Guía de Seguridad de las TIC
CCN-STIC 1003

Procedimiento de Empleo Seguro
Sophos XDR



Noviembre 2026

Edita:





CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
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 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 9
6 FASE DE CONFIGURACIÓN 13
6.1 MODO DE OPERACIÓN SEGURO 13
6.1.1 CONFIGURACIÓN ADICIONAL DE PROTECCIÓN 13
6.1.2 CONFIGURACIÓN DE CONTROL DE PERIFÉRICOS 14
6.1.3 CONFIGURACIÓN DE CONTROL DE NAVEGACIÓN 14
6.1.4 CONFIGURACIÓN DE CONTROL DE FUGA DE DATOS 15
6.1.5 CONTROL DE FIREWALL DE SISTEMA OPERATIVO 15
6.2 AUTENTICACIÓN 15
6.3 ADMINISTRACIÓN DEL PRODUCTO 16
6.3.1 CONFIGURACIÓN DE ADMINISTRADORES 16
6.3.2 GESTIÓN DE USUARIOS 17
6.4 SERVIDORES DE AUTENTICACIÓN 18
6.5 ACTUALIZACIONES 19
6.6 GESTIÓN DE CERTIFICADOS 19
6.7 AUTO CHEQUEOS 19
6.8 AUDITORÍA 20
6.8.1 REGISTRO DE EVENTOS 20
6.8.2 ALMACENAMIENTO LOCAL 21
6.8.3 ALMACENAMIENTO REMOTO 22
7 REFERENCIAS 23
8 ABREVIATURAS 25

ÍNDICE DE FIGURAS

Ilustración 4-1 Requisitos Windows 7
Ilustración 4-2 Requisitos Windows Server 7
Ilustración 4-3 Requisitos MacOS 7
Ilustración 4-4 Requisitos Linux 8
Ilustración 5-1 Certificado de Sophos Central 9
Ilustración 5-2 Instaladores 10
Ilustración 5-3 Descargas 10
Ilustración 5-4 Descargas de Servidor 11
Ilustración 5-5 Certificado del instalador 11
Ilustración 6-1 Indicación que la política es la recomendada 13
Ilustración 6-2 Análisis periódico de los equipos 13
Ilustración 6-3 Política de Control de Periféricos 14
Ilustración 6-4 Control de navegación 14
Ilustración 6-5 Políticas de Firewall 15
Ilustración 6-6 Añadir Rol 17
Ilustración 6-7 Eventos 20
Ilustración 6-8 Auditoría 20
Ilustración 6-9 Detecciones EDR/XDR 21
Ilustración 6-10 Ejemplo búsqueda con IA 21

1 INTRODUCCIÓN

Sophos XDR es una herramienta de antivirus y EDR/XDR (Endpoint Detection and Response) que presenta las siguientes funcionalidades:

a) Protección antimalware basada en:
   i. Firmas.
   ii. Deep Learning (inteligencia artificial).
   iii. Consultas a Sophos Labs en tiempo real.
   iv. AntiExploit.
   v. Control de comportamiento.
   vi. Detección de técnicas post-explotación.

b) EDR/XDR.

c) Control de navegación web.

d) Control de dispositivos.

e) Control de aplicaciones.

f) Gestión del firewall de Windows.

g) Prevención de fuga de datos.

h) Control de actualizaciones.

i) Bloqueo de servidores.

j) Detección de cambio de ficheros.

Las funcionalidades son gestionadas desde una consola en nube, Sophos Central, la cual además sirve para la gestión del resto del portfolio de Sophos, como seguridad de red (Sophos XG Firewall), seguridad de correo (Sophos Central Email), cifrado de equipos (Sophos Centran Device Encryption), gestión y protección de móviles (Sophos Central Mobile), educación de usuarios (Sophos PhishThreat), WorkSpace Protection (ZTNA, Protected Browser y DNS Protection) y redes inalámbricas (Sophos Cloud Wireless).

La solución puede ser empleada en equipos endpoint y servidor Windows, Windows Server, MacOS y Linux.

2 OBJETO Y ALCANCE

El propósito del presente documento es detallar las configuraciones de seguridad del producto Sophos XDR versión 2025.1, para que su protección y funcionamiento se realice de acuerdo a unas garantías mínimas de seguridad.

Sophos XDR es un producto software cuya instalación se realiza en los dispositivos que desea proteger, mediante el uso de agentes.

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 [REF2].

3 ORGANIZACIÓN DEL DOCUMENTO

Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

a) **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase previa al despliegue e instalación del producto.

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

c) **Apartado 0**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) **Apartado 7**. Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

e) **Apartado 8**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

El producto se recibe y gestiona desde la plataforma Sophos Central (REF3).

- En caso de no disponer ya de un usuario, se podrá crear uno mediante el uso de una dirección corporativa de correo electrónico. A través del procedimiento de creación de cuenta, se recibirán unos códigos para verificar la pertenencia de dicha cuenta de correo y se procederá a crear una contraseña de alta complejidad. El proceso terminará, obligatoriamente, con la creación de un OTP (Sistema de Password de un solo uso) o bien una PassKey.
- Se deberá también recibir, por parte del comercializador de Sophos, un documento PDF con las claves de registro, las cuales serán introducidas en la consola de Sophos para licencias el producto y permitir su uso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Ninguno de los componentes de Sophos XDR requiere de instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

4.3 REGISTRO Y LICENCIAS

En la siguiente página oficial de Sophos se detalla el procedimiento de licenciamiento: REF4.

4.4 CONSIDERACIONES PREVIAS

Todas las comunicaciones de los endpoints contra central.sophos.com se establecen a través del puerto 443. Dicha comunicación no puede ser interceptada mediante inspección HTTPS o similar, ya que, si el certificado que llega al endpoint no es el original de Sophos, la comunicación no se establece. Esto es así para evitar ataques *Man in the Middle*, por lo que, si existe ese tipo de análisis web, se deben de realizar las exclusiones correspondientes a las URL que se indican en los siguientes puntos.

Como se comentará en el Entorno de instalación seguro, es posible tener equipos que no dispongan de conexión a Internet gracias al uso de las Cachés de Actualizaciones y los Repetidores de Mensajes. Se necesitará que al menos estos sí dispongan de acceso a los servicios de Sophos por los puertos TCP 80 y TCP 443, desde la red de la organización a los recursos listados a continuación:

a) *.sophos.com
b) *.sophosupd.com
c) *.sophosupd.net
d) *.sophosxl.net
e) ocsp2.globalsign.com
f) crl.globalsign.com

Si no fuese posible realizar excepciones de los firewalls/proxies con "*", la lista completa de dominios puede encontrarse en: REF5

Respecto a las características que deben cumplir los equipos: REF6

Windows Endpoints:

Fully supported platforms	Windows 10 64-bit Windows 11				
Legacy platforms	Windows 7 (requires Extended Support license) Windows 8.1 (requires Extended Support license) Windows 10 32-bit				
Product	**Sophos Endpoint**	**Sophos XDR**		**Sophos MDR**	
		Minimum	**Recommended**	**Minimum**	**Recommended**
Free disk space	4 GB	8 GB	8 GB	8 GB	8 GB
RAM	4 GB	4 GB	16 GB	4 GB	16 GB
Cores	2	2	4	2	4
Disk type	SSD is strongly recommended for a boot drive				

Ilustración 4-1 Requisitos Windows

Windows Server:

Fully supported Server platforms	Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2025				
Legacy Server platforms	Windows Server 2008R2 (requires Extended Support license) Windows Server 2012/Server 2012 R2 (requires Extended Support license)				
Product	**Sophos Endpoint - Server**	**Sophos XDR - Server**		**Sophos MDR - Server**	
		Minimum	**Recommended**	**Minimum**	**Recommended**
Free disk space	8 GB	10 GB	10 GB	10 GB	10 GB
RAM	8 GB	8 GB	16 GB	8 GB	16 GB
Cores	2	2	4	2	4
Disk type	SSD is strongly recommended for a boot drive				

Ilustración 4-2 Requisitos Windows Server

MacOS:

Supported platforms	**Endpoint Protection**	**Intercept X Advanced (MDR Included)**
macOS 13, 14, 15, 26 Intel-based Macs (64-bit) and Apple Silicon M Series (ARM)	Disk space: 2 GB free RAM: 2 GB	Disk space: 2 GB free RAM: 2 GB

Ilustración 4-3 Requisitos MacOS

Linux:



Ilustración 4-4 Requisitos Linux

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

No se requieren componentes extra en el entorno de operación. Si bien es cierto que Sophos XDR puede integrarse con EntraID, Google Directory o Directorio Activo, así como también con elementos terceros (de ahí la X -eXtended- de XDR), no es mandatorio.

5 FASE DE INSTALACIÓN

La instalación del producto se realiza a través de la consola de gestión de Sophos Central. El acceso a la misma se realiza a través del portal REF7, accesible mediante navegador web utilizando HTTPS y cuyo certificado (en el momento de escribir esta guía) es:

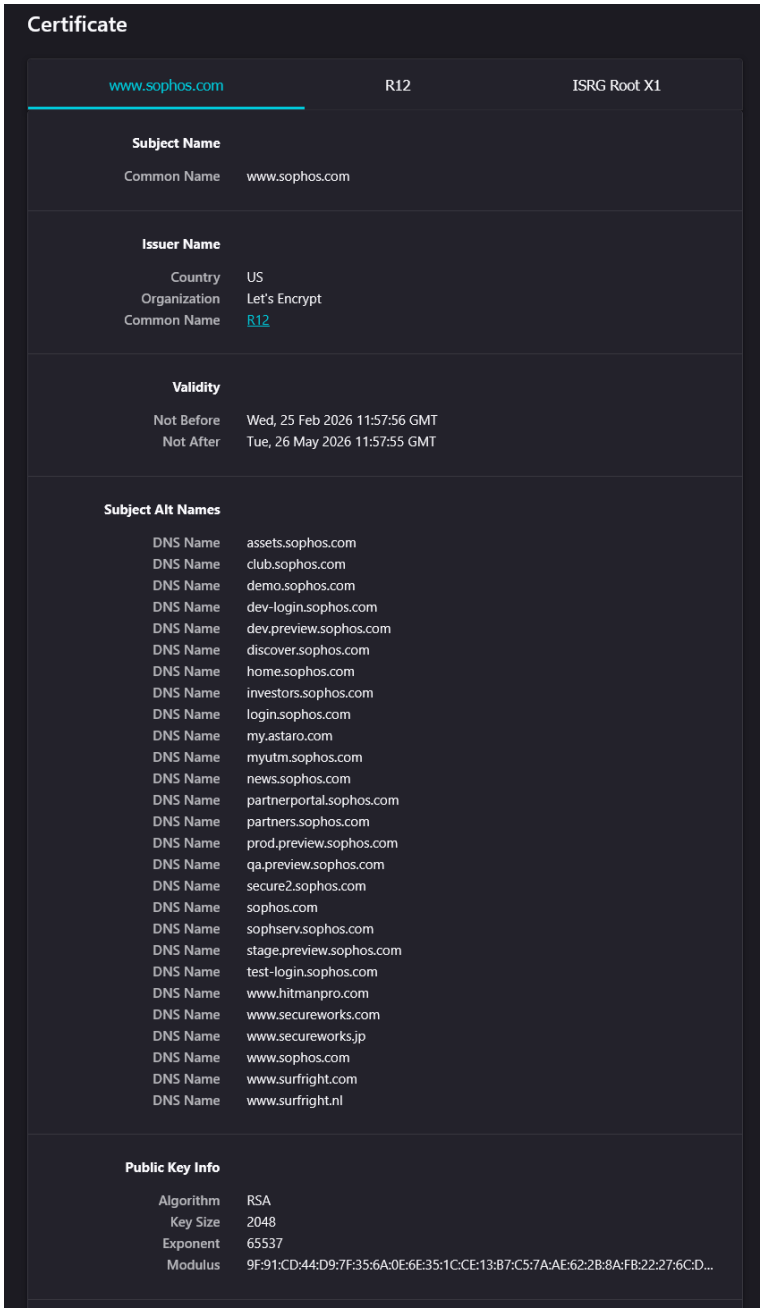


Ilustración 5-1 Certificado de Sophos Central

El acceso a la consola se realiza con un usuario suministrado por el fabricante a través de correo electrónico. La contraseña es generada por el propio usuario, con la supervisión de la consola de Sophos que exige contraseñas de alta complejidad.

Este primer usuario generado tendrá el rol de “superadministrador” y será el que genere sucesivos usuarios. De igual forma, el sistema envía un correo de confirmación, para que sea el propio usuario el que genere su contraseña.

La descarga del instalador de los agentes utilizados para proteger los dispositivos finales se realiza desde el menú Mi Entorno → Instaladores:

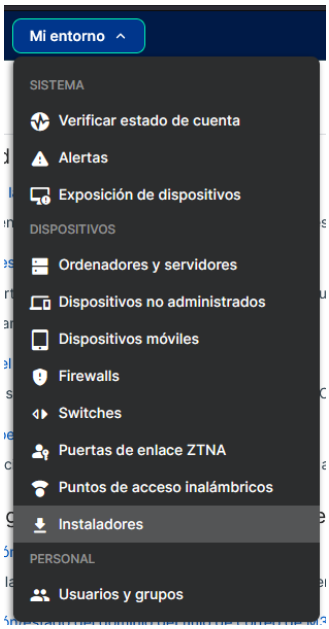


Ilustración 5-2 Instaladores

Las opciones Descargar instalador de Windows Completo proporcionan un instalador para dispositivos Windows y macOS según la opción seleccionada, con todos los productos para endpoint incluidos en la licencia obtenida por la organización.

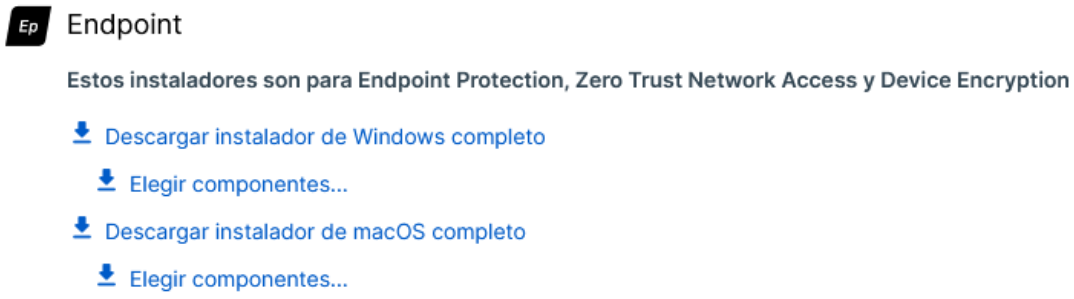


Ilustración 5-3 Descargas

La opción de “Elegir componentes...”, bajo cada una de las opciones recién mencionadas, permite seleccionar un instalador solo con los productos deseados, para cada tipo de dispositivo.

Para equipos Windows Server y Linux, se deberá hacer uso de la opción de descarga para Servidores:

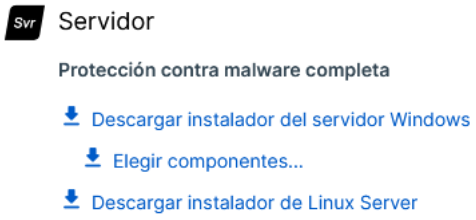


Ilustración 5-4 Descargas de Servidor

Se puede verificar la autenticidad del fichero *.EXE del agente descargado comprobando que este se encuentra firmado utilizando el siguiente certificado:

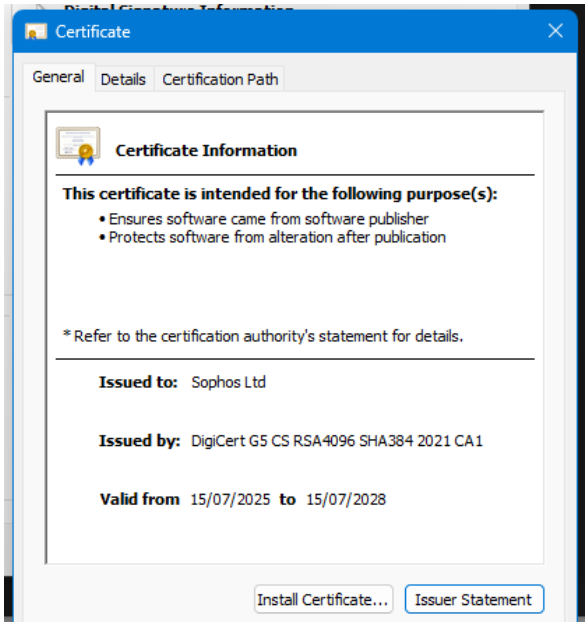


Ilustración 5-5 Certificado del instalador

En caso de que no exista conexión directa a internet o nos encontremos ante redes aisladas o muy restringidas, es posible seleccionar aquellos dispositivos que queramos configurar como:

a) Caché de Actualización: usará el puerto TCP 8191 para actuar como servidor de actualizaciones de firmas y motores para los dispositivos en la red de la organización.

b) Repetidor de Mensajes: usará el puerto TCP 8190 para hacer de proxy de mensajería entre los equipos y la nube de Sophos Central.

El despliegue de los elementos anteriores permite centralizar las actualizaciones y las comunicaciones en aquellas ubicaciones (típicamente datacenters) que se desee, o incluso definir estas parejas por cada delegación, centralizando así tráficos y ahorrando anchos de banda.

Para configurar una Caché de Actualización o un Repetidor de Mensajes, se accede a central.sophos.com:

a) Ir a Configuración General > Gestionar cachés de actualización y repetidores de mensajes.

b) En el filtro sobre la tabla, seleccionar 'Servidores con capacidad de caché' u 'Ordenadores con capacidad de caché' para ver qué equipos (servidores u ordenadores) tienen la capacidad de actuar como alguno de estos componentes. Dichos servidores serán los que previamente tengan instalado el agente de endpoint de Sophos. Además, necesitan cumplir los siguientes prerrequisitos técnicos: REF8

c) Seleccionar el equipo o equipos que se desea configurar como Cache o Repetidor.

d) Hacer clic en 'Configurar caché/repetidor'.

Una vez seleccionados los servidores, el producto configura de forma automática los dispositivos en la red de la organización para utilizar el Caché de Actualizaciones o Repetidor de Mensajes creado. También pueden asignarse los dispositivos a un Cache/Repetidor de forma manual:

a) Ir a Configuración General > Gestionar cachés de actualización y repetidores de mensajes.

b) Para el equipo elegido, seleccionar el enlace que muestra el número de dispositivos utilizando dicho Cache/Repetidor.

c) Hacer clic en 'Asignación Manual'.

d) Seleccionar los dispositivos deseados.

e) Hacer clic en 'Salvar'.

Cada instalador está personalizado para cada cliente. Por lo tanto, una vez descargado desde la consola de central, se procederá a la ejecución del agente en el dispositivo endpoint en cuestión.

En caso de necesitar una instalación personalizada, es posible añadir ciertos modificadores detallados en: REF9

Si se desea realizar un despliegue en multitud de dispositivos de forma simultánea, Sophos proporciona diversos métodos para ello, según las plataformas disponibles indicadas en el siguiente enlace: REF10

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Una vez que se ha desplegado el software, el equipo queda configurado con las opciones por defecto, pero con ciertas protecciones deshabilitadas (como el control de aplicaciones, el control de dispositivos, el control de navegación y DLP). Se deben crear políticas para la activación y gestión de las protecciones. Detalles de cómo configurar las políticas adicionales de protección en REF11

Estas políticas se configuran en la plataforma Sophos Central, desde la sección 'Políticas', haciendo clic en 'Añadir Política' y seleccionando aquella que quiera configurarse.

Se debe realizar la siguiente configuración para la política de Protección Contra Amenazas: Dejar la política tal y como viene por defecto, pues es la configuración recomendada por Sophos.



Ilustración 6-1 Indicación que la política es la recomendada

Adicionalmente, se puede añadir:

6.1.1 CONFIGURACIÓN ADICIONAL DE PROTECCIÓN

En la política de prevención de amenazas, se recomienda activar, en caso de que no estuviesen ya activas, las siguientes funcionalidades:

a) Impedir el tráfico de red malicioso con la inspección de paquetes (IPS): para disponer de IPS para detectar intentos de ataque a través de sus paquetes de red.

b) Activar la protección en modo seguro: para que incluso en "safe mode", la protección de Sophos siga estando. IMPORTANTE: si por cualquier motivo se desea desinstalar la protección sin disponer de la clave de anti-manipulación, no será posible en este modo.

c) Bloquear conexiones de navegador QUIC: evita el uso de dicho sistema de navegación para tratar de eludir los controles de navegación

d) Descifrado SSL/TLS de sitios web HTTPS: El endpoint descifrará el tráfico SSL evitando hacerlo a nivel de firewall, permitiendo entender qué está descargando el usuario en tiempo real.

e) Aislamiento de dispositivo: en caso de ataque, el endpoint procederá a auto-bloquear sus conexiones, excepto aquellas relacionadas con Sophos.

f) Escaneo programado: permitirá establecer una agenda de análisis del equipo:

a.

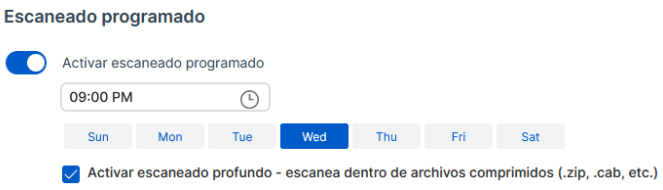


Ilustración 6-2 Análisis periódico de los equipos

6.1.2 CONFIGURACIÓN DE CONTROL DE PERIFÉRICOS

La política de control de periféricos, se recomienda configurar con al menos la supervisión:

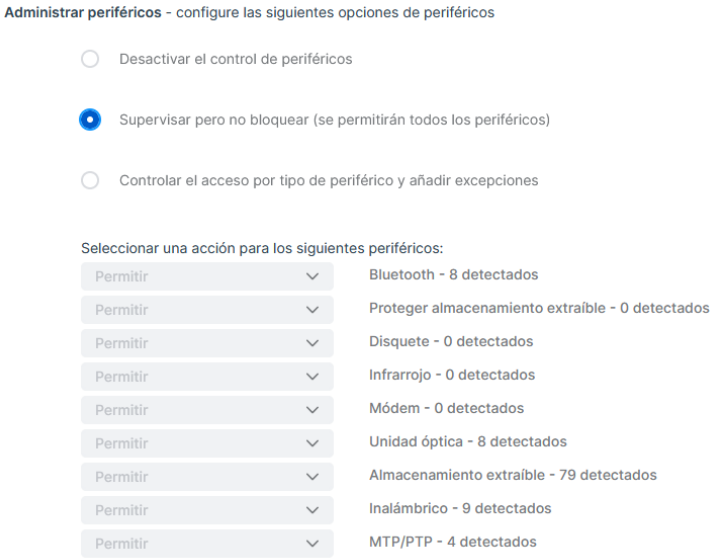


Ilustración 6-3 Política de Control de Periféricos

El modo 'Controlar el acceso por tipo de periférico y añadir excepciones' permite la creación de políticas de control de acceso para los dispositivos.

6.1.3 CONFIGURACIÓN DE CONTROL DE NAVEGACIÓN

Se recomienda realizar la siguiente configuración para la política de control web (navegación). Por defecto, el control de navegación de Sophos bloquea descargas potencialmente maliciosas (*.exe) así como el acceso a páginas de proxies y traductores (usados muchas veces como proxies). Será necesario revisar la política para ajustarla como mejor se adecue a las necesidades de la organización:

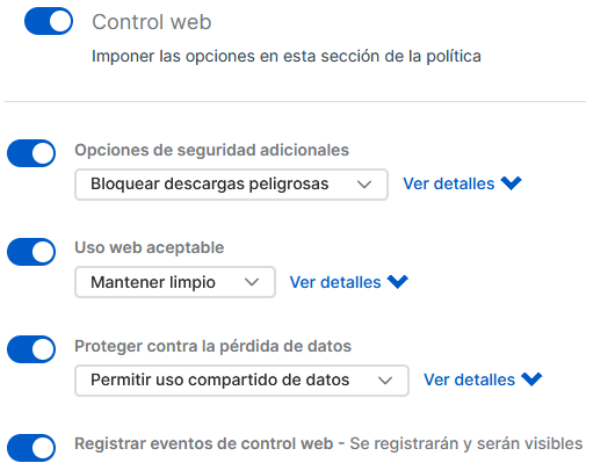


Ilustración 6-4 Control de navegación

6.1.4 CONFIGURACIÓN DE CONTROL DE FUGA DE DATOS

El DLP o control de fuga de datos permite definir qué ficheros deben salir de la organización. Esta debe definir qué datos se consideran sensibles y no deben salir al exterior de la red corporativa, bien por contenido o por tipo de fichero. Como "best practice" podría ser recomendable configurar una política de control desde el correo electrónico y el navegador de los ficheros más habituales, como son las hojas de cálculo, los documentos de texto, las presentaciones, etc. La política podría permita la salida de información pero implementar una monitorización exhaustiva de lo que sale del perímetro de la organización. La política define si se permite la transferencia, se bloquea o se deja la decisión al usuario en función de:

a) El contenido. Se pueden definir expresiones regulares (regex) para mirar dentro del fichero y decidir si se permite o no la transferencia.

b) El tipo de fichero. Se define si se permite o no la transferencia en función de si el fichero es una imagen, un video, un contenedor, presentaciones, etc. No se analiza el contenido del fichero.

c) El destino. Se establecen políticas en función de los posibles destinos: correo electrónico, navegador, mensajería, voz IP, almacenamiento, etc.

6.1.5 CONTROL DE FIREWALL DE SISTEMA OPERATIVO

Sophos puede controlar el firewall de Windows. Se puede habilitar, bloquear todo el tráfico o bloquear todo con las exclusiones que lleguen por GPO desde el controlador de dominio. Se recomienda bloquear todo tráfico entrante de redes fuera de la corporativa:

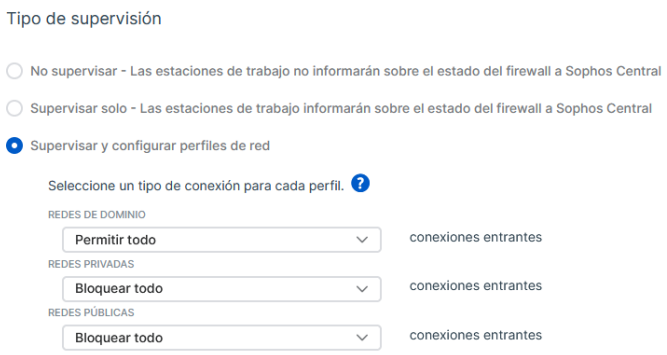


Ilustración 6-5 Políticas de Firewall

6.2 AUTENTICACIÓN

La autenticación en la plataforma de gestión Sophos Central se realiza mediante usuario/contraseña con MFA (OTP) o bien vía Passkey. Se pueden crear y gestionar usuarios, o se puede integrar con un servidor de directorio (AD o EntraID).

La complejidad de las contraseñas de usuario no es configurable. Por defecto, los parámetros de robustez de contraseñas que permite el producto son los siguientes:

a) Longitud mínima de 8 caracteres (valor recomendado mínimo: 9 caracteres).

b) Inclusión de mayúsculas y minúsculas.

c) Inclusión de caracteres especiales.

d) No utilización de una contraseña que sea la misma que la anterior.

Pero siempre se recomienda seguir detalladamente la Guia CCN-STIC-807 donde se detalla cómo debe ser una contraseña considerada segura.

Existen otros parámetros de robustez, de implementación procedimental, que deben ser tenidos en cuenta por los administradores:

a) No usar palabras que puedan encontrarse en diccionarios

b) No utilizar la repetición de, al menos, las 5 últimas contraseñas utilizadas.

c) El valor recomendado para la vigencia y expiración de contraseñas no debe superar los 6 meses.

d) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

Aún con todo lo anterior, Sophos exige un método adicional de autenticación que podrá ser:

a) Código temporal de un solo uso (OTP) el cual puede ser obtenido mediante una aplicación tipo "authenticator": Durante la creación del usuario (o bien al recibir el email de invitación a ser usuario de Central), aparecerá un código QR, que deberá escanearse con la aplicación para vincular el dispositivo, posteriormente se deberá introducir el código mostrado para finalizar la vinculación. Las posibles aplicaciones que pueden utilizarse para este método son Google Authenticator, 2FAS, Microsoft Authenticator, etc…

b) Passkey: En caso de seleccionar este método al crear la cuenta (o a posteriori en las opciones de autenticación), será necesario contar un sistema de gestión de passwords en el equipo, el cual guardará el passkey para su uso cuando la autenticación de Sophos le sea requerida.

6.3 ADMINISTRACIÓN DEL PRODUCTO

La gestión del producto se realiza de forma remota, vía navegador web HTTPS a través del portal https://central.sophos.com.

6.3.1 CONFIGURACIÓN DE ADMINISTRADORES

El producto permite el RBAC (Role Based Administration Control) y, por defecto, tiene varios perfiles de administrador creados, los cuales no pueden modificarse ni eliminarse:

a) SuperAdmin: Permite realizar cualquier operación en la consola. Es el único rol con la capacidad gestionar y asignar roles.

b) Admin: Similar al rol SuperAdmin. Puede realizar cualquier operación, salvo crear/modificar roles y crear nuevos usuarios.

c) HelpDesk: Permite acceso en modo Solo Lectura a todos los ajustes en Sophos Central. Pueden realizar también las siguientes tareas:

   i. Ver logs y reportes.

   ii. Recibir y solucionar alertas.

iii. Actualizar el agente de un dispositivo.

iv. Escanear dispositivos.

d) ReadOnly: Similar al rol HelpDesk. Permite el acceso en modo Solo Lectura a todos los ajustes en Sophos Central. Pueden también realizar las siguientes tareas:

i. Ver logs y reportes.

ii. Recibir alertas

En cualquier caso, es posible añadir nuevos roles con los permisos que se deseen a partir de los roles ya existentes. Para esto:

Ir a Configuración > Administración de Roles > Añadir Rol.

Seleccionar el 'Rol Base' a partir del cual se creará el nuevo rol.

Asignar un nombre y los permisos deseados al rol y hacer clic en 'Save'.

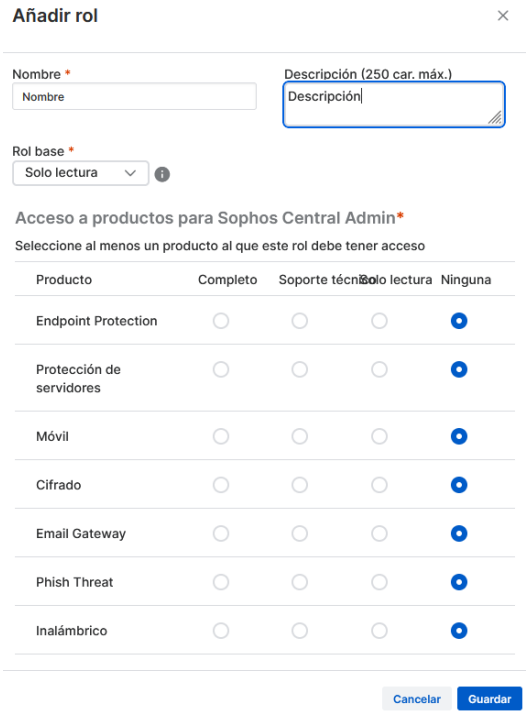


Ilustración 6-6 Añadir Rol

La consola permite la multiconcurrencia de administradores, por lo que es posible que un usuario con rol Helpdesk pueda estar trabajando mientras un usuario con rol Admin realiza cambios y otro con rol ReadOnly comprueba los logs. Esta característica no es configurable.

6.3.2 GESTIÓN DE USUARIOS

El producto permite la creación manual de usuarios:

Ir Mi Entorno > Usuarios y Grupos > Añadir.

En el diálogo que aparecerá, introducir el nombre, rol y dirección de email.

Hacer clic en Guardar.

Adicionalmente, al ejecutar el instalador para proteger los dispositivos el producto crea automáticamente los usuarios vistos en cada dispositivo. Dicho usuario solo tendrá validez para poder asignar políticas y tendrá asignado el rol de "user". Se recomienda sincronizar un servicio de Directorio, pues si el producto crea por sí mismo los usuarios, éstos serán:

NOMBRE_MAQUINA\usuario

Lo que puede dar lugar a que un mismo usuario sea reconocido no como uno, sino como múltiples, ya que el 'NOMBRE_MAQUINA' será distinto para cada equipo. Si por el contrario tenemos un servicio de directorio, al saber que dichos usuarios pertenecen al mismo dominio, éstos no se crearán con el Nombre de Máquina como parte de su nombre, sino con el usuario a "secas", pudiendo ser el mismo en múltiples equipos y, por tanto, contabilizándose como uno.

Por defecto, todas las sesiones de cualquier rol de usuario caducan tras 30 minutos de inactividad. Esta opción no es configurable.

6.4 SERVIDORES DE AUTENTICACIÓN

Es posible sincronizar un Servidor de Directorio para obtener el listado de usuarios y grupos. Este servidor de Directorio puede ser:

a) EntraID

b) Directorio Activo Local

c) Google Directory

Para la sincronización de estos servicios, desde Configuración Global → Servicio de Directorio → Añadir Servicio de Directorio. Cabe destacar que la sincronización es unidireccional, es decir, en caso de crear usuarios/grupo en la consola Central, éstos no serán replicados en ninguno de los servicios de directorio. Por otro lado, la sincronización con los servicios de directorio se realiza cada x horas, según su configuración.

Directorio Activo: REF12

IMPORTANTE: el AD local requiere de un pequeño software que se desplegará en cualquier equipo (no obligatoriamente en los DCs) pero que tenga acceso a los DCs para realizar la lectura.

EntraID: REF13

Google Directory: REF14

También es posible federar la autenticación para logarse tanto administradores (y roles secundarios) como usuarios en el portal de autoservicio (no usado por XDR, pero sí útil para Central Email -cuarentena, buzón de emergencia y gestión permitidos/boqueados-, Mobile -enrolamiento y gestión de dispositivos-, Workspace Protection -autenticación de Navegador Protegido). Para ello, Sophos permite la federación de varios tipos:

EntraID: REF15

OpenID: REF16

AD FS: REF17

Así como la integración de fabricantes terceros:

- Microsoft

- Okta
- Google Workspace
- OneLogin
- Ping Identity

6.5 ACTUALIZACIONES

El producto recibe diversos tipos de actualizaciones:

a) Firmas: depende del día y la actividad, pudiendo llegar a 20 al día, con tamaño promedio de 20KB.

b) Motores:

i. AntiExploit y Deep Learning: Cada 6 u 8 semanas recibe una actualización. Tamaño promedio: 30MB.

ii. Motor AV: aproximadamente dos (2) veces por año. Tamaño promedio: 200MB.

Por defecto, los dispositivos reciben las actualizaciones de forma periódica y automática. El producto comprueba cada 10 minutos si se encuentran actualizaciones disponibles. Las actualizaciones de motores se pueden programar, las de firmas no.

Para programar las actualizaciones, es necesario crear una Política Gestión de Actualizaciones. Para esto, ir a Políticas > Gestión de actualizaciones e introducir los días y horas en los que se desea que se realicen las actualizaciones. También es posible indicar la versión de los paquetes de Software, aunque está completamente desaconsejado por parte de Sophos cambiar sus parámetros y sólo hacerlo guiado de Soporte oficial.

6.6 GESTIÓN DE CERTIFICADOS

El producto hace uso de certificados en las comunicaciones HTTPS entre los dispositivos y los Update Caches, así como entre Sophos Central y los dispositivos/Update Caches, para la obtención y distribución de las actualizaciones. Dichos certificados no son configurables y en caso de no detectarse el certificado de Sophos en alguna comunicación, esta no se inicia.

6.7 AUTO CHEQUEOS

El producto de forma automática y continuada realiza una evaluación de su configuración y, en caso de detectar un servicio caído o en un estado incorrecto, tratará de corregirlo. Si tras varios intentos sigue sin poder resolver la situación, entrará en modo de auto-reparación, donde el producto se reinstala de forma silenciosa y automática.

En este caso, las configuraciones que ya estuvieran establecidas se vuelven a asignar de manera automática, dependiendo de la máquina o usuario logueado. No es necesario realizar ninguna acción para que la maquina reinstalada se configure.

El objetivo es garantizar que el producto está siempre en perfecto estado y, con su auto-reparación, minimizar la necesidad de soporte.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

Sophos Central dispone de dos (2) tipos de logs:

Eventos: se registran todos los eventos relacionados con el producto. Como detecciones, incidentes, etc. Todo ello almacenado en la nube por 90 días, independientemente del número de eventos. Gracias a la API de SIEM es posible exportarlos a un servicio externo. Detalles en REF18

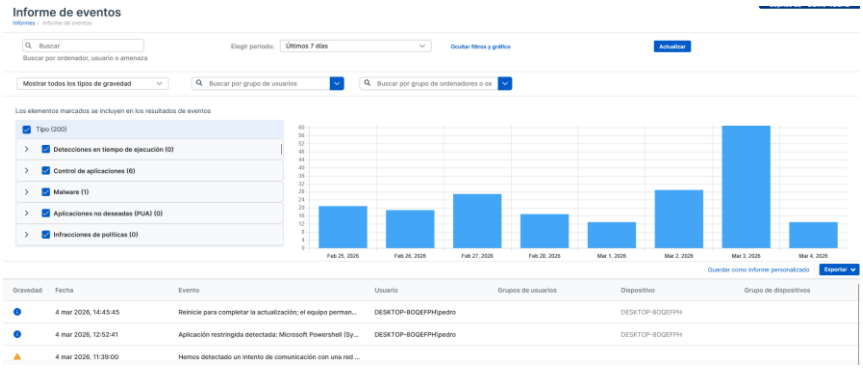


Ilustración 6-7 Eventos

Auditoría: cambios realizados en la configuración: quién lo ha hecho, sobre qué, etc… Todo ello se almacena en la nube por 90 días, independientemente del número de eventos. El periodo de retención en la nube no es configurable.

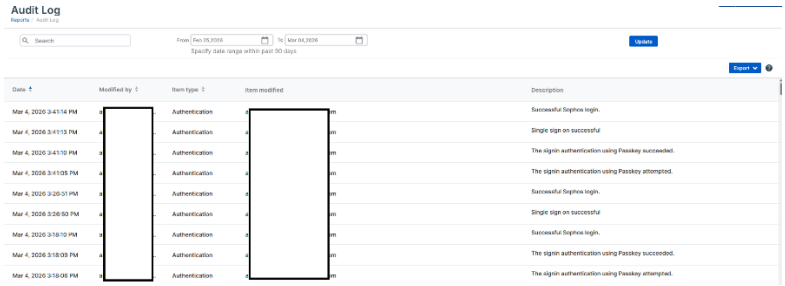


Ilustración 6-8 Auditoría

Detecciones EDR/XDR: En el caso de disponer de EDR/XDR, se tendrán las detecciones realizadas por este servicio, así como los datos almacenados en el Lago de Datos. El tiempo por defecto es de 90 días (con todos los detalles), pero es posible mediante licencia adicional ampliar hasta un año.

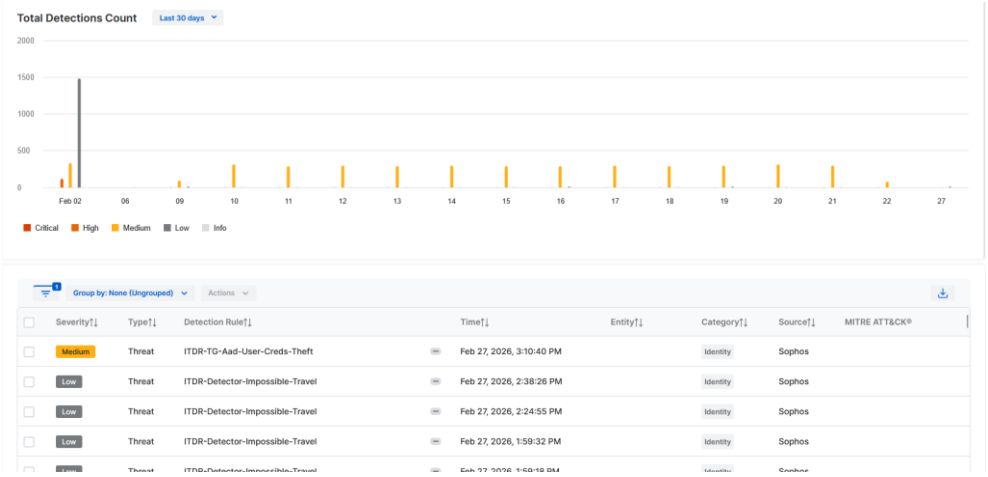


Ilustración 6-9 Detecciones EDR/XDR

Si se dispone de EDR/XDR, es posible realizar acciones de búsqueda para casi cualquier tipo de evento. Por ejemplo, si un grupo de equipos ha intentado resolver el DNS www.sophos.com hace 47 días, se puede saber qué proceso lo ha hecho, con qué usuario, etc. Es lo que se denomina Live Discover y permite la consulta de tablas almacenadas en los propios equipos en tiempo real. El detalle de tablas que se pueden consultar está en: REF19 aunque gracias a la inclusión de la IA generativa, se dispone de la opción 'Búsqueda con IA' que permite realizar consultas en lenguaje natural, generando la sentencia SQL (para guardarla en la biblioteca si se desea) y realizando la búsqueda:

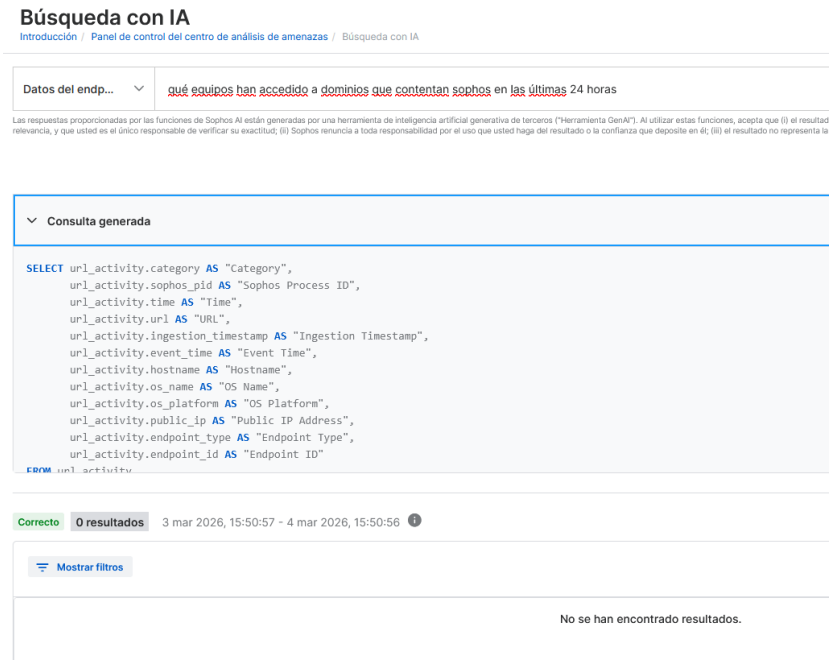


Ilustración 6-10 Ejemplo búsqueda con IA

6.8.2 ALMACENAMIENTO LOCAL

Es posible realizar un almacenamiento local de los eventos mediante el uso de una API que permite el reenvío de los eventos a un servidor de auditoría Syslog o bien a un sistema

SIEM. Todas las comunicaciones de Sophos se realizan a través de TLS 1.2, con intercambio de claves ECDHE_RSA y cifrado AES_128_GCM. Esta configuración no es parametrizable.

Detalles al respecto en REF20

6.8.3 ALMACENAMIENTO REMOTO

El almacenamiento remoto de los logs se realiza de forma automática en la nube de Sophos. Estos datos son accesibles desde la consola de gestión, desde la página Informes.

Adicionalmente, es posible exportar los logs de auditoría del producto desde la consola de gestión, para posteriormente almacenarlos en la ubicación deseada:

Ir a 'Informes' y seleccionar 'Registros de Auditoría'.

Hacer clic en 'Exportar' y seleccionar una de las opciones:

ii. CSV de la vista actual.

iii. PDF de la vista actual.

Estas opciones exportan, en el formato elegido, los logs de auditoría de la vista actual.

CSV de los últimos 90 días.

PDF de los últimos 90 días.

Estas opciones exportan en el formato elegido, todos los logs de auditoría de los últimos 90 días

7. FASE DE OPERACIÓN

La operativa habitual de este producto consistirá en, de forma periódica:

Revisar las alertas y detecciones EDR/XDR (en caso de disponer de éstas últimas). Están ordenadas por criticidad: alta, media, baja

Resolver lo antes posible las alertas de criticidad ALTA, siguiendo con las de MEDIA y finalmente las de BAJA.

Realizar la exportación de logs y enviar a un SIEM o Syslog.

En caso de tener una detección, contextualizar el para comprobar el verdadero origen de la amenaza.

Si se dispone de EDR/XDR, además de revisar sus detecciones, realizar búsquedas periódicas para detectar acciones "extrañas", conexiones "extrañas", etc… Si se dispone de EDR,

Los detalles de EDR permitirán realizar una limpieza preventiva del binario que, si bien no ha detonado una amenaza, tras los pasos de análisis se descubre sospechoso e inadecuado, pudiendo de forma centralizada realizar la limpieza global.

Verificar que el producto está correctamente actualizado, tanto las firmas como los motores.

Verificar que el modo de operación seguro sigue operativo de acuerdo con su configuración recomendada en esta guía.

7 REFERENCIAS

Indicar documentación que se haya referenciado a lo largo de la guía.

REF1 Guía de Administración de Sophos Central
https://docs.sophos.com/central/Customer/help/es-es/GettingStarted/index.html

REF2 CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

REF3 Sophos Central
https://central.sophos.com

REF4 Guía de Licenciamiento
https://docs.sophos.com/central/customer/help/es-es/LicensingGuide/index.html

REF5 Guía de IPs y Dominios
https://docs.sophos.com/central/customer/help/es-es/PeopleAndDevices/ProtectDevices/DomainsPorts/index.html

REF6 Requisitos mininos
https://support.sophos.com/support/s/article/KBA-000002793?language=en_US

REF7 Portal Central
https://central.sophos.com

REF8 Cachés de actualización
https://docs.sophos.com/central/customer/help/es-es/ManageYourProducts/GlobalSettings/ProductsServices/Endpoint/UpdateCaches/index.html

REF9 Modificadores del ejecutable de instalación
https://docs.sophos.com/central/partner/help/es-es/Help/Configure/Installers/WindowsCommandLine/index.html.

REF10 Detalles de despliegue en distintas plataformas
https://support.sophos.com/support/s/article/KBA-000003140?language=en_US.

REF11 Detalles de configuración de políticas de protección adicionales
https://docs.sophos.com/central/customer/help/es-es/ManageYourProducts/EndpointProtection/index.html

REF12 Configuración de Directorio Activo
https://docs.sophos.com/central/Customer/help/es-es/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithActiveDirectory/index.html

REF13 Configuración de EntraID
https://docs.sophos.com/central/Customer/help/es-es/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithAzureAD/index.html

REF14 Configuración de Directorio de Google
https://docs.sophos.com/central/Customer/help/es-es/PeopleAndDevices/DirectoryService/SetUpSynchronizationWithGoogleDirectory/index.html

REF15 Federación de EntraID
https://docs.sophos.com/central/partner/help/es-es/Help/GlobalSettings/AccessControl/SigninandIdentity/SophosSignin/AzureADIDP/index.html

REF16 Federación de OpenID
https://docs.sophos.com/central/partner/help/es-es/Help/GlobalSettings/AccessControl/SigninandIdentity/SophosSignin/OpenIDConnectIDP/index.html

REF17 Federación de ADFS
https://docs.sophos.com/central/partner/help/es-es/Help/GlobalSettings/AccessControl/SigninandIdentity/SophosSignin/ADFSIDP/index.html

REF18 Documentación de la API de Sophos
https://developer.sophos.com/docs/siem-v1/1/overview

REF19 Esquema de Base de Datos para hacer consultas
https://support.sophos.com/support/s/article/KBA-000006434?language=en_US

REF20 Detalle de API de integración con SIEM
https://developer.sophos.com/docs/siem-v1/1/overview

8 ABREVIATURAS

EDR	Endpoint Detection and Response.
ENS	Esquema Nacional de Seguridad.
HTTPS	Hyper Text Transfer Protocol Secure.
MFA	Multi Factor Authentication
OTP	One Time Password
RBAC	Role Based Access Control
TCP	Transmission Control Protocol