Aranda Security Compliance

Es una solución de monitoreo que permite a las empresas definir las políticas de cumplimiento basado en las normas de seguridad establecidas por la compañía, detectar y visibilizar los riesgo de seguridad en dispositivos de punto final, así como controlar aplicativos, firewall y navegadores encontrados.

Las políticas implementadas se ejecutan de forma automática en los dispositivos donde se encuentra desplegado el agente, facilitando hacer una evaluación activa del dispositivo mediante la validación de cumplimiento de las políticas establecidas y las posterior remediación de los no cumplimientos.

El administrador de Aranda Security podrá conocer de primera mano el estado del endpoint, sobre el cumplimiento de las políticas implementadas; evaluando la vulnerabilidad y riesgos de seguridad en el punto final.

Para empezar

Un usuario de Aranda Security debe considerar tres etapas esenciales para la gestión y seguimiento de las políticas de cumplimiento.

La primera etapa el administrador se encarga de definir las políticas de cumplimiento que se requieren implementar y asociarlas a un grupo de dispositivos.

La segunda etapa se realiza el despliegue o distribución del agente de Aranda Security encargado de establecer la comunicación con los dispositivos.

La tercera etapa es el proceso de monitoreo de los dispositivos para identificar y hacer el seguimiento del cumplimiento de las políticas.

Para quién es este manual?

Esta manual está diseñado para un administrador que pueda definir las políticas, asociar grupos, configurar usuarios, consultar y hacer seguimiento a las políticas y establecer las tareas correctivas.

Esta manual está diseñado para un especialista que pueda definir las políticas, asociar grupos, consultar y hacer seguimiento a las políticas definidas.

Cuál es el valor de Aranda Security?

- Es el complemento ideal de las soluciones de seguridad que funcionan en la infraestructura de la compañía, integrando los requerimientos regulatorios a las políticas de cumplimiento.
- Identifica las vulnerabilidades en los dispositivos monitoreados, reduciendo brechas de seguridad y mitigando riesgos.
- Alta demanda de Soluciones orientadas a Seguridad

¿Cuál es nuestra documentación?

- Guia de Inicio Aranda Security Compliance ASEC
- Manual de Usuario Aranda Security Compliance ASEC

Definición Políticas

Definición Políticas ASEC

Una política es una entidad que define las reglas y condiciones asociadas a componentes de seguridad, que se aplican a un programa bajo criterios que cumplen los marcos regulatorios de protección de la información.

La definición y configuración de políticas de Seguridad permiten establecer mecanismos de diagnóstico,control y protección de la información en diferentes niveles.

Quién define las políticas

El administrador y especialista son los roles establecidos en ASEC que podrán definir los criterios de cumplimiento de las políticas.

Estructura de las políticas

Una política en Aranda Security está compuesta por los siguientes criterios

- **Datos básicos**: Información básica de la política como nombre, estado, descripción y tiempo de monitoreo.
- **Criterios de configuración**: Cada política en Aranda Security agrupa las aplicaciones o componentes de seguridad requeridos en una estación de trabajo, en categorías de acuerdo a su función. Los criterios habilitados en ASEC son: ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT y WEB BROWSER.

> **Nota:** Para entender el alcance de las validaciones por cada uno de los programas de seguridad que agrupan los criterios de políticas de ASEC, de acuerdo al sistema operativo (windows, linux y mac), conozca cómo Visualizar el Listado de Aplicaciones de seguridad

- **Validaciones**: Son los parámetros encargados de verificar, de acuerdo al programa escogido por criterio de configuración, el cumplimiento de las políticas de seguridad en cada una de las estaciones de trabajo. Validaciones por criterio de configuración.

- **Grupos de Dispositivos**: Agrupación de dispostivos vinculados con el agente de ASEC, para ser asociados a la política de cumplimiento.

En la sección de políticas de la consola de Aranda Security Compliance, podrá definir las políticas de cumplimiento.

Qué hace una política en un dispositivo?

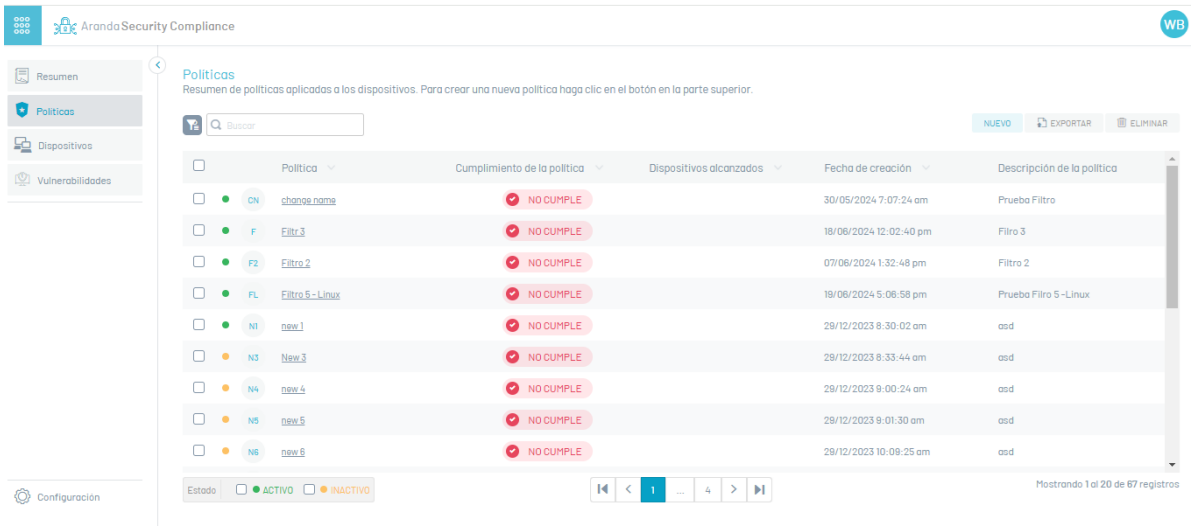
Establece los lineamientos de seguridad para detectar y responder ante posibles vulnerabilidades

Gestionar Políticas

En el proceso de gestión y administración de las políticas de cumplimiento en la aplicación Aranda Security podrá visualizar, crear, editar y eliminar las políticas de seguridad.

Visualizar Políticas

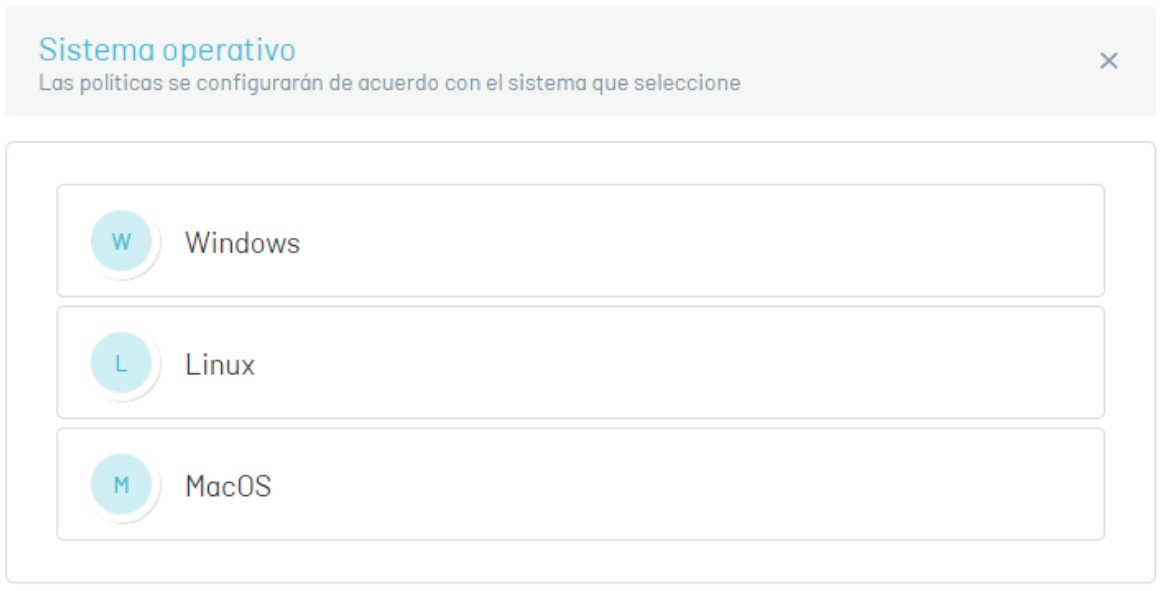
1. Ingrese a la consola de Aranda Security Compliance con rol de administrador, seleccione la opción **Políticas** del menú principal. En la vista de información se podrá visualizar el listado políticas disponibles y ordenar la información agrupada por nombre, dispositivos alcanzados (asociados a la política) y fecha de creación.

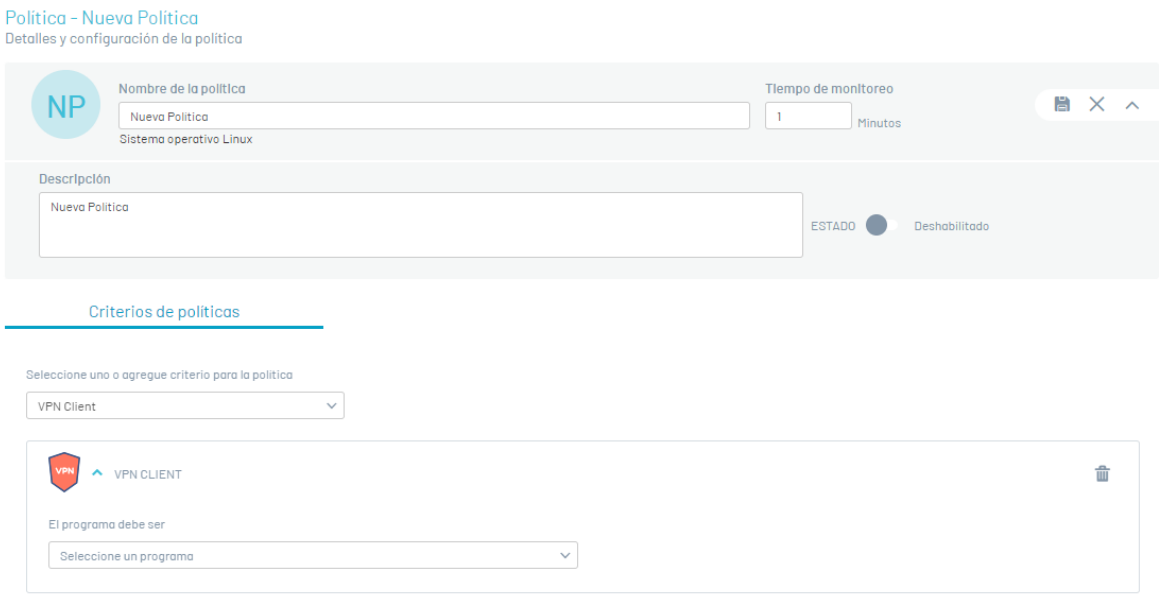


2. En la vista de información de las políticas, tendrá disponibles acciones de gestión y organización de la información.
[Vista de Información en Entorno Web ASEC]

Creación de Políticas

1. Para crear una política, ingrese a la consola de Aranda Security con rol de administrador o especialista, en la sección de **Políticas** del menú principal. En la vista de información seleccione el botón **Nuevo**; se habilita la ventana **Sistema Operativo**, seleccione un Sistema Operativo para continuar con el formulario donde debe ingresar la información básica de la política:



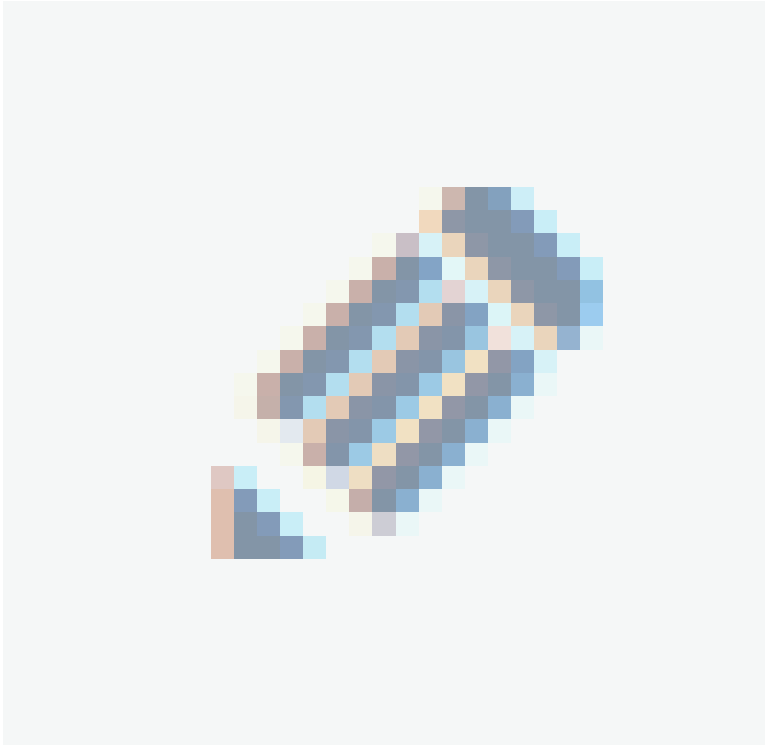


Campo	Descripción
Nombre de la política	Nombre que identifica la política.
Descripción	Descripción de la política.
Estado	Estado de la política, se indica si va iniciar Activa inmediatamente, o va iniciar Inactiva.
Tiempo de Monitoreo	Intervalo de tiempo donde los agentes van estar notificando el cumplimiento de la política.

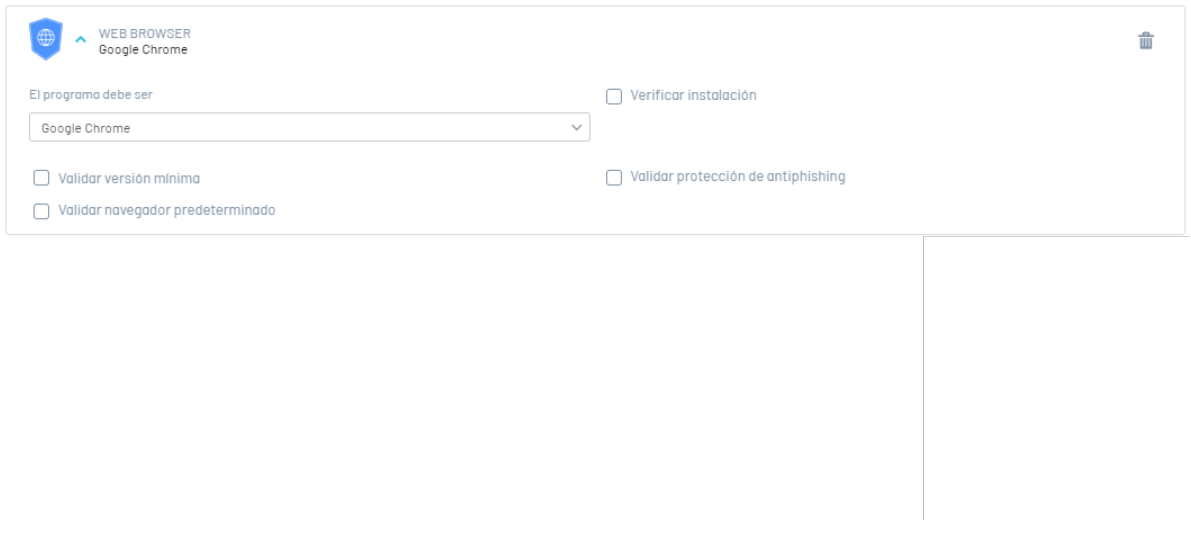
Criterios de Políticas

2. En la vista de información para la nueva política, seleccione la pestaña **criterios de politicas** y escoja del listado un criterio de software de configuración. Los criterios habilitados en ASEC son: ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT y WEB BROWSER.

3. Al seleccionar el criterio de software (Antimalware, browser, firewall), haga clic en el ícono **Editar**

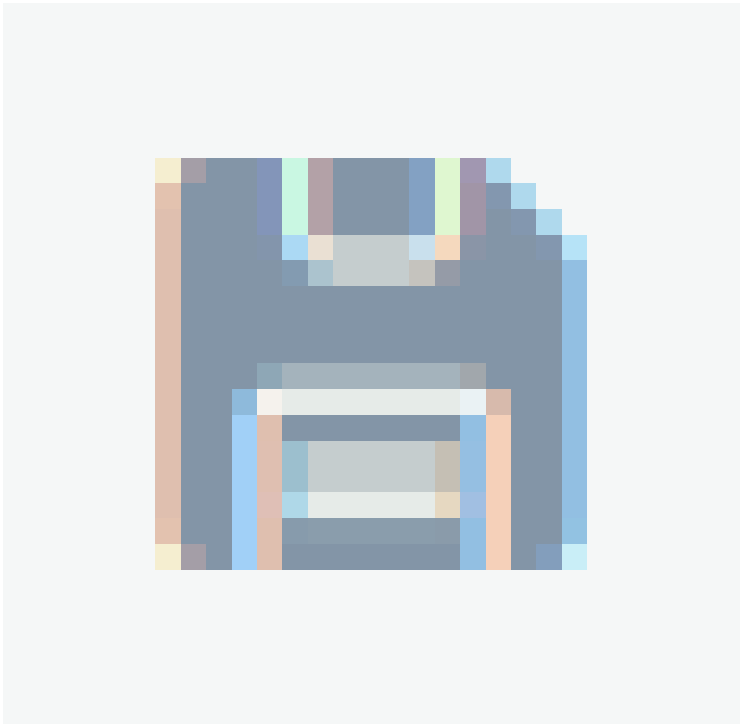


y elija un programa del listado existente.



⚐ **Nota:** Al seleccionar un programa del criterio de la política se activan los métodos o validaciones correspondientes al programa definido. Para cada programa se activarán distintos opciones de validación. Ver validaciones por criterio de configuración

4. Seleccione los items de validación habilitados para determinar los niveles de cumplimiento de esa instancia de la política de seguridad y haga clic en el botón **Guardar**



, para confirmar los cambios realizados.

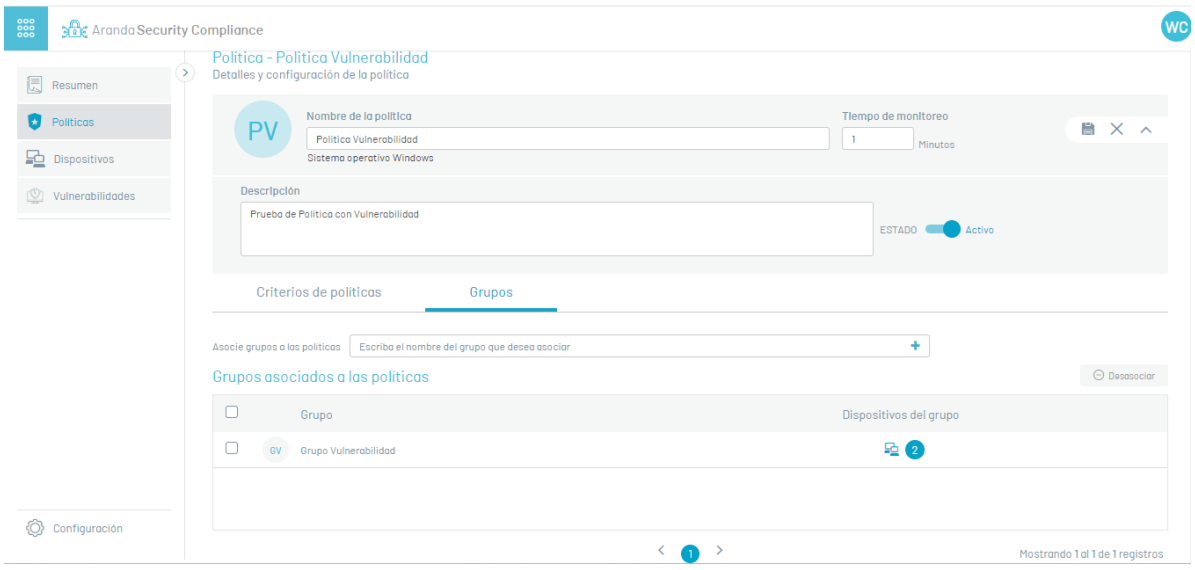
Estos criterios son los que se evalúan y determinan si una política se cumple o no.

⚐ **Nota:** Para eliminar los detalles del criterio de software, en cualquier momento, haga clic en el ícno respectivo para borrar la configuración.

5. Después de creada una política se habilita la pestaña para asociar grupos de dispositivos a la política definida.

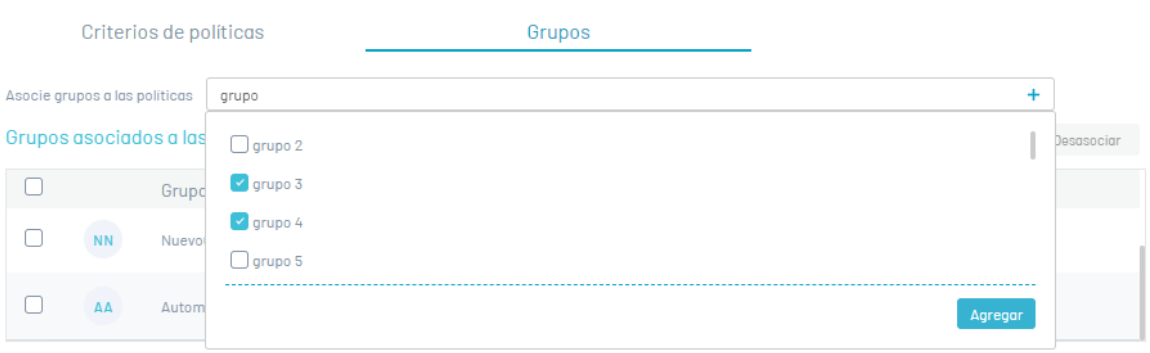
Asociar Grupos

6. Al terminar de configurar la información básica de la política, ingrese de nuevo a la consola de Aranda Security y seleccione la política creada; en la vista de información se habilita la pestaña **Grupos** donde podrá asociar grupos de dispositivos a la política definida.



7. En el campo **Asociar Grupos** ingrese un nombre para buscar un grupo o digite un nombre para crear un nuevo grupo. Haga clic en el botón **(+)** para crear un nuevo grupo. Cada política podrá contener muchos grupos.

8. Para asociar un grupo creado a la política, seleccione un grupo del listado disponible y haga clic en el botón **Agregar**

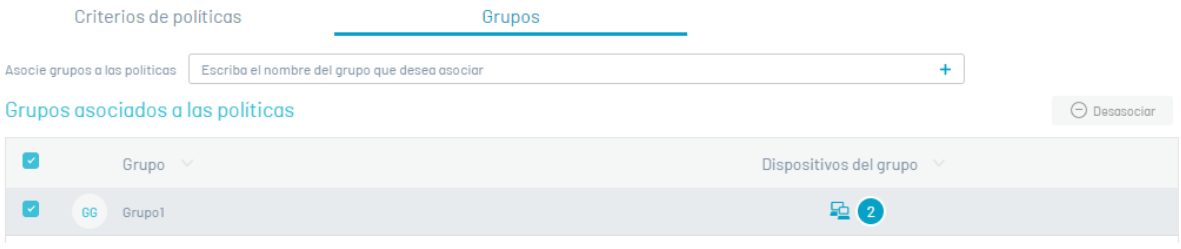


9. En el listado de grupos asociados seleccione el nombre del grupo con dispositivos vinculados, para acceder al [detalle de Cumplimiento de los Dispositivos](#).

Desasociar Grupos

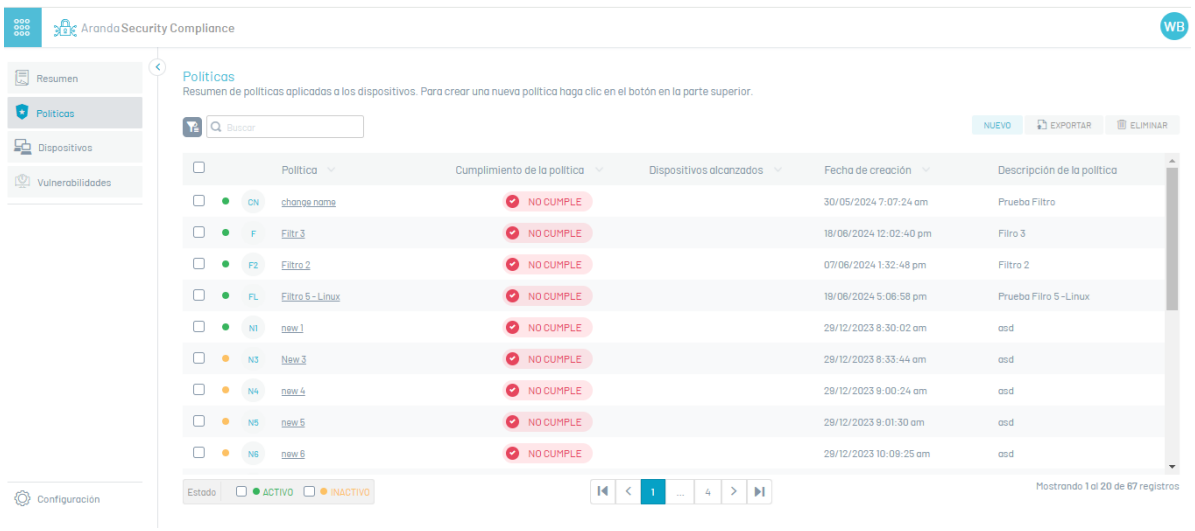
10. Para eliminar uno o varios grupos, en la vista de información de la política, en la pestaña **Grupos**, seleccione un registro de los grupos creados y haga clc en el botón **Desasociar** para borrar la información asociada.

11. Al definir los grupos para la política haga clic en el botón **Guardar**, para confirmar los cambios realizados.

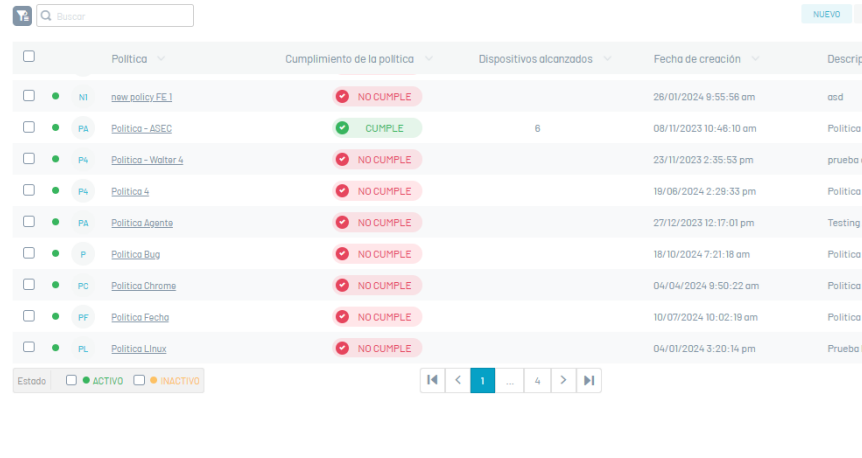


Eliminar Políticas

12. Para eliminar políticas ingrese a la consola de Aranda Security con rol de administrador, en la sección de **Políticas** del menú principal. En la vista de información se podrá visualizar el listado de políticas disponibles; seleccione uno o varios registros y haga clic en el botón **Eliminar Políticas**.



13. Se habilita un mensaje de advertencia donde debe confirmar el borrado de la política.

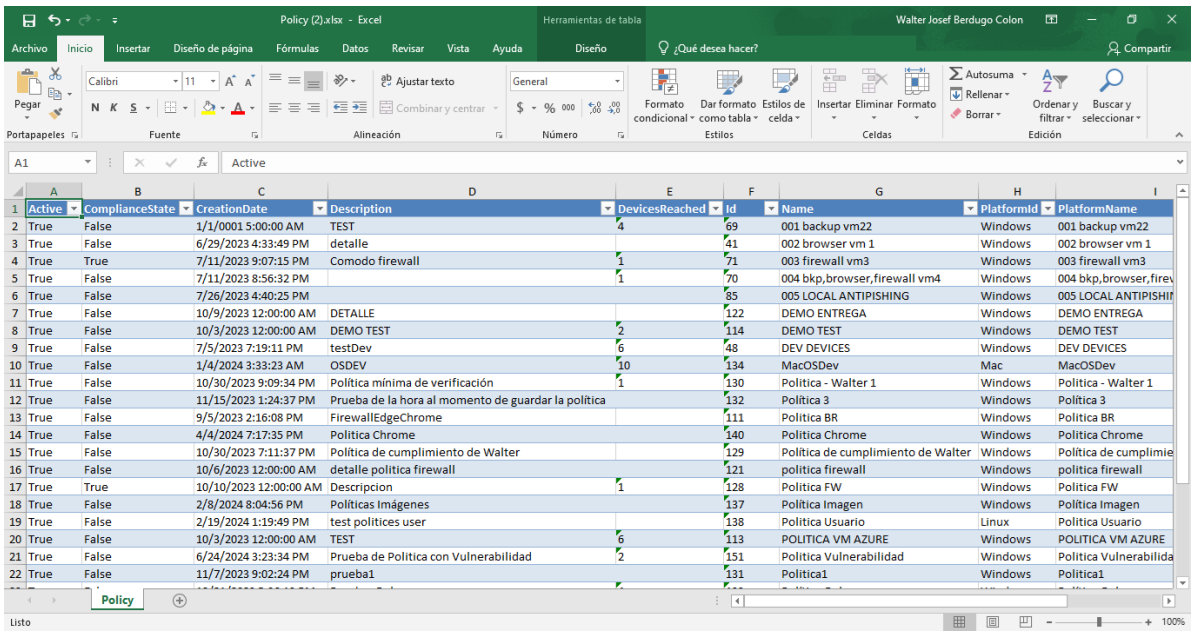


Exportar Políticas

1. Para exportar la información de políticas, ingrese a la consola de Aranda Security con rol de administrador, en la sección de **Políticas** del menú principal. En la vista de información se podrá visualizar el listado políticas disponibles; filtre uno o varios registros en el campo **Buscar** y haga clic en el botón **Exportar**.

2. En el menú encabezado de la consola de administración de Aranda Security, se habilita la oción de **Descargas** donde podrá visualizar el formato generado del listado de políticas en formato excel

3. Haga clic en el archivo para descargar la información de las políticas. El archivo descargado incluye todos los campos de la política.



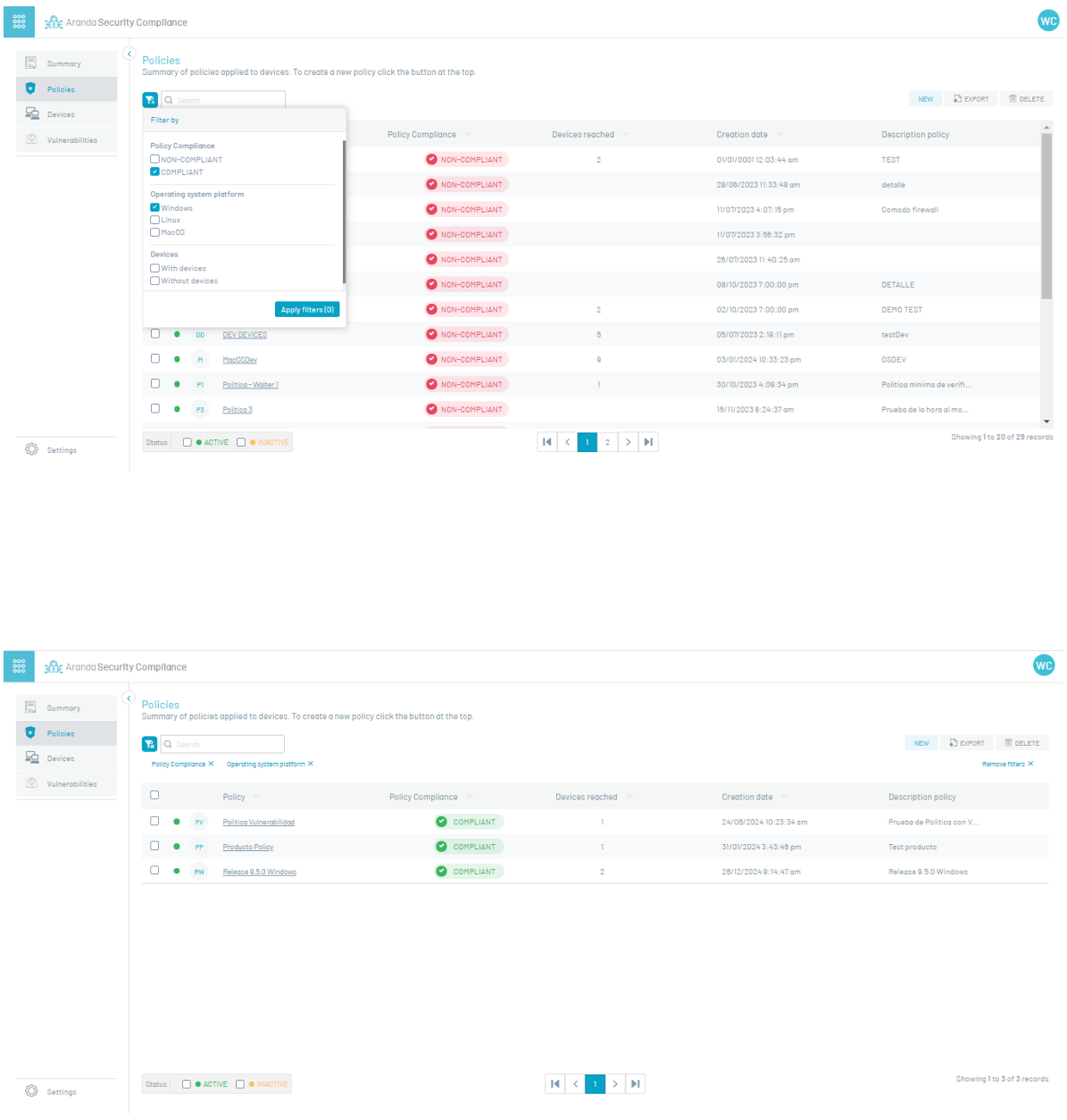
	A	B	C	D	E	F	G	H	I
1	Active	ComplianceState	CreationDate	Description	DevicesReached	Id	Name	PlatformId	PlatformName
2	True	False	1/1/0001 5:00:00 AM	TEST	4	69	001 backup vm22	Windows	001 backup vm22
3	True	False	6/29/2023 4:33:49 PM	detalle		41	002 browser vm 1	Windows	002 browser vm 1
4	True	True	7/11/2023 9:07:15 PM	Comodo firewall	1	71	003 firewall vm3	Windows	003 firewall vm3
5	True	False	7/11/2023 8:56:32 PM		1	70	004 bkp,browser,firewall vm4	Windows	004 bkp,browser,firev
6	True	False	7/26/2023 4:40:25 PM			85	005 LOCAL ANTIPISHING	Windows	005 LOCAL ANTIPISHI
7	True	False	10/9/2023 12:00:00 AM	DETALLE		122	DEMO ENTREGA	Windows	DEMO ENTREGA
8	True	False	10/3/2023 12:00:00 AM	DEMO TEST	2	114	DEMO TEST	Windows	DEMO TEST
9	True	False	7/5/2023 7:19:11 PM	testDev	6	48	DEV DEVICES	Windows	DEV DEVICES
10	True	False	1/4/2024 3:33:23 AM	OSDEV	10	134	MacOSDev	Mac	MacOSDev
11	True	False	10/30/2023 9:09:34 PM	Política mínima de verificación	1	130	Politica - Walter 1	Windows	Politica - Walter 1
12	True	False	11/15/2023 1:24:37 PM	Prueba de la hora al momento de guardar la política		132	Política 3	Windows	Política 3
13	True	False	9/5/2023 2:16:08 PM	FirewallEdgeChrome		111	Política BR	Windows	Política BR
14	True	False	4/4/2024 7:17:35 PM	Política Chrome		140	Política Chrome	Windows	Política Chrome
15	True	False	10/30/2023 7:11:37 PM	Política de cumplimiento de Walter		129	Política de cumplimiento de Walter	Windows	Política de cumplimie
16	True	False	10/6/2023 12:00:00 AM	detalle política firewall		121	política firewall	Windows	política firewall
17	True	True	10/10/2023 12:00:00 AM	Descripcion	1	128	Política FW	Windows	Política FW
18	True	False	2/8/2024 8:04:56 PM	Políticas Imágenes		137	Política Imagen	Windows	Política Imagen
19	True	False	2/19/2024 1:19:49 PM	test polities user		138	Política Usuario	Linux	Política Usuario
20	True	False	10/3/2023 12:00:00 AM	TEST	6	113	POLITICA VM AZURE	Windows	POLITICA VM AZURE
21	True	False	6/24/2024 3:23:34 PM	Prueba de Política con Vulnerabilidad	2	151	Política Vulnerabilidad	Windows	Política Vulnerabilida
22	True	False	11/7/2023 9:02:24 PM	prueba1		131	Política1	Windows	Política1

Filtrar Políticas

1. En la vista de información de Políticas seleccione el Filtro de políticas (ícono) y active los criterios de consulta como Cumplimiento de la política, Plataforma del sistema operativo y Dispositivos. Al terminara haga clic en el botón Aplicar Filtros.

2. Adicionalmente podrá combinar la consulta, utilizando el filtro por estado de la política para tener una vista más detallada y personalizada.

⚐ **Nota:** Aplicar los filtros de la política y filtro por estados permite identificar dispositivos o sistemas que requieren seguimiento, acciones correctivas o atención prioritaria.



Validaciones por Criterios

Las políticas configuradas en Aranda Security evaluan los niveles de cumplimiento de aplicaciones de seguridad en diferentes estaciones de trabajo. Este diagnóstico es posible por las validaciones que se aplican para los diferentes programas de criterios de políticas

Para cada programa de seguridad se activarán distintos opciones de validación. Cada validación podrá ser utilizada

en los criterios de política disponibles.

Las opciones de validación disponibles en Aranda Security son:

Criterios de Políticas	Validaciones
	1. Validar navegador predeterminado. 2. Validar estado de protección en tiempo real. 3. Validar estado de ejecución. 4. Validar instalación. 5. Validar protección firewall. 6. Validar protección de antiphishing. 7. Validar versión mínima. 8. Validar estado de la copia de seguridad

⚐ **Nota:** Para entender el alcance de las validaciones por cada uno de los programas de seguridad que agrupan los criterios de políticas de ASEC, de acuerdo al sistema operativo (windows, linux y mac), conozca cómo Visualizar el Listado de Aplicaciones de seguridad.

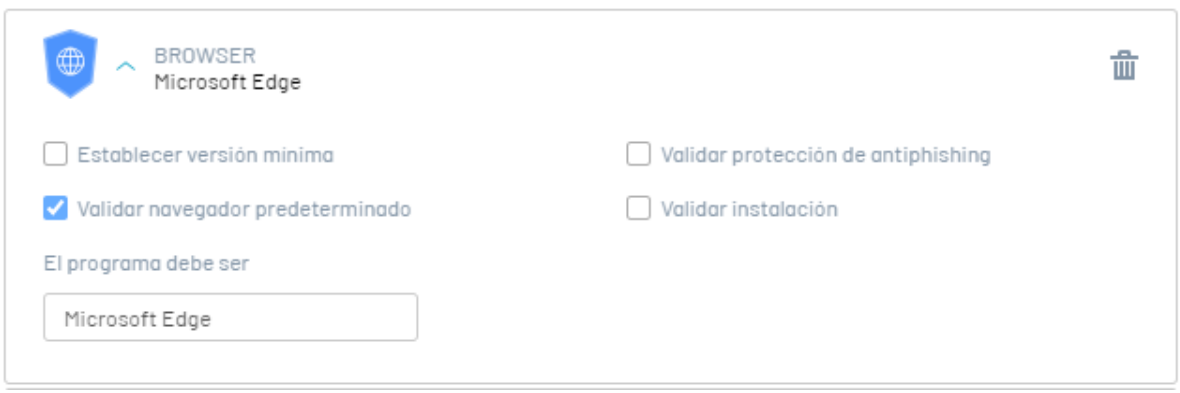
A continuación podrá encontrar algunos casos en la configuración de criterios de políticas y sus validaciones:

1. Validar Navegador Predeterminado

Esta opción valida que el navegador seleccionado esté configurado como navegador predeterminado en la estación de trabajo. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el navegador está configurado como predeterminado en la estación de trabajo.
NO CUMPLE	Si el navegador no está configurado como predeterminado o si no está instalado

Ejemplo	Se valida en la estación de trabajo si el programa **Microsoft Edge** está configurado como predeterminado.

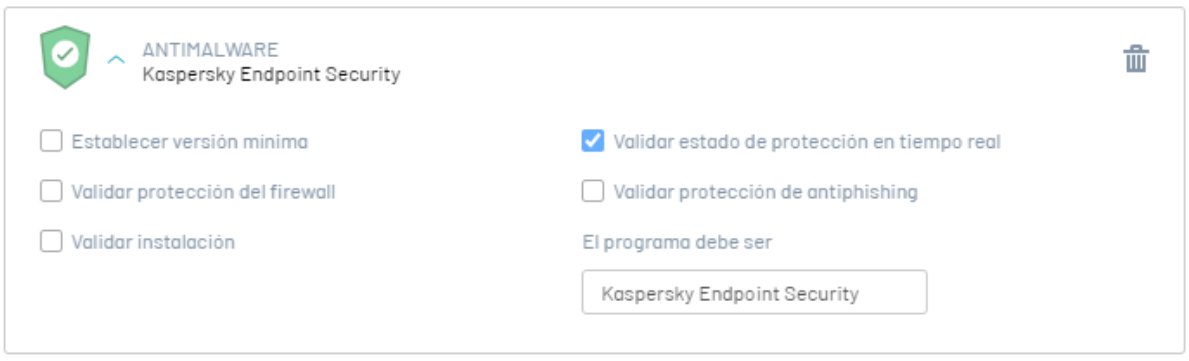


2. Validar Estado de Protección en Tiempo Real

Esta opción valida que el software tenga habilitada la protecció en tiempo real. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el software tiene habilitada la proteccion en tiempo real.
NO CUMPLE	Si el software NO tiene habilitada la protección en tiempo real o si no está instalado.

Ejemplo	Se valida que el sofware **Kaspersky Endpoint Security** tenga la protección en tiempo real habilitada.

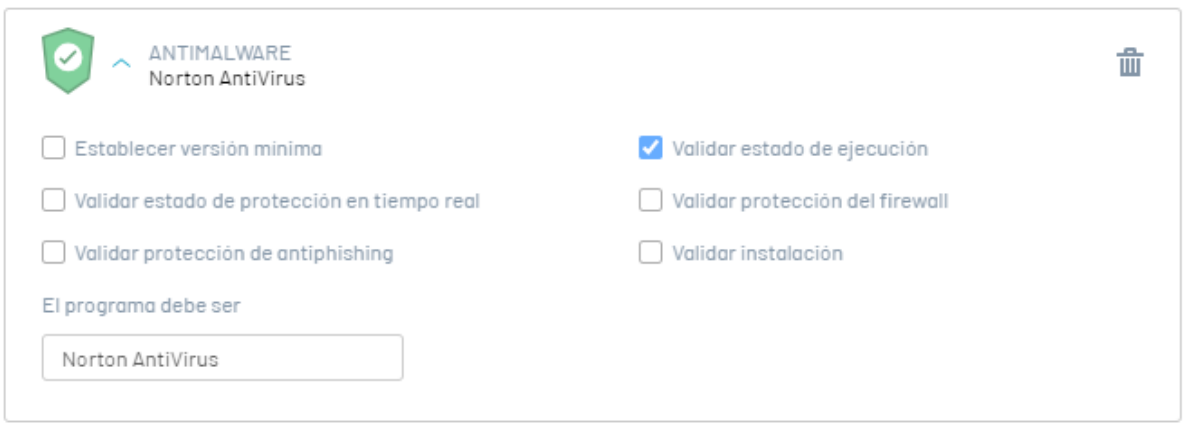


3. Validar Estado de Ejecución

Esta opción valida si el software se está ejecutando en la estación de trabajo. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el software se está ejecutando.
NO CUMPLE	si el software NO se está ejecutando o si no está instalado.

Ejemplo	Se valida si el **Software Norton Antivirus** se está ejecutando.



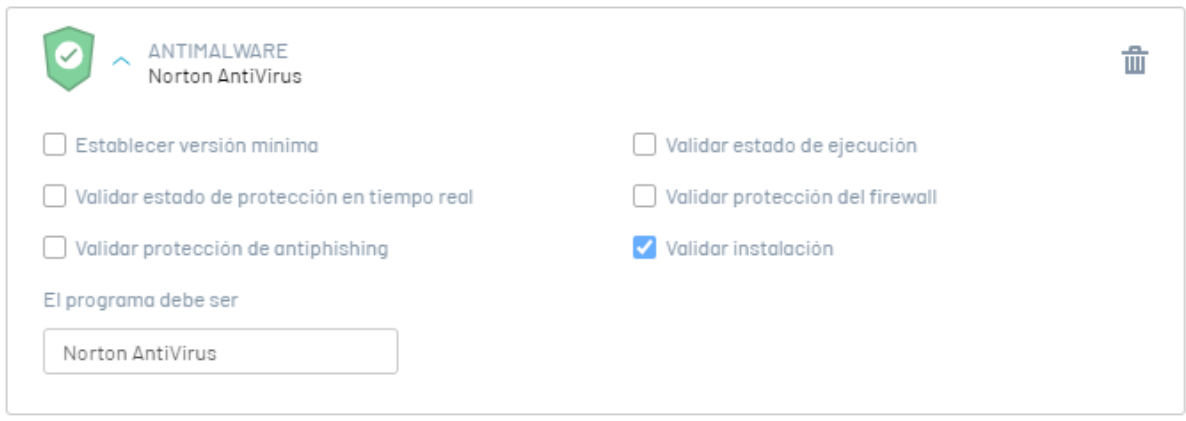
4. Validar Instalación

Esta opción valida si el software se encuentra instalado en la estación de trabajo. Las opciones de respuesta a la

validación son:

Retorno	Descripción
CUMPLE	Si el software está instalado.
NO CUMPLE	si el software NO está instalado.

Ejemplo	Se valida si el **Software Norton Antivirus** se encuentra instalado en la estación de trabajo.



5. Validar Proteccion Firewall

Esta opción valida si el software tiene habilitada la protección de FIREWALL. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el software tiene habilitada la protección de FIREWALL.
NO CUMPLE	Si el software NO tiene habilitada la protección de FIREWALL o si No está instalado.

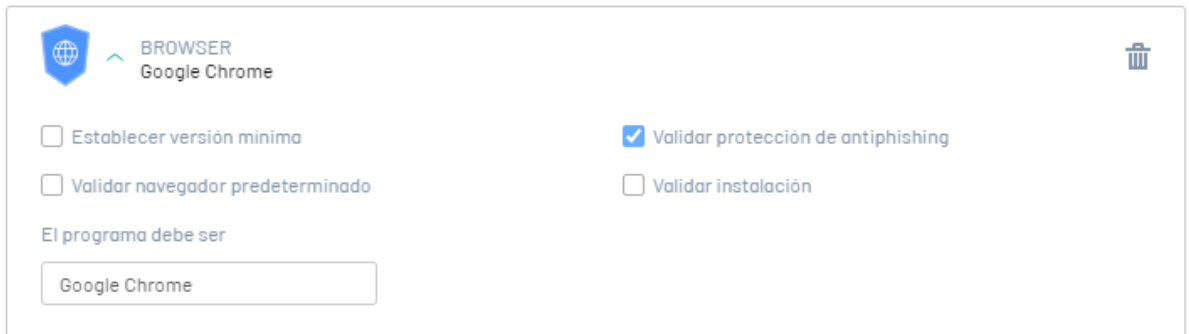
Ejemplo	Valida que el sofware **Windows Firewall** tenga activa la protección del FIREWALL.

6. Validar Proteccion Antipishing

Esta opción valida si el software tiene habilitada la protección Antipishing. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el software tiene habilitada la protección Antipishing.
NO CUMPLE	Si el software NO tiene habilitada la protección Antipishing o si No está instalado el software.

Ejemplo	Valida que el sofware **google Chrome** tenga activa la protección Antipishing.



7. Establecer Versión Mínima

Esta opción establece una versión mínima para posteriormente validarla contra la versión instalada en la estación de trabajo. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Se cumple este criterio cuando se especifica una versión completa o cuando la versión es mayor a una versión parcial
NO CUMPLE	No se cumple el criterio cuando el software instalado tiene una versión diferente o menor, dependiendo el caso.

Ejemplo	Valida que la versión de **AVG internet security** instalada en la estación de trabajo sea mayor o igual a la versión 1.0.1

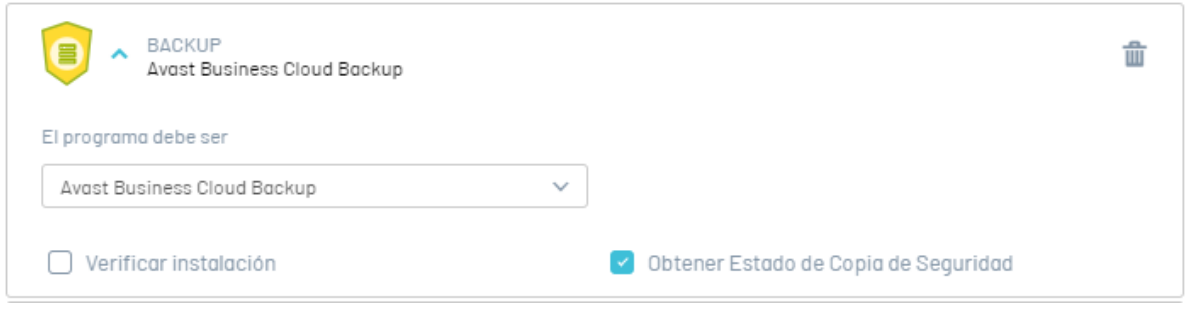
|**Ejemplo**|Valida que la versión de **Sea Monkey** instalada en la estación de trabajo sea mayor o igual a la versión 1.0.1

8. Validar estado de Copia de Seguridad

Esta opción valida el estado de la copia de seguridad del software. Las opciones de respuesta a la validación son:

Retorno	Descripción
CUMPLE	Si el software tiene habilitada la opción de obtener el estado de copia de seguridad.
NO CUMPLE	Si el software NO tiene habilitada la opción de obtener el estado de copia de seguridad.

Ejemplo	Se valida que se pudea obtener el estado de copia de seguridad del sofware **Avast Business Cloud Backup** .

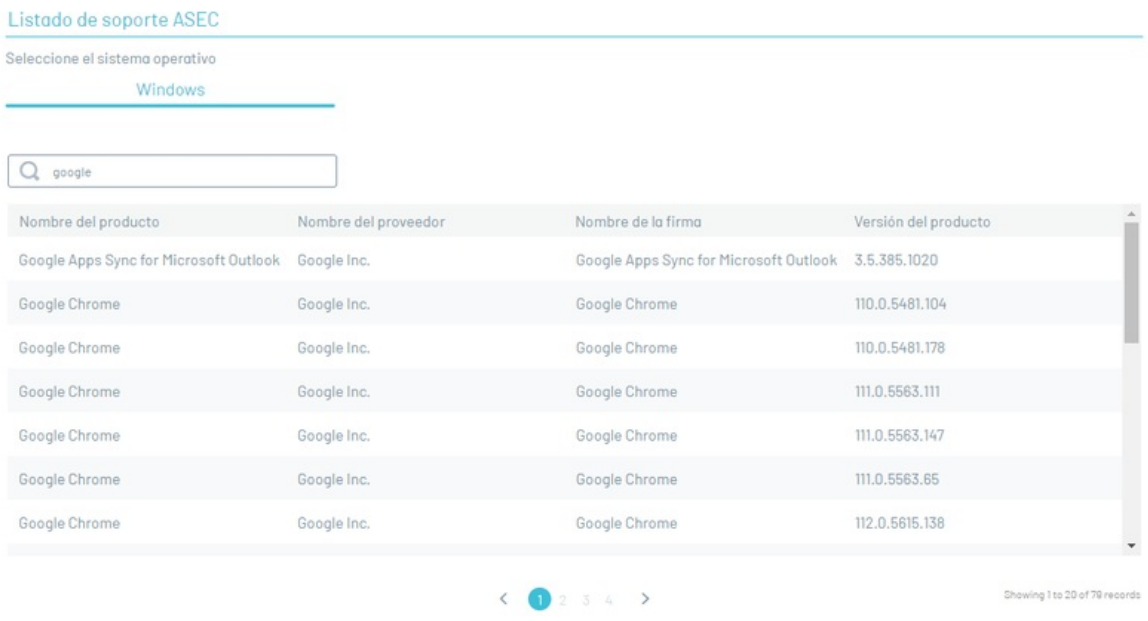


Visualizar Listado de Aplicaciones de seguridad

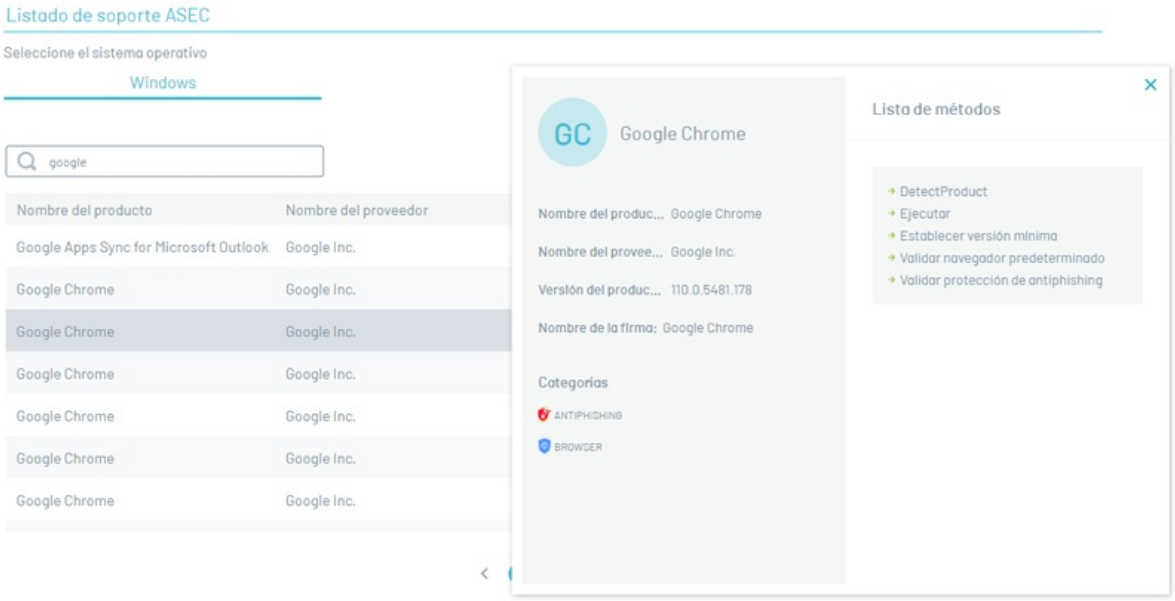
1. Ingrese al listado de soporte ASEC: https://docs.arandasoft.com/asec/supportchart

2. En la vista de información podrá Visualizar el listado de aplicaciones de seguridad y las versiones soportadas para realizar la gestión de poliítcas de cumplimiento de ASEC.

3. En el buscador podrá realizar una consulta de las aplicaciones de seguridad y versiones soportadas, ingresando el nombre del programa.



4. Al seleccionar un registro del listado de aplicaciones de seguridad podrá visualizar la información relacionada como nombre del producto, nombre del proveedor, criterio de configuración al que pertenece (ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT y WEB BROWSER.) y las [validaciones o métodos](#) que soporta.



Criterios Políticas

Los Criterios de Políticas se organizan en categorías que determinan la clasificación de los programas según sus funcionalidades. Cada programa presenta diversas opciones de validación y puede pertenecer a distintos Criterios.

Criterio	Descripción
ANTIMALWARE	Los programas Antimalware son aplicaciones diseñadas para detectar, prevenir y eliminar software malicioso de los dispositivos informáticos. Ayudan a proteger contra virus, troyanos, spyware y otras amenazas en línea, siendo una parte fundamental de la seguridad digital. Ejemplos incluyen Windows Defender y Kaspersky Anti-Virus.
ANTIPHISHING	Los programas Antiphishing son herramientas que protegen a los usuarios contra ataques de phishing, que intentan engañarlos para que revelen información confidencial. Estos programas detectan y bloquean correos electrónicos, mensajes o sitios web falsos que intentan robar datos personales o financieros. Ayudan a mantener la seguridad y la privacidad en línea. Ejemplos incluyen McAfee WebAdvisor y K7SecureWeb.
	Las aplicaciones de Backup contribuyen a que las organizaciones mantengan la inmortalidad de sus datos, lo que a su vez mejora la continuidad del negocio y fortalece las capacidades de

Criterio	Descripción
	recuperación ante desastres. Ejemplos incluyen IDrive y MEGAsync.
	Los programas de Cloud Storage son herramientas que permiten almacenar, gestionar y acceder a datos de manera remota a través de Internet. Facilitan la sincronización de archivos entre dispositivos, el intercambio de archivos y la seguridad de los datos, siendo utilizados tanto por usuarios individuales como por empresas para almacenamiento y colaboración en línea. Ejemplos incluyen Dropbox, Google Drive y Microsoft OneDrive.
	Los programas de Communication Tools son herramientas digitales que facilitan la comunicación entre personas y equipos a través de diversos medios, como mensajería instantánea, videoconferencias y gestión de proyectos. Ejemplos incluyen Slack y Zoom permitiendo una colaboración efectiva y un trabajo en equipo remoto.
	Los programas de Data Loss Prevention (DLP) son herramientas que previenen la pérdida o filtración de datos confidenciales de una organización. Monitorean, detectan y controlan el flujo de información dentro y fuera de la red empresarial para proteger datos sensibles, como información financiera o personal, secretos comerciales y propiedad intelectual. Ejemplos incluyen Wave Data Protection Agent y Dr.Web Security Space.
	Los programas de Endpoint Encryption son herramientas que cifran los datos almacenados en dispositivos finales como computadoras portátiles y teléfonos móviles. Ayudan a proteger la información sensible en caso de pérdida o robo del dispositivo, manteniéndola inaccesible sin la clave de descifrado adecuada. Ejemplos incluyen CipherShed y CryptoExpert.
	Los programas Firewall son aplicaciones o dispositivos diseñados para proteger redes informáticas al controlar y filtrar el tráfico de datos que entra y sale de ellas. Funcionan como una barrera de seguridad, examinando cada paquete de datos y decidiendo si permitir su paso o bloquearlo según reglas predefinidas. Son fundamentales para prevenir intrusiones no autorizadas, proteger datos sensibles y mantener la integridad de los sistemas informáticos. Ejemplos incluyen Smart Heal Total Security y SpyShelter Firewall.
	Los programas Health Agent forman parte de conjuntos de seguridad de endpoints que se administran de manera centralizada. Estos agentes aplican políticas y llevan a cabo tareas en el lado del cliente, como la implementación, configuración y actualización de otros componentes de la suite de seguridad. Estos componentes adicionales pueden abarcar desde el firewall personal y el motor antimalware, hasta la protección antiphishing, el agente de prevención de pérdida de datos, el agente de cifrado de disco y el agente de control de acceso a la red, entre otras formas de protección de terminales que ofrecen diversos proveedores de seguridad en sus productos. Ejemplos incluyen HP Support Assistant y Windows Security Health Agent.
	Los programas Remote Control son herramientas que permiten a los usuarios controlar y acceder a dispositivos de forma remota a través de una conexión de red, como Internet. Se utilizan para visualizar la pantalla, interactuar y solucionar problemas en dispositivos ubicados en diferentes lugares geográficos. Son útiles para asistencia técnica, administración de sistemas, teletrabajo y colaboración en equipo. Ejemplos incluyen TeamViewer, AnyDesk y Microsoft Remote Desktop.

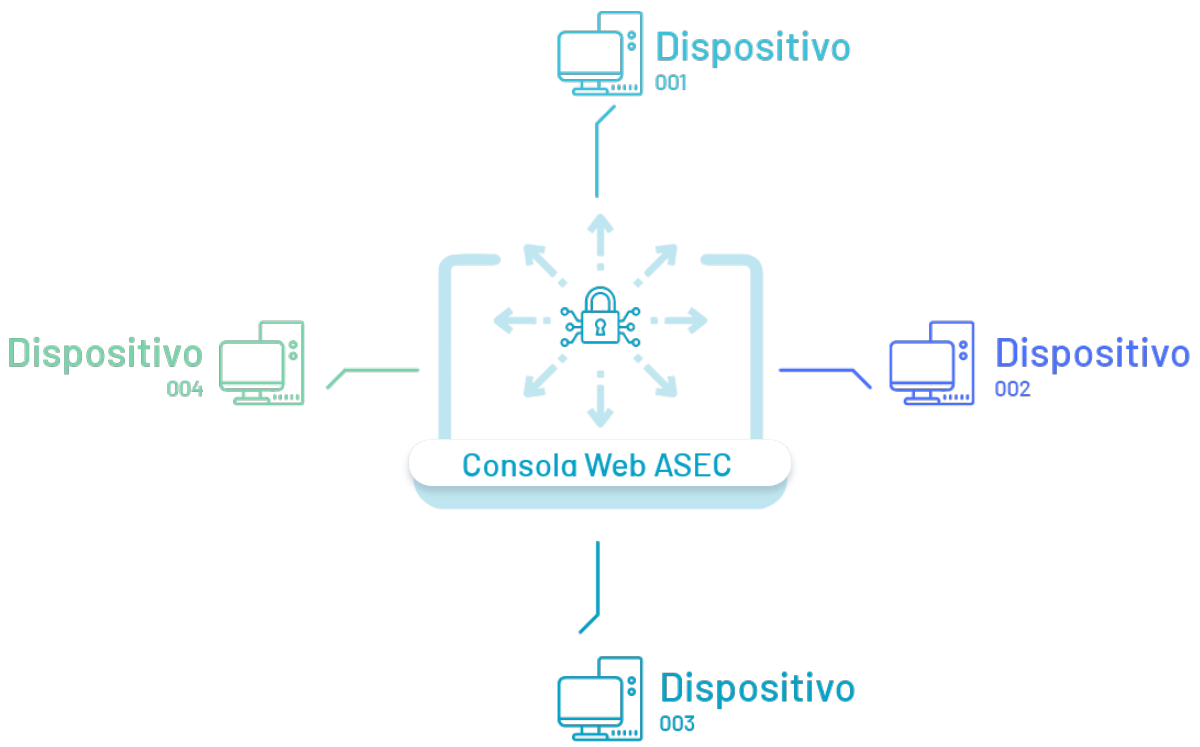
Criterio	Descripción
VIRTUAL MACHINE	Software que permite la virtualización en sistemas informáticos. Crean y gestionan máquinas virtuales, entornos aislados que ejecutan sistemas operativos y aplicaciones de manera independiente. Ejemplos incluyen VirtualBox y VMware Workstation.
VPN CLIENT	Los programas VPN Client son aplicaciones que permiten a los usuarios establecer conexiones seguras a una red privada virtual (VPN) desde sus dispositivos. Estas conexiones cifradas garantizan la privacidad y seguridad de la comunicación, especialmente en redes Wi-Fi públicas. Ejemplos incluyen Cisco AnyConnect, y ExpressVPN.
WEB BROWSER	Los programas Web Browser, o navegadores web, son aplicaciones que permiten a los usuarios acceder y navegar por páginas web en Internet. Ofrecen funciones como abrir múltiples pestañas, gestionar marcadores y buscar en la web. Ejemplos populares incluyen Google Chrome, Mozilla Firefox, Microsoft Edge, Safari y Opera. Son fundamentales para la experiencia de navegación en Internet.

Despliegue e Instalación

Agente Aranda Security

El agente en ASEC es el componente encargado de validar que las políticas de seguidad implementadas en los dispositivos cumplan el objetivo propuesto.

Después de instalado en los dispositivos, el agente ASEC hace una lectura del cumplimiento de las políticas definidas y genera unas alertas que podrán ser visualizadas por el administrador a través de la consola web.



En la consola web de Aranda Security el administrador general será el encargado de realizar la siguiente tarea:

Despliegue Agente

El despliegue del agente es el proceso de distribución de este componente en los dispositivos que se requiere monitorear. Desde la consola web de ASEC se copiará el comando generado para su posterior instalación en cada disopsitivo.

El despliegue del agente en ASEC puede efectuarse de tres formas:

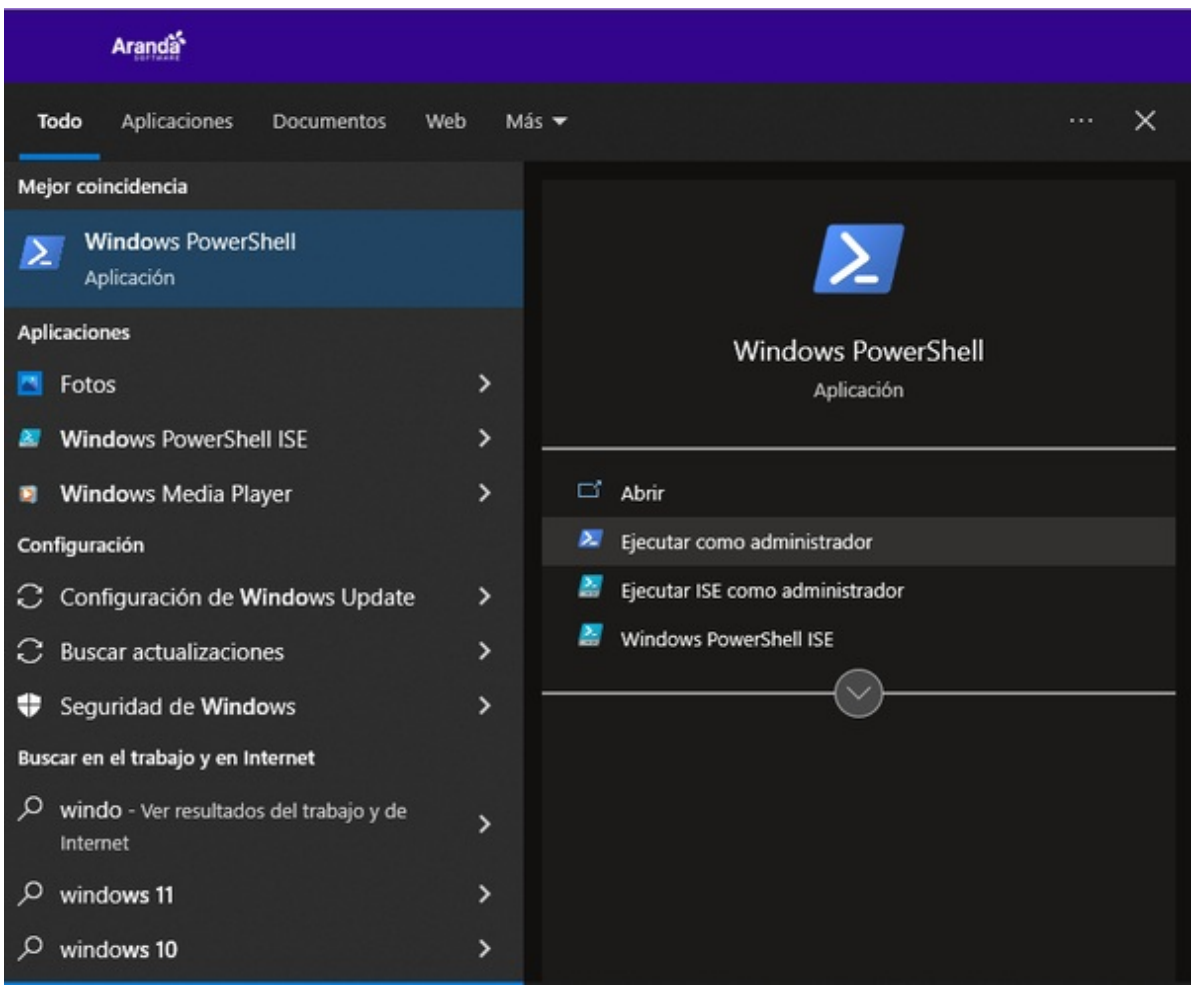
- **Despliegue Por Dispositivos**: A través de la consola web de Aranda Security podrá hacer el despliegue y posterior instalación del agente ASEC en los dispositivos.

- **Despliegue por Política de Dominio**: La instalación del agente podrá realizarse a través de la política de dominio.
- **Despliegue con ADM**: Utilizando Aranda Device Management ADM podrá cargar el paquete de agente de ASEC e iniciar el proceso de distribución del agente ASEC en los dispositivos.

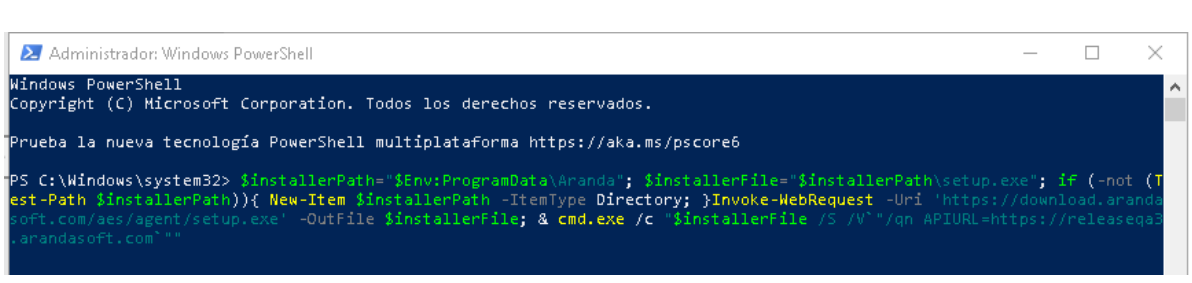
Despliegue e Instalación de Agente por Dispositivos

Para la instalación del agente es necesario contar con permisos de administrador en el dispositivo.

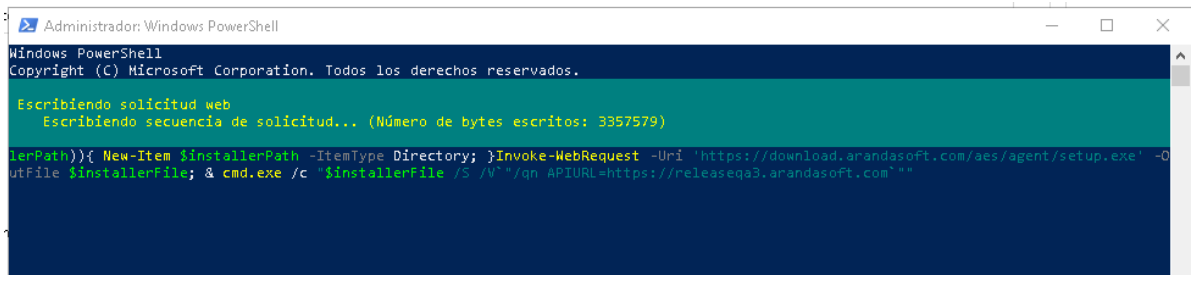
1. Abra Windows PowerShell y ejecute el programa como administrador.



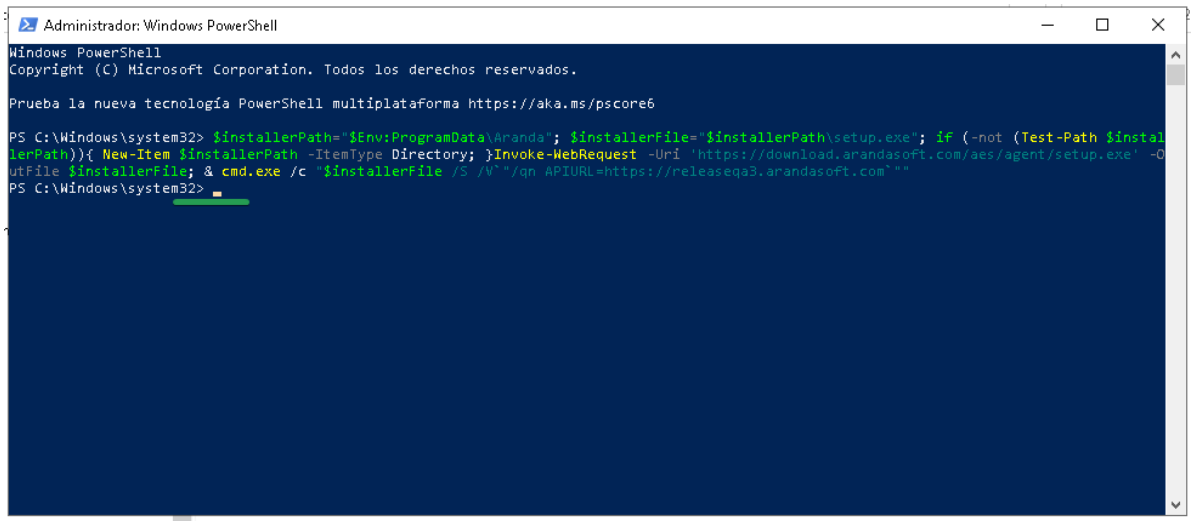
2. El comando copiado de la pantalla [Desplegar Agente] en la consola web de ASEC, péguelo en el PowerShell y de **Enter**. Se iniciará la instalación del agente en el dispositivo.



3. Inicia un contador de bytes que representa la descarga e instalación del agente en el dispositivo



4. Finalizado el proceso de instalación, se presentará de nuevo el cursor sobre la consola de PowerShell y a partir de ese momento el agente iniciará la verificación de las políticas.

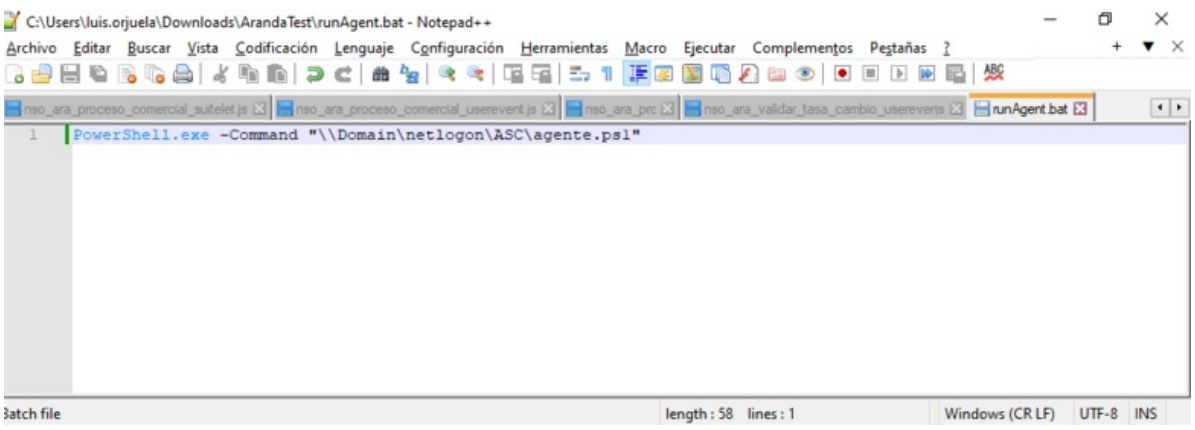


Despliegue del Agente ASEC por Política de Dominio

Crear Archivos de ejecución

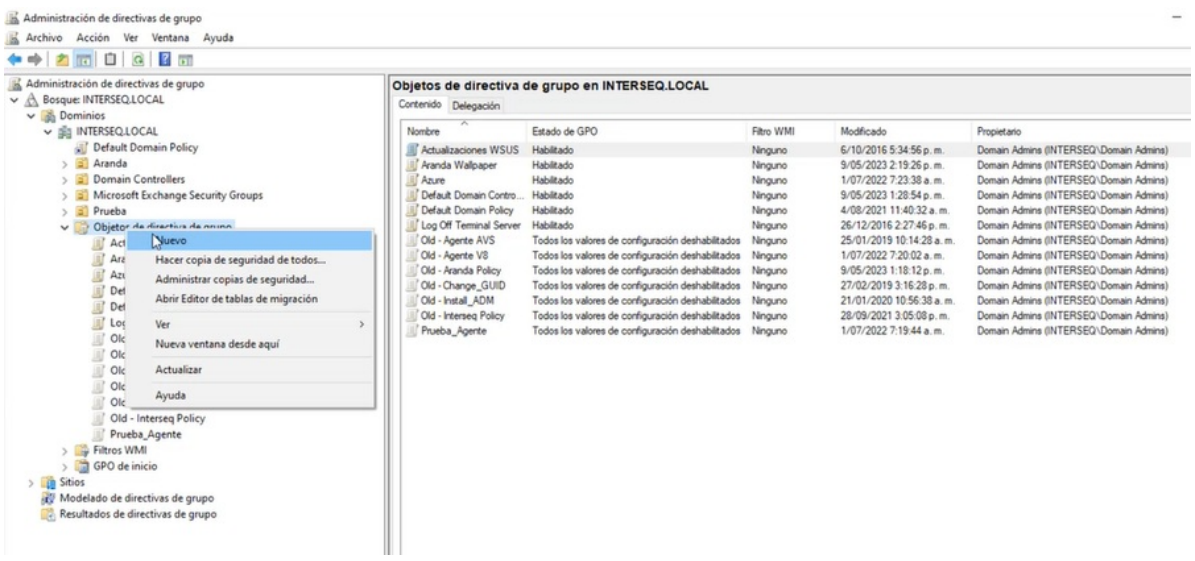
1. Después de copiar el comando de ejecución del agente ASEC, durante el Despliegue del Agente en la consola web de ASEC, genere un archivo con **extenión ps1** incluyendo el comando copiado, para posteriormente ejecutarlo en el dominio requerido.

2. Defina un archivo .bat con la ruta del dominio requerido.



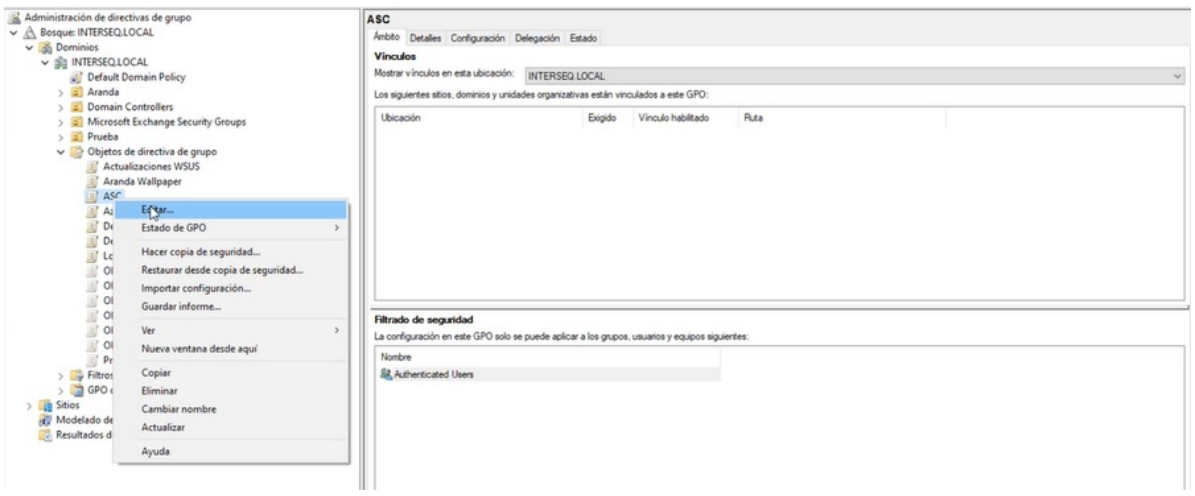
Crear Políticas de Grupo

1. Ingrese a la opción de **Administración de directivas de grupo**, en el dominio local seleccione la carpeta **Objetos de directiva de grupo** y haga clic en la opción **Nuevo**.



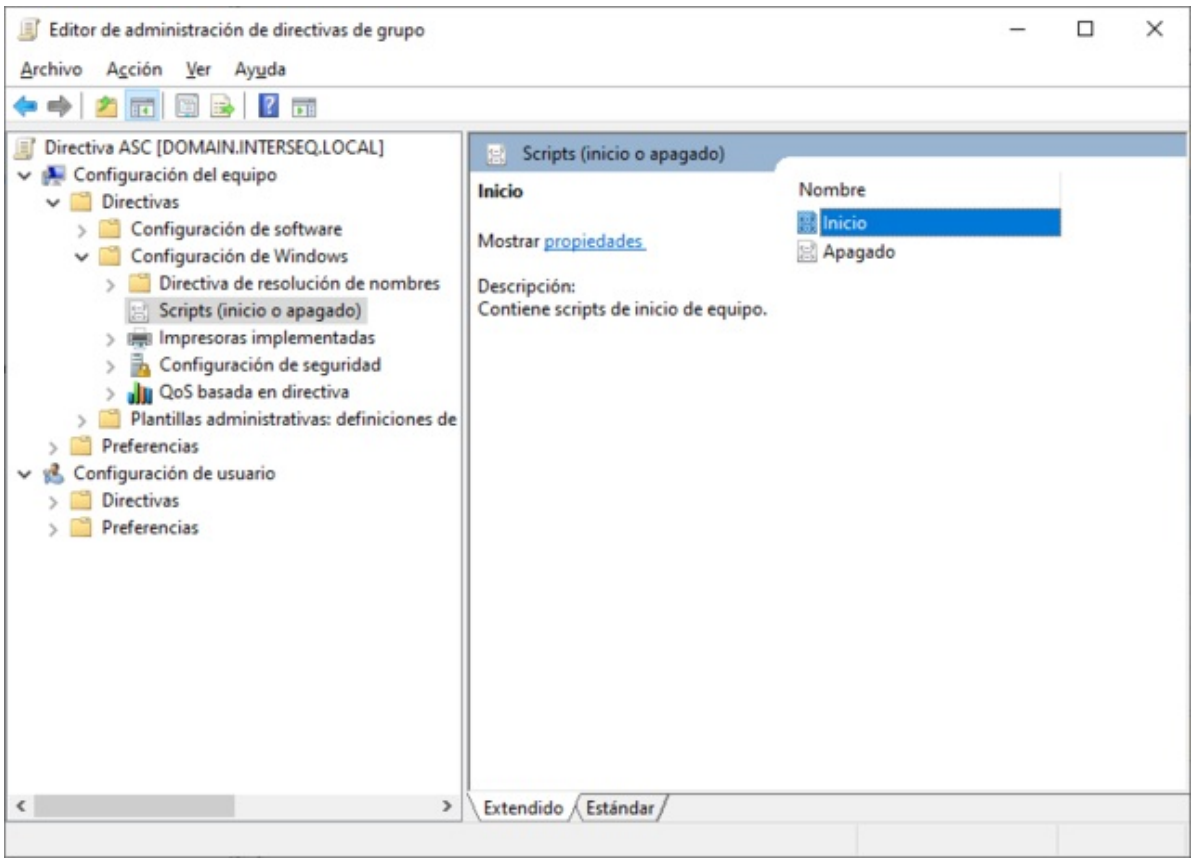
2. En la ventana **Nuevo GPO** ingrese un nombre de la nueva directiva. Ejemplo: ASC.

3. Seleccione la nueva directiva creada y haga clic en la opción **Editar**.

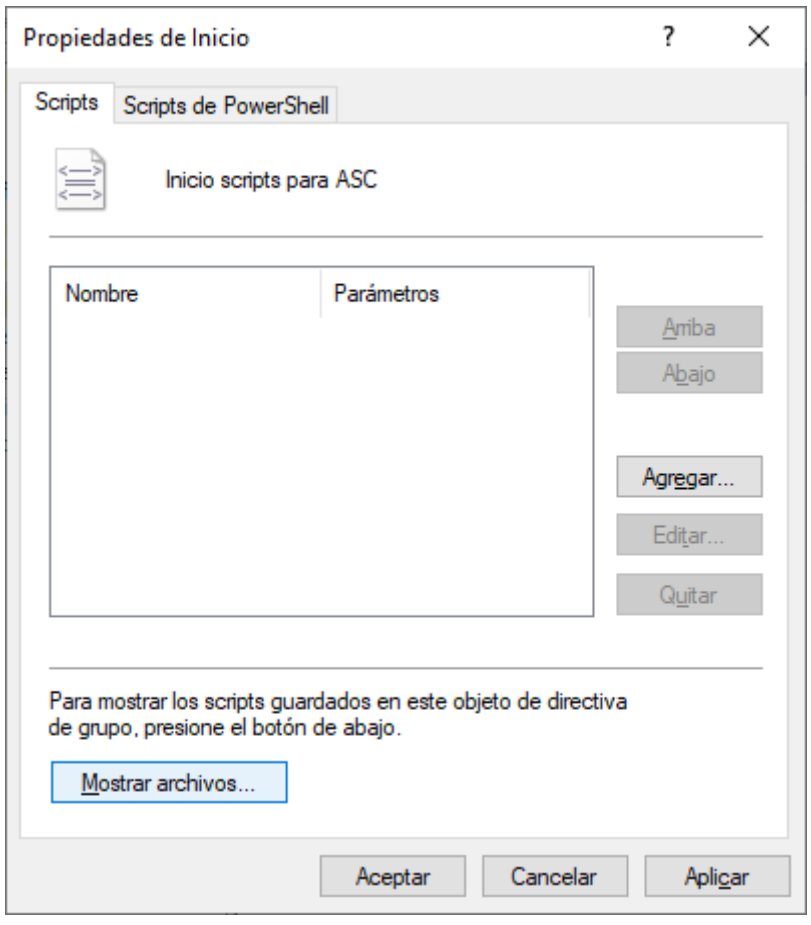


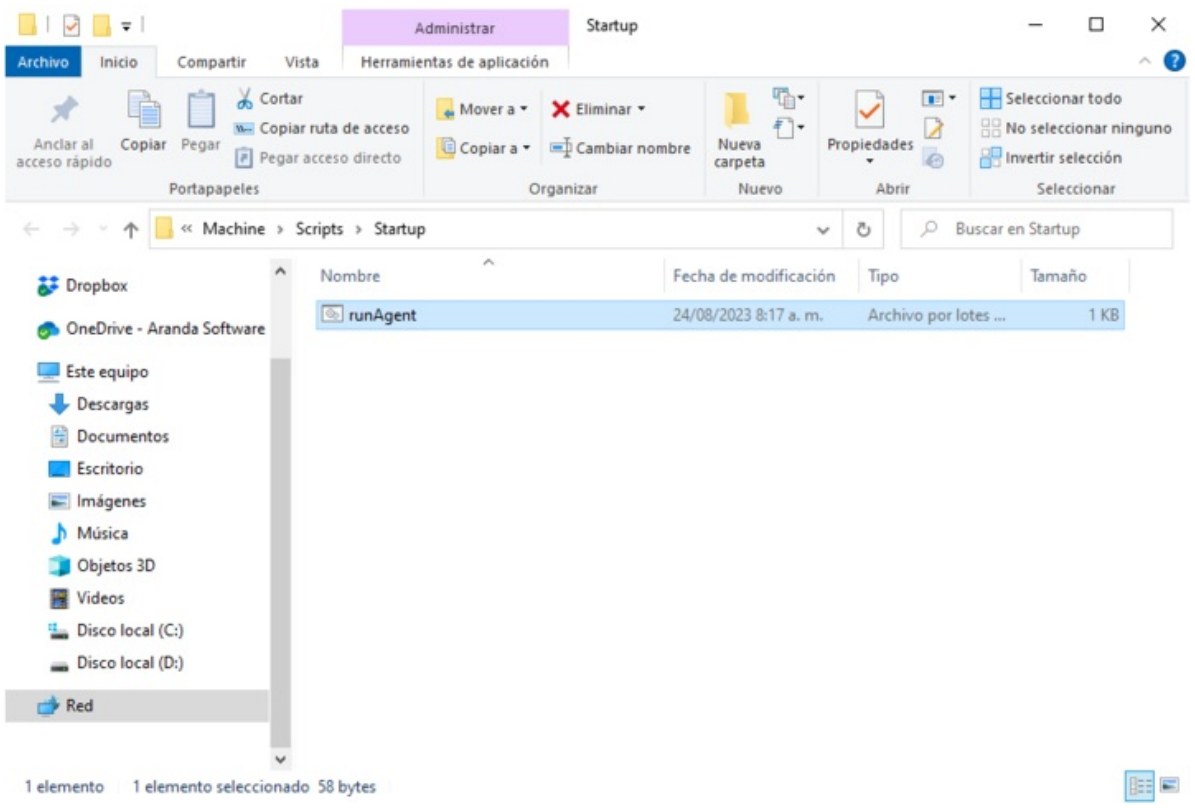
4. En el **Editor de Administración de Directivas de grupo**, seleccione la opción Configuración de Equipo, Directivas, Configuración de Windows y la opción **Scripts**. En la vista de información seleccione la opción **Inicio** .

⚐ **Nota:** Configurar la directiva de inicio, permite que el agente de ASEC se ejecute al momento de iniciar sesión.

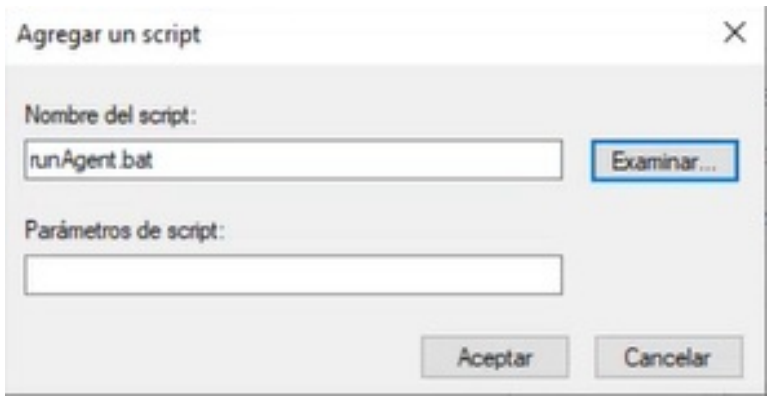


5. En la ventana **Propiedades de inicio**, seleccione el botón **Mostrar Archivos** para pegar el archivo **.bat** del agente de ASEC.



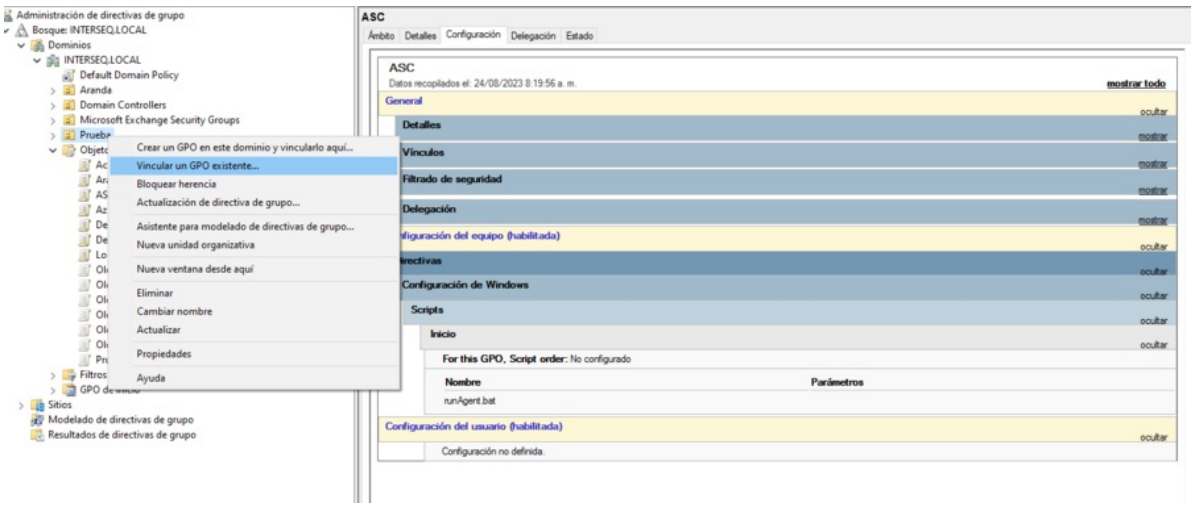


6. En la ventana **Propiedades de inicio**, seleccione el botón **Agregar** y en la ventana **Agregar un Script** seleccione el botón **Examinar** para seleccionar el **archivo .bat** del agente ASEC, al terminar haga clic en **Aceptar**.



Asociar la Política a la Unidad Organizacional

1. Ingrese a la opción de **Administración de directivas de grupo**, en el dominio local seleccione la unidad organizacional a la cual va a vincular la GPO creada y haga clic en la opción **Vincular un GPO existente**.



2. En la ventana que se habilita seleccione la directiva de la política creada .

> ⚐ **Nota:** En la vista de información seleccione la pestaña **configuración** para validar que la directiva configurada con el agente de ASEC está habilitada.

Monitoreo Políticas

Monitoreo Cumplimiento Políticas

El monitoreo es el proceso de seguimiento y validación de los niveles de cumplimiento de las políticas implementadas.

El administrador y especialista podrán consultar y verificar los resultados generados después del análisis realizado por el agente en cada uno de los dispositivos, teniendo en cuenta los siguientes enunciados:

1. Resumen de Políticas

Consulte el análisis generado por Aranda Security para determinar los niveles de cumplimiento de las políticas de seguridad en los diferentes dispositivos.

2. Dispositivos

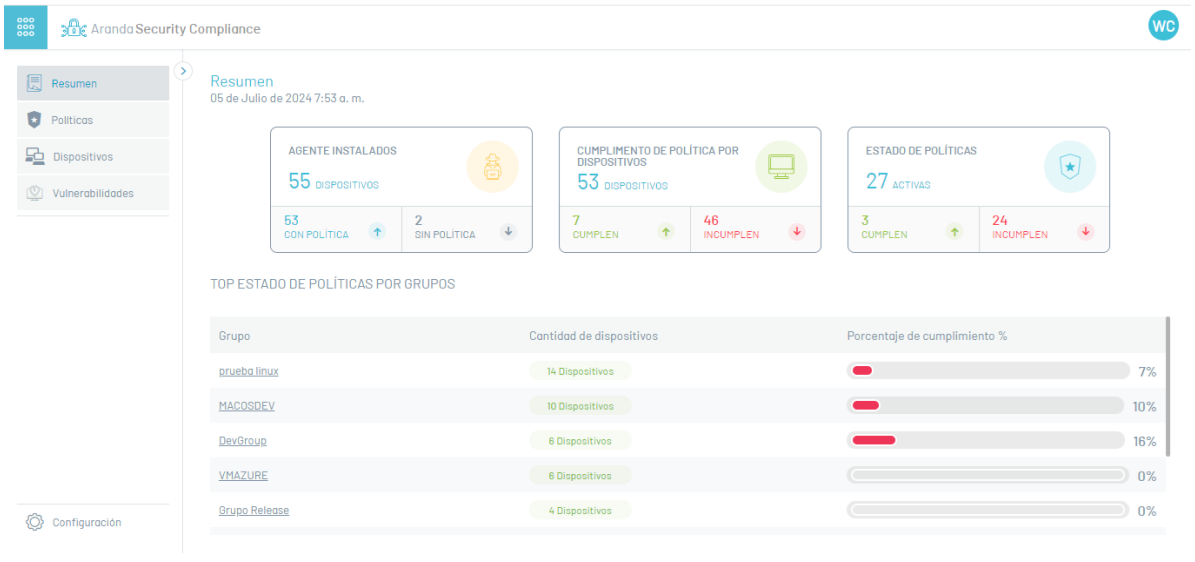
Consulte el listado de dispositivos registrados con detalles sobre su asociación a grupos de cumplimiento y las vulnerabilidades detectadas.

3. Vulnerabilidades

Consulte las vulnerabilidades reportadas por cada dispositivo registrado, mostrando los niveles de criticidad como soporte para la implementación de planes y políticas.

Resumen Políticas

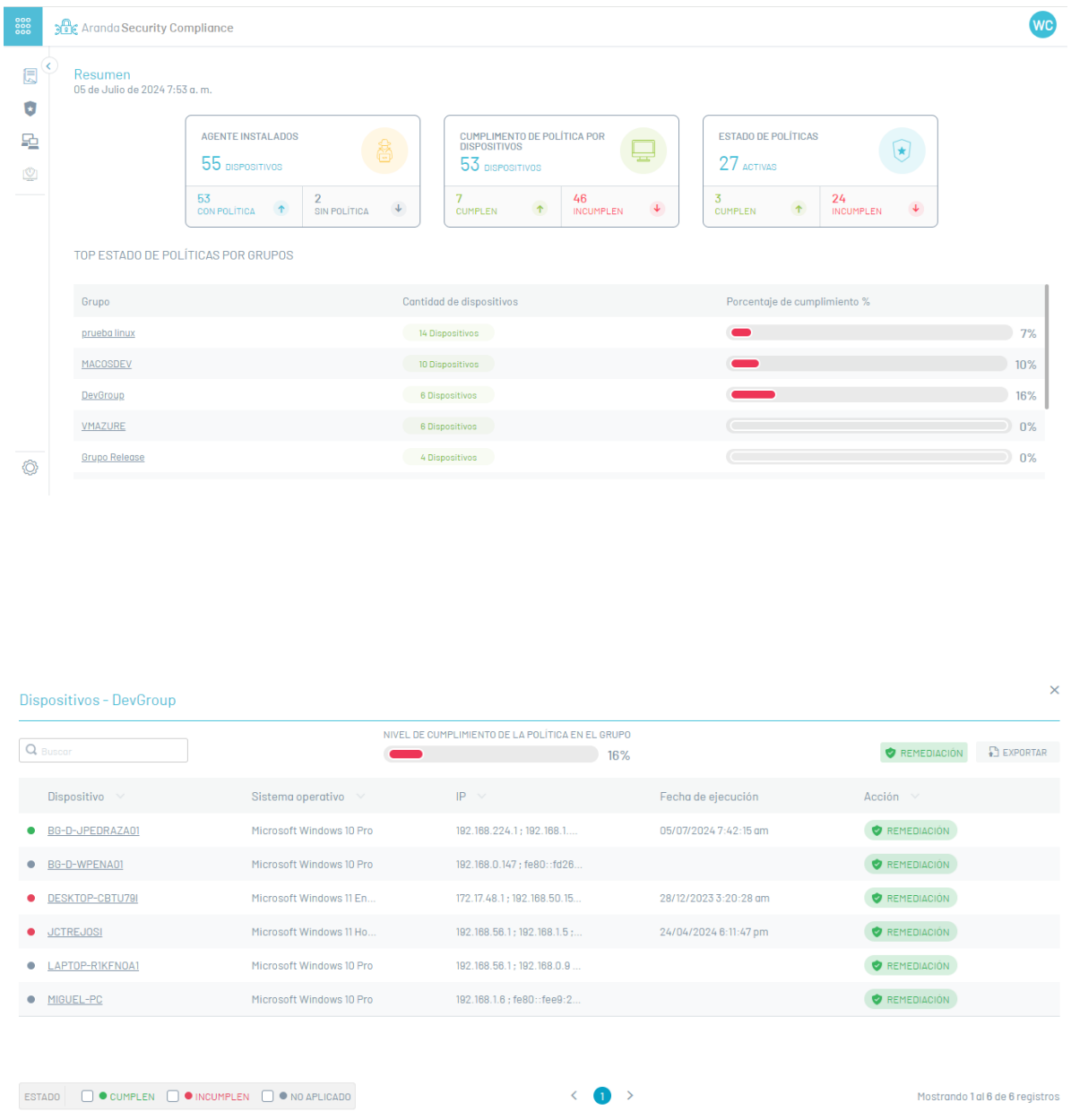
1. Ingrese a la consola de Aranda Security Compliance con rol de administrador, seleccione la opción **Resumen** del menú principal. En la vista de información se podrá visualizar los resultados del análisis de cumplimiento de las políticas de seguridad en los dispositivos vinculados. La información generada está agrupada por niveles de cumplimiento, agentes instalados, estado de las políticas y el top de estado de políticas por grupos.



⚐ Nota:

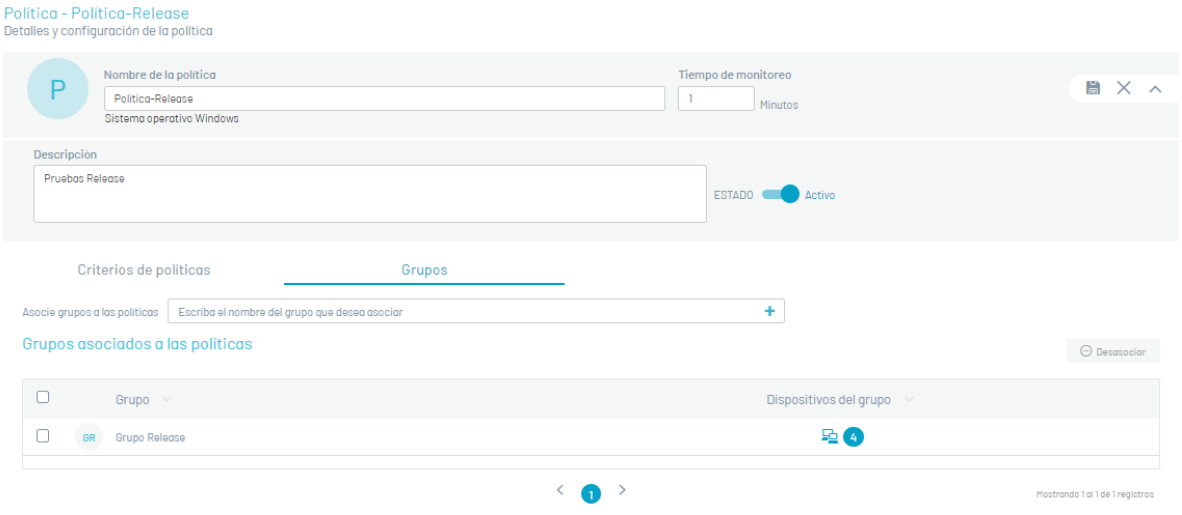
1. El reporte consolidado de los niveles de cumplimiento presenta una visión global del estado de los dispositivos en relación a las políticas de seguridad aplicadas.
2. En el resumen generado sólo se podrán visualizar la información de los 10 últios registros de dispositivos vinculados con el agente de ASEC.

2. En la vista de Resumen al seleccionar un grupo del top de estado de políticas, podrá acceder al [detalle de cumplimiento del dispositivo](#) asociado al grupo.

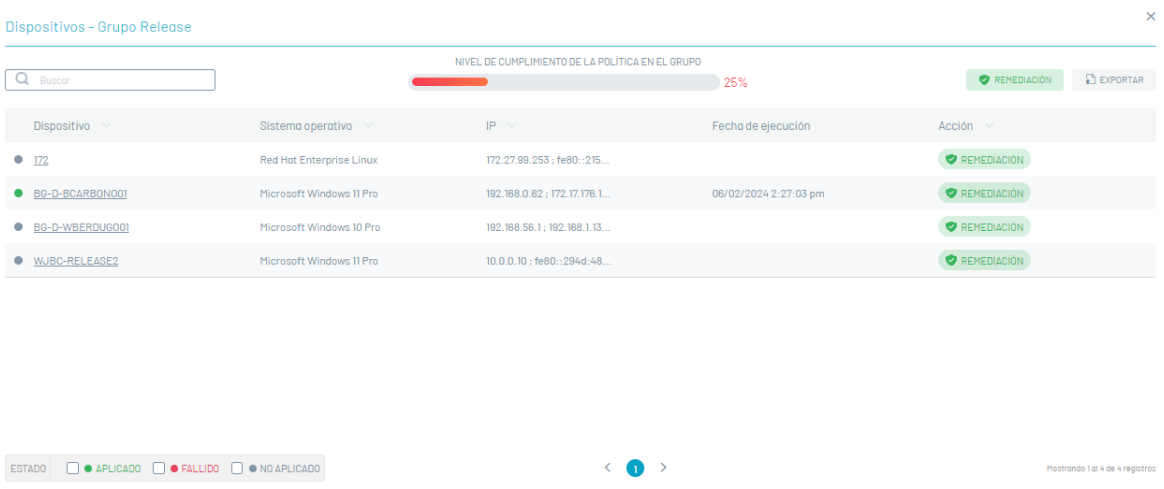


Detalle Cumplimiento de Dispositivos

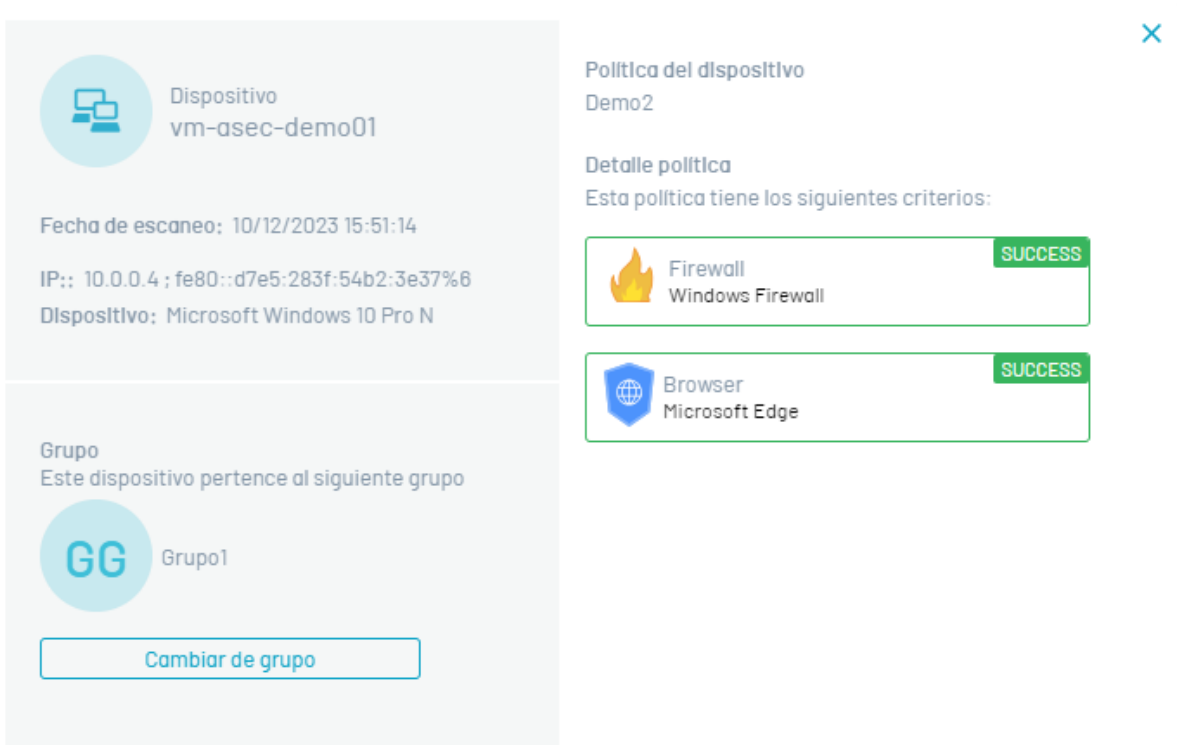
1. En la vista de información de la Política en Aranda Security Compliance, en la pestaña **Grupos** podrá visualizar el listado de grupos asociados a las políticas. Al seleccionar un grupo con dispositivos asociados podrá visualizar la ventana **Dispositivos** con el detalle de cumplimiento de los dispositivos.



2. En la ventana **Dispositivos** podrá visualizar la información relacionada de los dispositivos asociados a un grupo. Estos datos están organizados por nombre, sistema operativo, IP, fecha de inicio y acción de remediación a ejecutar del nivel de cumplimiento del grupo.

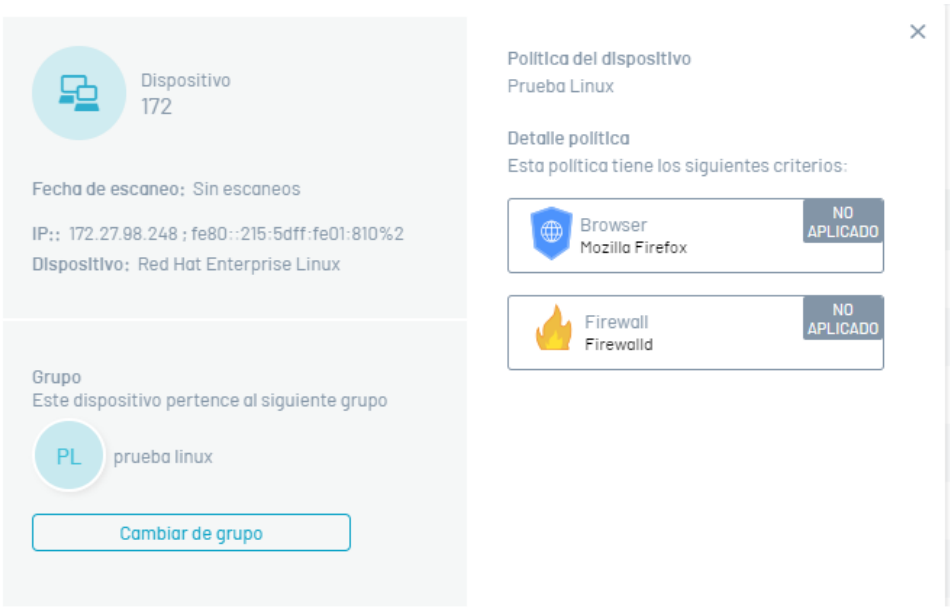


3. Al seleccionar el nombre del dispositivo podrá visualizar en detalle información relevante como nombre del dispositivo, nombre de la política, la fecha del escaneo, grupo al que pertenece y criterio de la política aplicado.



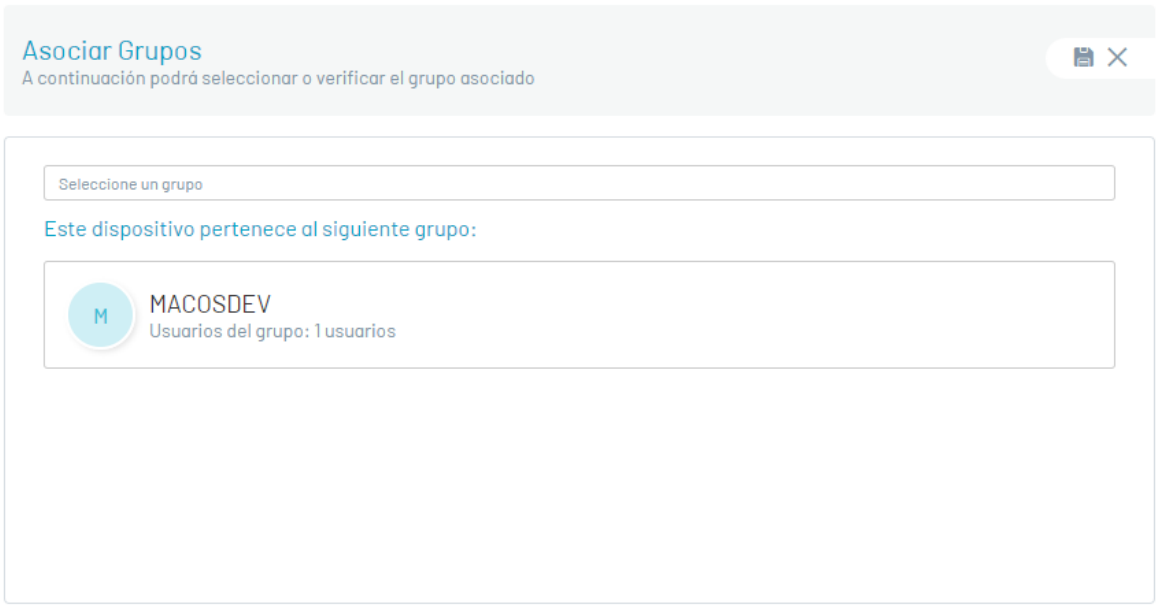
4. El detalle de la política aplicada al dispositivo podrá visualizar el nivel de cumplimiento de los criterios de las políticas implementados, a través de los Estados referenciados:

Estados	Descripción
SUCCESS	El estado Exitoso se visualiza cuando se cumple el criterio de la política, aplicado al dispositivo.
FAILED	El estado fallido se visualiza cuando NO se cumple el criterio de la política, aplicado al dispositivo
NOT APPLIED	El estado No Aplica se visualiza cuando el dispositivo no se ha escaneado.



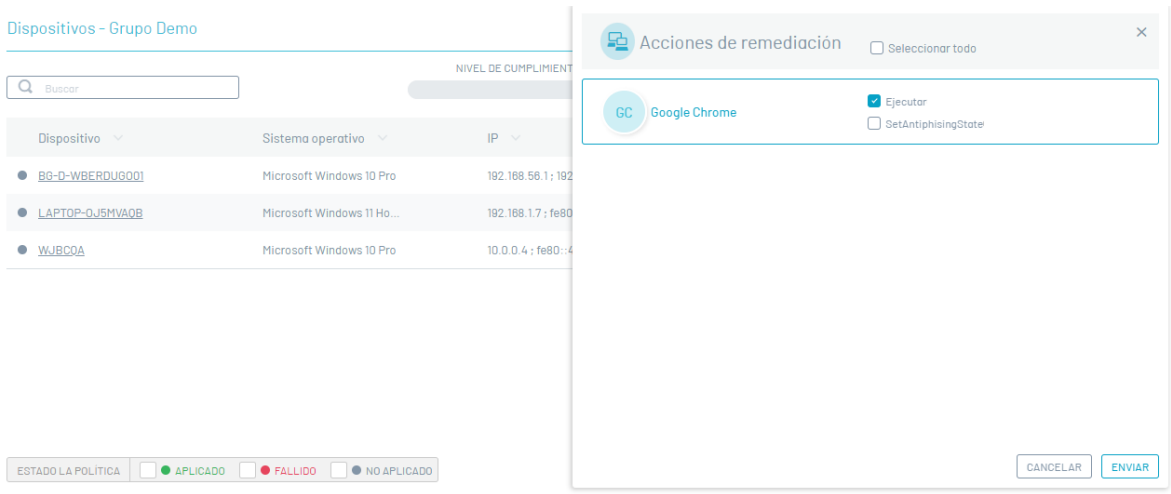
5. En el detalle de la política, al seleccionar el estado generado se despliegan las validaciones del caso.

⚐ **Nota:** En el detalle del dispositivo seleccione el botón**Cambiar Grupo** para modificar la asociación del grupo existente.



Acciones de Remediación

6. Independiente del estado generado (Exitoso,Fallido o No Aplica) durante el análisis de cumplimiento de políticas en los dispositivos, podrá ejecutar las acciones de remediación requeridas. seleccione el botón **Remediación** para ejecutar las acciones habilitadas para el criterio de seguridad implementado.

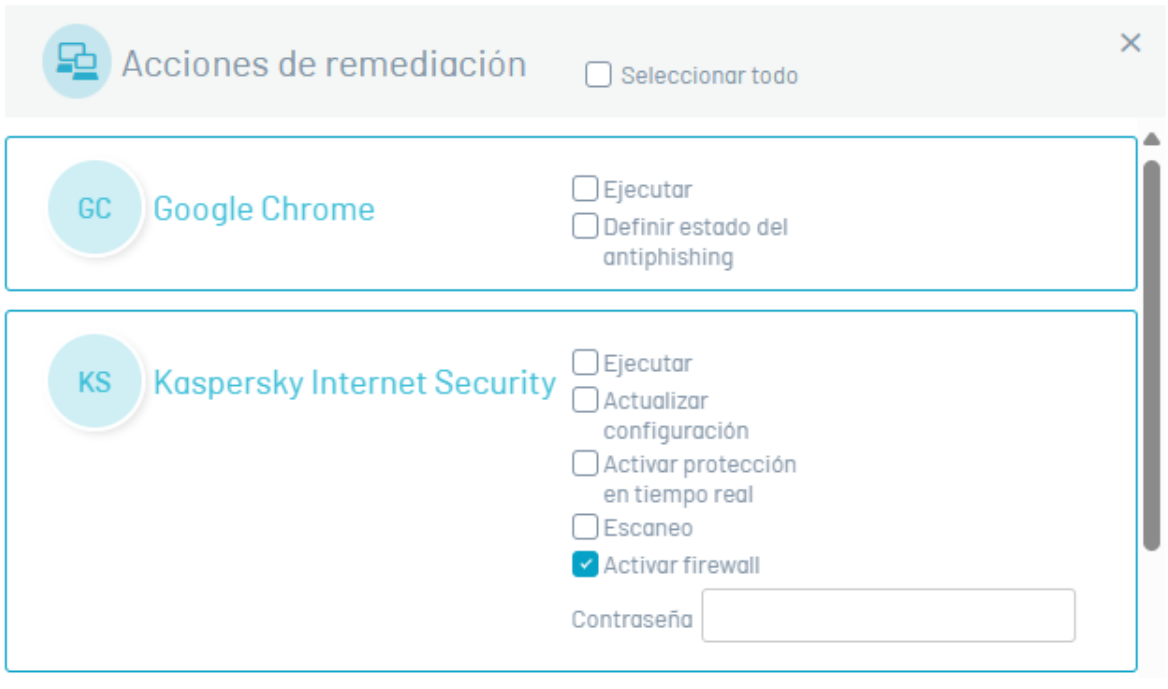


⚐ **Nota:** Al seleccionar el botón **Enviar** se implementarán las acciones de remediación elegidas.

⚐ **Nota:** Al seleccionar la opción del menú **Grupos de cumplimiento** del listado, únicamente se realizan las remediaciones en las opciones de la columna **Dispositivos del grupo**

7. Las acciones de remediación que solicitan contraseña requieren la clave del producto de administración. Estas claves son necesarias para acceder a la configuración avanzada del software.

El campo **Contraseña** no es obligatorio y puede dejarse en blanco, salvo que el producto requiera una clave de administración para realizar modificaciones.

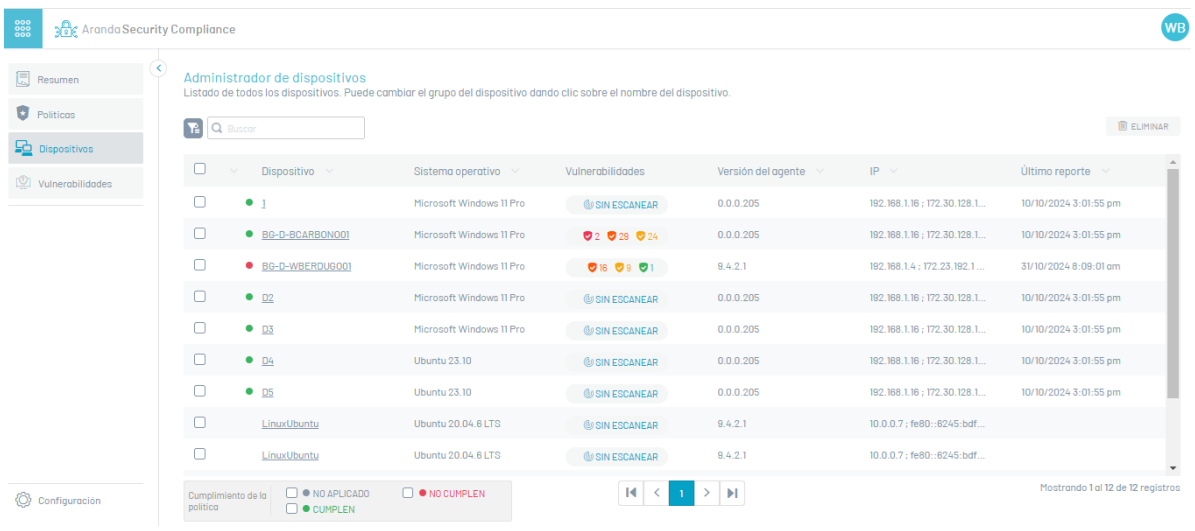


⚐ **Nota:** Claves de Administración o Cambio:

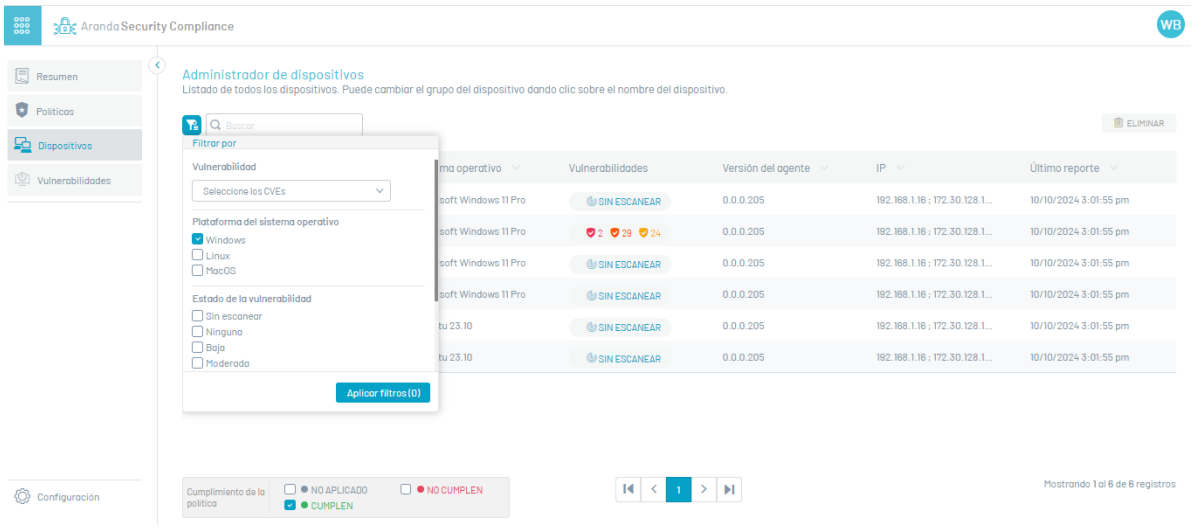
- 1. Requeridas para realizar cambios significativos en la configuración o en la administración del software.
- 2. Previenen accesos no autorizados y modificaciones no deseadas.
- 3. Ejemplos: Claves de administrador en sistemas operativos, claves de root en dispositivos móviles con Android, claves para acceder a configuraciones avanzadas en sistemas de seguridad o software empresarial..

Dispositivos

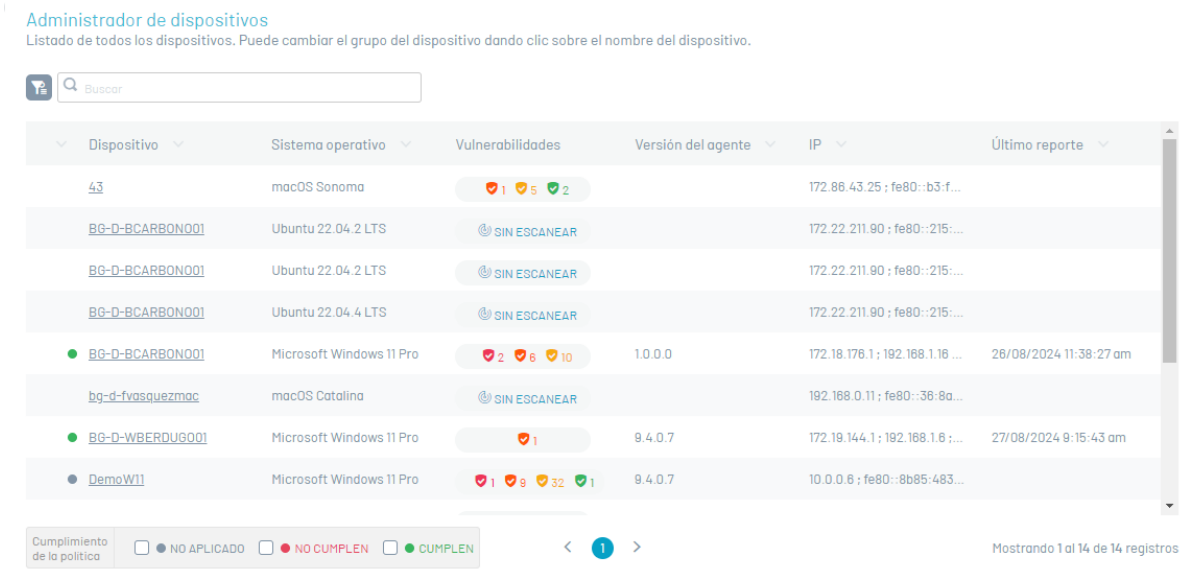
1. Ingrese a la consola de Aranda Security Compliance con rol de administrador, seleccione la opción **Dispositivos** del menú principal. En la vista de información podrá visualizar el listado de dispositivos registrados a través del Agente, donde se muestra el nombre, el sistema operativo, las vulnerabilidades y el último reporte de la política.



2. En la vista de Dispositivos se habilita la opción de filtro en la parte superior izquierda, dividido por las secciones de **Vulnerabilidad**,**Plataforma del Sistema Operativo**,**Estado de la vulnerabilidad**.Este filtro permite a los usuarios refinar la lista de dispositivos mostrada, facilitando la identificación de aquellos que cumplen con criterios específicos según el estado de su seguridad, el tipo de dispositivo y su estado de evaluación más reciente.

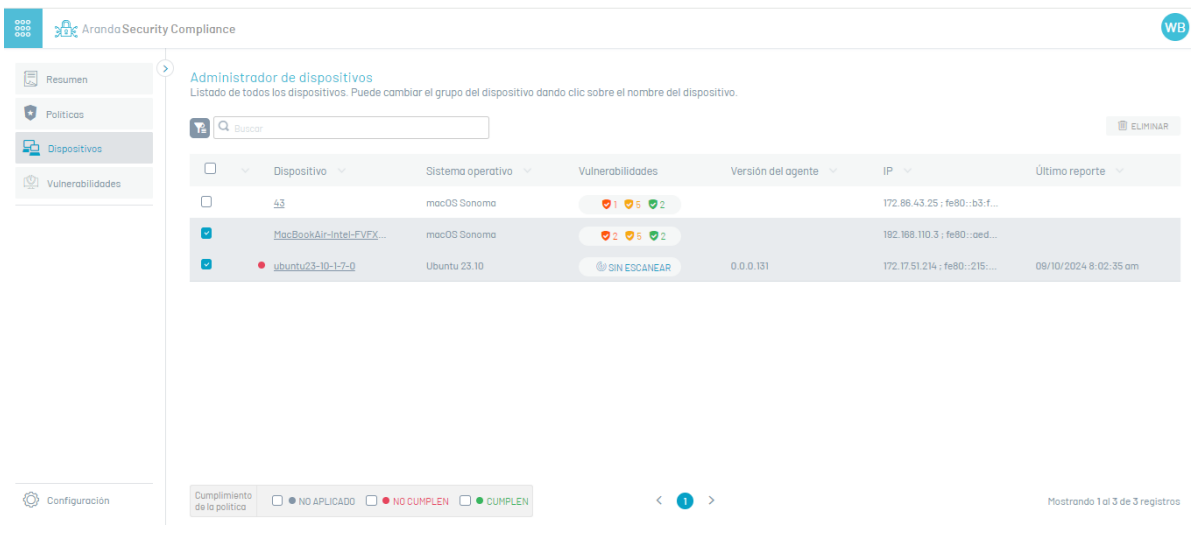


3. El filtro de cumplimiento de políticas, ubicado en el pie de página, está diseñado para filtrar dispositivos en función de su alineación con las políticas de seguridad establecidas. Al activar este filtro, los usuarios pueden visualizar únicamente los dispositivos que cumplen o no cumplen con los requisitos de dichas políticas, facilitando la identificación rápida de equipos que requieren acciones correctivas o que están en conformidad con los estándares establecidos. Esto permite una gestión más eficiente del estado de cumplimiento en todo el entorno de dispositivos.

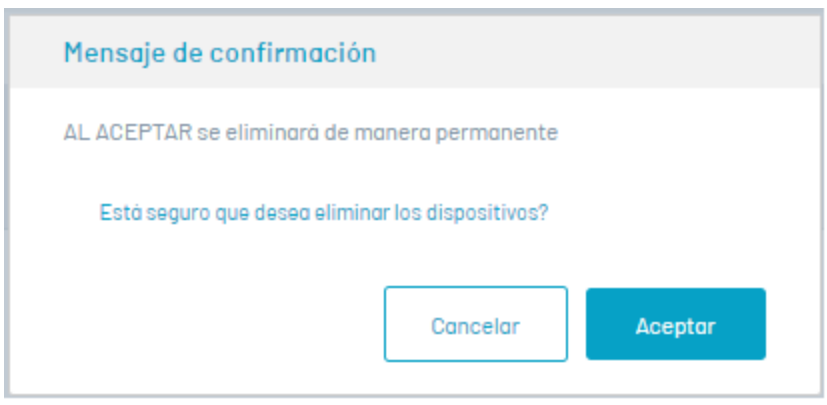


Eliminar Dispositivos

4. Para eliminar dispositivos seleccione uno o varios registros y haga clic en el botón **Eliminar**.

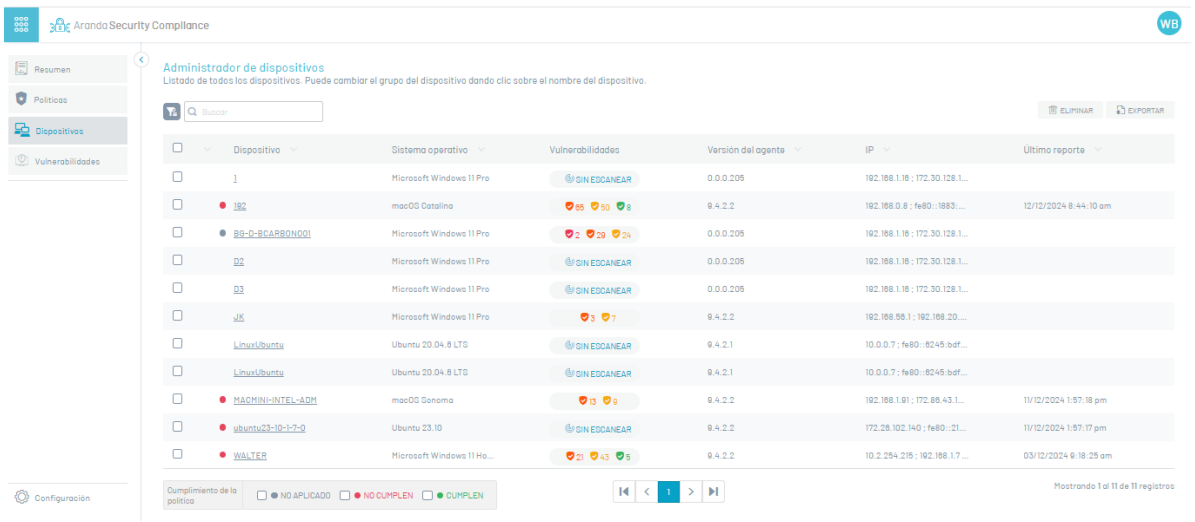


5. Se habilita un mensaje de advertencia donde debe confirmar el borrado del dispositivo.



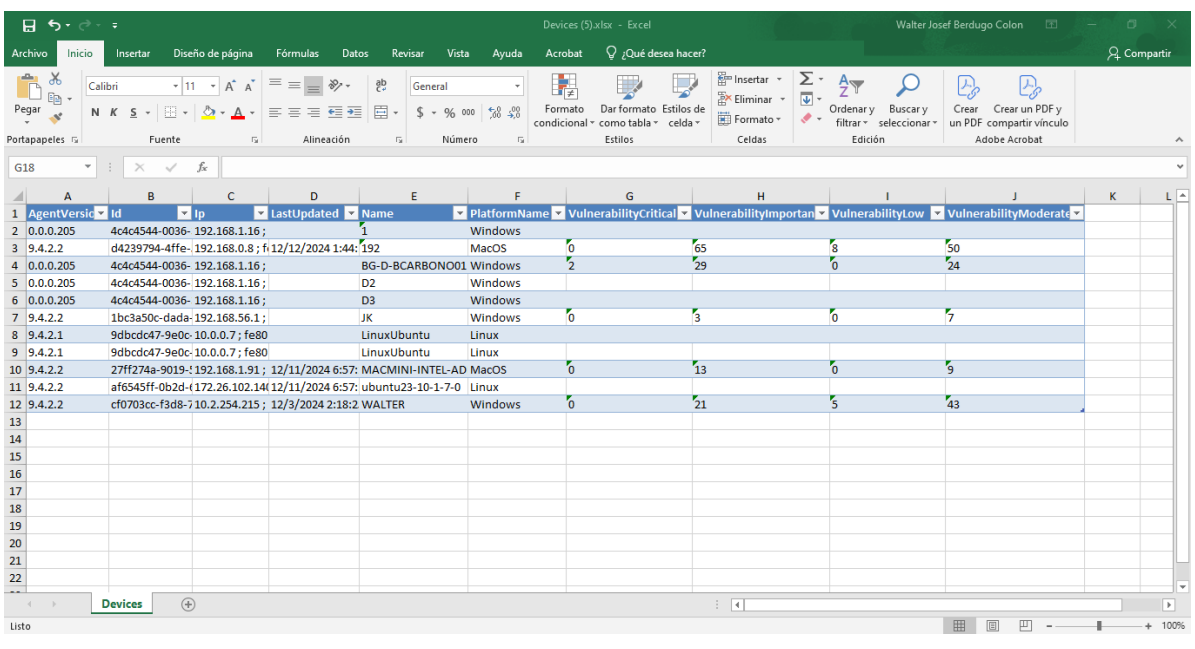
Exportar Dispositivos

1. En la vista de información de Dispositivos, después de filtrar los datos respectivos y obtener el listado de dispositivos disponibles, haga clic en el botón **Exportar**.



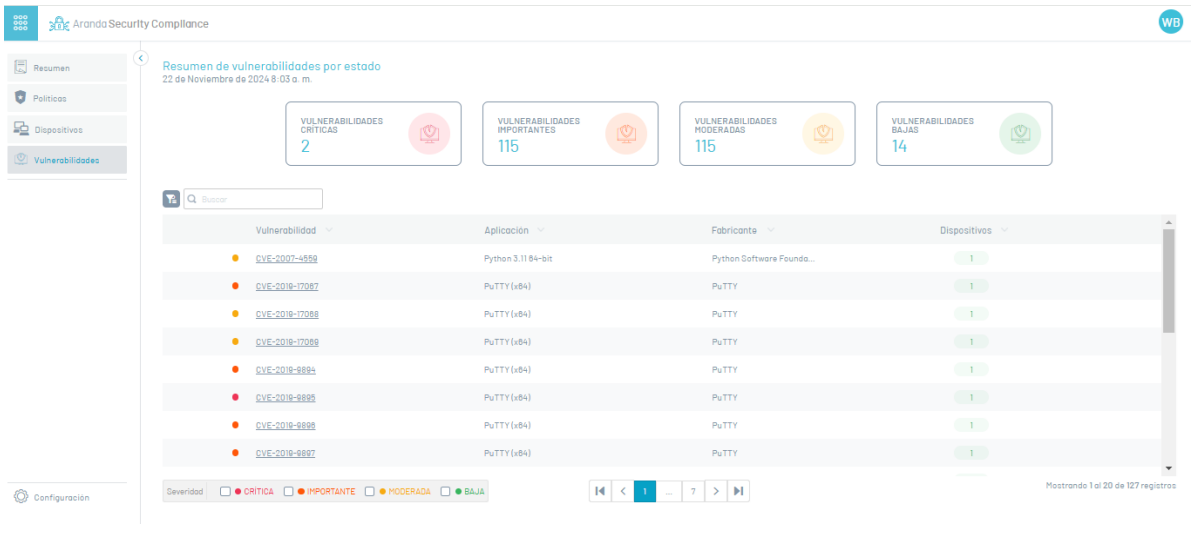
2. En el menú encabezado de la consola de administración de Aranda Security, se habilita la oción de **Descargas** donde podrá visualizar el formato generado del listado de dispositivos en formato excel

3. Haga clic en el archivo para descargar la información de los dispositivos. El archivo descargado incluye todos los campos del dispositivo.



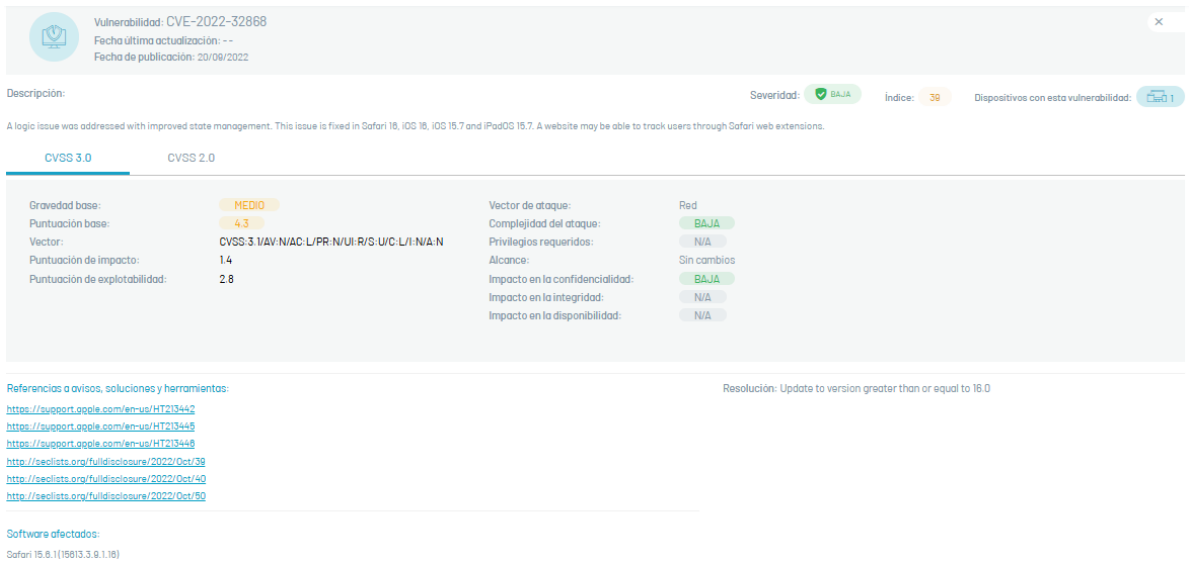
Vulnerabilidades

1. Ingrese a la consola de Aranda Security Compliance, seleccione la opción **Vulnerabilidades** del menú principal. En la vista de resumen se podrá visualizar los resultados del análisis del listado de vulnerabilidades clasificados por severidad y agrupados por dispositivos



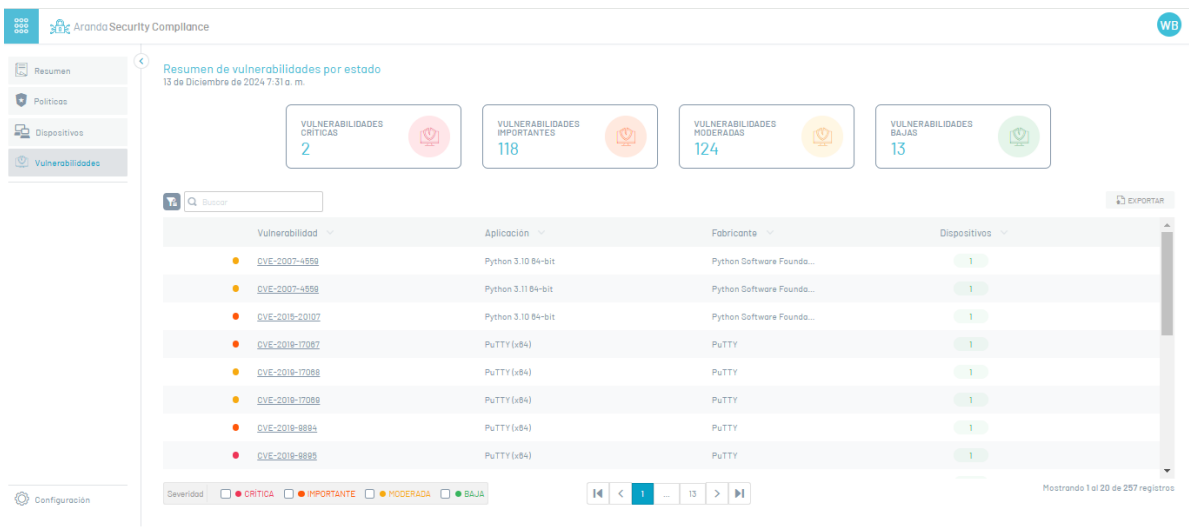
⚐ **Nota:** El reporte generado del análisis de vulnerabilidades realizado por los agentes solo está disponible para los sistemas operativos Windows y MacOS. Si utiliza un sistema operativo diferente, no podrá acceder a este informe.

2. En la vista de Vulnerabilidades al seleccionar el nombre de una vulnerabilidad, se despliega una nueva vista donde se muestra el nombre, descripción, fecha última actualización, fecha de publicación, severidad , software afectado y la cantidad de dispositivos que registran la misma con acceso a filtrar los dispositivos.



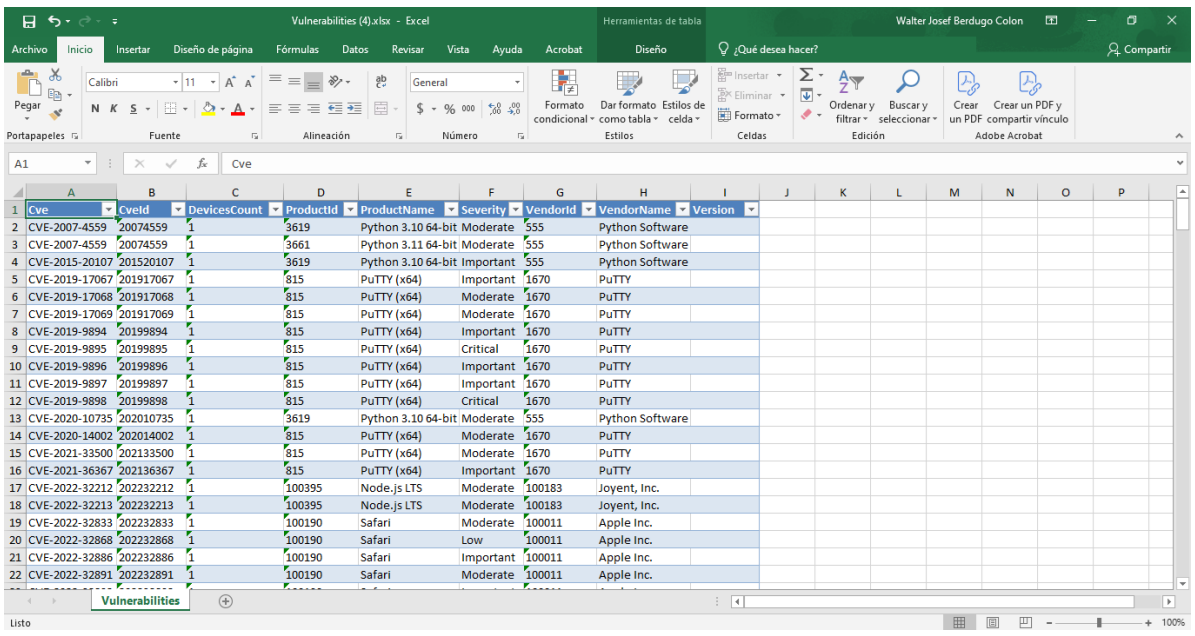
Exportar Vulnerabilidades

1. En la vista de información de Vulnerabilidades, después de filtrar los datos respectivos y obtener el listado de vulnerabilidades asociadas a dispositivos, haga clic en el botón **Exportar**.



2. En el menú encabezado de la consola de administración de Aranda Security, se habilita la oción de **Descargas** donde podrá visualizar el formato generado del listado de vulnerabilidades en formato excel

3. Haga clic en el archivo para descargar la información de las vulnerabilidades. El archivo descargado incluye todos los campos de la vulnerabilidad.

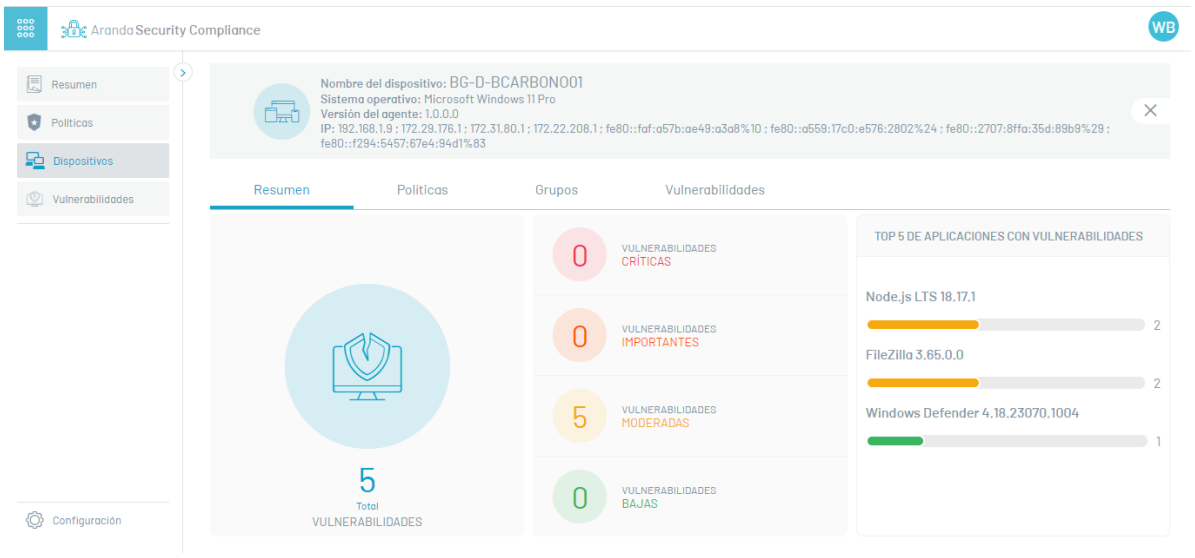


Detalle de Dispositivos

Desde la vista del listado de Dispositivos, se podrá acceder a un detalle donde se visualizará el resumen de vulnerabilidades, el listado de vulnerabilidades y el grupo con su política asociada.

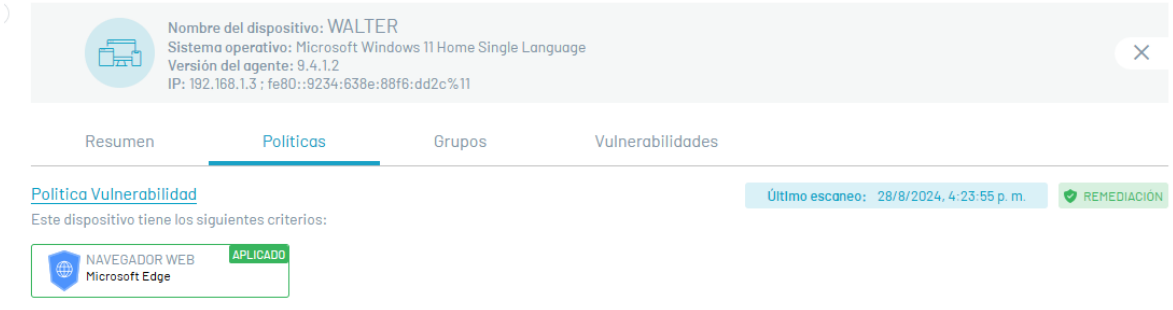
Resumen Vulnerabilidades

Al seleccionar la pestaña **Resumen** se mostrará un resumen de las vulnerabilidades registradas en el Dispositivo, se indicará el total de vulnerabilidades por severidad y el top 5 de aplicaciones con más vulnerabilidades.



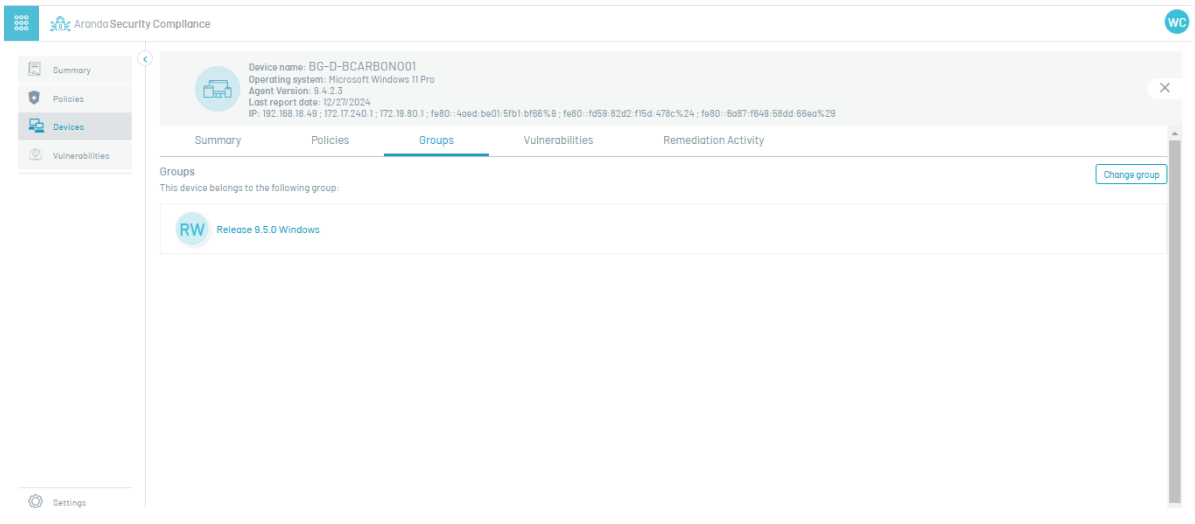
Políticas

Al seleccionar la pestaña **Políticas**, se podrán visualizar los criterios asociados al dispositivo, junto con el nombre de la política. También se mostrarán las opciones de remediación y la fecha del último escaneo, permitiendo identificar los cambios más recientes.



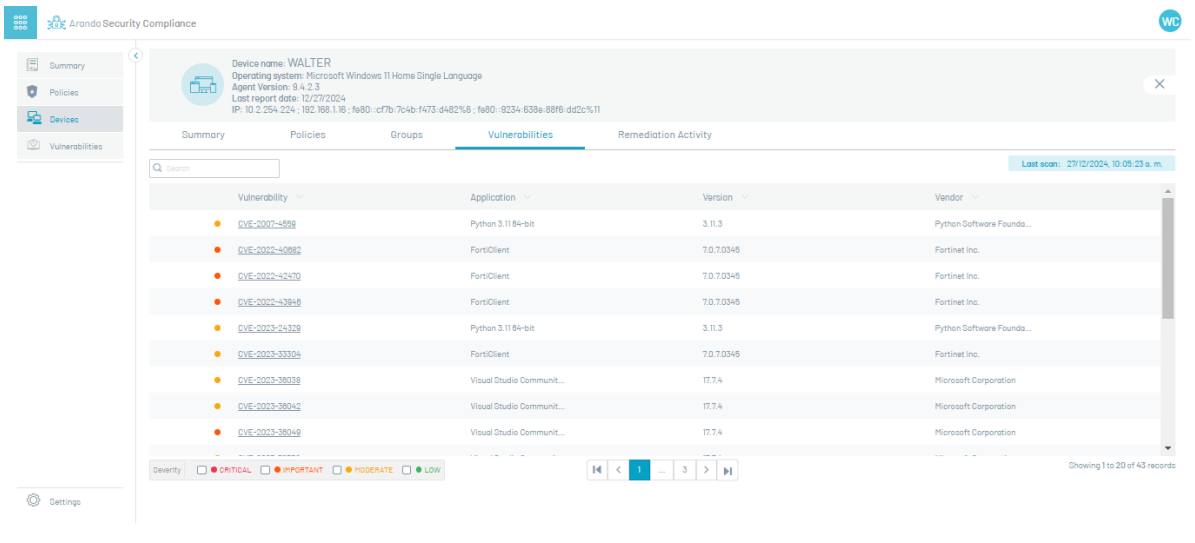
Grupos

Al acceder a la pestaña **Grupos**, se mostrará el nombre del único grupo al que está asociado el dispositivo. Esta funcionalidad permite identificar de manera rápida y precisa la relación entre el dispositivo y su grupo correspondiente, facilitando su gestión dentro de la plataforma.



Vulnerabilidades

Al seleccionar la pestaña **Vulnerabilidades**, se desplegará un listado detallado de las vulnerabilidades detectadas que están asociadas al dispositivo. Además, la herramienta ofrece opciones de filtrado por severidad, lo que facilita priorizar aquellas vulnerabilidades más críticas que requieren atención inmediata.

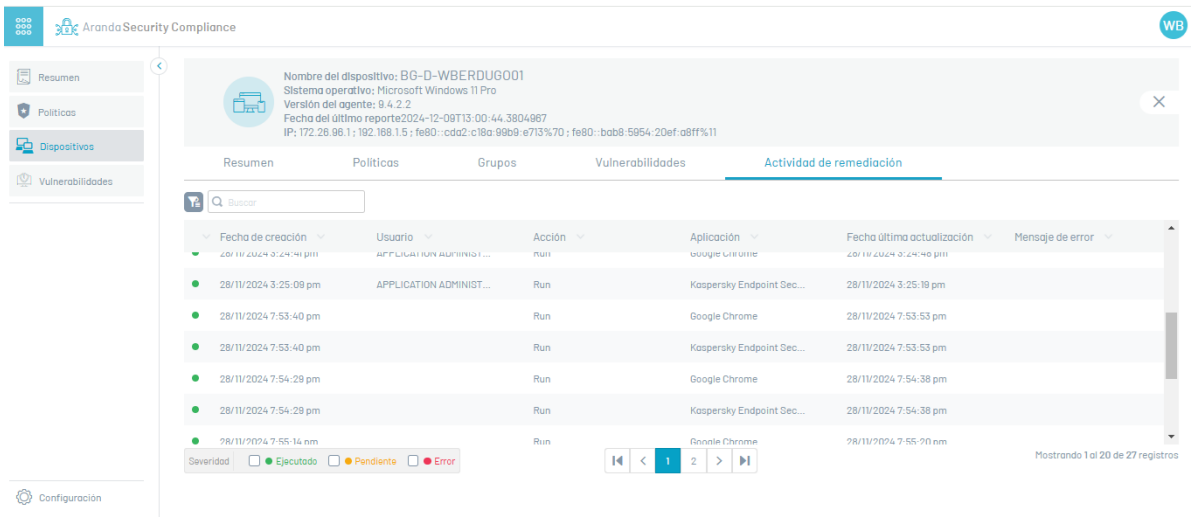


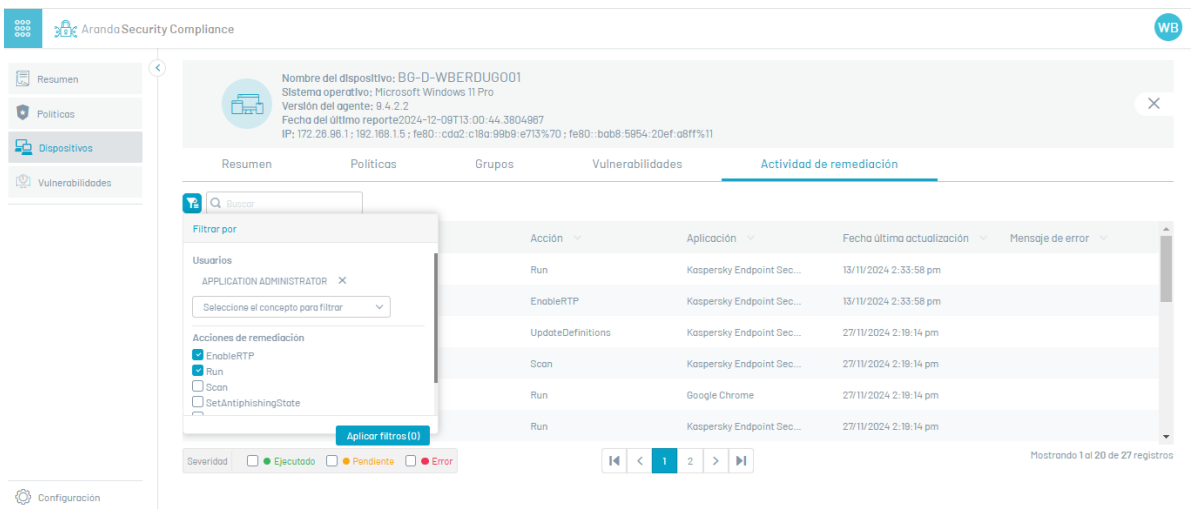
Actividad de Remediación

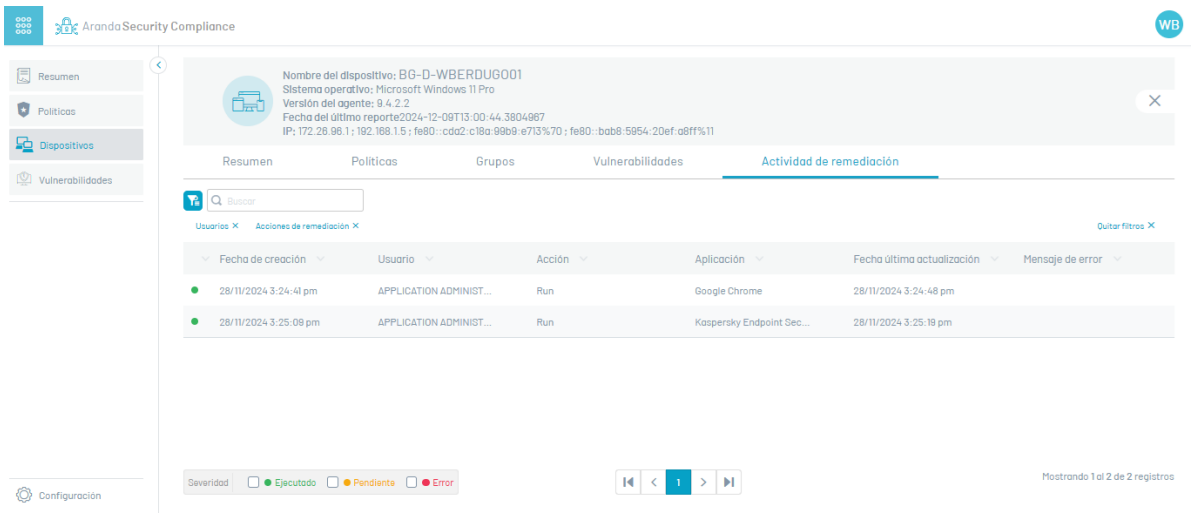
Al seleccionar la pestaña **Actividad de Remediación**, podrá visualizar el listado de las acciones realizadas en el dispositivo, permitiendo un seguimiento detallado de acuerdo a su estado de evolución (Ejecutado, Pendiente o Error) y facilitando la supervisión y gestión de las remediaciones.

⚐ **Nota:** En esta sección podrá Aplicar los filtros avanzados para buscar acciones específicas por usuario y/o acciones de remediación y/o utilizar los filtros por estado para identificar dispositivos o sistemas que requieren seguimiento, acciones correctivas o atención prioritaria.

Esta gestión agiliza la localización de intervenciones y asegura un acceso rápido a la información necesaria para el análisis y la toma de decisiones.







Configuración ASEC

Configuración ASEC

El administrador general desde la consola Web de ASEC podrá realizar las siguientes tareas de configuración:

1. Desplegar Agente

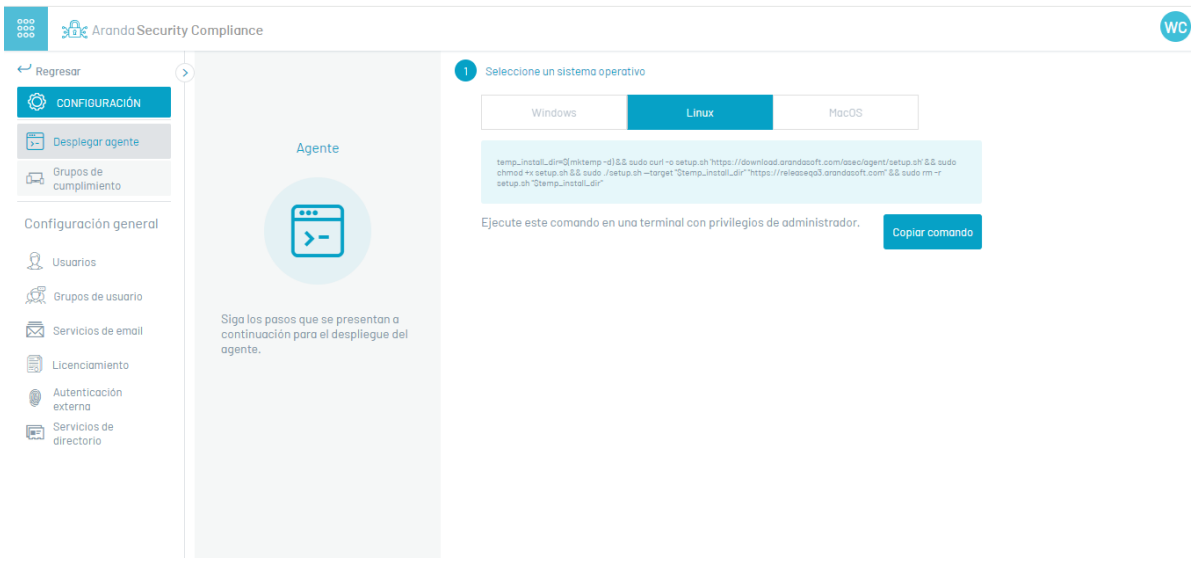
Distribuir el agente de Aranda Security en los diferentes dispositivos que requieran la evaluación de cumplimiento de las políticas de seguridad.

2. Grupos de Políticas

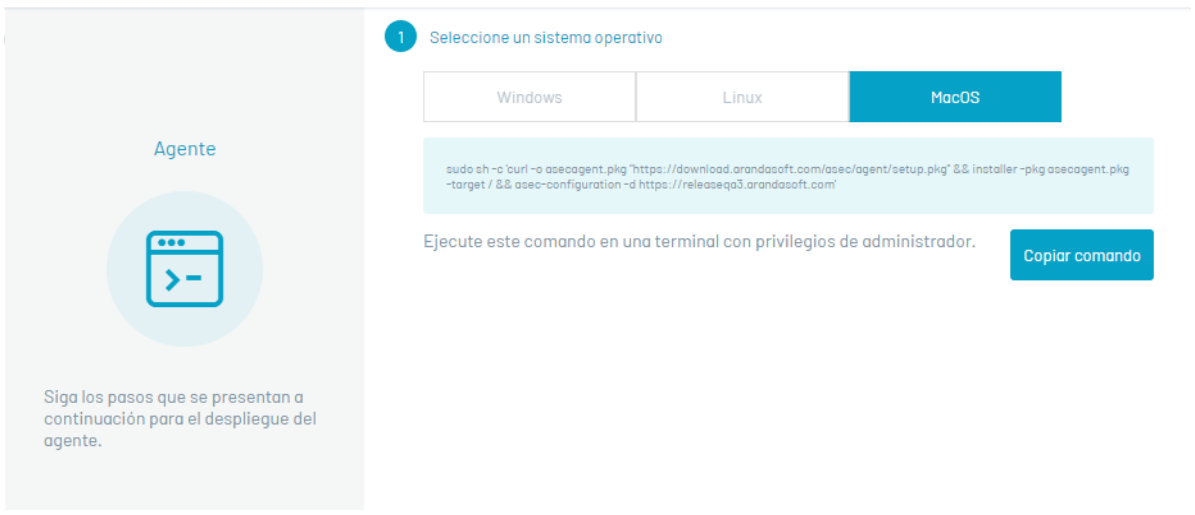
Gestionar los grupos asociados a las políticas de cumplimiento e incluir los dispositvos para cada grupo.

Desplegar Agente

1. Para desplegar el agente, ingrese a la consola de Aranda Security Compliance como administrador, en la sección de **Configuración** del menú principal, seleccione la opción **Desplegar Agente**. En la vista de información se podrá visualizar los pasos para desplegar el agente en los dispositivos.



2. En la vista de información de despliegue del agente, seleccione un sistema operativo (Wndows,Linux, Mac).



3. Al seleccionar el sistema operatvo, se habilita el script para instalar e inscribir al agente. Haga clic en el botón **Copiar Comando**; esta información será guardada en el portapapeles.

4. Copie el comando de ejecución y continue el procceso de distribución e instalación del agente ASEC, de acuerdo al tipo de despliegue definido:

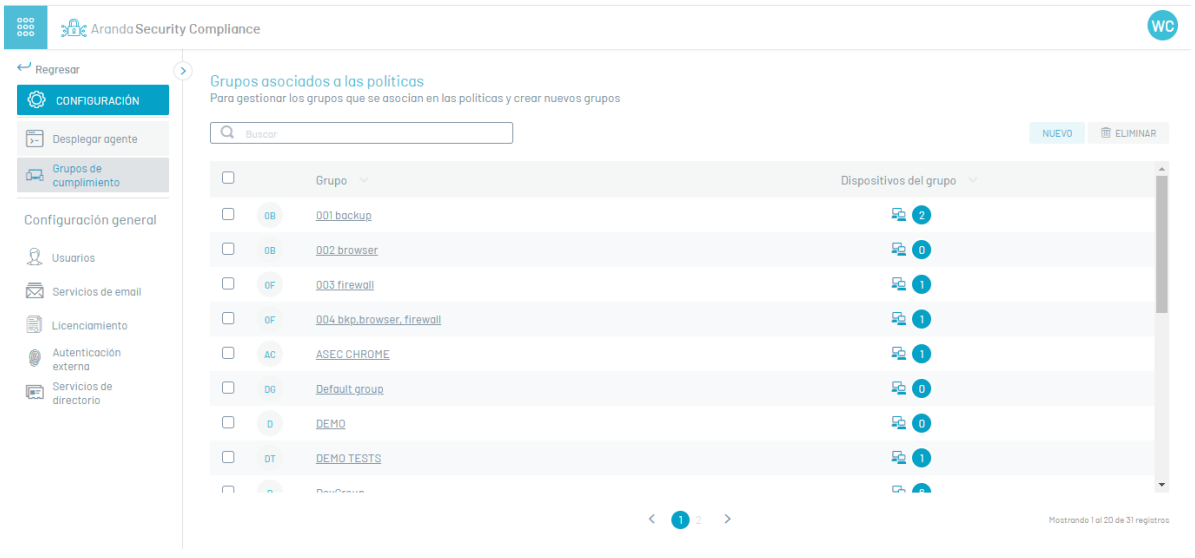
- Instalación por Dispositivos ↪
- Instalación por Política de Dominio ↪
- Instalación y distribución con Aranda Device Management ADM ↪

Grupos de Políticas

En la sección se encuentran los grupos que son creados desde la consola de Aranda Security Compliance.

Visualizar grupos y Dispositivos

1. Ingrese a la consola de Aranda Security Compliance con rol de administrador, en la sección de **Configuración** del menú principal, seleccione la opción **Grupos de cumplimiento**. En la vista de información se podrá visualizar el listado grupos disponibles y ordenar la información por nombre de grupos y dispositivos.



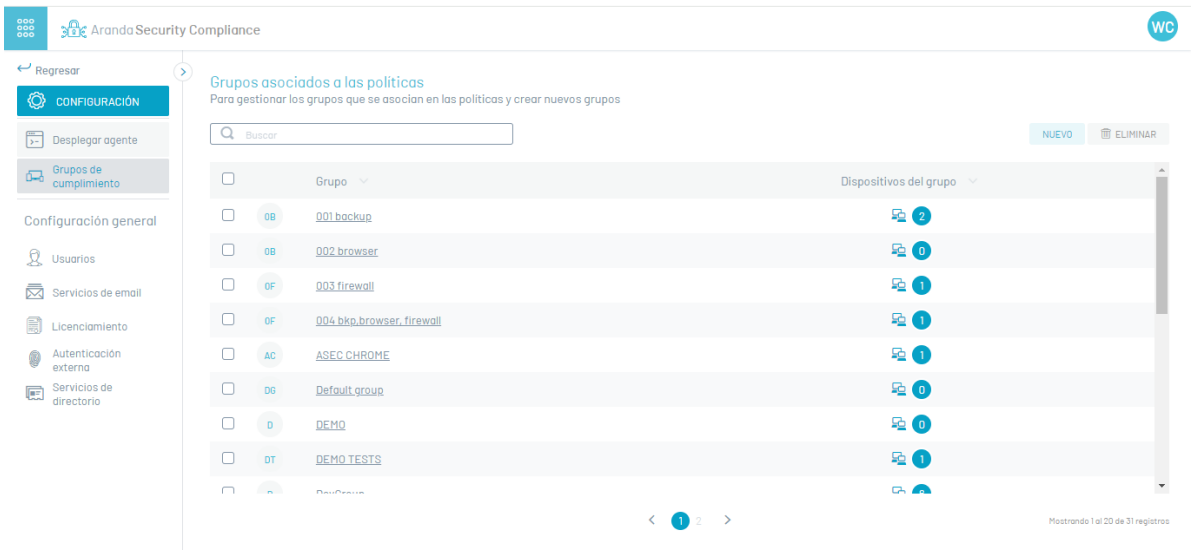
2. En la vista de información de grupos también podrá visualizar el listado de dispositivos que pertenecen a cada grupo.

> ⚐ **Nota:** Si el grupo tiene una política asociada presentará el estado de dispositivos y las respectivas acciones de remediación que se puedan aplicar.

Creación de grupos

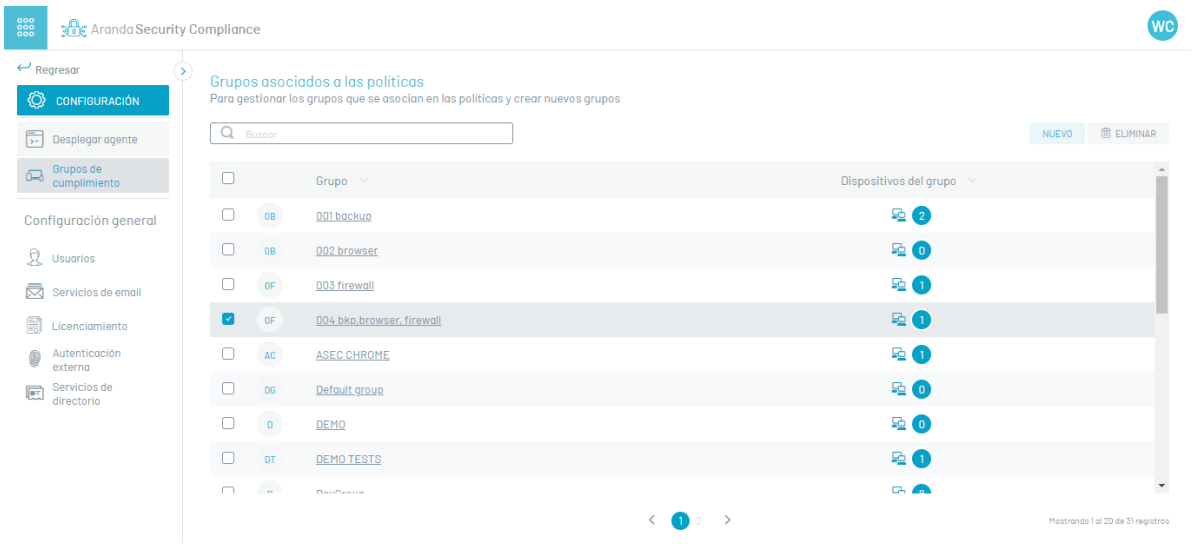
3. Para crear grupos de políticas, en la vista de información de grupos seleccione el botón **Nuevo**; se habilita la ventana **Dispositivos** donde podrá ingresar el nombre del grupo.

Al ingresar de nuevo al grupo creado tendrá habilitadas las opciones para asociar y desasociar dispositivos.



Eliminar de grupos

4. Para eliminar grupos, en la vista de información de grupos seleccione un registro del listado y haga clic en el botón Eliminar.

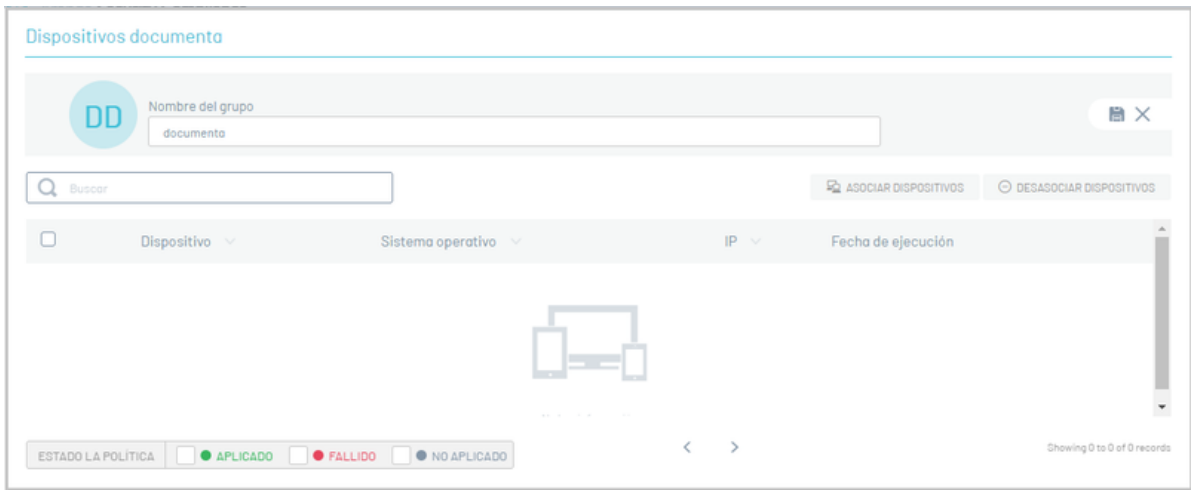


En la ventana que se habilita podrá confirmar o denegar la acción de eliminar el grupo.

⚐ **Nota:** Si el grupo tiene dispositivos asociados, al momento de confirmar la acción, los dispositivos quedarán disponibles para ser asociados a otro grupo.

Asociar dispositivos

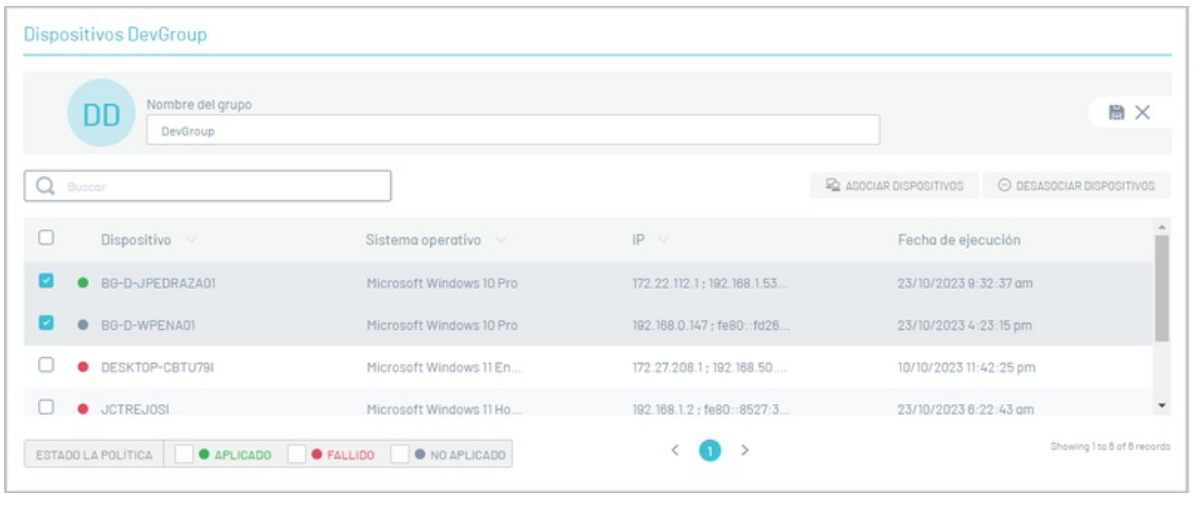
5. Para asociar dispositivos, en la vista de información de grupos, ingrese a un registro de un grupo creado y en la ventana **Dispositivos** haga clic en el botón **Asociar Dispositivos**.



En el listado de dispositivos seleccione un registro y haga clic en el botón **Asociar Dispositivos** , para asociar el dispositivo al grupo.

Desasociar dispositivos

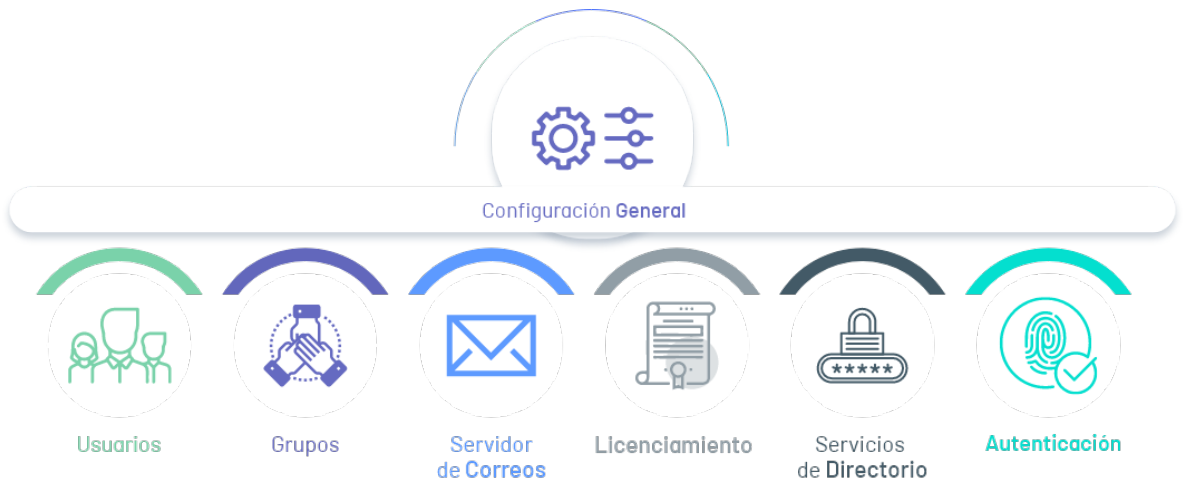
6.Para desasociar dispositivos, en la ventana Dispositivos seleccione un registro y haga clic en el botón Desasociar Dispositivos.



Configuración General

Configuración General

El administrador general desde la consola Web de ASEC podrá configurar los siguientes módulos transversales:



1. Usuarios

En este módulo de Aranda Common podrá configurar los usuarios encargados de la gestión de las políticas de seguridad . Estas configuraciones sólo las puede realizar un usuario con rol de administrador. Adicionalmente podrá asignar los roles Administrador y Especialista.

Para mayor información consulte el módulo Gestión de Usuarios ↪.

2. Grupos de usuarios

En este módulo de Aranda Common podrá configurar y administrar los grupos de usuarios para realizar la asignación de roles de una manera más eficiente.

Para mayor información consulte el módulo Gestión de Grupos ↪.

3. Configurar Servidores de Correo

En este módulo de Aranda Common podrá configurar un proveedor de correo para la operación de Arandda Security Compliance, desde este servidor se enviarán notificaciones a los usuarios. Se configura el correo para poder realizar la recuperación de contraseña de usuarios que hayan sido creados manualmente (No aplica para los que son importados).

Para mayor información consulte la Gestión de Servidor de Correos ↪.

3. Gestionar Licencias

Aranda Security Compliance permite gestionar las licencias adquiridas y asociarlas a los dispositivos requeridos para realizar una adecuada gestión de las políticas de seguridad.

Para mayor información consulte la Gestión de Licencias ↪.

4. Servicios de Directorio

En este módulo de Aranda Common podrá configurar los servicios de directorio que pueden ser usados en la aplicación de Aranda Security, como el protocolo ligero de acceso a directorios **LDAP**, que permite configurar la conexión con otros directorios empresariales o el servicio de directorios **Azure Active Directory**

Para mayor información consulte la Gestión Servicios de Directorio ↪.

5. Configurar Proveedores de Autenticación

En este módulo de Aranda Common podrá definir los proveedores de autenticación externa, que siguen el estandar SAML (Security Assertion Markup Language) para realizar la autenticación del usuario en la aplicación.

Para mayor información consulte la Gestión Proveedores de Autenticación ↪.