



# ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

## POLITICAS DE CIBERSEGURIDAD -SOPHOS CENTRAL

**2022**



## Contenido

Consola Administración Centralizada de Sophos.....	3
Tecnologías next-gen .....	3
Análisis de datos en profundidad.....	3
Potentes paneles de control .....	3
Implementación de políticas de restricción .....	4
Implementación de políticas generales .....	4
Restricción de Aplicaciones.....	4
Control de periféricos.....	6
Control Web .....	7



## Consola Administración Centralizada de Sophos

Sophos Central es la consola de administración de ciberseguridad en la nube la cual te permite tener control de todos los dispositivos y gestionar los eventos e incidente de ciberseguridad de manera fácil

### Tecnologías next-gen

- Prevención predictiva con IA
- Detección de nivel empresarial
- Respuesta automatizada a incidentes

### Análisis de datos en profundidad

- Telemetría entre productos sincronizados
- Información sobre amenazas de SophosLabs Intelix
- Investigaciones entre productos

### Potentes paneles de control

- Potentes paneles de control, generación de informes y notificaciones
- Acceda a resúmenes rápidos con paneles de control visuales
- Profundice en la información con potentes informes y análisis



## Implementación de políticas de restricción

### Implementación de políticas generales

Mediante la consola de administración centralizada de Sophos Central podemos implementar políticas de control sobre los dispositivos que tiene instalado la solución de EndPoint de Sophos como mecanismo de prevención protección contra Ransomware

Note: The policies at the top of the list override the policies at the bottom of the list.

Name	Status	Type (single / group)	Last modified
<b>Threat Protection (1)</b>			
Base Policy - Threat Protection	✓ Enforced		Oct 22, 2021
<b>Peripheral Control (2)</b>			
Bloqueo de USB	✓ Enforced	Computer IO / 368	Oct 12, 2021
Base Policy - Peripheral Control	✓ Enforced		Jun 16, 2020
<b>Application Control (2)</b>			
Restricción de Aplicaciones	✓ Enforced	Computer IO / 371	Nov 29, 2022
Base Policy - Application Control	✓ Enforced		Jun 16, 2020
<b>Data Loss Prevention (2)</b>			
DLP política CD	✓ Enforced	User IO / 01	Sep 20, 2021
Base Policy - Data Loss Prevention	✓ Enforced		Jun 28, 2021
<b>Web Control (1)</b>			
Base Policy - Web Control	✓ Enforced		Nov 10, 2022

### Control de Políticas Generales

### Restricción de Aplicaciones

A continuación se describe algunas aplicaciones que podemos controlar a través de la gestión del antivirus, tales como:

- 710 Gauge Utility
- Adobe Dreamweaver
- Allplan
- ArtiosCAD
- AutoCAD
- Autodesk Application Manager
- Autodesk Inventor 2017



- Autodesk Inventor 2018
- Autodesk Revit
- Autodesk Windows Components
- Corel Video Studio Pro X
- Creo
- Dassault Systemes SolidWorks
- Draftsight
- Gates Design Flex Pro
- GaugeTools
- Google SketchUp
- LibreCAD
- Maple
- Maxon Cinema 4D
- Micromine 2016
- MityGUI
- NetFabb
- Photo Pos Pro
- PlanGrid
- Rhinoceros
- SketchBook Express
- Sparx Systems
- The Print Shop
- UniGraphics
- Webots Robot Simulator

Mecanismo de control evidenciado en la siguiente imagen

Controlled Applications	Selected / Total	Control New Apps
Design tool	25 / 42	
Document viewer	1 / 55	
Download manager	61 / 65	
Game	367 / 368	
Jailbreak Software	3 / 3	
Media player	1 / 145	
Optical burning tool	21 / 22	
Optical media emulation	5 / 5	
Password / license recovery tool	25 / 31	
Pranking Software	1 / 2	
Remote management tool	96 / 125	

Detection Options

- Detect controlled applications when users access them (You will be notified)
  - Allow the detected application
  - Block the detected application
- Detect controlled applications during scheduled and on-demand scans

## Restricción de aplicaciones



## Control de periféricos

Los totales que aparecen a continuación incluyen todos los periféricos detectados, ya sea en estaciones de trabajo o servidores:

- AutorizarBloquear
- Bluetooth - 0 detectados
- AutorizarSolo lecturaBloquear
- Proteger almacenamiento extraíble - 0 detectados
- AutorizarSolo lecturaBloquear
- Disquete - 0 detectados
- AutorizarBloquear
- Infrarrojo - 0 detectados
- AutorizarBloquear
- Módem - 0 detectados
- AutorizarSolo lecturaBloquear
- Unidad óptica - 0 detectados
- AutorizarSolo lecturaBloquear
- Almacenamiento extraíble - 0 detectados
- AutorizarBloquear puenteBloquear
- Inalámbrico - 0 detectados
- AutorizarBloquear
- MTP/PTP - 0 detectados

Mecanismo de control evidenciado en la siguiente imagen

**SOPHOS** Endpoint Protection - view Computer Policy

ALCALDIA MAYOR DE CARTAGENA DE INDIAS - Bolívar Admin

POLICY NAME: Equipo de USB

POLICY TYPE: Peripheral Control - Device

0 COMPUTERS 36 GROUPS 0 SETTINGS POLICY ENFORCED

Manage Peripherals - set your peripheral settings below

Enable peripheral control

Monitor but do not block (all peripherals will be allowed)

Control access by peripheral type and add exemptions

The totals listed below include all peripherals detected, whether on endpoint computers or servers:

Device Type	Count
Bluetooth	481 detected
Secure removable storage	0 detected
Floppy drive	2 detected
Infrared	0 detected
Modem	98 detected
Optical drive	688 detected
Removable storage	5289 detected
Wireless	178 detected
MTP/PTP	1223 detected

Peripheral Exemptions >

Desktop Messaging

Enable Desktop Messaging for Peripheral Control

Configure a message to be added to the end of the standard notification

Política de periféricos activada, para más información contacte a mesa de ayuda - SAUS

Note: Custom messages will not be displayed for Intercept X events.

## Control de periféricos



## Control Web

Se establecerá políticas para bloquear o permitir las siguientes acciones de acceso web para las estaciones de trabajo.

Detalle	Acción
Categorías relacionadas con la productividad	Permitir
Redes sociales	Permitir
Categorías de adultos y potencialmente inapropiadas	Bloquear
Categorías susceptibles de provocar un uso excesivo del ancho de banda	Bloquear
Categorías de sitios relativos al trabajo	Permitir

Mecanismo de control evidenciado en la siguiente imagen

The screenshot displays the Sophos Web Control policy configuration page. The left sidebar shows the navigation menu with 'Policies' selected. The main content area is titled 'Web Control' and includes a 'POLICY ENFORCED' indicator. The 'Web Control' section is active, with a note about HTTPS decryption. Below this, the 'Additional security options' section is expanded, showing settings for Advertisements, Uncategorized, and Risky File Types. The 'Acceptable web usage' section is also expanded, showing settings for Productivity-related categories, Social Networking, Adult and potentially inappropriate categories, and Categories likely to cause excessive bandwidth usage. The 'Protect against data loss' section is expanded, showing settings for Allow data sharing and a table of actions for Downloads and Web-based Email. The 'Log web control events' and 'Control sites' sections are also visible.