints monitorizado.

b) Archivo potencialmente malicioso, almacenando toda la información posible sobre este.

c) Acciones tomadas sobre Virus o Malware detectado: bloqueo, cuarentena o borrado.

42. Todos estos eventos generados en el producto contienen, al menos, la siguiente información de forma que puedan identificarse correctamente:

a) Fecha y hora del evento.

b) Tipo de evento identificado.

c) Resultado del evento.

d) Usuario que produce el evento (si aplica).

43. Será gracias a estos registros con los que los administradores podrán comprobar la trazabilidad de un comportamiento malicioso en alguno de los endpoints monitorizados, además de controlar qué acciones se han tomado para cada uno de ellos.

44. Todos estos eventos son generados gracias a que Symantec Endpoint Security Complete ofrece un sistema de configuración de reglas, las cuales generarán una alerta en el momento en que se cumpla alguna condición específica. Para entender correctamente el funcionamiento de estas reglas, se recomienda seguir la guía oficial de Uso de Reglas de Alerta [REF8].

6.7.2 ALMACENAMIENTO REMOTO

45. Toda la información referente a los registros generados previamente mencionados es almacenada en el entorno Cloud sobre el que Symantec Endpoint Security Complete es desplegado. Este primeramente recibirá la información recogida por los agentes desplegados, y generará los registros correspondientes según el análisis realizado y las reglas de alerta configuradas.
46. Estos registros de auditoría serán almacenados internamente en el entorno cloud de Google, y serán mostrados a través del Symantec Integrated Cyber Defense Manager, solo accesible por los administradores autorizados.
47. Por otro lado, Symantec ofrece la posibilidad de exportar los registros a un servidor Syslog externo, aunque no ha sido incluido en la evaluación cualificada. Para realizar esta configuración se recomienda atender a la guía oficial de exportación a un servidor externo [REF14].
48. Finalmente, se recomienda el almacenamiento de logs un tiempo de retención mínimo de 2 años.

6.8 POLÍTICAS ANTI-MALWARE

49. Para el correcto funcionamiento de Symantec Endpoint Security Complete se deben de configurar las políticas Anti-Malware, de acuerdo con la finalidad de estas en la organización.
50. Para hacer un uso correcto de estas políticas se recomienda atender a la guía oficial de Uso de Políticas y Grupos de Políticas [REF9]. En esta guía se especifica a detalle cómo hacer uso de las políticas y las plantillas y grupos de estas. De esta forma se podrán adaptar a las necesidades de detección y respuesta ante un malware detectado.
51. Por otro lado, también se recomienda atender a la guía oficial de Gestión de las Políticas [REF10]. Esta se trata de una guía más detallada sobre los diferentes tipos de políticas y cómo hacer uso de esta. Dentro de esta, es recomendable acceder a la sección “Configuración de la Política Antimalware” [REF11] y completar la información de esta con la guía oficial de Configuraciones Avanzadas de la Política Antimalware [REF12].

7 REFERENCIAS

REF1 Guía de Suscripciones y Licencias para Symantec Endpoint Security: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Subscriptions.html

REF2 Guía de Gestión para los Agentes Symantec: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Installing-the-Symantec-Agent-and-enrolling-devices.html

REF3 Guía CCN STIC 105, Catálogo de Productos y Servicios STIC: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

REF4 Guía de creación de una cuenta de Administrador: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Administrators,-Passwords,-and-Authentication/configuring-administrators-and-roles-v120087753-d4161e849/creating-an-administrator-account-v120922956-d4161e874.html

REF5 Guía de roles en ICDm: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Administrators,-Passwords,-and-Authentication/configuring-administrators-and-roles-v120087753-d4161e849/default-administrator-roles-in-the-cloud-console-v121515173-d4161e987.html

REF6 Guía de configuración de administradores y roles: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Administrators,-Passwords,-and-Authentication/configuring-administrators-and-roles-v120087753-d4161e849.html

REF7 Guía de Requisitos de Red para Symantec Endpoint Security: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Getting-Started/urls-to-whitelist-for-v129099891-d4155e9710.html

REF8 Guía de Uso de Reglas de Alerta EDR/EPP: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Alerts-and-Events/alerts-overview-v119868301-d4161e1703/using-alert-rules-v120087756-d4161e1763.html

REF9 Guía de Uso de Políticas y Grupos de Políticas: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Policies-and-Policy-Groups.html

REF10 Guía de Gestión de Políticas y sus Configuraciones: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Settings.html

REF11 Guía de Configuración de Políticas Antimalware: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Protection/antimalware-policy-advanced-settings-v128420816-d4155e13131/antimalware-policy-settings-v127972728-d4155e12968.html

REF12 Guía de Configuración Avanzada de la Política Antimalware: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Protection/antimalware-policy-advanced-settings-v128420816-d4155e13131.html

REF13 Guía de Buenas Prácticas para Symantec Endpoint Security Complete: https://knowledge.broadcom.com/external/article?legacyId=tech181685#mcetoc_1ff84e6opb

REF14 Guía de exportación de registros de auditoría a un servidor Syslog externo: https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Monitoring-Reporting-and-Enforcing-Compliance/viewing-logs-v7522439-d37e464/exporting-data-to-a-syslog-server-v8442743-d15e1107.html

REF15 Portal de Soporte de Broadcom: https://support.broadcom.com/

8 ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos STIC
EDR	*Endpoint Detection and Response*, Detección y Respuesta en el Endpoint
ENS	Esquema Nacional de Seguridad
EPP	*Endpoint Protection Platform*, Plataforma de Protección del Endpoint
GPO	*Group Policy Object*, Objeto de Directiva de Grupo
HTTP	*Hypertext Transfer Protocol*, Protocolo de Transferencia de Hipertexto
HTTPS	HTTP sobre TLS
ICDm	*Symantec Integrated Cyber Defense Manager*, Gestor Integrado de Symantec para CiberDefensa
IDP	*Identity Provider*, Proveedor de Identidades.
SO	Sistema Operativo
SSL	*Secure Sockets Layer*, Capa de Sockets Seguros
TLS	*Transport Layer Security*, Seguridad de la Capa de Transporte