maestre corporación

Informe de configuración Endpoint SOPHOS CENTRAL

ALCANCE

Dar a conocer las configuraciones realizadas en la consola de Sophos Central del **Alcaldía de Mosquera**, según los acuerdos del proyecto, a fin de brindar la protección adecuada a las estaciones de trabajo y servidores de la organización.

CLIENTE

Cliente

Alcaldía de Mosquera

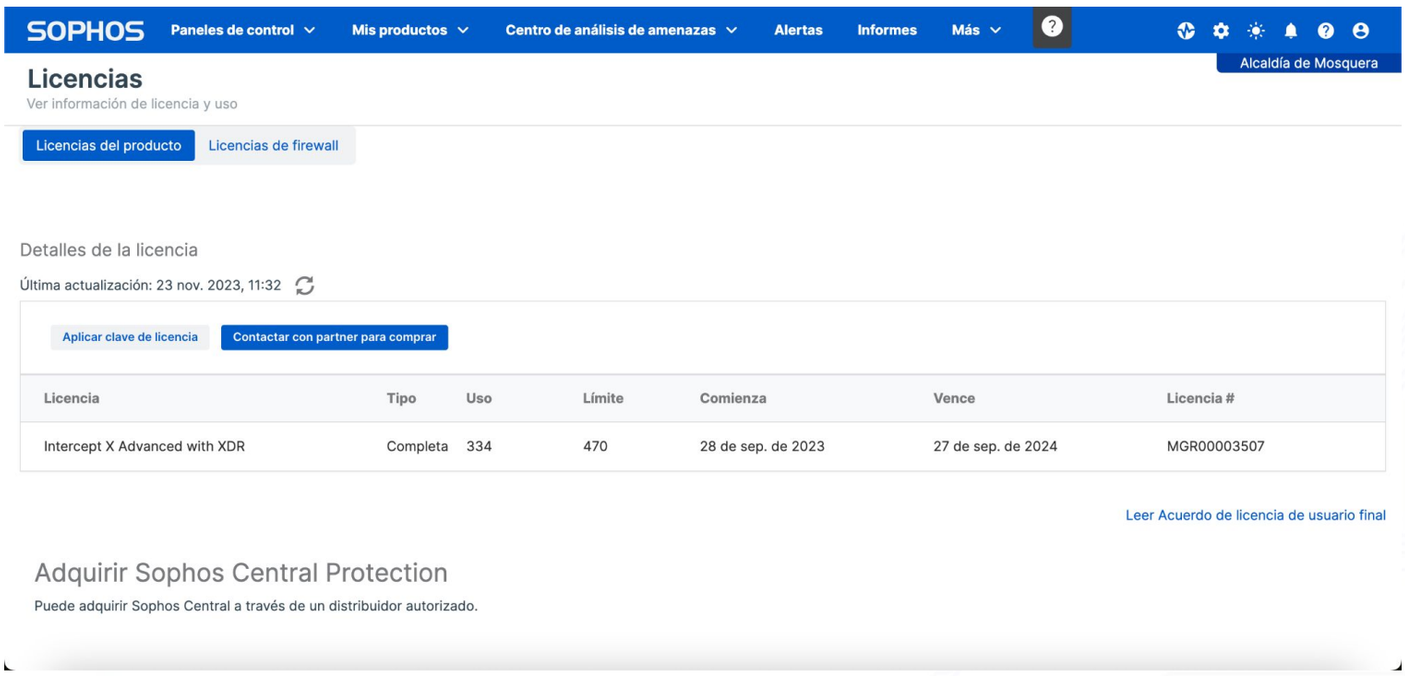
Producto

Intercept X Advanced with XDR

LICENCIA ACTUAL

El **Alcaldía de Mosquera** dispone de un límite de 470 (cuatrocientos setenta) licencias de Intercept X Advanced with XDR para estaciones de trabajo, de las cuales 334 (trescientos treinta y cuatro) están actualmente en uso.

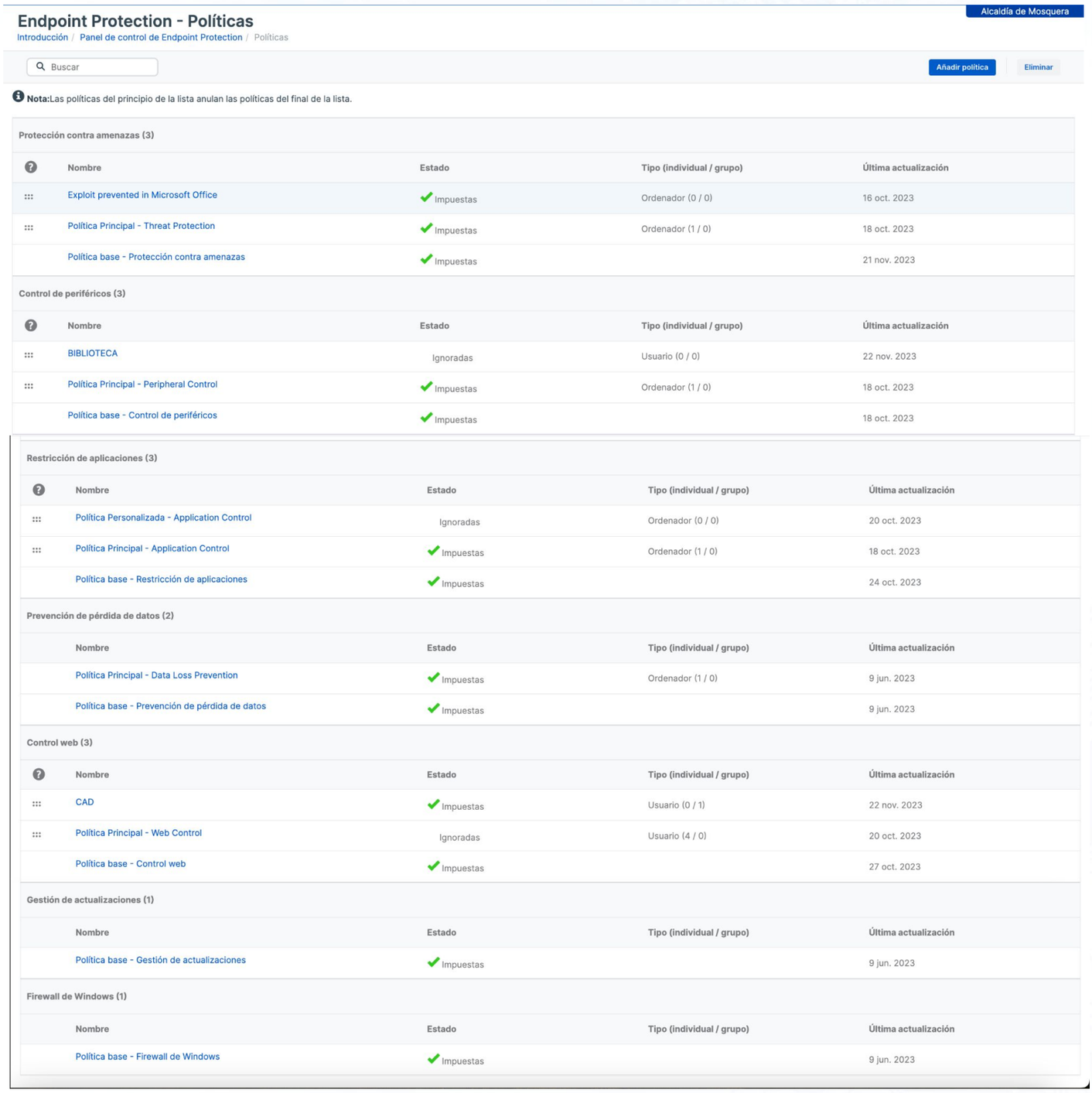
Partner: Corporación Maestre SAS



maestre
corporación

Endpoint

Políticas del Computador



Endpoint Protection - Políticas

Alcaldía de Mosquera

Introducción / Panel de control de Endpoint Protection / Políticas

Buscar | Añadir política | Eliminar

Nota: Las políticas del principio de la lista anulan las políticas del final de la lista.

Protección contra amenazas (3)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
Exploit prevented in Microsoft Office	Impuestas	Ordenador (0 / 0)	16 oct. 2023
Política Principal - Threat Protection	Impuestas	Ordenador (1 / 0)	18 oct. 2023
Política base - Protección contra amenazas	Impuestas		21 nov. 2023

Control de periféricos (3)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
BIBLIOTECA	Ignoradas	Usuario (0 / 0)	22 nov. 2023
Política Principal - Peripheral Control	Impuestas	Ordenador (1 / 0)	18 oct. 2023
Política base - Control de periféricos	Impuestas		18 oct. 2023

Restricción de aplicaciones (3)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
Política Personalizada - Application Control	Ignoradas	Ordenador (0 / 0)	20 oct. 2023
Política Principal - Application Control	Impuestas	Ordenador (1 / 0)	18 oct. 2023
Política base - Restricción de aplicaciones	Impuestas		24 oct. 2023

Prevención de pérdida de datos (2)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
Política Principal - Data Loss Prevention	Impuestas	Ordenador (1 / 0)	9 jun. 2023
Política base - Prevención de pérdida de datos	Impuestas		9 jun. 2023

Control web (3)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
CAD	Impuestas	Usuario (0 / 1)	22 nov. 2023
Política Principal - Web Control	Ignoradas	Usuario (4 / 0)	20 oct. 2023
Política base - Control web	Impuestas		27 oct. 2023

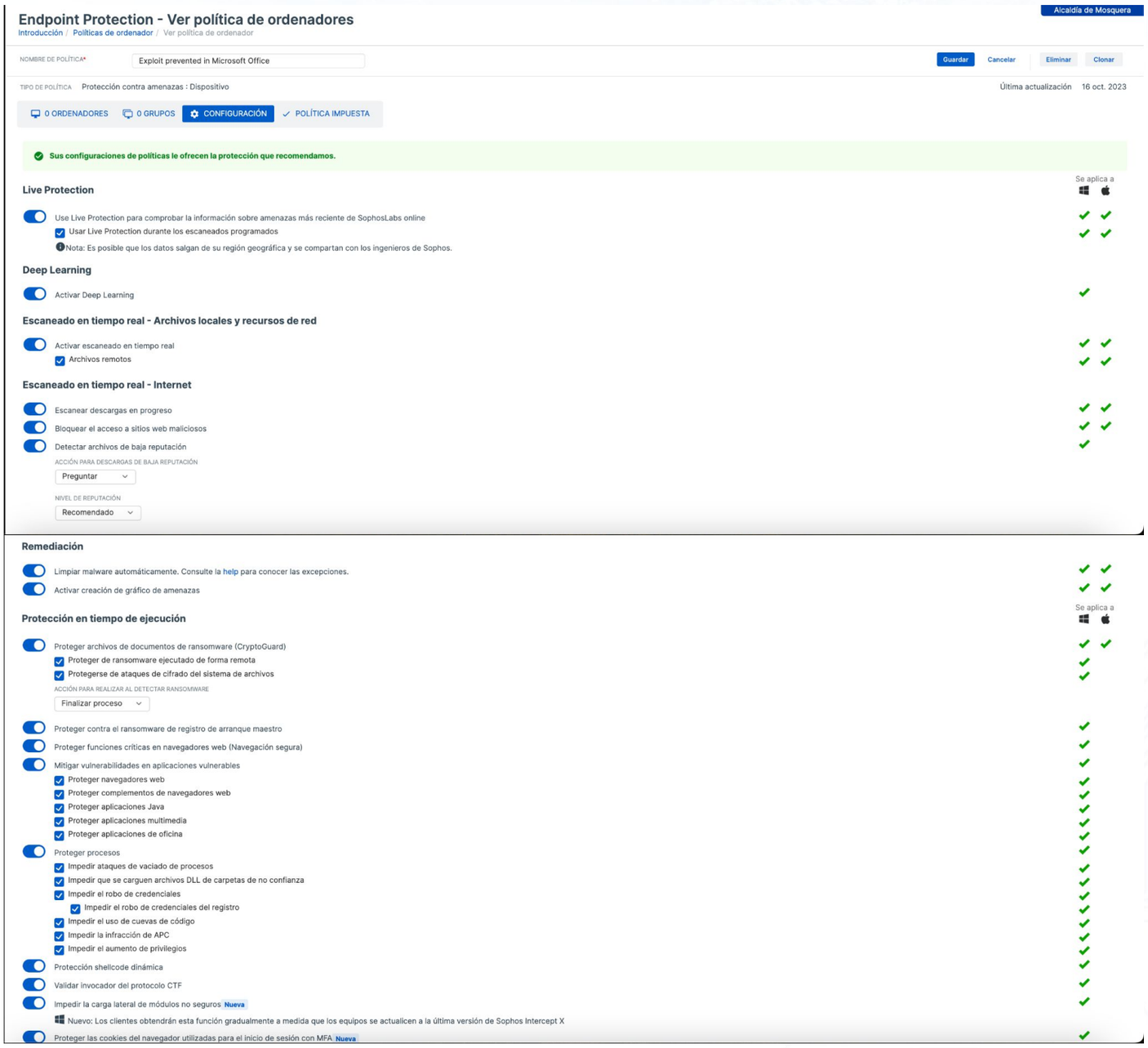
Gestión de actualizaciones (1)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
Política base - Gestión de actualizaciones	Impuestas		9 jun. 2023

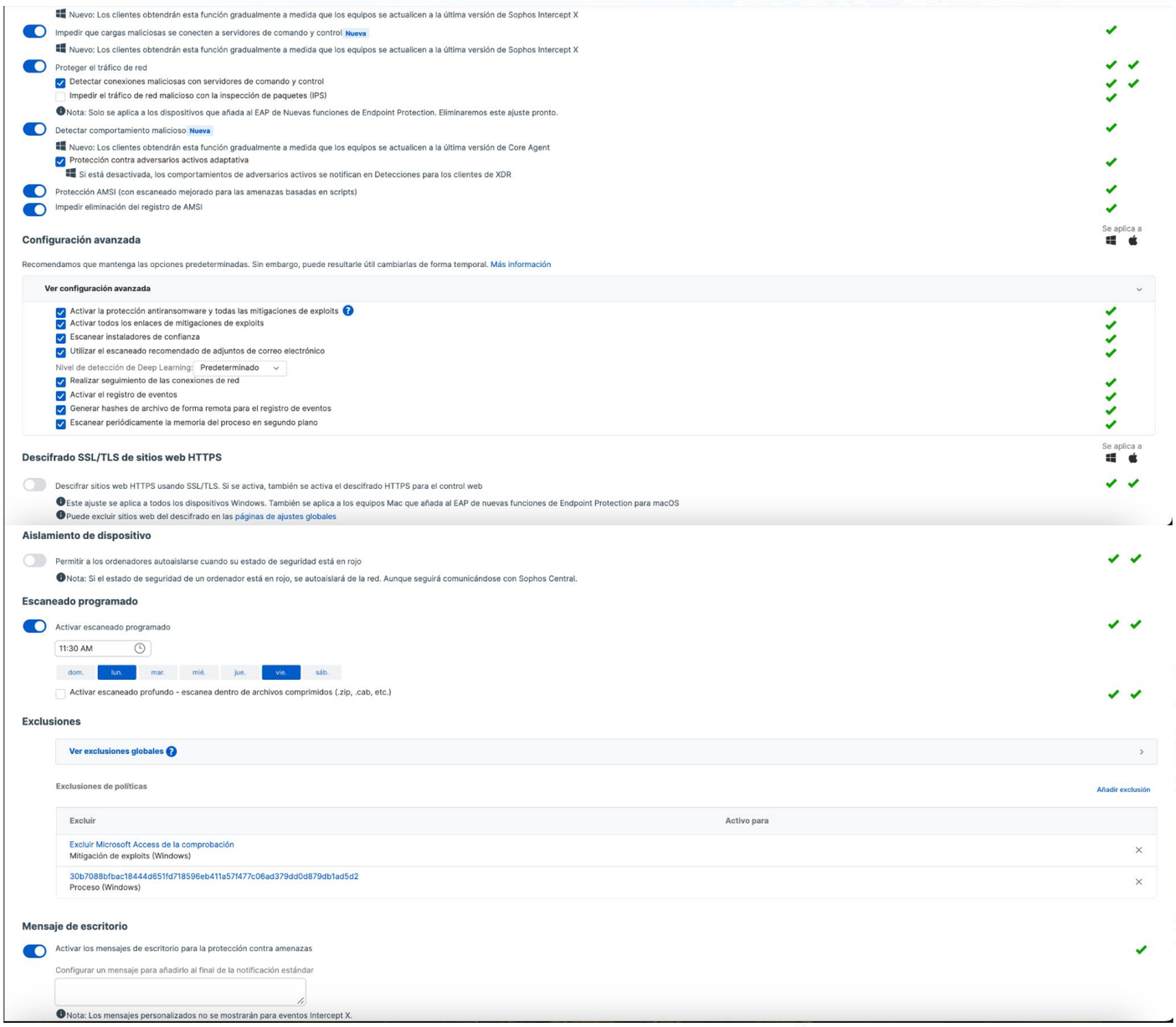
Firewall de Windows (1)

Nombre	Estado	Tipo (individual / grupo)	Última actualización
Política base - Firewall de Windows	Impuestas		9 jun. 2023

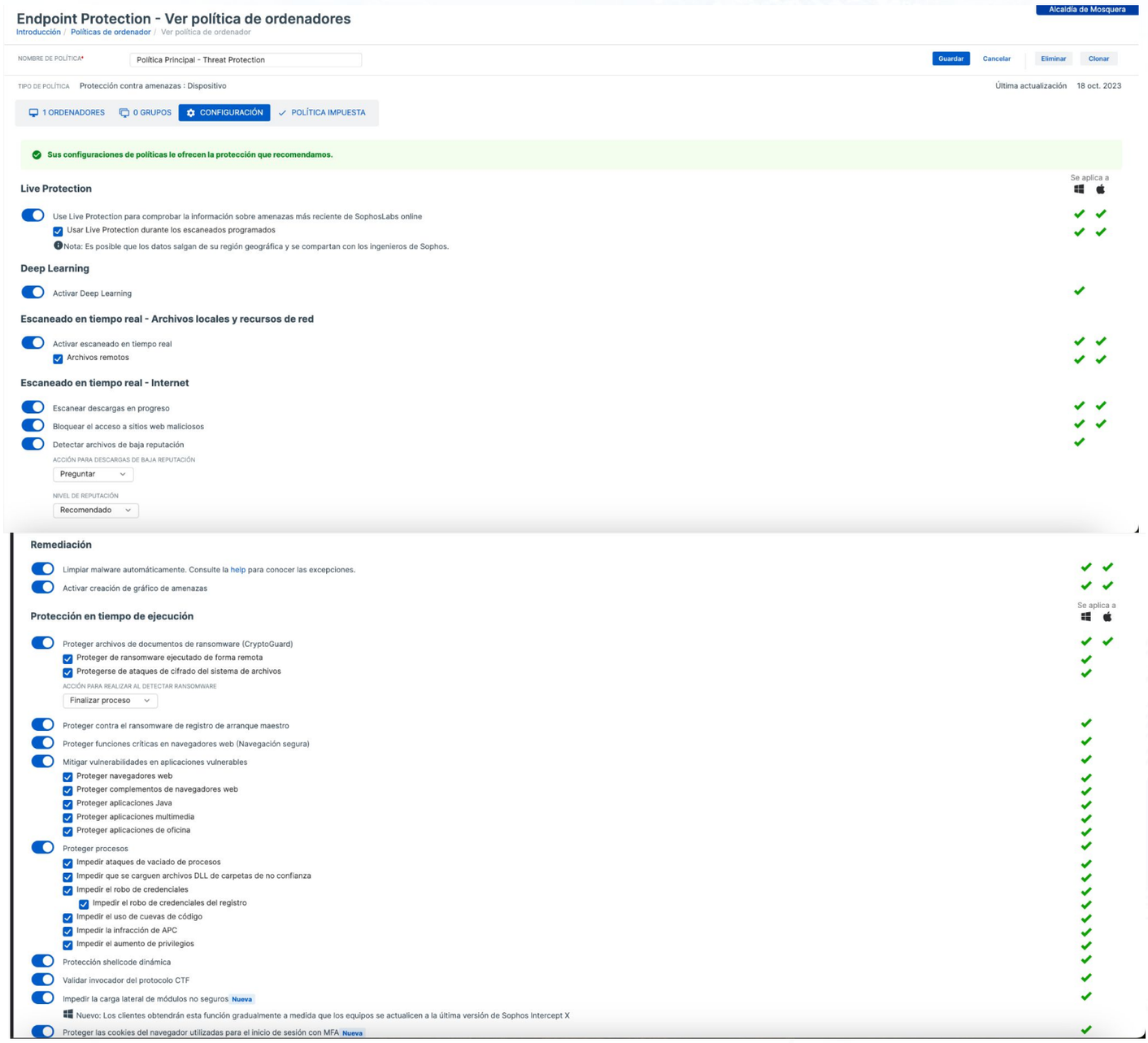
Protección contra amenazas (Threat Protection) - Exploit prevented in Microsoft Office:



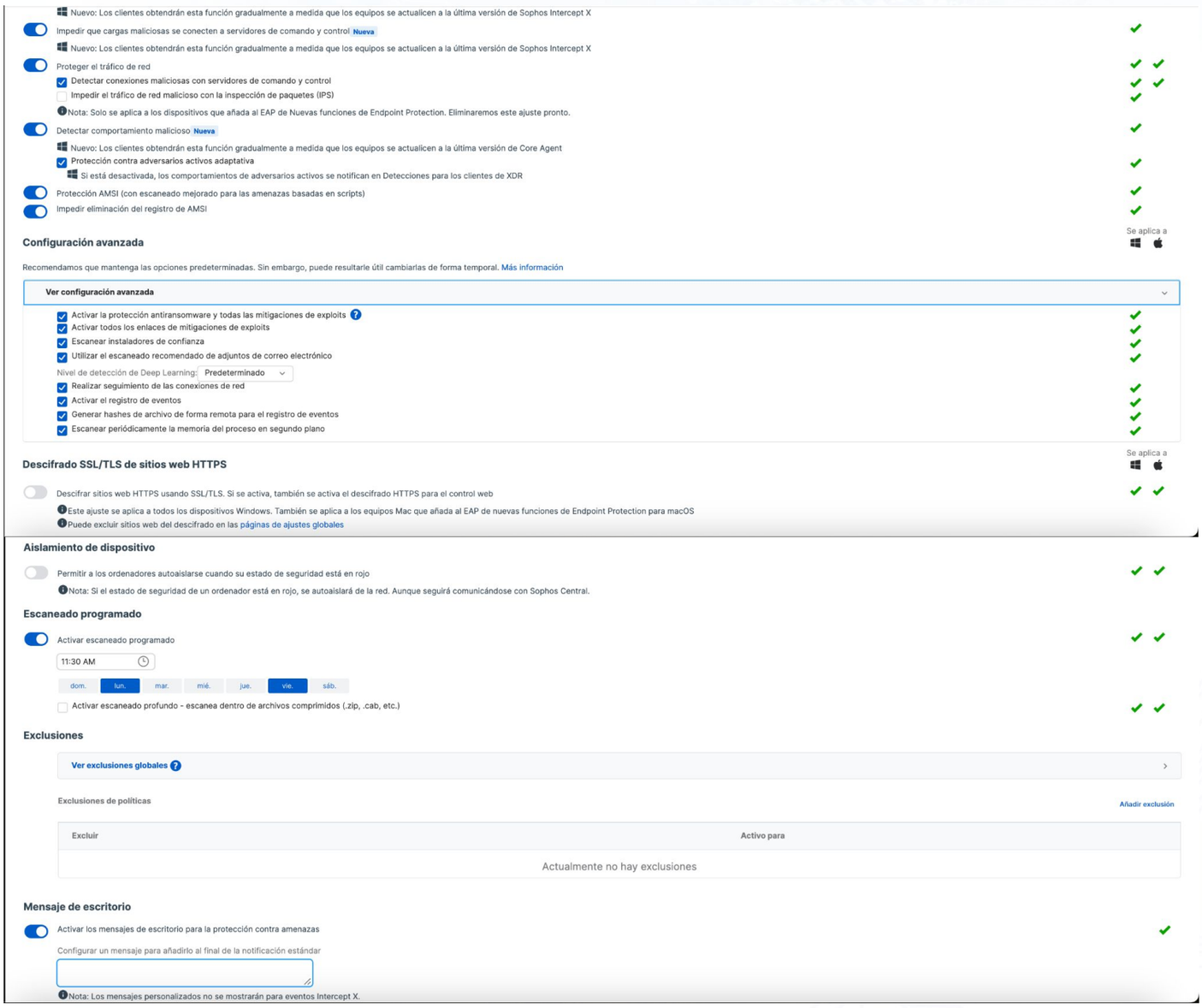
Protección contra amenazas (Threat Protection) - Exploit prevented in Microsoft Office:



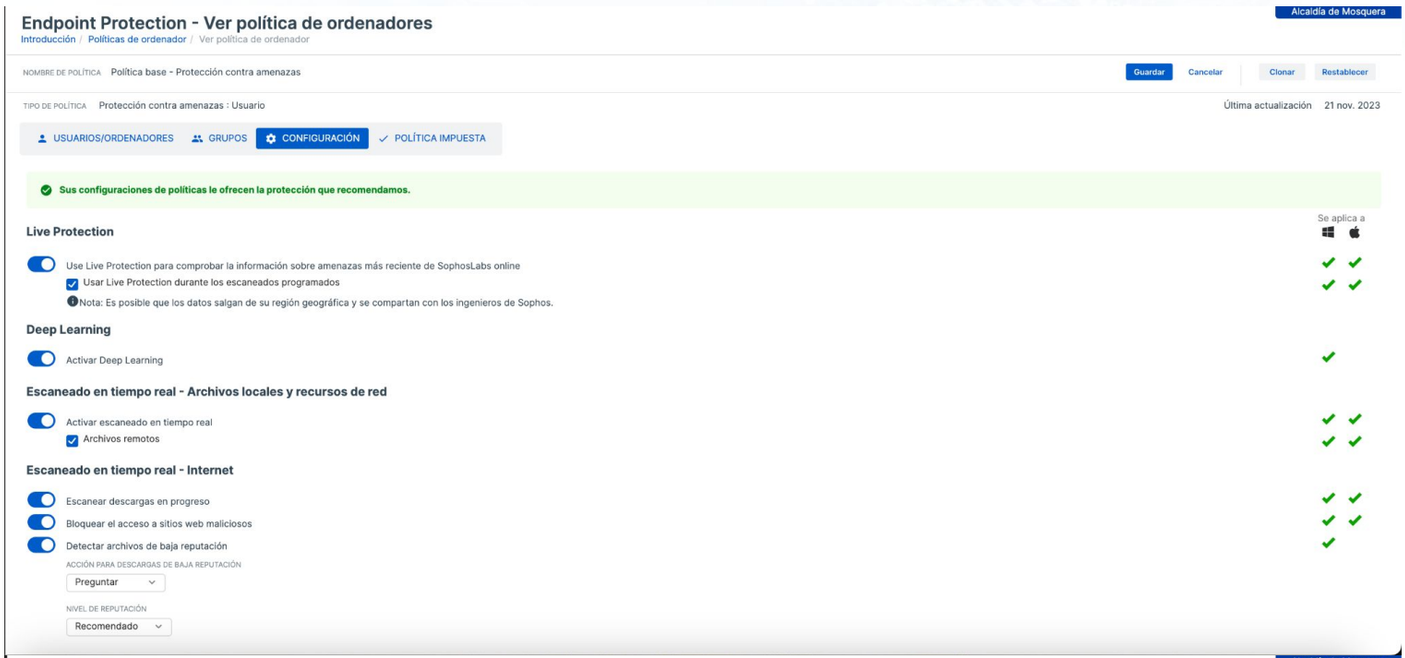
Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

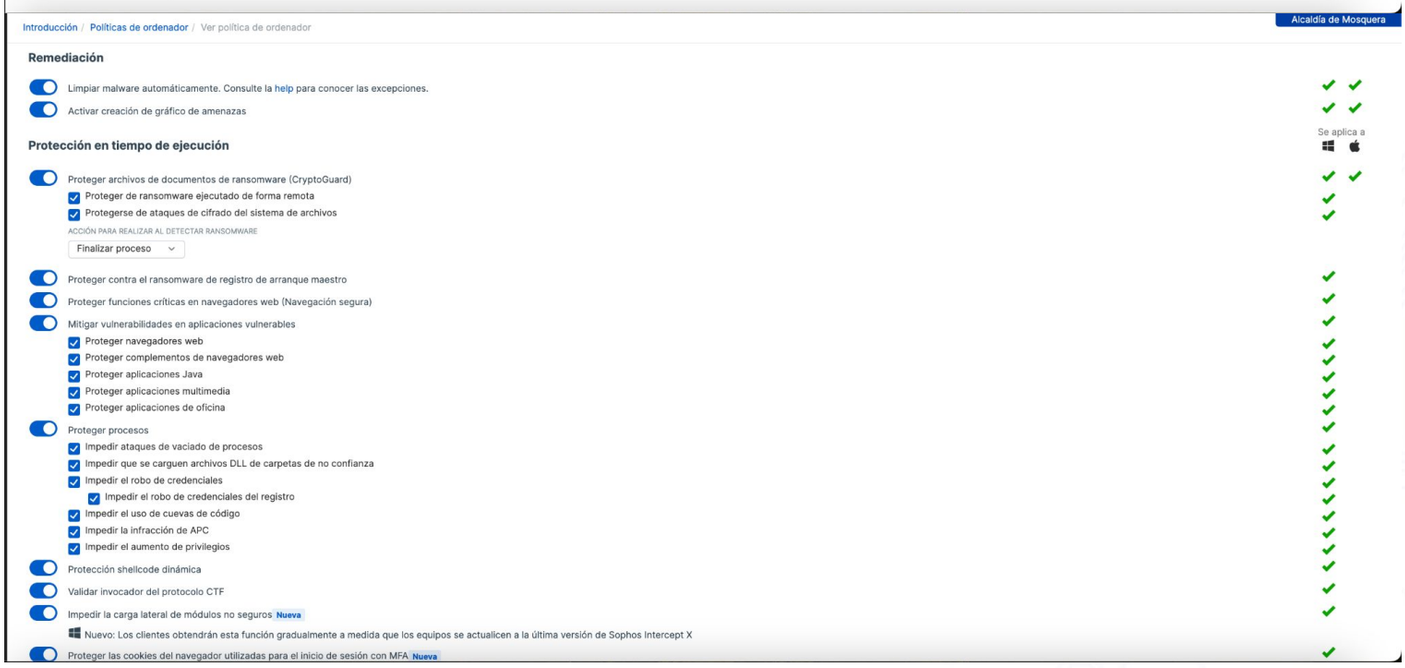


Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

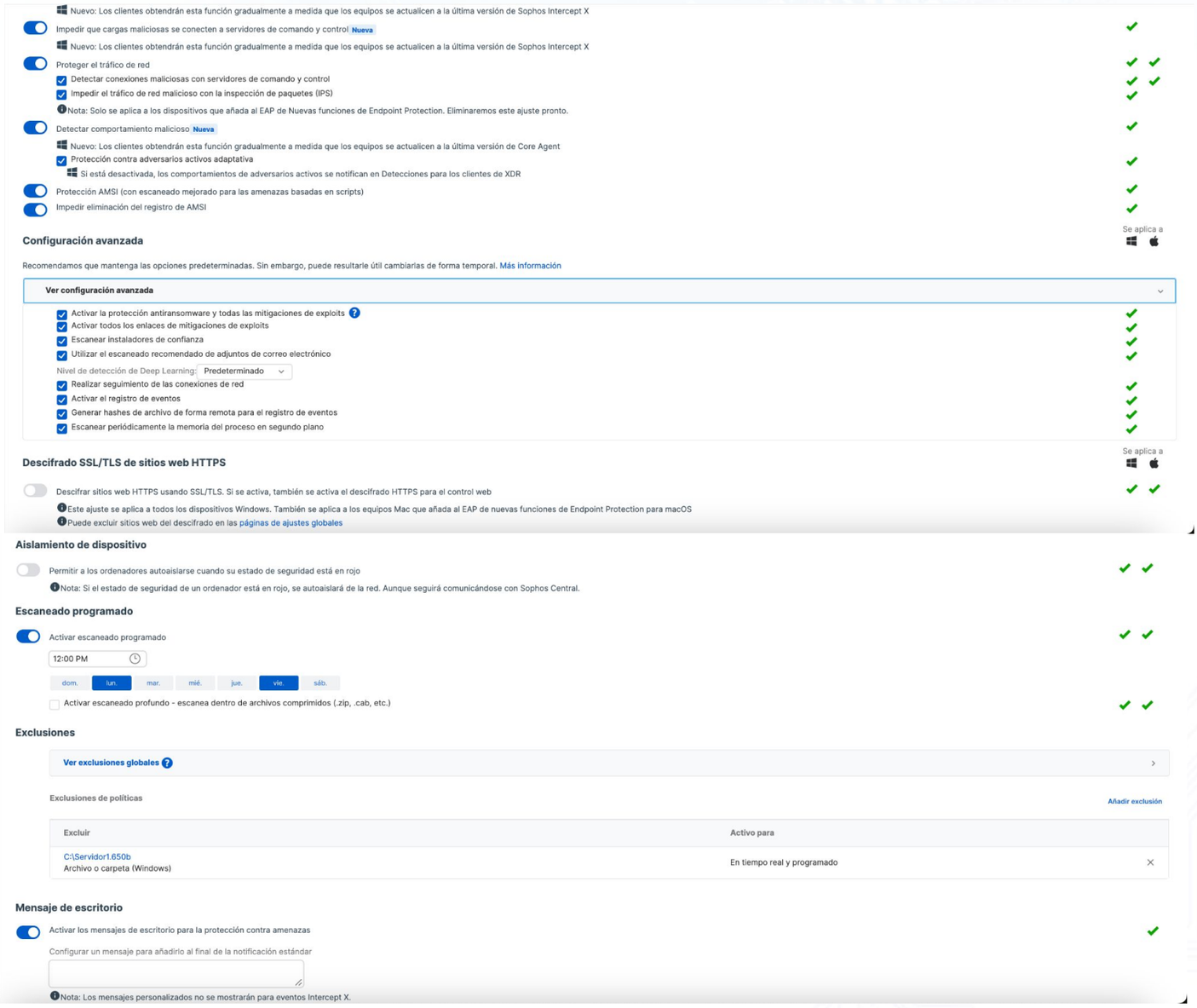


Protección contra amenazas (Threat Protection) - Política base - Protección contra amenazas:





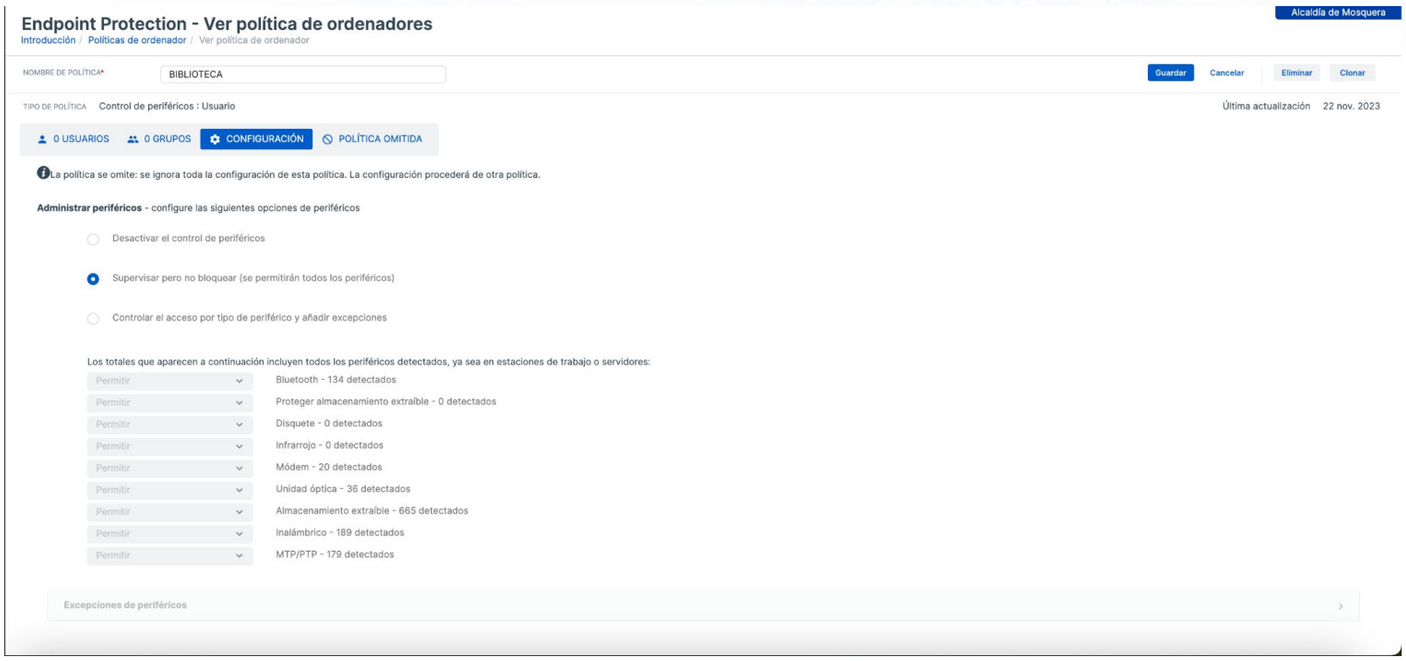
Protección contra amenazas (Threat Protection) - Política base - Protección contra amenazas:



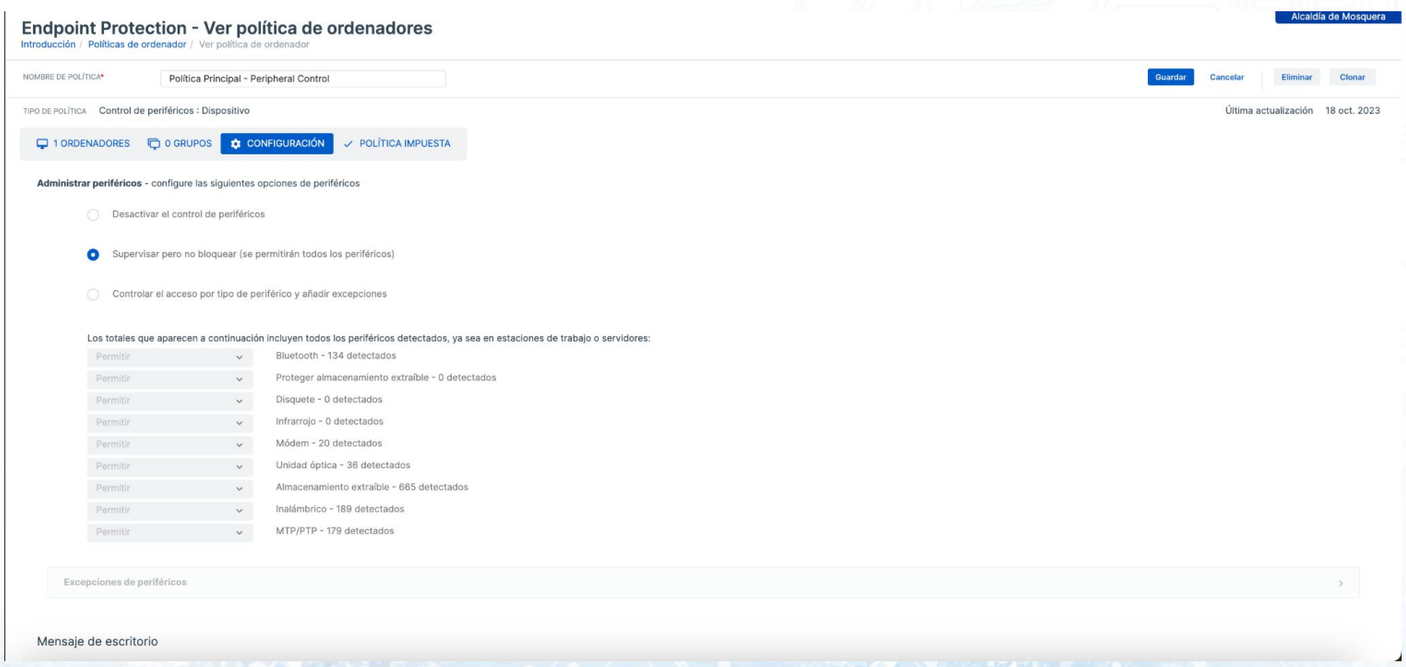
Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

Protección contra amenazas (Threat Protection) - Base Policy - Threat Protection:

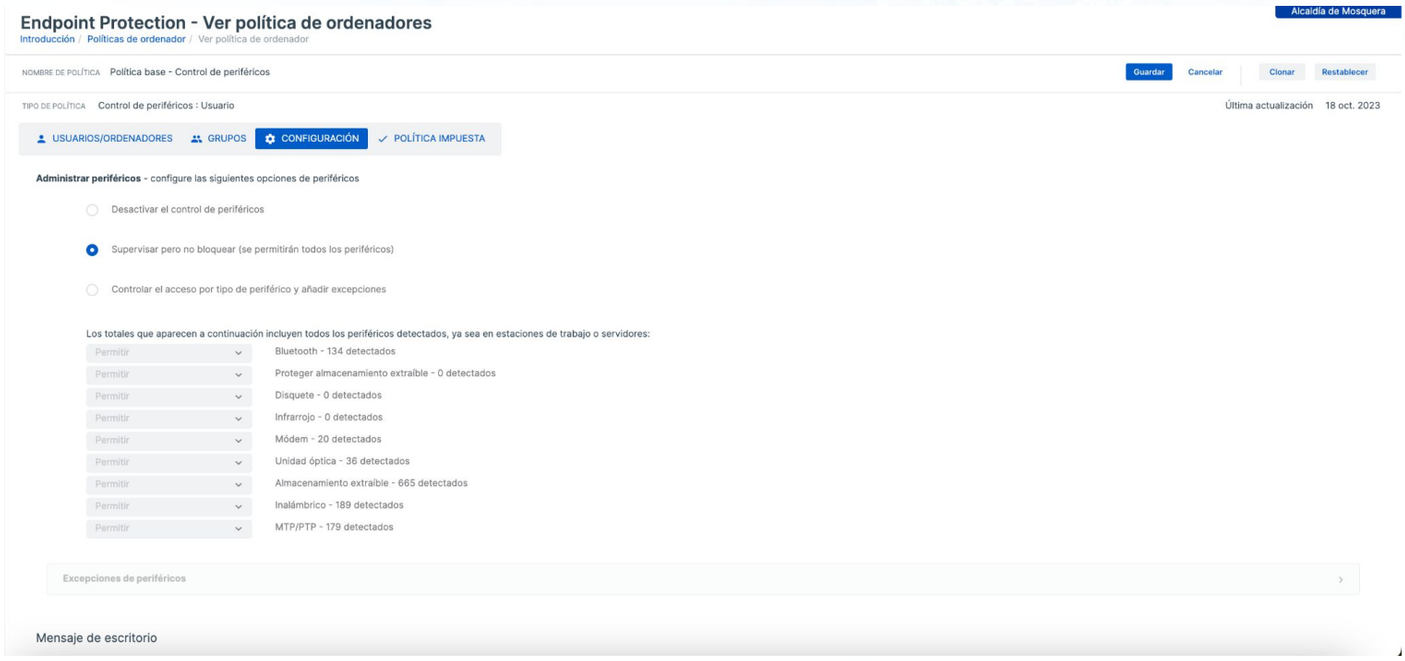
Control de periféricos (Peripheral Control) - BIBLIOTECA:



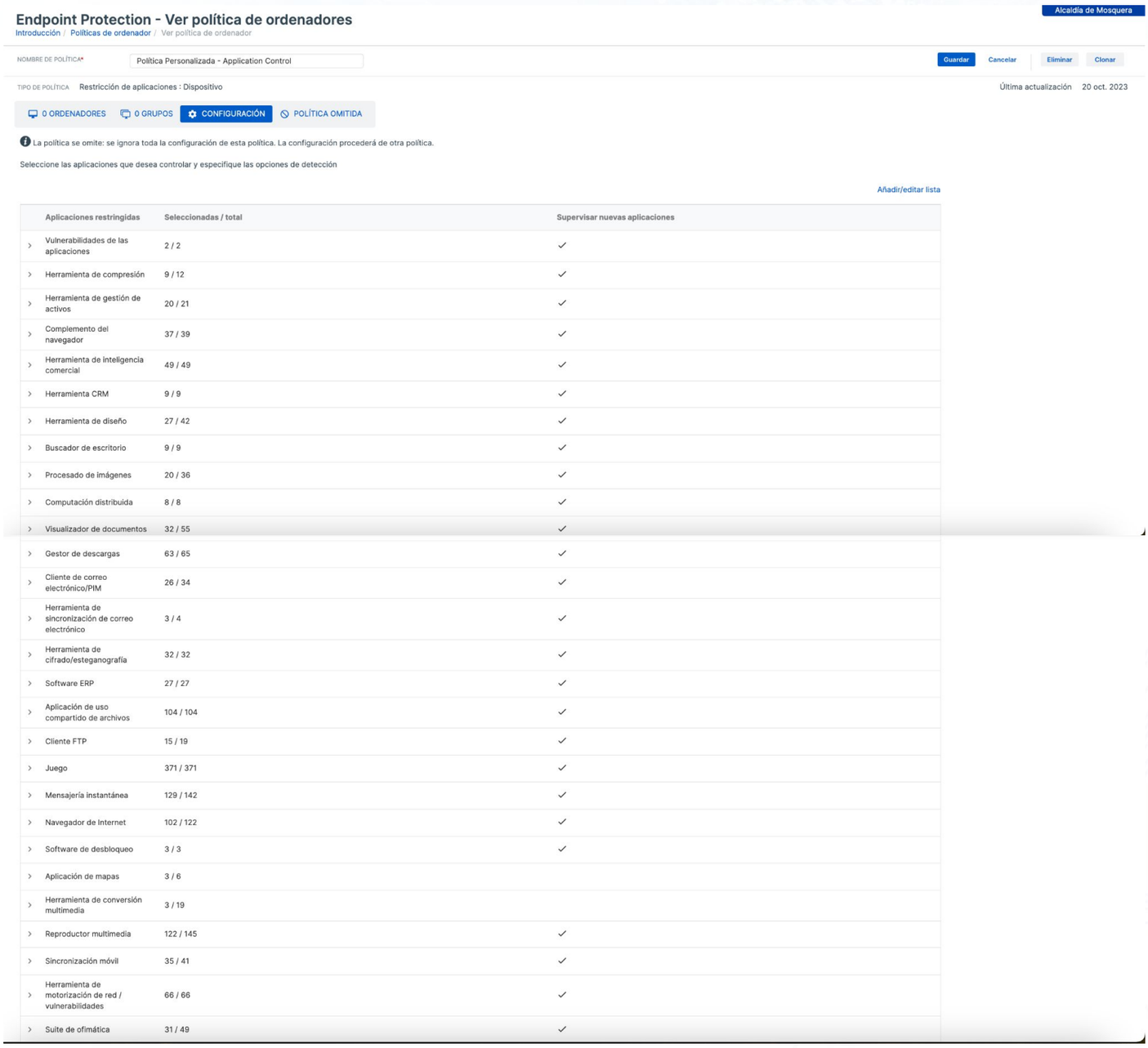
Control de periféricos (Peripheral Control) - Política Principal - Peripheral Control:



Control de periféricos (Peripheral Control) - Política base - Control de periféricos:



Control de Aplicaciones (Application Control) - Política Personalizada - Application Control:



Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

Alcaldía de Mosquera

NOMBRE DE POLÍTICA* Política Personalizada - Application Control

Guardar Cancelar Eliminar Clonar

TIPO DE POLÍTICA Restricción de aplicaciones : Dispositivo

Última actualización 20 oct. 2023

0 ORDENADORES 0 GRUPOS CONFIGURACIÓN POLÍTICA OMITIDA

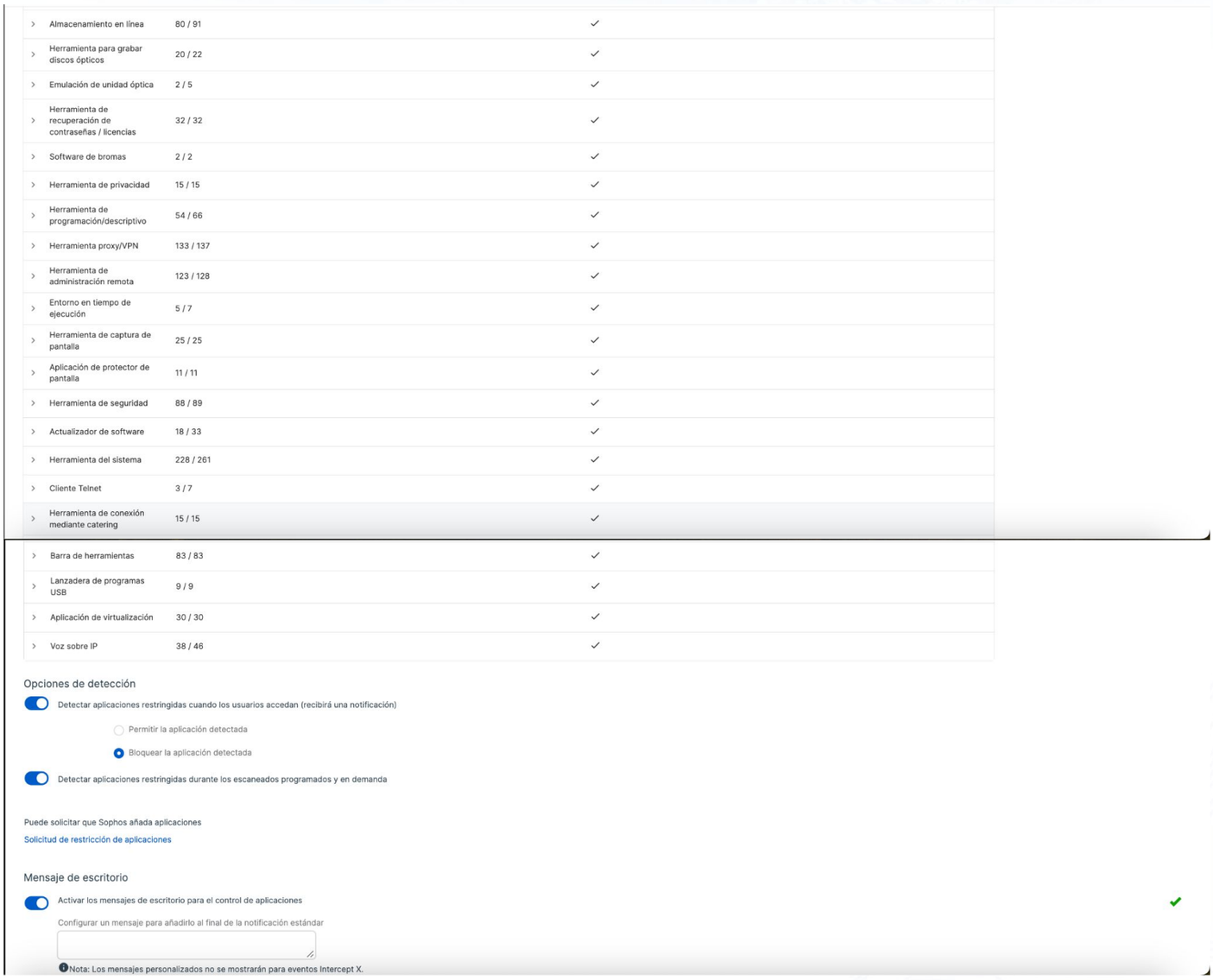
La política se omite: se ignora toda la configuración de esta política. La configuración procederá de otra política.

Seleccione las aplicaciones que desea controlar y especifique las opciones de detección

Añadir/editar lista

Aplicaciones restringidas	Seleccionadas / total	Supervisar nuevas aplicaciones
Vulnerabilidades de las aplicaciones	2 / 2	✓
Herramienta de compresión	9 / 12	✓
Herramienta de gestión de activos	20 / 21	✓
Complemento del navegador	37 / 39	✓
Herramienta de inteligencia comercial	49 / 49	✓
Herramienta CRM	9 / 9	✓
Herramienta de diseño	27 / 42	✓
Buscador de escritorio	9 / 9	✓
Procesado de imágenes	20 / 36	✓
Computación distribuida	8 / 8	✓
Visualizador de documentos	32 / 55	✓
Gestor de descargas	63 / 65	✓
Cliente de correo electrónico/PIM	26 / 34	✓
Herramienta de sincronización de correo electrónico	3 / 4	✓
Herramienta de cifrado/esteganografía	32 / 32	✓
Software ERP	27 / 27	✓
Aplicación de uso compartido de archivos	104 / 104	✓
Cliente FTP	15 / 19	✓
Juego	371 / 371	✓
Mensajería instantánea	129 / 142	✓
Navegador de Internet	102 / 122	✓
Software de desbloqueo	3 / 3	✓
Aplicación de mapas	3 / 6	
Herramienta de conversión multimedia	3 / 19	
Reproductor multimedia	122 / 145	✓
Sincronización móvil	35 / 41	✓
Herramienta de motorización de red / vulnerabilidades	66 / 66	✓
Suite de ofimática	31 / 49	✓

Control de Aplicaciones (Application Control) - Política Personalizada - Application Control:



Almacenamiento en línea	80 / 91	✓
Herramienta para grabar discos ópticos	20 / 22	✓
Emulación de unidad óptica	2 / 5	✓
Herramienta de recuperación de contraseñas / licencias	32 / 32	✓
Software de bromas	2 / 2	✓
Herramienta de privacidad	15 / 15	✓
Herramienta de programación/descriptivo	54 / 66	✓
Herramienta proxy/VPN	133 / 137	✓
Herramienta de administración remota	123 / 128	✓
Entorno en tiempo de ejecución	5 / 7	✓
Herramienta de captura de pantalla	25 / 25	✓
Aplicación de protector de pantalla	11 / 11	✓
Herramienta de seguridad	88 / 89	✓
Actualizador de software	18 / 33	✓
Herramienta del sistema	228 / 261	✓
Cliente Telnet	3 / 7	✓
Herramienta de conexión mediante catering	15 / 15	✓
Barra de herramientas	83 / 83	✓
Lanzadera de programas USB	9 / 9	✓
Aplicación de virtualización	30 / 30	✓
Voz sobre IP	38 / 46	✓

Opciones de detección

Detectar aplicaciones restringidas cuando los usuarios accedan (recibirá una notificación)

Permitir la aplicación detectada

Bloquear la aplicación detectada

Detectar aplicaciones restringidas durante los escaneados programados y en demanda

Puede solicitar que Sophos añada aplicaciones

Solicitud de restricción de aplicaciones

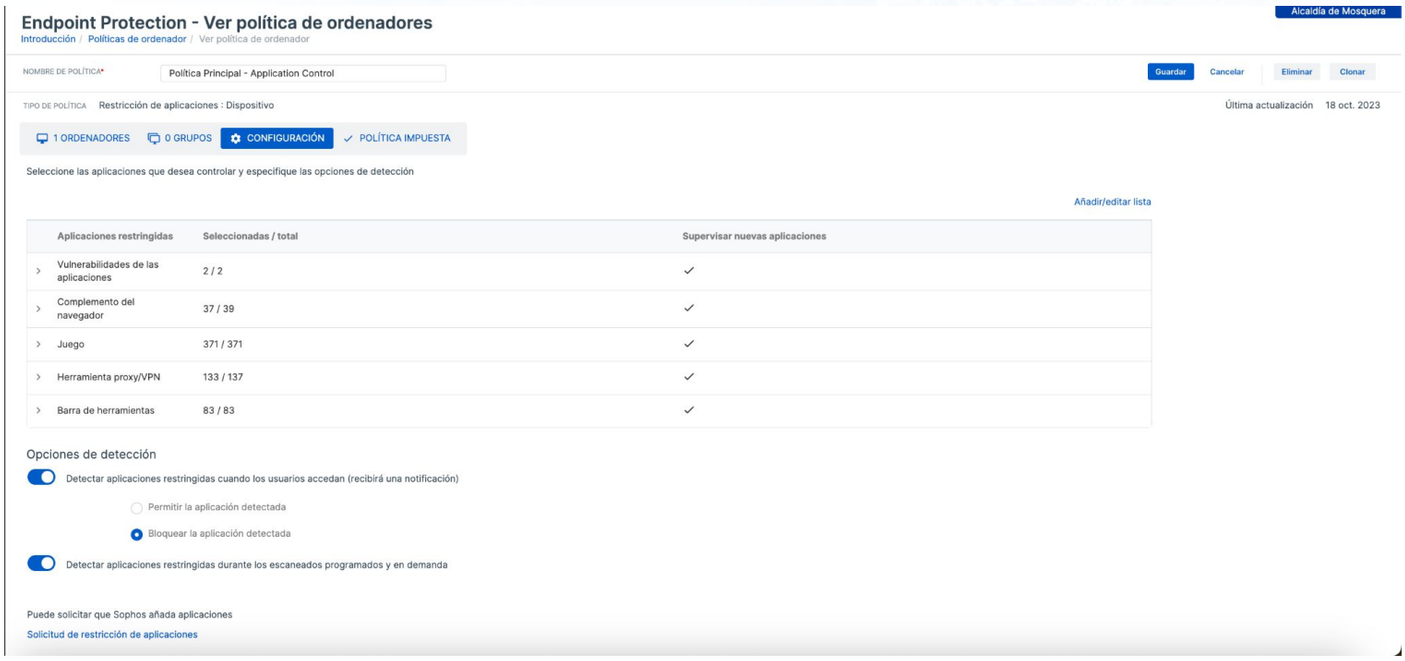
Mensaje de escritorio

Activar los mensajes de escritorio para el control de aplicaciones

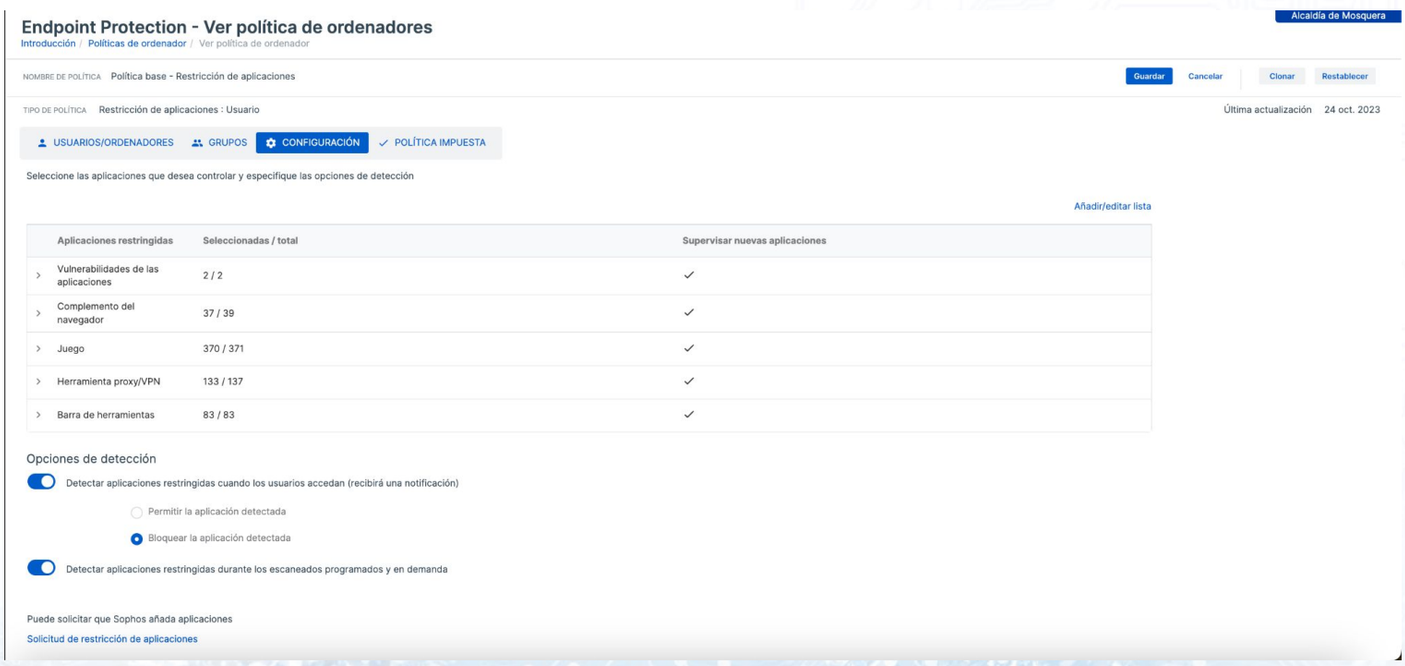
Configurar un mensaje para añadirlo al final de la notificación estándar

Nota: Los mensajes personalizados no se mostrarán para eventos Intercept X.

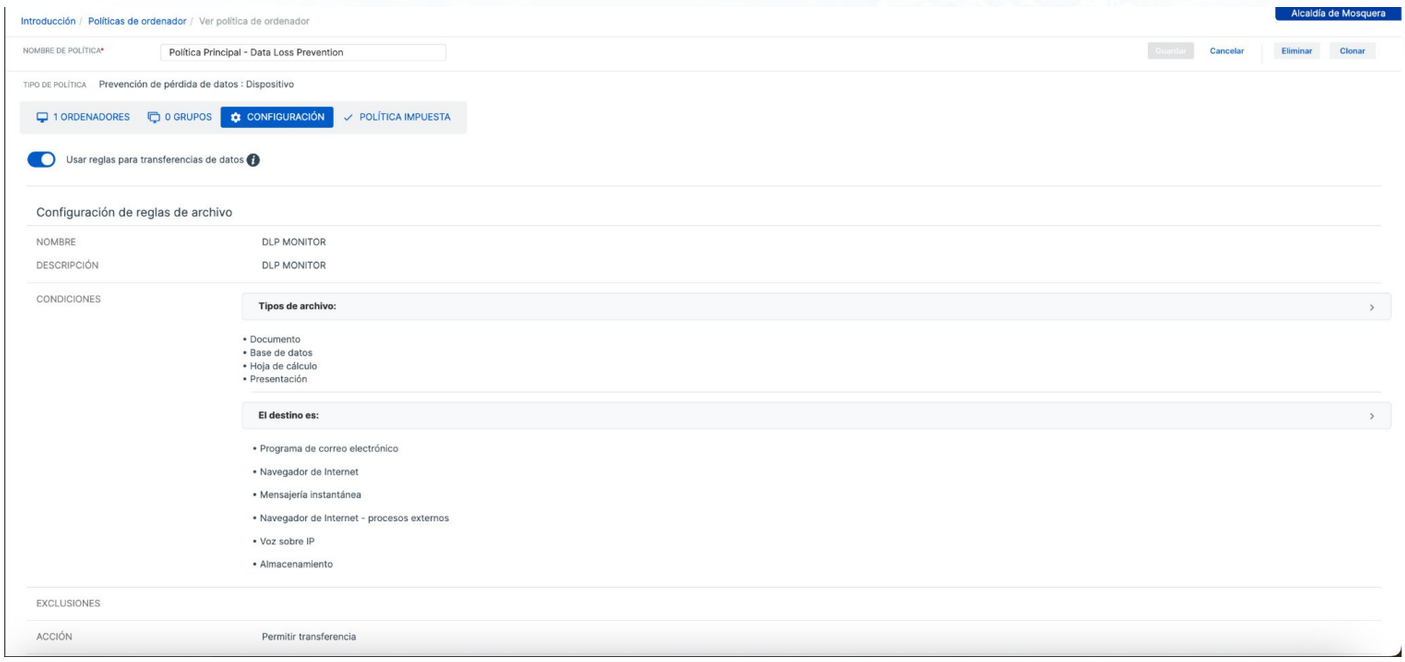
Control de Aplicaciones (Application Control) - Política Principal - Application Control:



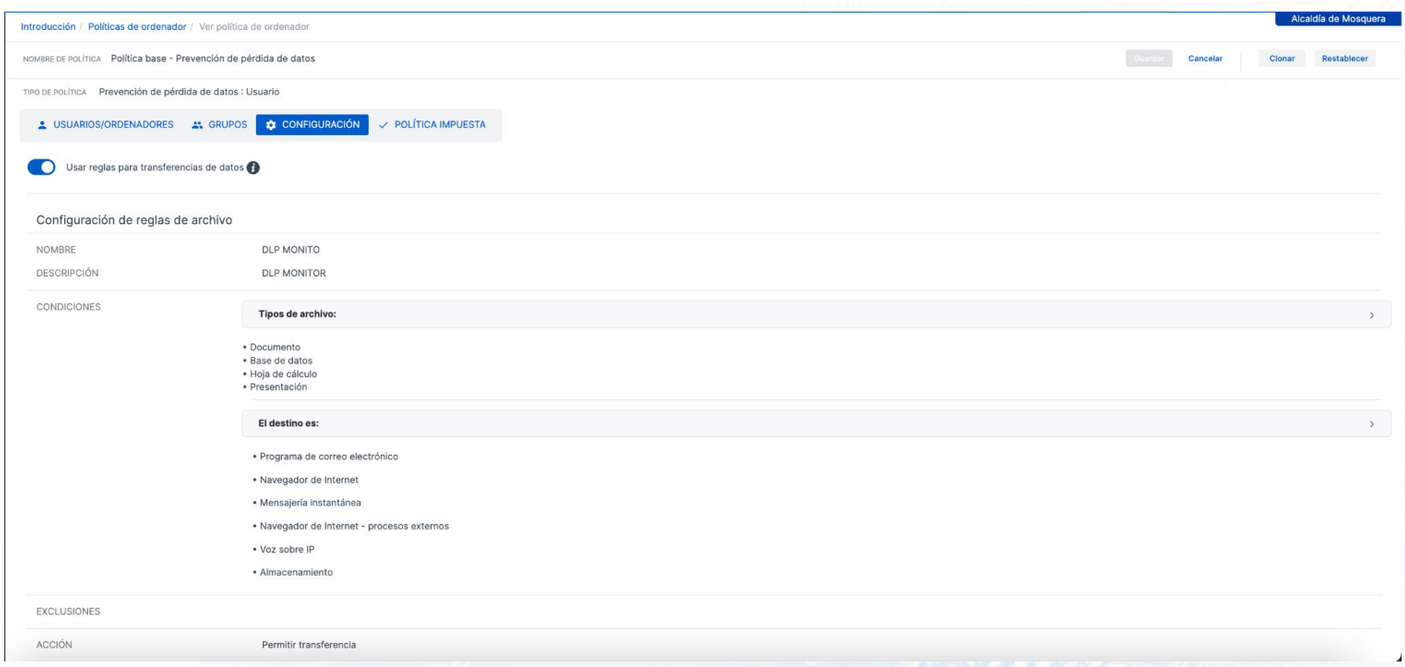
Control de Aplicaciones (Application Control) - Política base - Restricción de aplicaciones:



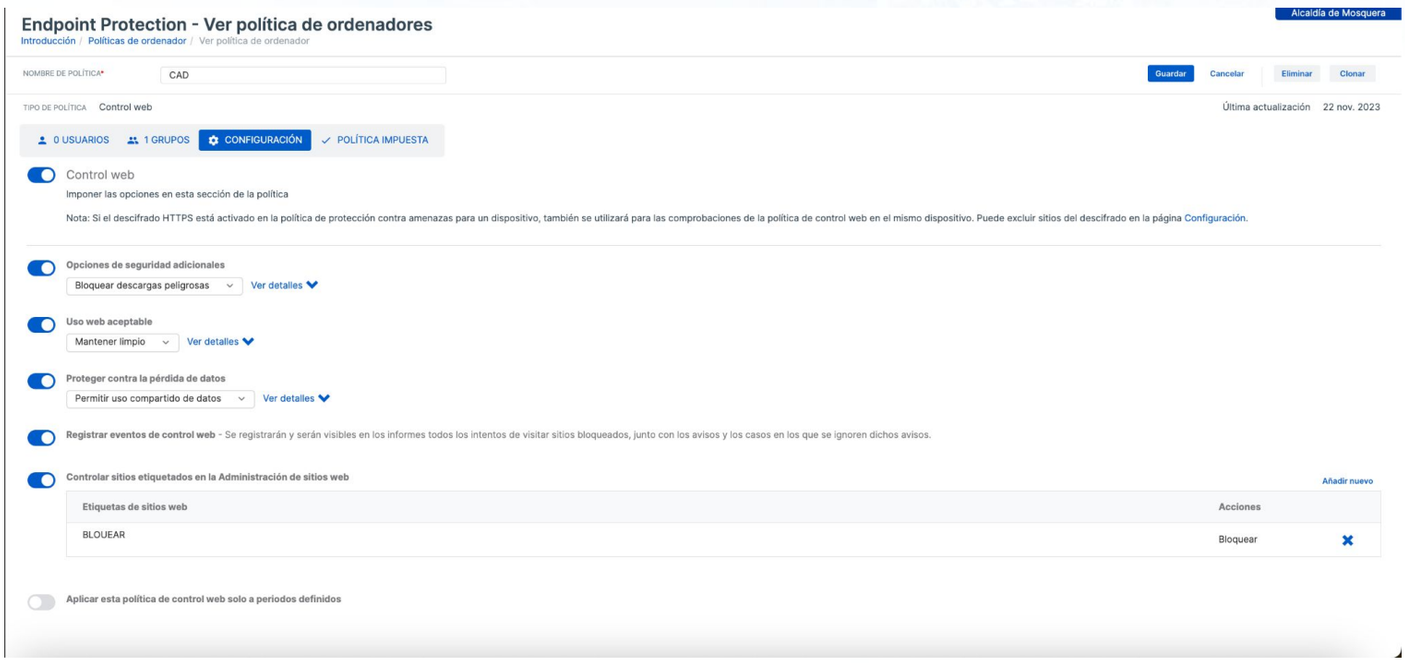
Prevención de pérdida de datos (Data Loss Prevention) - Política Principal - Data Loss Prevention:



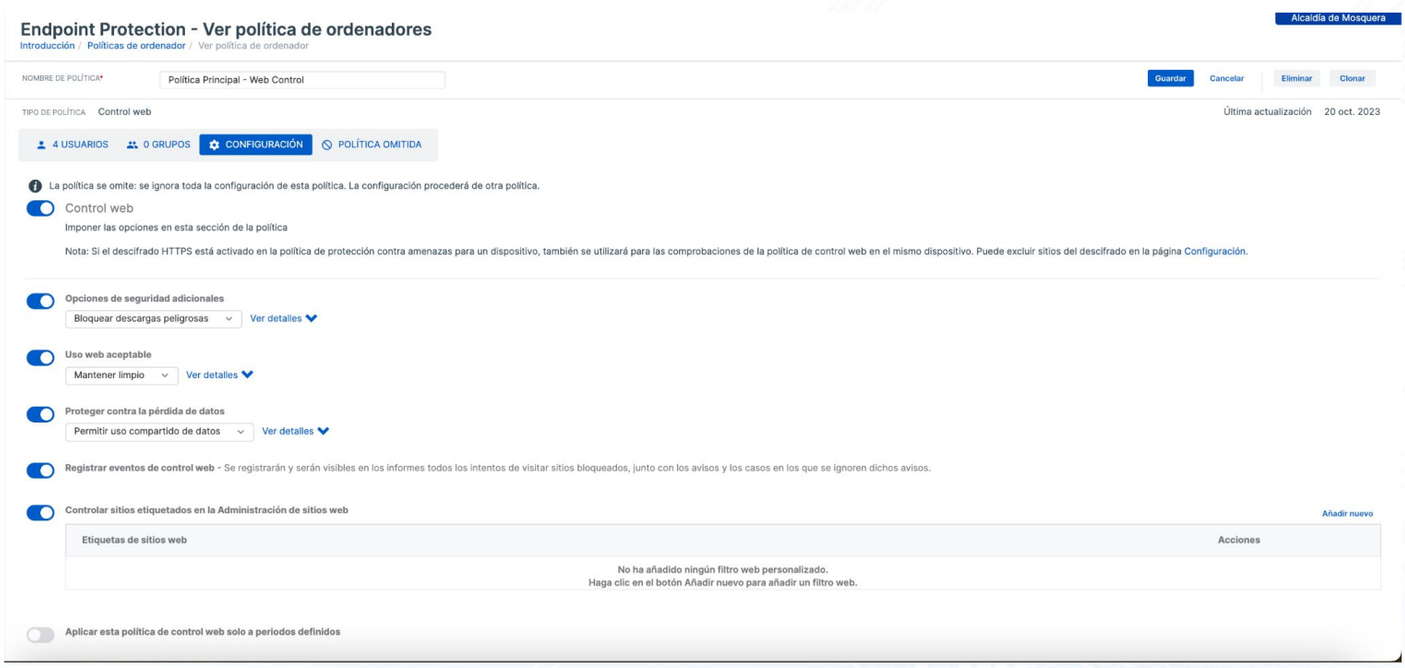
Prevención de pérdida de datos (Data Loss Prevention) - Política base - Prevención de pérdida de datos:



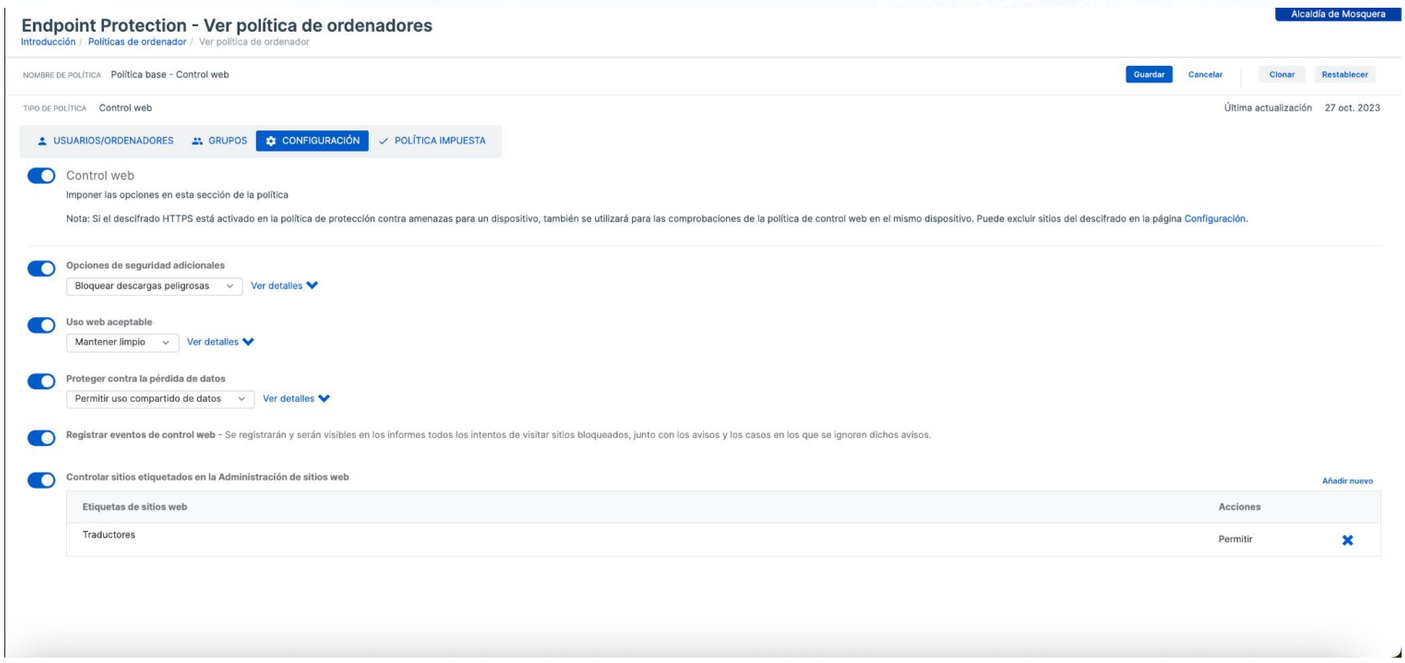
Control Web (Web Control) - CAD:



Control Web (Web Control) - Política Principal - Web Control:



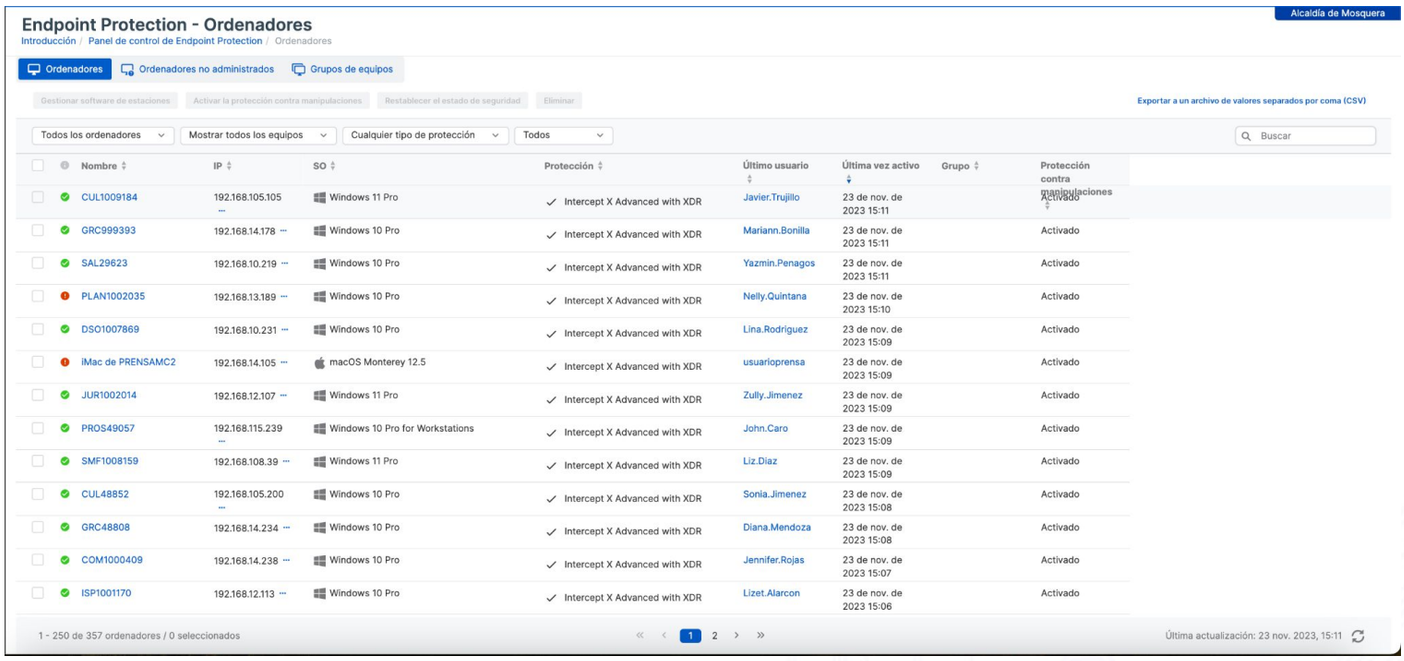
Control Web (Web Control) - Política base - Control web:



Dispositivos

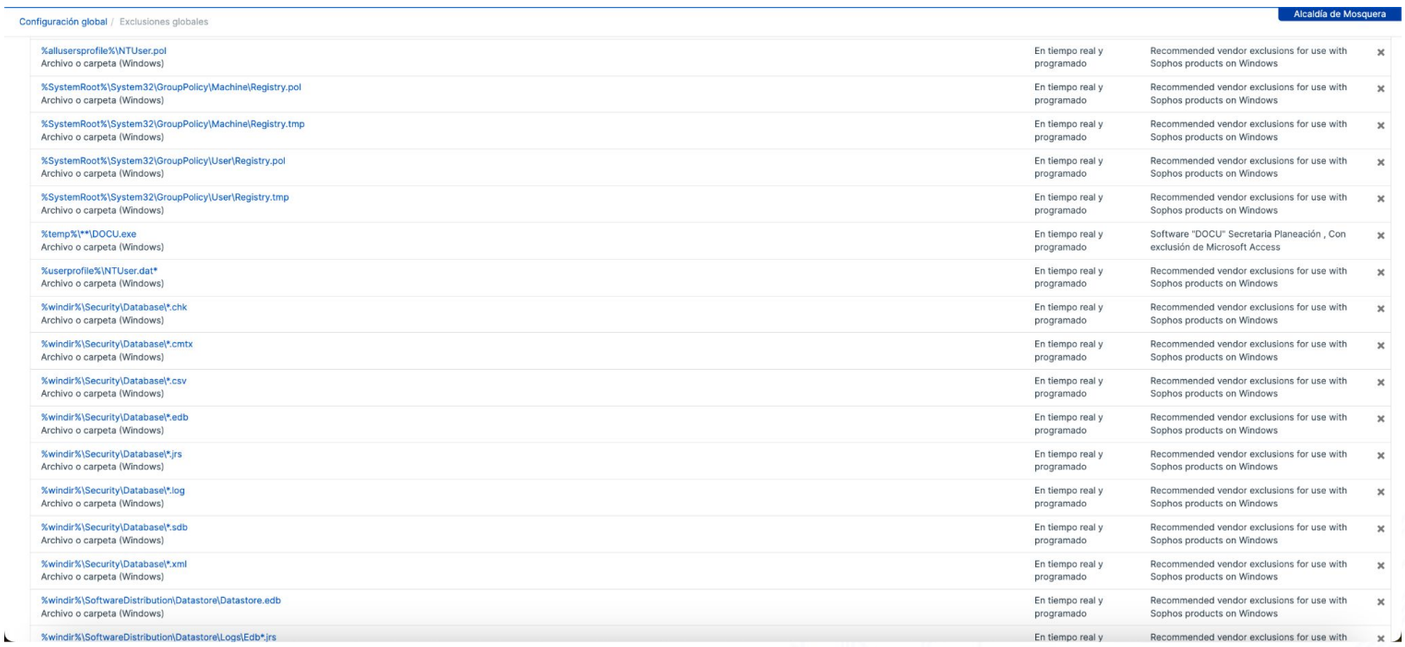
Equipos:

Estaciones de Trabajo Administradas: 357 Dispositivos registrados.
Dispositivos con Alertas Amarillas y Rojas: 24 Dispositivos.



Exclusiones globales (Global Exclusions)

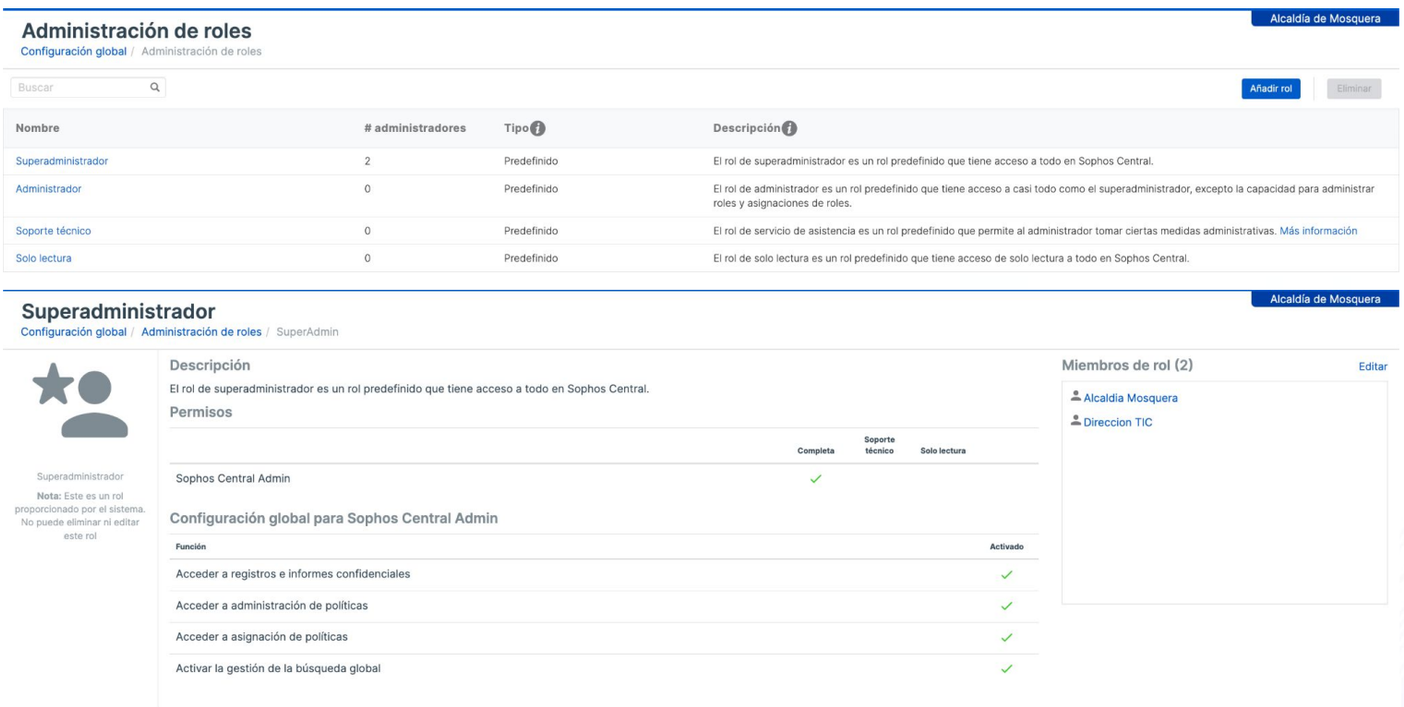
Exclusiones Recomendadas por Sophos y Microsoft



Roles de administración

Los roles de administración dividen la administración de seguridad en función del nivel de responsabilidad. Sophos Central incluye varios roles predefinidos.

El rol de administrador que tiene asignado determina lo que puede hacer.



APROBACIÓN DE CONFIGURACIÓN

Por medio de la presente se deja constancia la aceptación de la configuración realizada a la solución Sophos Central, según lo establecido en el alcance y las pruebas realizadas en conjunto con el equipo de Alcaldía de Mosquera , siendo estas todas satisfactorias.

Se entrega informe de configuración de la Implementación de Sophos Central, realizado por la Gerencia de ingeniería e implementación de Corporación Maestre.

En Bogotá, a los Veinticuatro (24) días del mes de Noviembre de 2023

Yessika Salazar
Gerente. de Ingeniería e Implementación
CORPORACIÓN MAESTRE, S.A.S

Jeofrey Sulbaran
Ing. Implementación y Soporte
CORPORACIÓN MAESTRE, S.A.S

Conforme Aprueba
Mireya Calderon
Supervisora del Contrato
ALCALDÍA DE MOSQUERA