



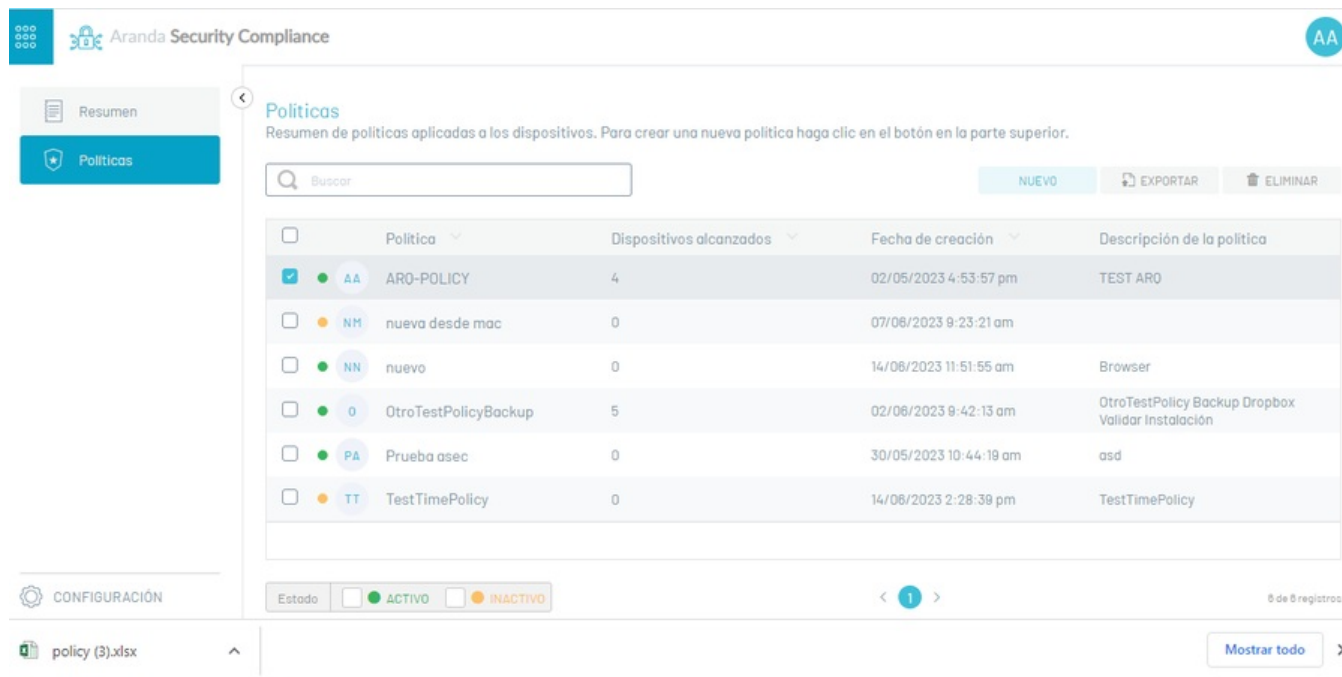
Aranda Security Compliance

Exportar

title: Exportar chapter: ""

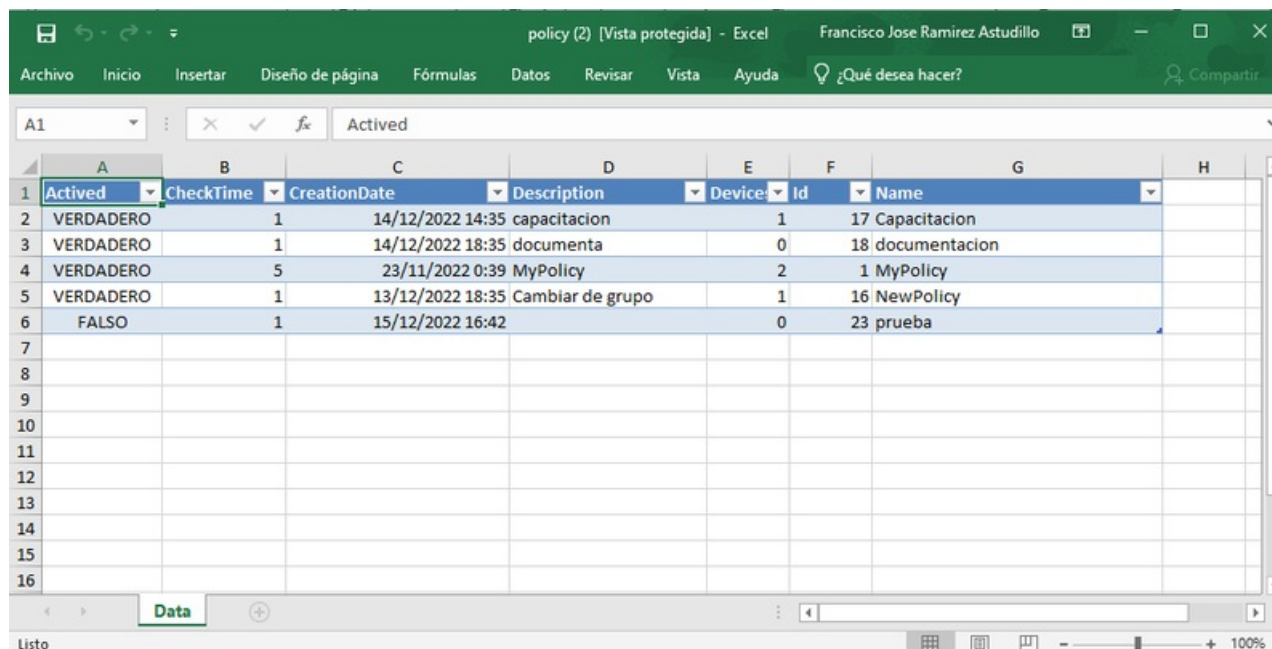
Exportar Políticas

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; seleccione uno o varios registros y haga clic en el botón Exportar.



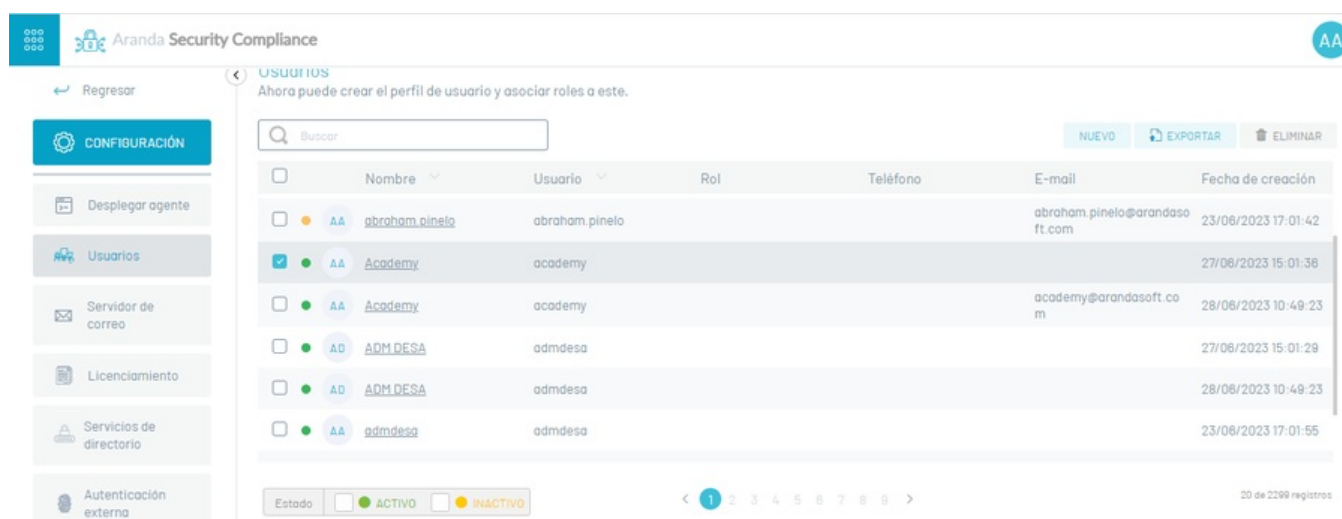
2. En el menú encabezado de la consola de administración de Aranda Security, se habilita la opción de Descargas donde podrá visualizar el formato generado del listado de políticas en formato excel

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



Exportar Usuarios

1. Para exportar la información de usuarios, ingrese a la consola de Aranda Security con rol de administrador, en la sección de Configuración del menú principal, seleccione la opción Usuarios. En la vista de información se podrá visualizar el listado usuarios disponibles; seleccione uno o varios registros y haga clic en el botón Exportar.



2. El sistema Descarga el formato generado con el listado de usuarios seleccionado en formato excel. El archivo descargado incluye todos los campos de usuarios.

Created	Email	Id	IsActive	Name	Phone	UserNa	Role
23/06/2023 22:01	francois.jeanneret@arandasoft.com	146	FALSO	fjeanneret		fjeanneret	
27/06/2023 20:01		1535	VERDADERO	Francisco Gabriel Melgarejo Delgado		francisco.melgarejo	
28/06/2023 15:48	francisco.melgarejo@arandasoft.com	1596	VERDADERO	Francisco Gabriel Melgarejo Delgado		francisco.melgarejo	
28/06/2023 15:48	francisco.gomez@arandasoft.com	1820	FALSO	Francisco Jose Gomez		francisco.gomez	
27/06/2023 20:01		1052	FALSO	Francisco Jose Gomez		francisco.gomez	
28/06/2023 15:51	francisco.ramirez@arandasoft.com	2222	VERDADERO	Francisco Jose Ramirez Astudillo		francisco.ramirez	
23/06/2023 22:01	francisco.gomez@arandasoft.com	284	FALSO	francisco.gomez		francisco.gomez	
23/06/2023 22:01	francisco.melgarejo@arandasoft.com	61	VERDADERO	francisco.melgarejo		francisco.melgarejo	
23/06/2023 22:04	francisco.ramirez@arandasoft.com	684	VERDADERO	francisco.i.7563000 ext: 355/354		francisco.ramirez	
27/06/2023 20:01		889	FALSO	Francois Jeanneret		fjeanneret	
28/06/2023 15:48	francois.jeanneret@arandasoft.com	1682	FALSO	Francois Jeanneret		fjeanneret	
28/06/2023 15:48		1687	VERDADERO	Juan Francisco Carrillo		jcarrillo	
27/06/2023 20:01		898	VERDADERO	Juan Francisco Carrillo		jcarrillo	
27/06/2023 20:01		1399	VERDADERO	Julian Ernesto Franco Salas		julian.franco	
28/06/2023 15:52	julian.franco@arandasoft.com	2240	VERDADERO	Julian Ernesto Franco Salas		julian.franco	
23/06/2023 22:04	julian.franco@arandasoft.com	701	VERDADERO	julian.franco	7563000	julian.franco	
27/06/2023 20:01		1015	FALSO	Wilfran Yesid Pacheco Tellez		wilfran.pacheco	
28/06/2023 15:48	wilfran.pacheco@arandasoft.com	1789	FALSO	Wilfran Yesid Pacheco Tellez		wilfran.pacheco	
23/06/2023 22:01	wilfran.pacheco@arandasoft.com	253	FALSO	wilfran.pacheco		wilfran.pacheco	

Exportar Servidores

1. Para exportar la información de servidores, ingrese a la consola de Aranda Security con rol de administrador, en la sección de Configuración del menú principal, seleccione la opción Servidor de Correo. En la vista de información podrá visualizar el listado servidores disponibles; seleccione uno o varios registros y haga clic en el botón Exportar.

Nombre	Servidor	Tipo	Usuario	Nombre remitente	E-mail
AS AMDM Mail Server	outlook.office365.com	OAuth		AEMM	javier.salazar@arandasoft.com
AM AQM basic mail	smtp.office365.com	Básica	store@arandasoft.com	Aranda Query Manager	store@arandasoft.com
AM AQM OAuth mail	smtp.office365.com	OAuth		Aranda Query Manager	store@arandasoft.com
AS ASEC QA Server	outlook.office365.com	Básica	fredy.cardenas@arandasoft.com	asec qa	fredy.cardenas@arandasoft.com
DD Default	malika.org	Básica	Douglas21@yahoo.com	Dr. David Rayner	Vada.Dickinson@yahoo.com
DD Default	jazmyn.org	Básica	Eva26@yahoo.com	Dwayne Schuppe	Sandy_Jenkins@yahoo.com
DD Default	delores.com	Básica	Gust.Hammes@yahoo.com	Edna Nolan	Margaretta_Kutch@yahoo.com

2. El sistema descarga el formato generado con el listado de servidores seleccionado en formato excel. El archivo descargado incluye todos los campos de servidores.

AccessToken	AuthorizationUrl	ClientId	ClientSecret	Default	Id	IsSSL	Port	RefreshToken	Scopes	Sender	ServerName
eyJ0eXAiOiJKV1QiOiJhttps://login.microsoftonline.com/9a-bcedcb9a-zUj8Q~ito				FALSO	28	VERDADERO	587	0.ARwA4xoffline_ac		javier.salazar	AMDM Mail outlook.o
				FALSO	28	VERDADERO	587			store@arand	Aranda Query Manager smtp.offic
eyJ0eXAiOiJKV1QiOiJhttps://login.microsoftonline.com/c49bd051-HNZ8Q~et				FALSO	29	VERDADERO	587	0.ARwA4xoffline_ac		store@arand	Aranda Query Manager AQM OAuth smtp.offic
				FALSO	27	VERDADERO	587			fredy.carden	asec qa ASEC QA S outlook.o
				FALSO	9	VERDADERO	239			Vada.Dickins	Dr. David I Default malika.org
				FALSO	11	VERDADERO	893			Sandy_Jenki	Dwayne S Default jazmyn.or
				FALSO	14	VERDADERO	715			Margaretta_	Edna Nola Default delores.cc
				FALSO	7	VERDADERO	634			Zoe.Hudson	Ervin Row Default danika.na
				FALSO	16	VERDADERO	550			Malinda.Wuc	Garry Schr Default sigrid.nam
				FALSO	24	VERDADERO	280			Ricky.Ernser	Jerome Fr Default lester.com
				FALSO	21	VERDADERO	618			Lulu_Pauceki	Karen D'A Default mara.com
				FALSO	17	VERDADERO	519			Bernhard_Ch	Kelly Dani Default lane.com
				FALSO	23	VERDADERO	960			Heather_Kee	Laurence I Default norbert.ne
				FALSO	8	VERDADERO	698			Malinda_Hoe	Leo King Default karl.biz
				FALSO	5	VERDADERO	706			Nikki34@gm	Maxine Yl Default kattie.net
				FALSO	12	VERDADERO	494			Maryjane36	Miss Ama Default jeramie.n
				FALSO	13	VERDADERO	64			Enid_Dicken	Myra Aber Default judge.org
				FALSO	6	VERDADERO	702			Ines_Leanno	Neal Smit Default gregorio.b
				FALSO	26	VERDADERO	587			nidia.alejo	Niida Default outlook.o
				FALSO	20	VERDADERO	195			Diego.Welch	Phil Schro Default jazlyn.org
				FALSO	25	VERDADERO	587			julieth.manc	Pruebas AFLS DEF smtp.offic
				FALSO	15	VERDADERO	872			Sydnie.Metz	Ray Skiles Default verlie.org

detectar y visibilizar los riesgos 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?

- [Guía de Inicio Aranda Security Compliance ASEC](#)
- [Manual de Usuario Aranda Security Compliance ASEC](#)

Definición Políticas ASEC

title: Definición Políticas ASEC chapter: "definicion_politicas" –

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 dispositivos 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

title: Gestionar Políticas chapter: "definicion_politicas" –

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.

Política	Dispositivos alcanzados	Fecha de creación	Descripción de la política
0V 001.backup_vm22	3	01/01/0001 12:03:44 am	TEST
01 002.browser_vm.1	0	29/08/2023 11:33:49 am	detalle
0V 003.firewall_vm3	1	11/07/2023 4:07:15 pm	Comodo firewall
0V 004.bkp.browser.firewall.y...	1	11/07/2023 3:58:32 pm	
0A 005.LOCAL.ANTIPHISHING	0	28/07/2023 11:40:25 am	
DE DEMO.ENTREGA	0	08/10/2023 7:00:00 pm	DETALLE
DT DEMO.TEST	2	02/10/2023 7:00:00 pm	DEMO TEST
DD DEV.DEVICES	6	05/07/2023 2:19:11 pm	testDev

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:

Sistema operativo

Las políticas se configurarán de acuerdo con el sistema que seleccione



W Windows

L Linux

M MacOS

Política - Nueva Política

Detalles y configuración de la política

NP Nombre de la política: Nueva Política
Sistema operativo Linux

Tiempo de monitoreo: 1 Minutos

Descripción: Nueva Política

ESTADO: Deshabilitado

Criterios de políticas

Seleccione uno o agregue criterio para la política

VPN Client

VPN CLIENT

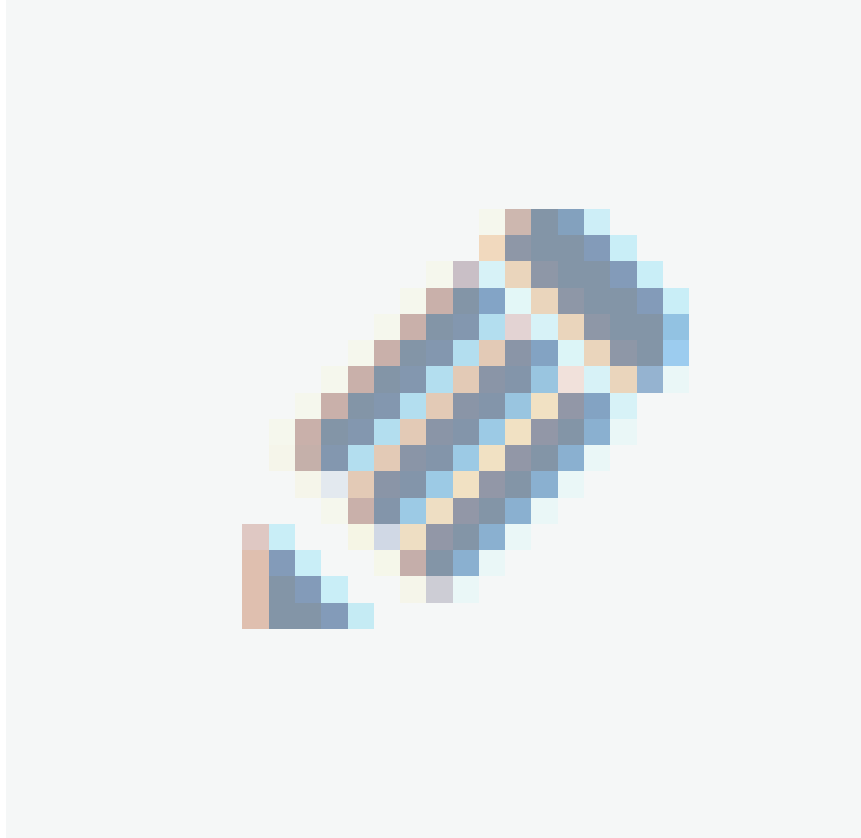
El programa debe ser: Seleccione un programa

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 políticas** y escoja del listado un criterio de software de configuración. Los [criterios habilitados](#) en ASEC son: ANTIMAWARE, ANTIPIHING, 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.

WEB BROWSER
Google Chrome

El programa debe ser

Google Chrome

Validar versión mínima

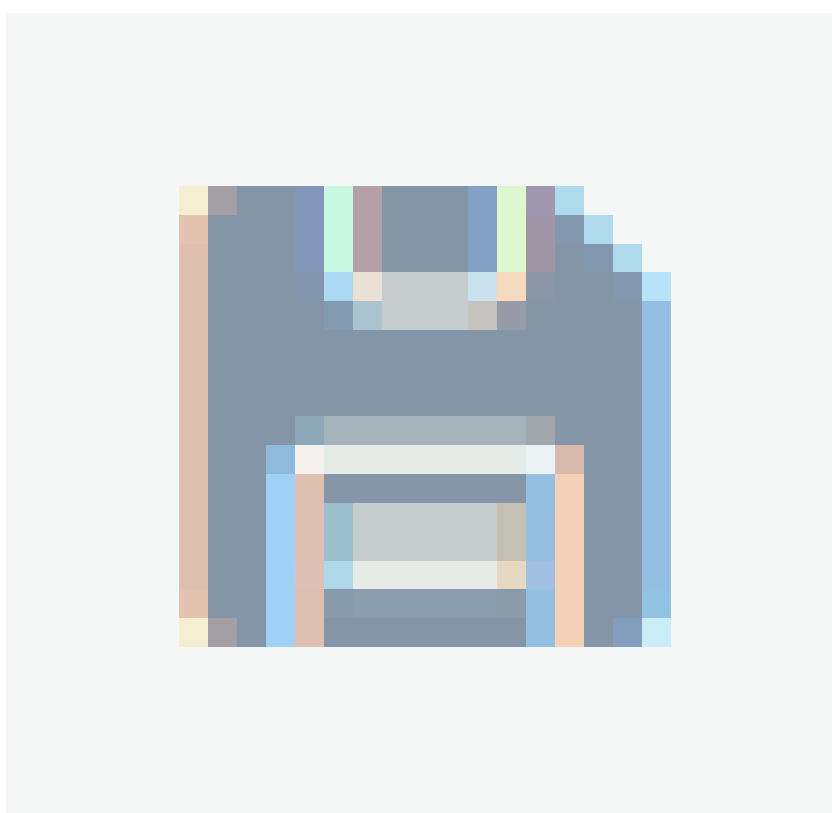
Validar navegador predeterminado

Verificar instalación

Validar protección de antiphishing

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 distintas 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.

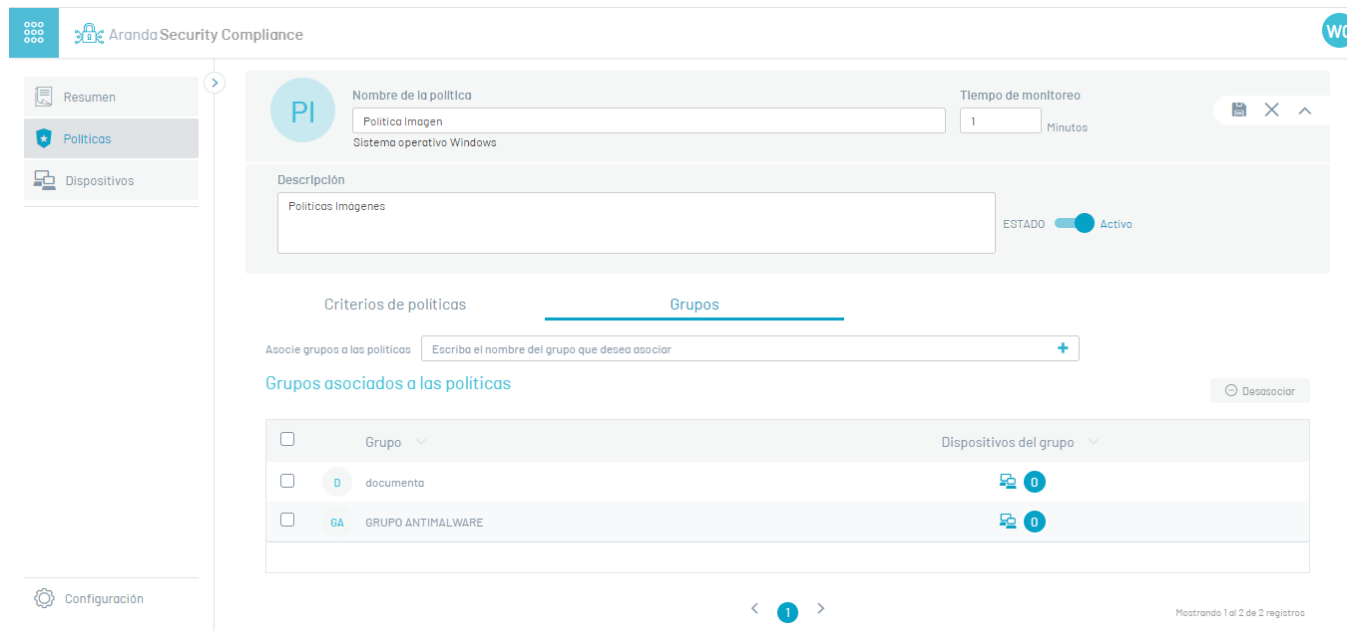
Estos criterios son los que se evalúan y determinan si una política se cumple o no.

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

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

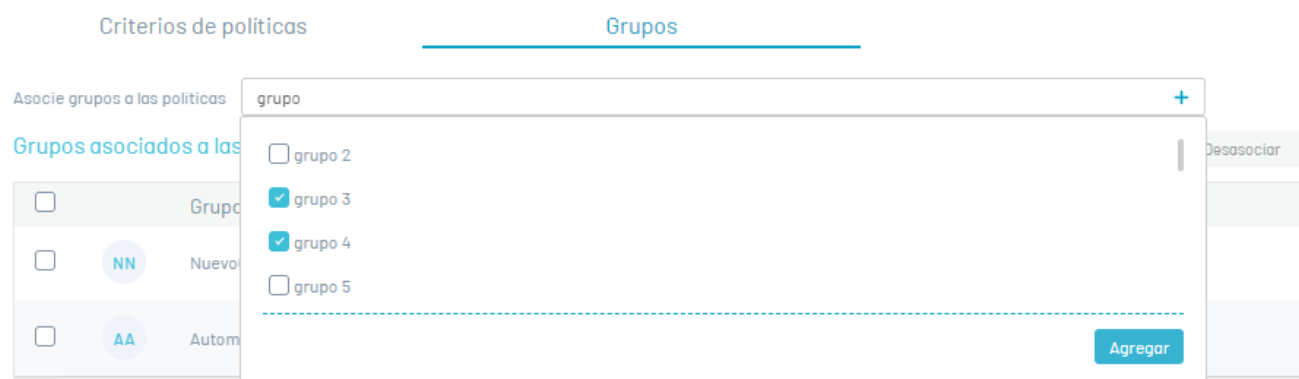
Asociar Grupos

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**

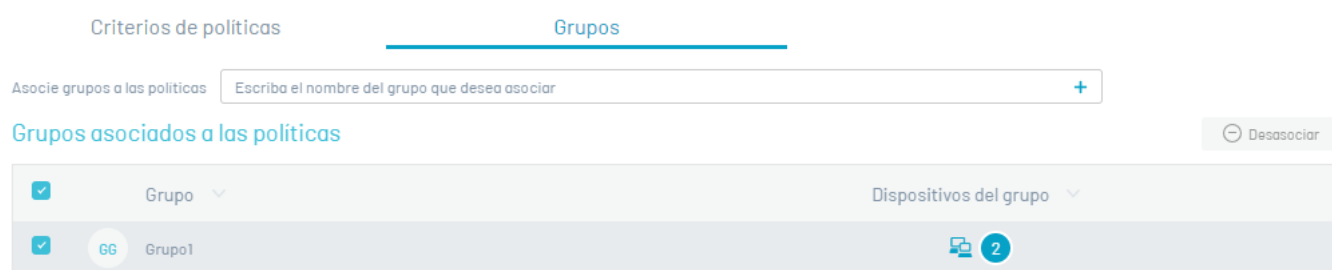


9. En el listado de grupos asociados seleccione el nombre del grupo con dispositivos vinculados, para acceder a [detalle de Cumplimiento de los Dispositivos](#)

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 clic 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 opción 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.

Active	CreationDate	Description	Device	Id	Name	Platform	PlatformName
True	10/30/2023 9:09:34 PM	Política mínima de verificación	1	130	Política - Walter 1	Windows	Política - Walter 1
True	9/5/2023 2:16:08 PM	FirewallEdgeChrome	0	111	Política BR	Windows	Política BR
True	10/6/2023 12:00:00 AM	detalle politica firewall	0	121	politica firewall	Windows	politica firewall
True	10/10/2023 12:00:00 AM	Descripcion	1	128	Política FW	Windows	Política FW
True	10/3/2023 12:00:00 AM	TEST	6	113	POLITICA VM AZURE	Windows	POLITICA VM AZURE
True	11/7/2023 9:02:24 PM	prueba1	0	131	Politica1	Windows	Politica1

Validaciones por Criterios

title: Validaciones por Criterios chapter: "definicion_politicas"

Las políticas configuradas en Aranda Security evalúan 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 distintas 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
	<ol style="list-style-type: none"> 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.

BROWSER
Microsoft Edge

Establecer versión mínima Validar protección de antiphishing

Validar navegador predeterminado Validar instalación

El programa debe ser

Microsoft Edge

2. Validar Estado de Protección en Tiempo Real

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

Retorno	Descripción
CUMPLE	Si el software tiene habilitada la protección 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 software **Kaspersky Endpoint Security** tenga la protección en tiempo real habilitada.

ANTIMALWARE
Kaspersky Endpoint Security

Establecer versión mínima Validar estado de protección en tiempo real

Validar protección del firewall Validar protección de antiphishing

Validar instalación

El programa debe ser

Kaspersky Endpoint Security

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.

ANTIMALWARE
Norton AntiVirus

Establecer versión mínima Validar estado de ejecución

Validar estado de protección en tiempo real Validar protección del firewall

Validar protección de antiphishing Validar instalación

El programa debe ser

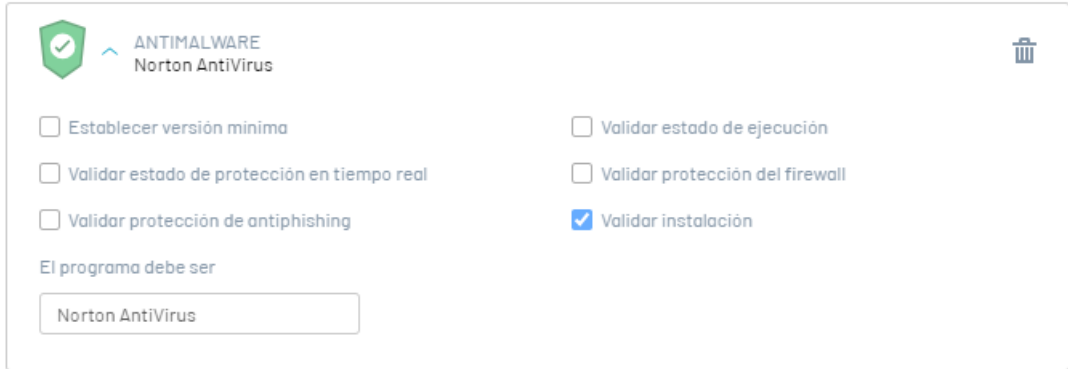
Norton AntiVirus

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.

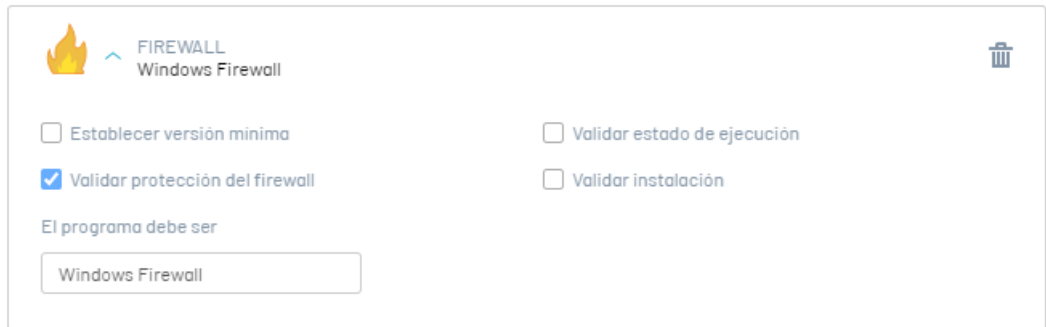


5. Validar Protección Firewall

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 software **Windows Firewall** tenga activa la protección del FIREWALL.



6. Validar Protección 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 software **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

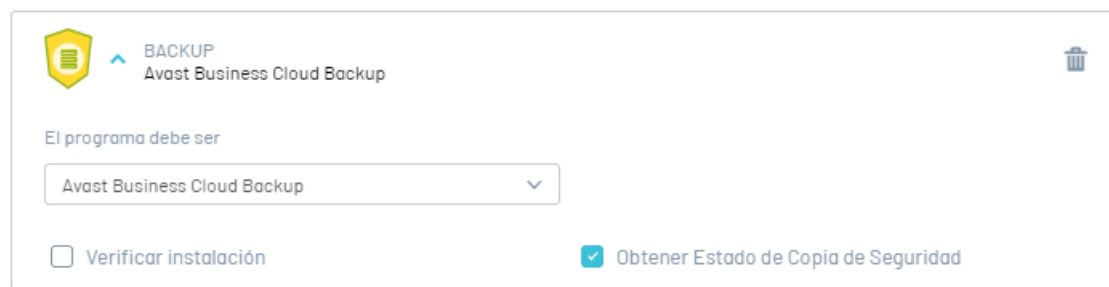
8. Validar estado de Copia de Seguridad

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

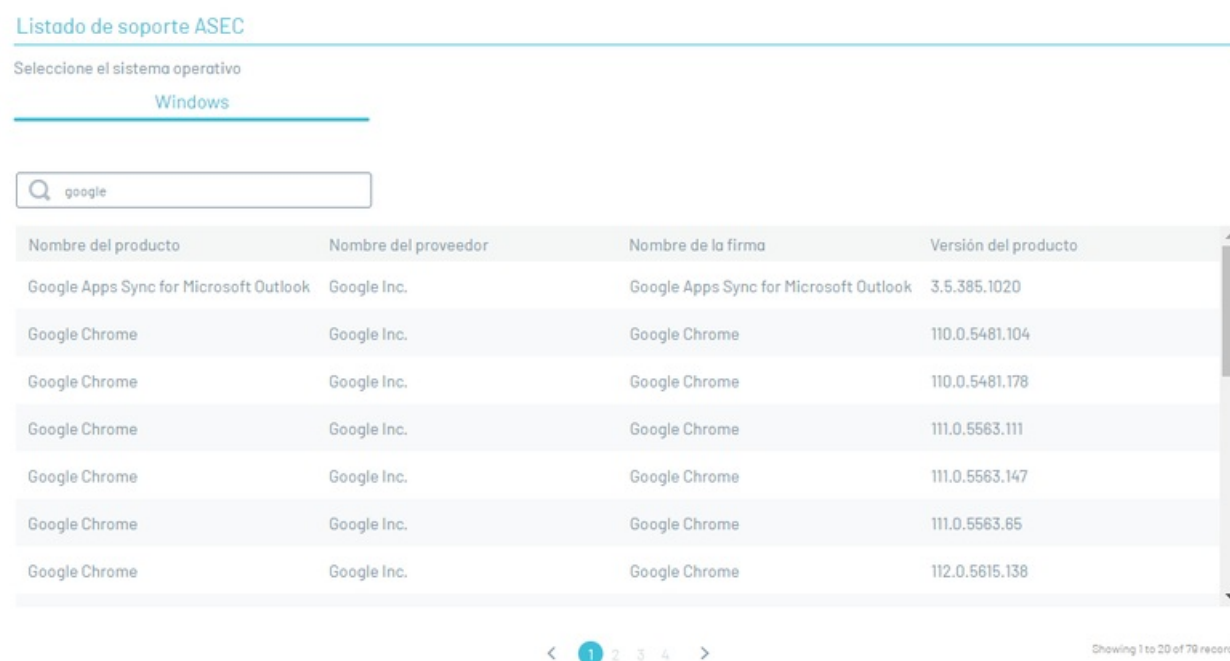
Se valida que se pueda obtener el estado de copia de seguridad del software Avast Business Cloud Backup .



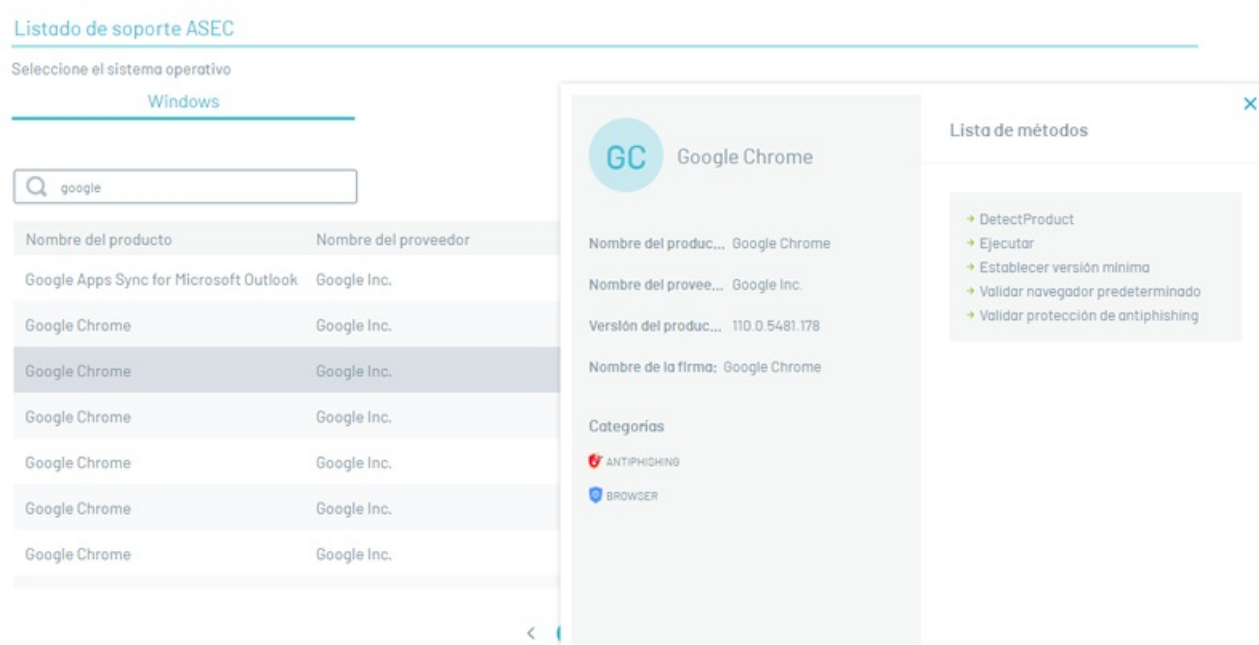
Visualizar Listado de Aplicaciones de seguridad

title: "Visualizar Listado de Aplicaciones de seguridad" chapter: "" –

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 políticas 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 (ANTIMWARE, ANTIPHISHING, 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.



Crterios Políticas

title: Criterios Políticas chapter: –

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
	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



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 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.



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.



Los programas VPN Client son aplicaciones que permiten a los usuarios establecer conexiones seguras a una red privada virtual (VPN) desde

Criterio

Descripción
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.

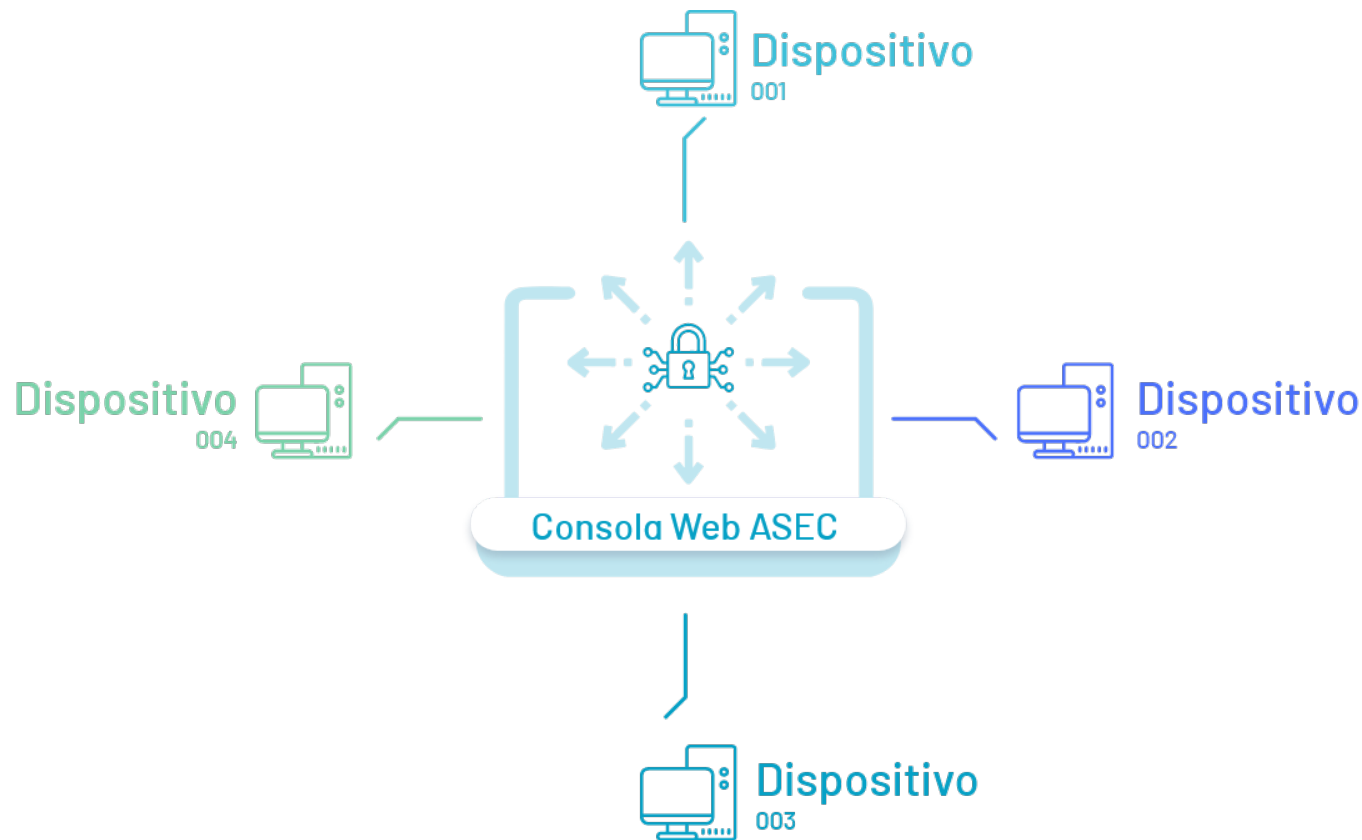


Los programas Web Browser, o navegadores web, son aplicaciones que permiten a los usuarios acceder y navegar por páginas web en Internet. Ofrecen funciones como abrir múltiples pestañas, gestionar marcadores y buscar en la web. Ejemplos populares incluyen Google Chrome, Mozilla Firefox, Microsoft Edge, Safari y Opera. Son fundamentales para la experiencia de navegación en Internet.

\n## Agente Aranda Security – title: Agente Aranda Security chapter: “despliegue_e_instalacion” –

El agente en ASEC es el componente encargado de validar que las políticas de seguridad 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 dispositivo.

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

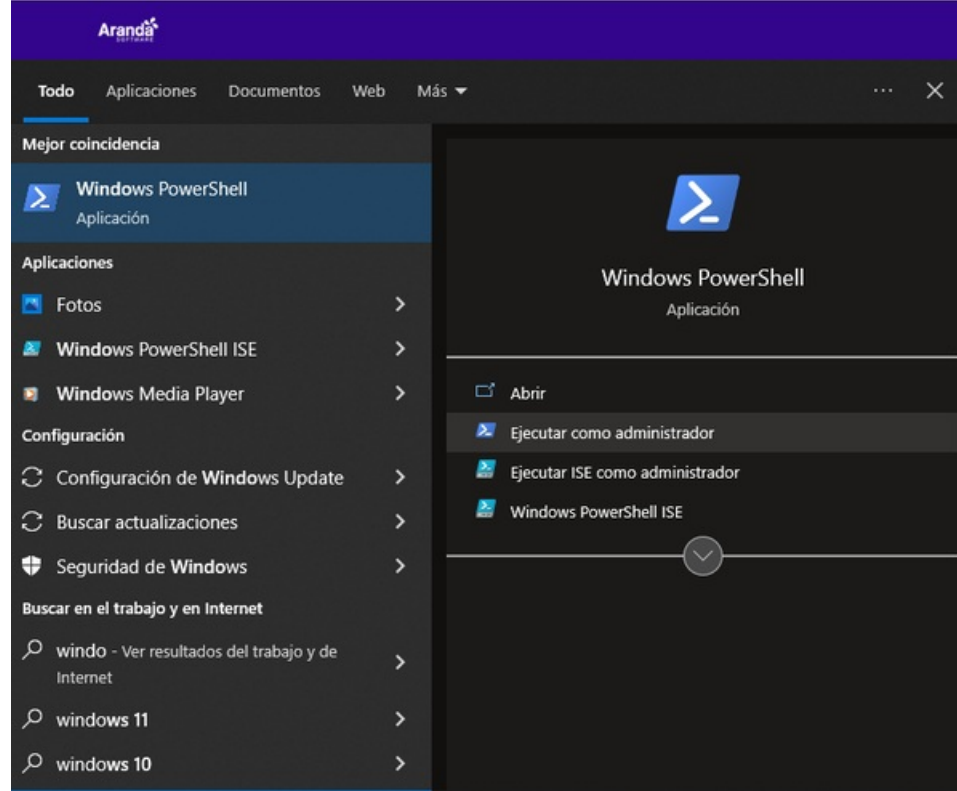
- **Despliegue Por Dispositivos:** A través de la consola web de Aranda Security podrá hacer el despliegue y posterior instalación del agente ASEC en los dispositivos.
- **Despliegue por Política de Dominio:** La instalación del agente podrá realizarse a través de la política de dominio.
- **Despliegue 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.

\n## Despliegue e Instalación de Agente por Dispositivos

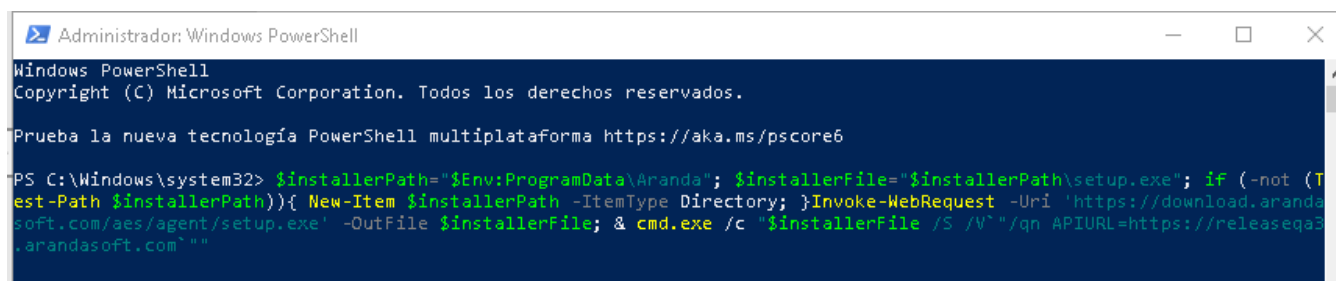
title: Despliegue e Instalación de Agente por Dispositivos chapter: "" –

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

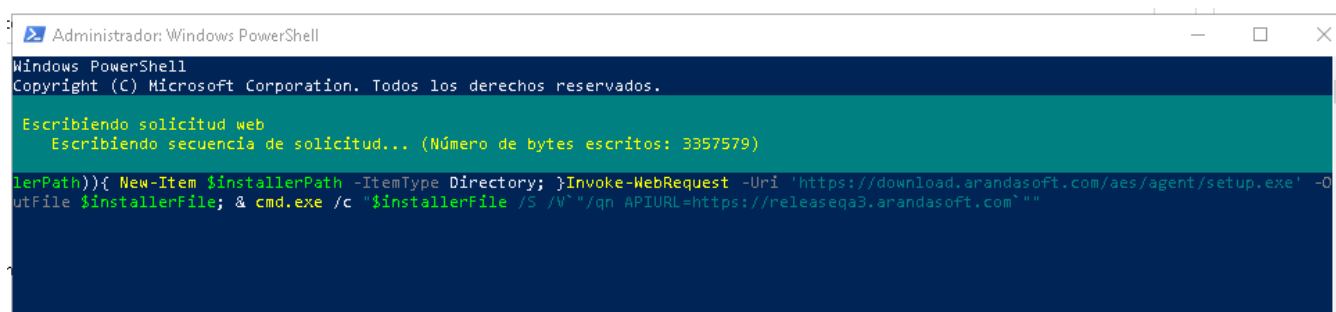
1. Abra Windows PowerShell y ejecute el programa como administrador.



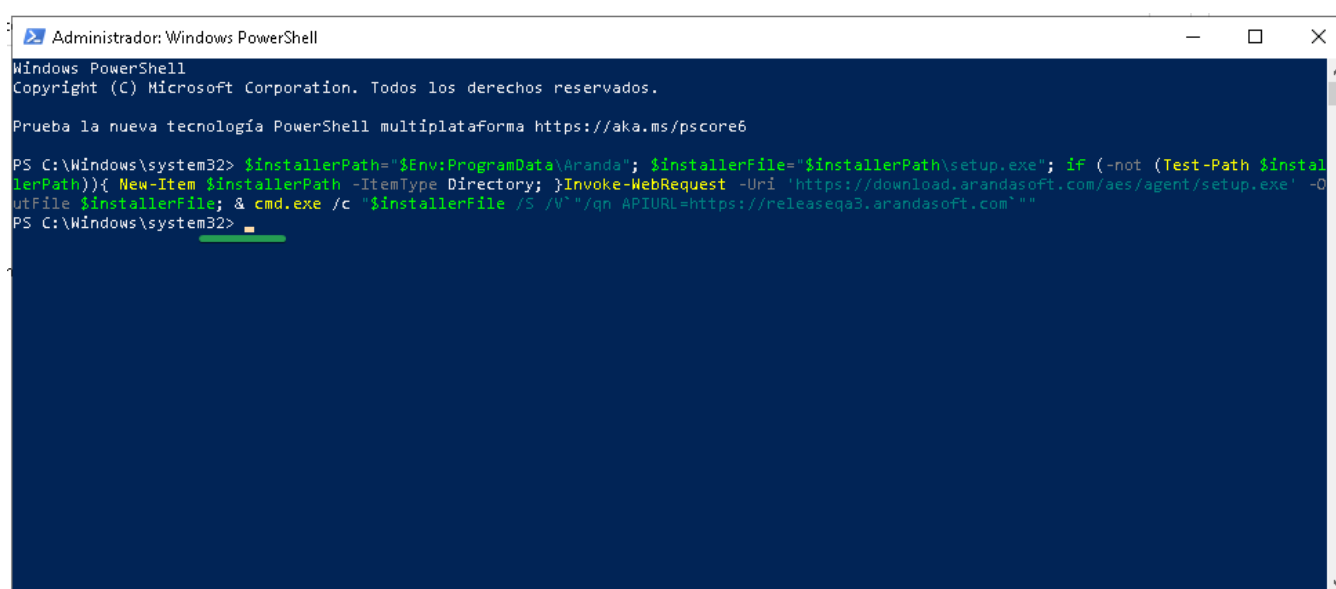
2. El comando copiado de la pantalla [Desplegar Agente](#) en la consola web de ASEC, péguelo en el PowerShell y deEnter. Se iniciará la instalación del agente en el dispositivo.



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



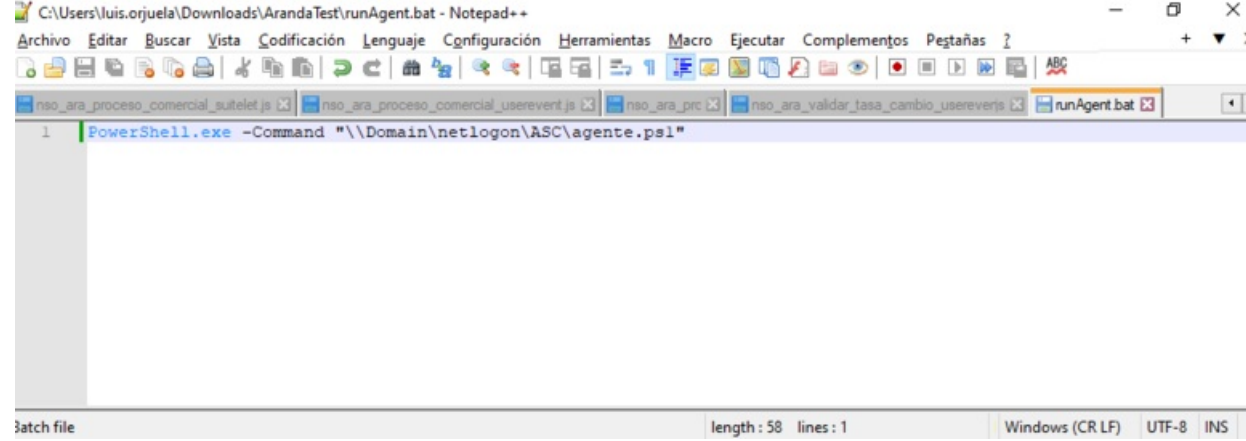
4. Finalizado el proceso de instalación, se presentará de nuevo el cursor sobre la consola de PowerShell y a partir de ese momento el agente iniciará la verificación de las políticas.



\n## Despliegue del Agente ASEC por Política de Dominio – title: Despliegue del Agente ASEC por Política de Dominio chapter: "" –

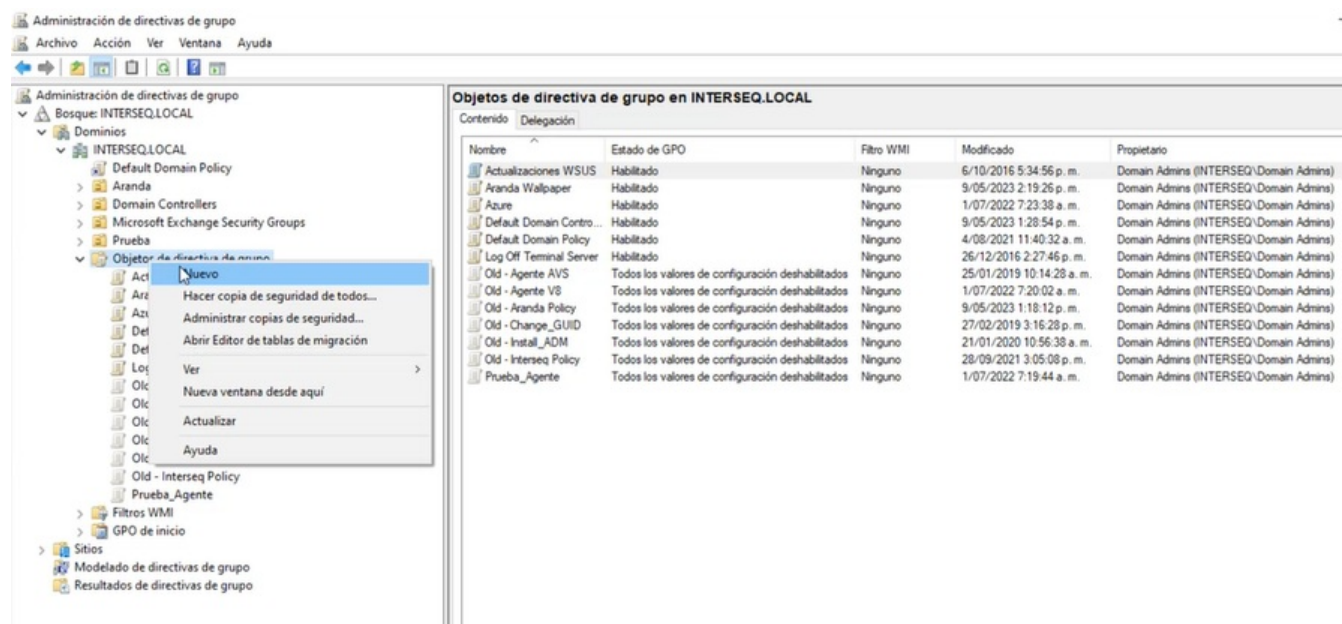
Crear Archivos de ejecución

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 extensión ps1 incluyendo el comando copiado, para posteriormente ejecutarlo en el dominio requerido.
2. Defina un archivo .bat con la ruta del dominio requerido.



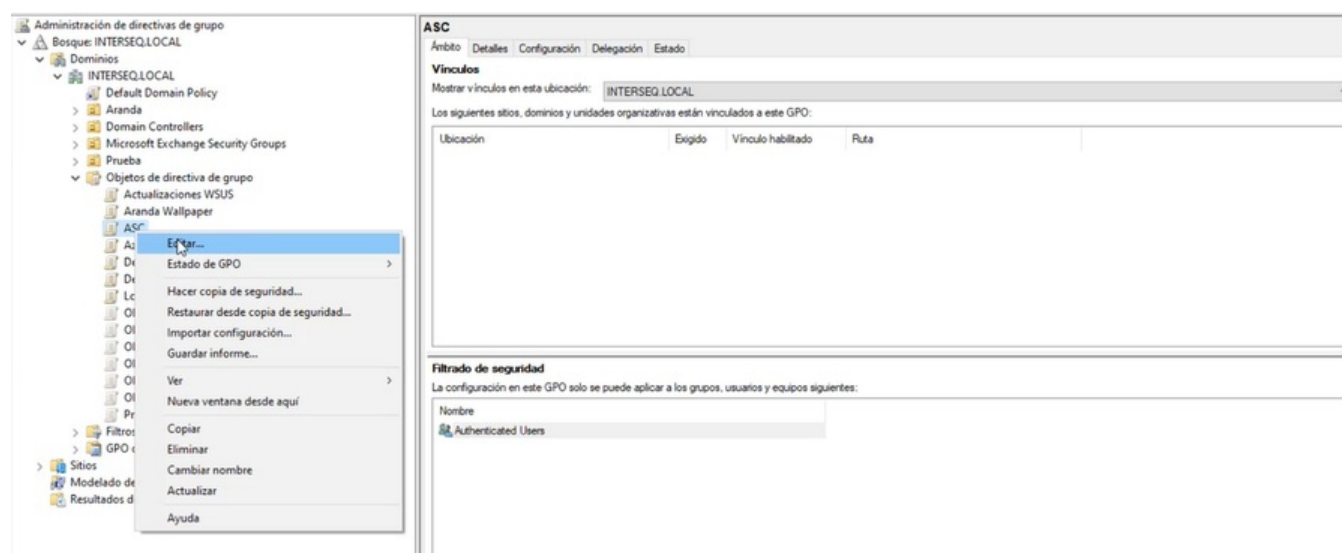
Crear Políticas de Grupo

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.

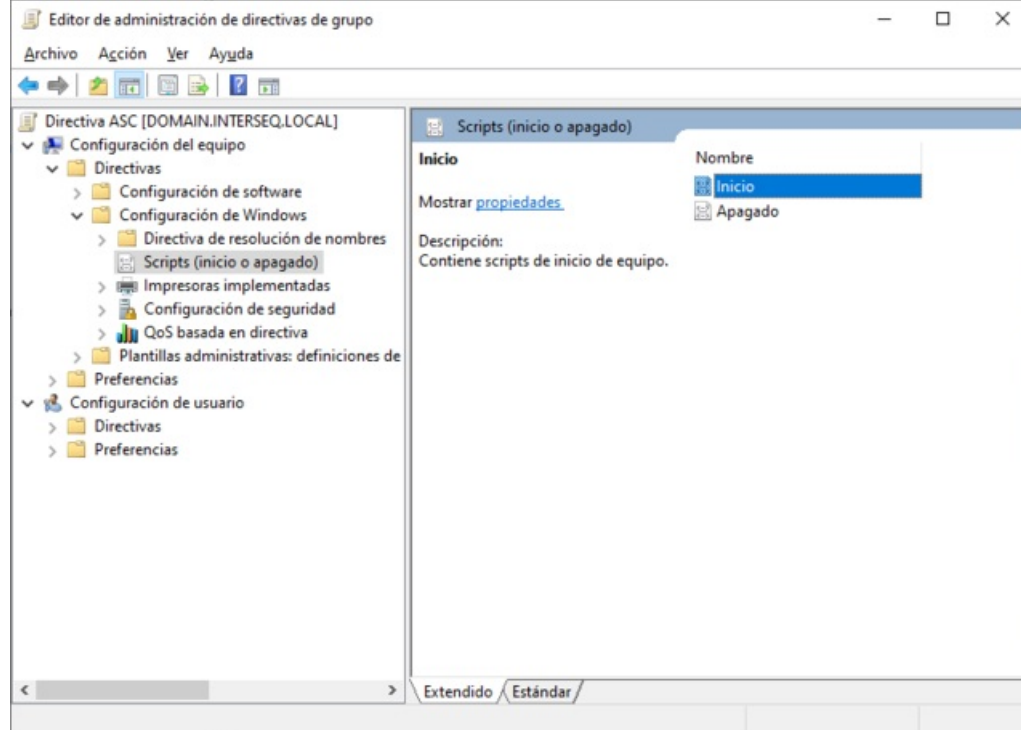
3. Seleccione la nueva directiva creada y haga clic en la opción Editar.



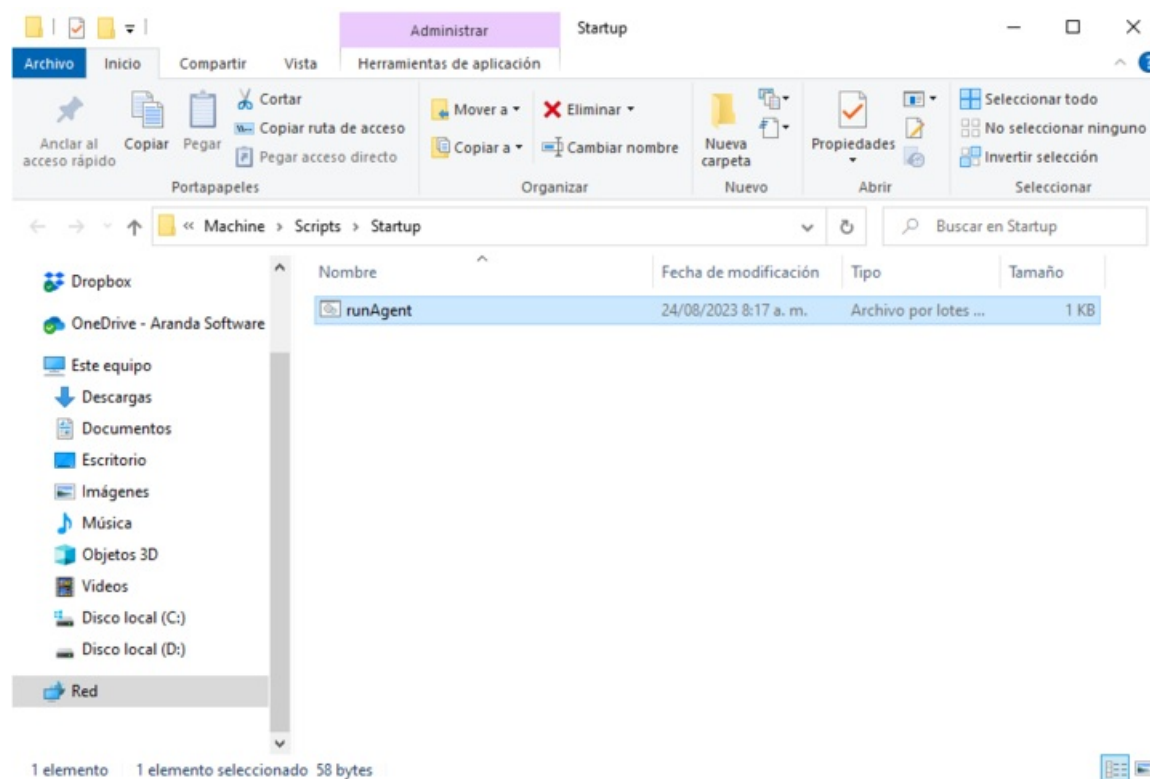
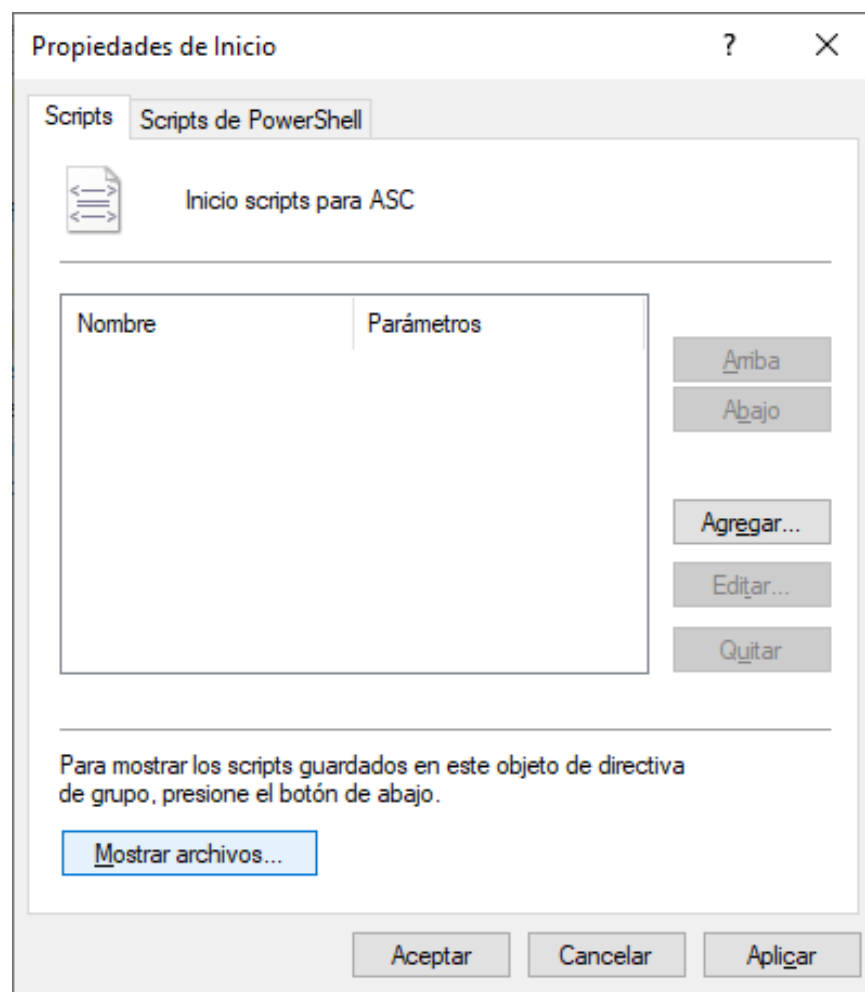
4. En el Editor de Administración de Directivas de grupo seleccione la opción Configuración de Equipo, Directivas, Configuración de Windows y la opción Scripts. En la vista de información seleccione la opción Inicio .

Nota

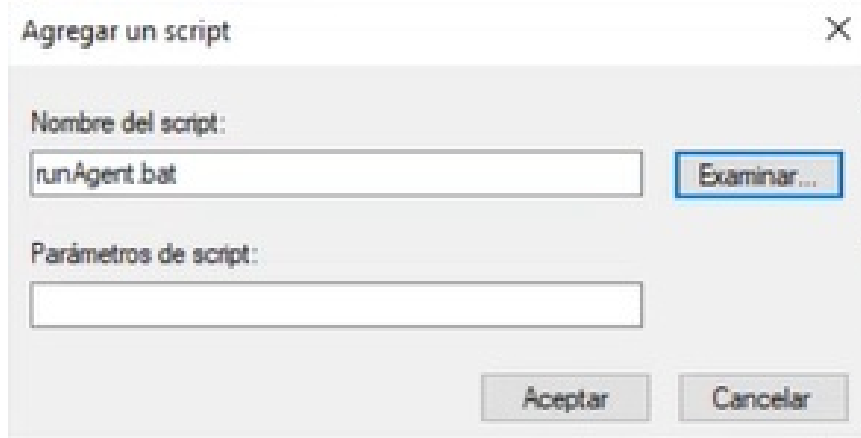
Configurar la directiva de inicio, permite que el agente de ASEC se ejecute al momento de iniciar sesión.



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

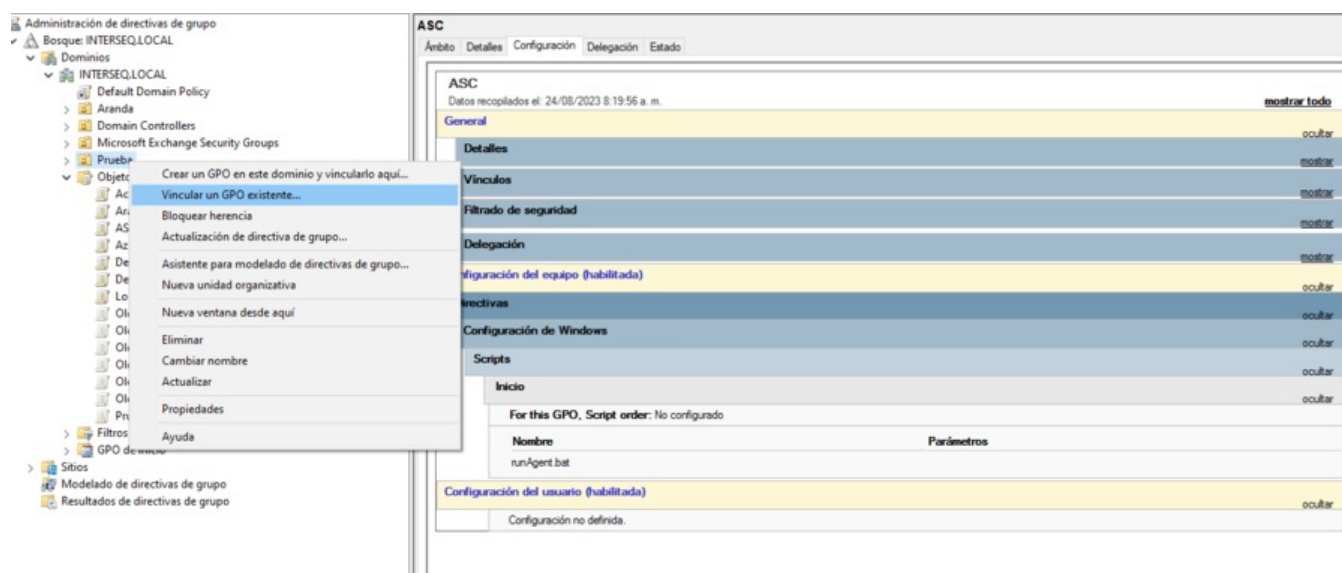


6. En la ventana Propiedades de inicio, seleccione el botón **Agregar** y en la ventana **Agregar un Script** seleccione el botón **Examinar** para seleccionar el archivo .bat del agente ASEC, al terminar haga clic en **Aceptar**.



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.

Monitorio Cumplimiento Políticas

title: Monitorio Cumplimiento Políticas chapter: "monitorio_politicas" —

El monitorio 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

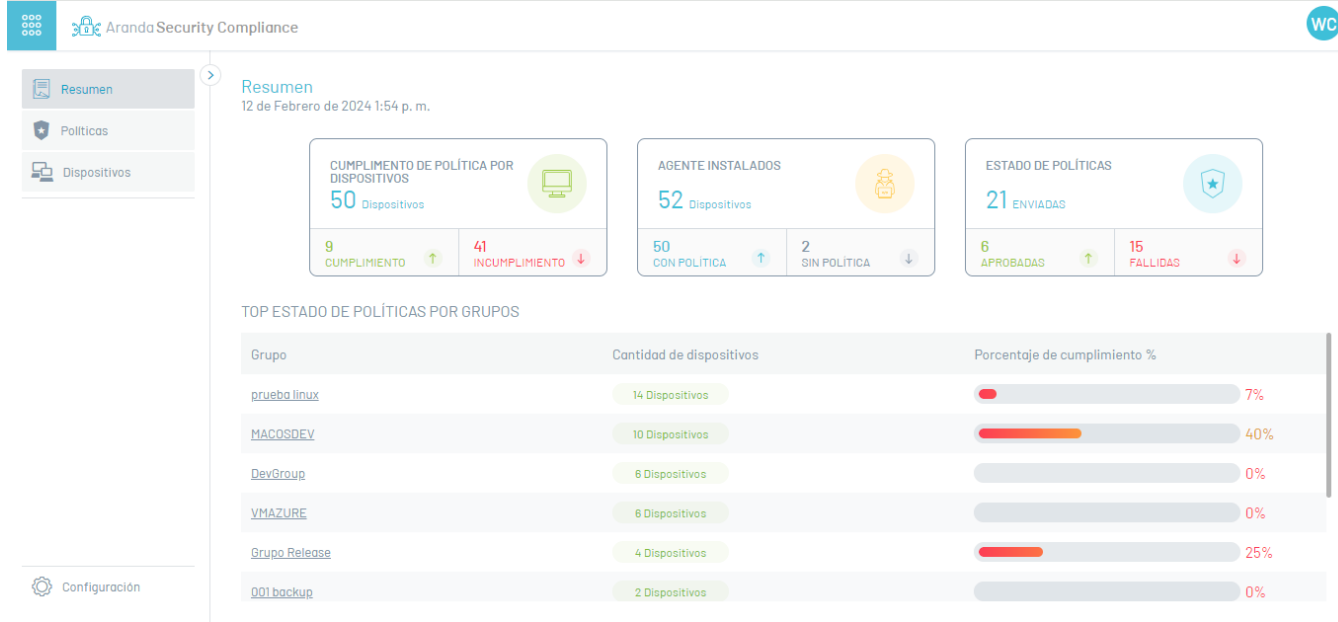
Consulte el análisis generado por Aranda Security para determinar los niveles de cumplimiento de las políticas de seguridad en los diferentes dispositivos.

2. Detalle de Cumplimiento

Consulte los niveles cumplimiento de los criterios seguridad implementados, facilitando al usuario la información específica de cada dispositivo, para tomar las acciones de remediación que den cumplimiento a la política.

title: Resumen Políticas chapter: "monitorio_politicas" —

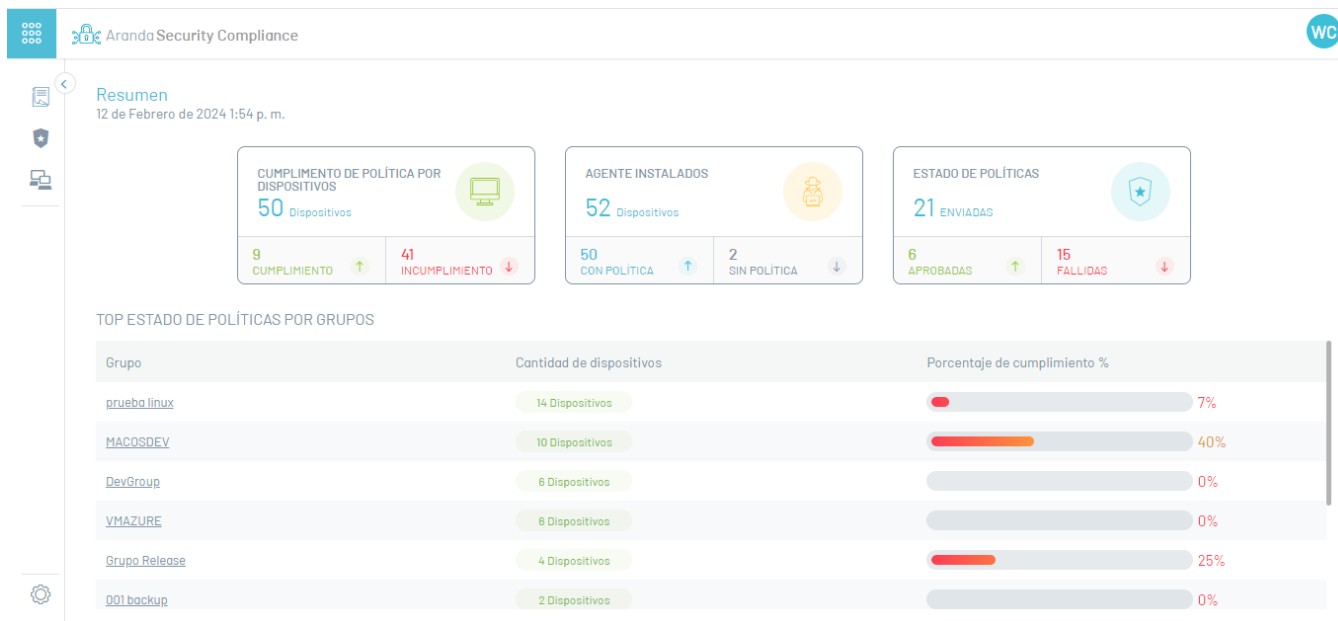
1. Ingrese a la consola de Aranda Security Compliance con rol de administrador, seleccione la opción Resumen del menú principal. En la vista de información se podrá visualizar los resultados del análisis de cumplimiento de las políticas de seguridad en los dispositivos vinculados. La información generada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



Notas

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 últimos 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 a [detalle de cumplimiento del dispositivo](#) asociado al grupo.



Dispositivos - Grupo Release

NIVEL DE CUMPLIMIENTO DE LA POLÍTICA EN EL GRUPO: 25%

REMEDIACIÓN | EXPORTAR

Dispositivo	Sistema operativo	IP	Fecha de ejecución	Acción
172	Red Hat Enterprise Linux	172.27.99.253 ; fe80::215...		REMEDIACIÓN
BG-D-BCARBON001	Microsoft Windows 11 Pro	192.168.0.82 ; 172.17.176.1...	08/02/2024 2:27:03 pm	REMEDIACIÓN
BG-D-WBERDU001	Microsoft Windows 10 Pro	192.168.56.1 ; 192.168.1.13...		REMEDIACIÓN
WJBC-RELEASE2	Microsoft Windows 11 Pro	10.0.0.10 ; fe80::294d:48...		REMEDIACIÓN

ESTADO: APLICADO FALLIDO NO APLICADO

Mostrando 1 al 4 de 4 registros

Detalle Cumplimiento de Dispositivos

title: Detalle Cumplimiento de Dispositivos chapter: "monitoreo_politicas" –

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.

P

Nombre de la política

Política-Release

Sistema operativo Windows

Tiempo de monitoreo

1 Minutos

🗄️ ✕ ⤴️

Descripción

Pruebas Release

ESTADO ● Activo

Criterios de políticas
Grupos

Asocie grupos a las políticas +

Grupos asociados a las políticas Desasociar

	Grupo	Dispositivos del grupo
<input type="checkbox"/>	GR Grupo Release	4

< 1 >

Mostrando 1 de 1 registros

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.

Dispositivos - Grupo Release
✕

NIVEL DE CUMPLIMIENTO DE LA POLÍTICA EN EL GRUPO

25%

REMEDIACIÓN
EXPORTAR

Dispositivo	Sistema operativo	IP	Fecha de ejecución	Acción
172	Red Hat Enterprise Linux	172.27.99.253 ; fe80::215...		REMEDIACIÓN
BG-D-BGARBON001	Microsoft Windows 11 Pro	192.168.0.62 ; 172.17.176.1...	08/02/2024 2:27:03 pm	REMEDIACIÓN
BG-D-WBERDUG001	Microsoft Windows 10 Pro	192.168.56.1 ; 192.168.1.13...		REMEDIACIÓN
WJBC-RELEASE2	Microsoft Windows 11 Pro	10.0.0.10 ; fe80::294d.48...		REMEDIACIÓN

ESTADO ● APLICADO ● FALLIDO ● NO APLICADO

< 1 >

Mostrando 1 de 4 registros

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.

D

Dispositivo

vm-asec-demo01

Fecha de escaneo: 10/12/2023 15:51:14

IP:: 10.0.0.4 ; fe80::d7e5:283f:54b2:3e37%6

Dispositivo: Microsoft Windows 10 Pro N

Política del dispositivo

Demo2

Detalle política

Esta política tiene los siguientes criterios:

Firewall

Windows Firewall

SUCCESS

Browser

Microsoft Edge

SUCCESS

Grupo

Este dispositivo pertenece al siguiente grupo

GG

Grupo1

Cambiar de grupo

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.

Dispositivo
172

Fecha de escaneo: Sin escaneos

IP:: 172.27.98.248 ; fe80::215:5dff:fe01:810%2
Dispositivo: Red Hat Enterprise Linux

Grupo
Este dispositivo pertenece al siguiente grupo

PL
prueba linux

Cambiar de grupo

Política del dispositivo
Prueba Linux

Detalle política
Esta política tiene los siguientes criterios:

Browser
Mozilla Firefox

NO
APLICADO

Firewall
Firewalld

NO
APLICADO

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

Dispositivo
192

Fecha de escaneo: 02/12/2024 08:11:29

IP:: 192.168.0.6 ; fe80::c6b:4ea3:3e8a:fe9f%5 ;
fe80::9c92:32ff:fed3:3ff3%10 ;
fe80::33e7:ebe3:f5c:d378%11 ;
fe80::31de:2477:c753:8213%12
Dispositivo: macOS Catalina

Grupo
Este dispositivo pertenece al siguiente grupo

M
MACOSDEV

Cambiar de grupo

Política del dispositivo
MacOSDev

Detalle política
Esta política tiene los siguientes criterios:

Browser
Safari

APLICADO

- ✔ DetectProduct
- ✔ Validar protección de antiphishing

Remote_control
AnyDesk

FALLIDO

✘ DetectProduct

VER

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

Asociar Grupos 🗑️ ✕

A continuación podrá seleccionar o verificar el grupo asociado

Seleccione un grupo

Este dispositivo pertenece al siguiente grupo:

M

MACOSDEV

Usuarios del grupo: 1 usuarios

Acciones de Remediación

5. 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.

Dispositivos - Grupo Demo

NIVEL DE CUMPLIMIENTO

Buscar

Dispositivo	Sistema operativo	IP
BG-D-WBERDU001	Microsoft Windows 10 Pro	192.168.58.1; 192...
LAPTOP-DJ5MVAQB	Microsoft Windows 11 Ho...	192.168.1.7; fe80...
WJBC0A	Microsoft Windows 10 Pro	10.0.0.4; fe80::4...

ESTADO LA POLÍTICA APLICADO FALLIDO NO APLICADO

Acciones de remediación Seleccionar todo

GC Google Chrome Ejecutar SetAntiphishingState

CANCELAR ENVIAR

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

Configuración ASEC – title: Configuración ASEC chapter: "configuracion_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 dispositivos para cada grupo.

– title: Desplegar Agente chapter: "despliegue_e_instalacion" –

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.

Aranda Security Compliance

← Regresar

CONFIGURACIÓN

Desplegar agente

Grupos de cumplimiento

Configuración general

Usuarios

Servicios de email

Licenciamiento

Autenticación externa

Servicios de directorio

Agente

Siga los pasos que se presentan a continuación para el despliegue del agente.

1 Seleccione un sistema operativo

Windows Linux MacOS

```
temp_install_dir=$(mktemp -d) && sudo curl -o setup.sh https://download.arandasoft.com/asec/agent/setup.sh && sudo chmod +x setup.sh && sudo ./setup.sh --target "$temp_install_dir" https://releases3.arandasoft.com" && sudo rm -r setup.sh "$temp_install_dir"
```

Ejecute este comando en una terminal con privilegios de administrador.

Copiar comando

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

1. Seleccione un sistema operativo


Windows Linux **MacOS**

```
sudo sh -c 'curl -o aseccagent.pkg "https://download.arandasoft.com/asec/agent/setup.pkg" && installer -pkg aseccagent.pkg -target / && asecc-configuration -d https://releaseq3.arandasoft.com'
```

Ejecute este comando en una terminal con privilegios de administrador.

Copiar comando

Agente



Siga los pasos que se presentan a continuación para el despliegue del agente.

3. Al seleccionar el sistema operativo, 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 continúe el proceso de distribución e instalación del agente ASEC, de acuerdo al tipo de despliegue definido:

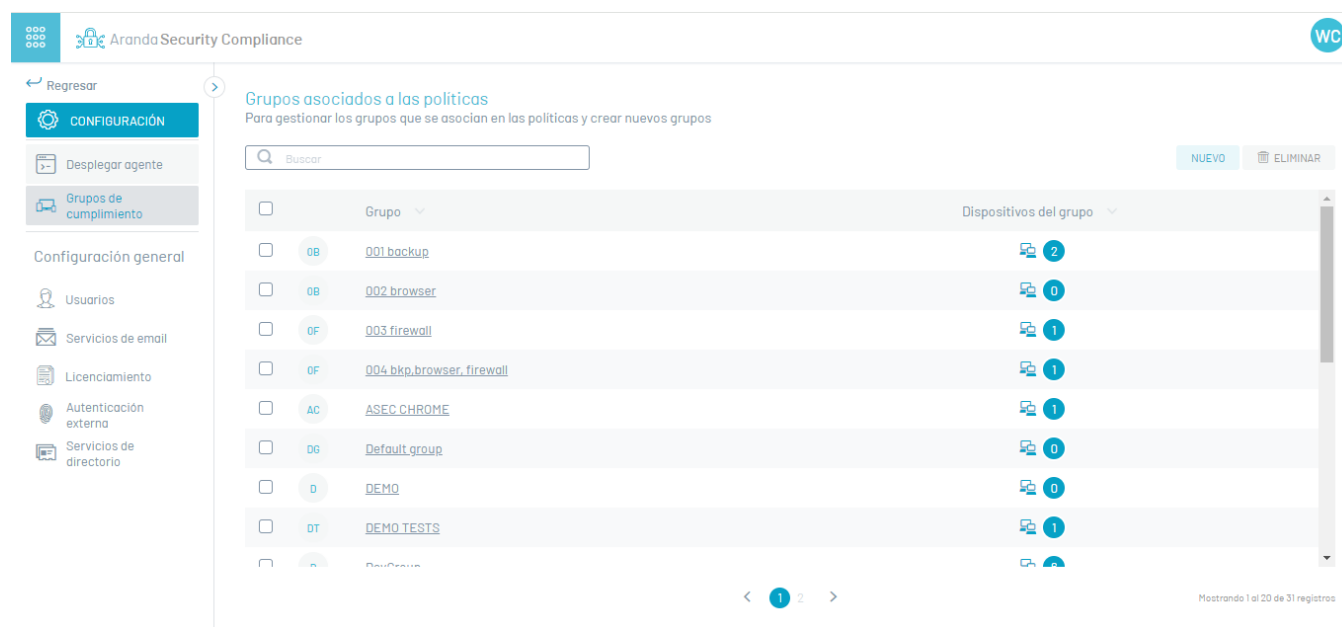
- [Instalación por Dispositivos.](#)
- [Instalación por Política de Dominio](#)
- [Instalación y distribución con Aranda Device Management ADM](#)

title: Grupos de Políticas chapter: "configuracion_asec" —

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 de grupos disponibles y ordenar la información por nombre de grupos y dispositivos.



Grupo	Dispositivos del grupo
001 backup	2
002 browser	0
003 firewall	1
004 bkp.browser.firewall	1
ASEC CHROME	1
Default group	0
DEMO	0
DEMO TESTS	1

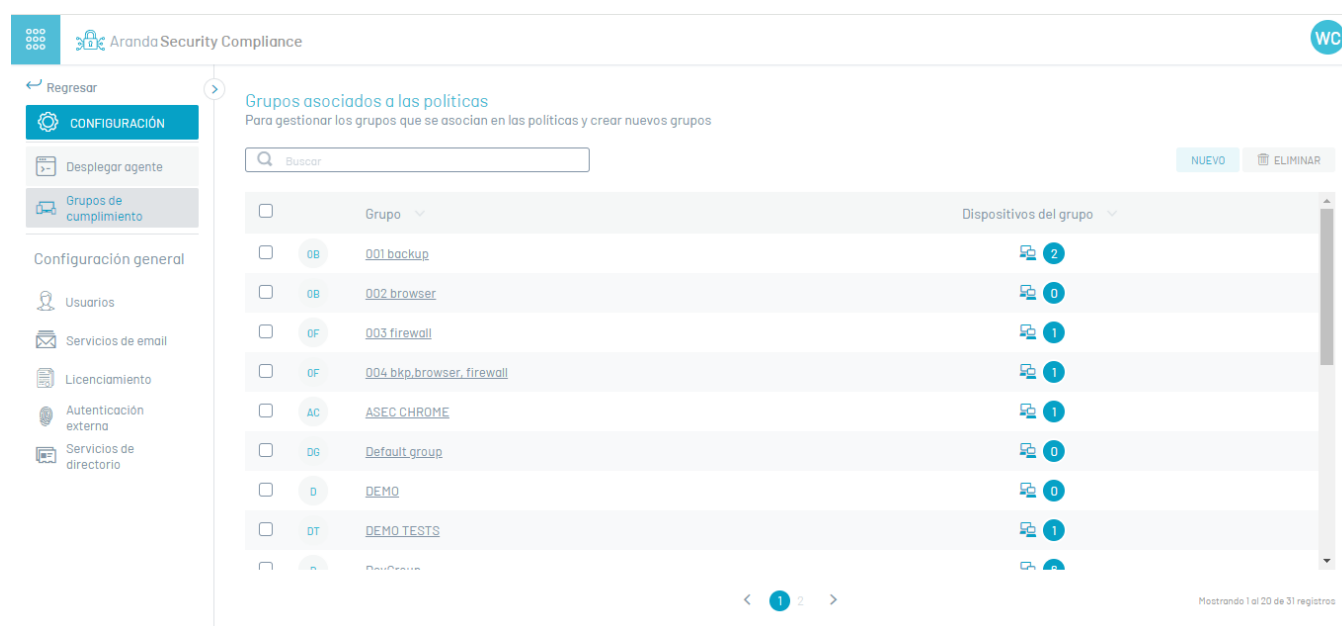
2. En la vista de información de grupos también podrá visualizar el listado de dispositivos que pertenecen a cada grupo.

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.

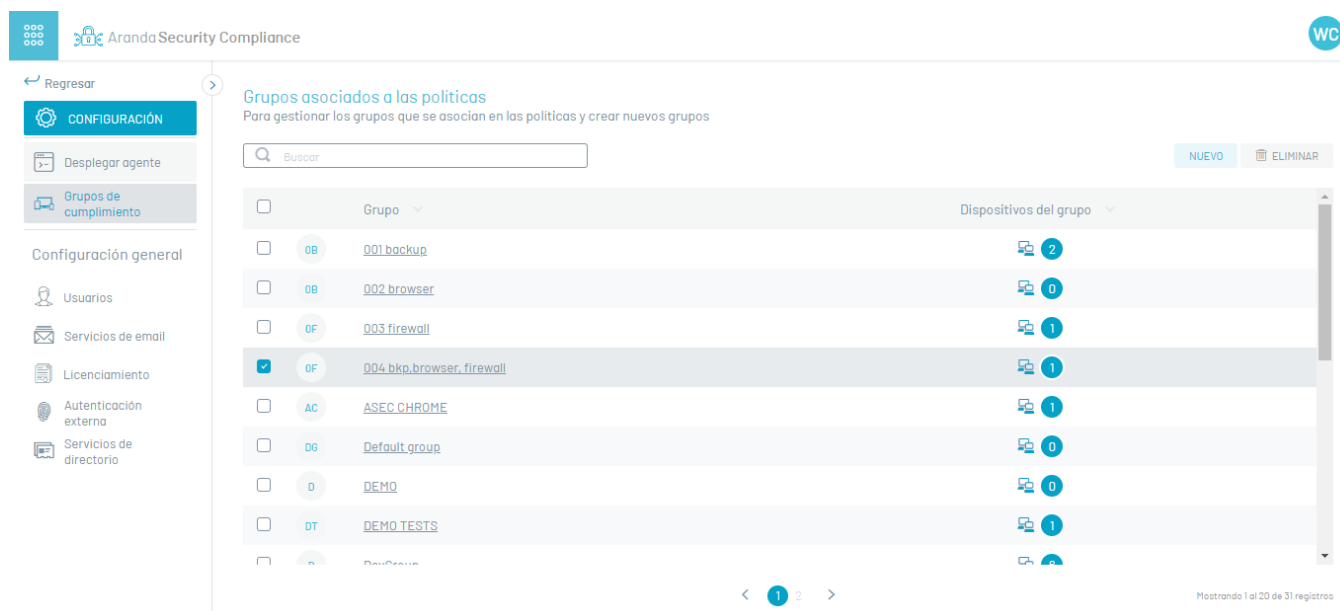
Al ingresar de nuevo al grupo creado tendrá habilitadas las opciones para asociar y desasociar dispositivos.



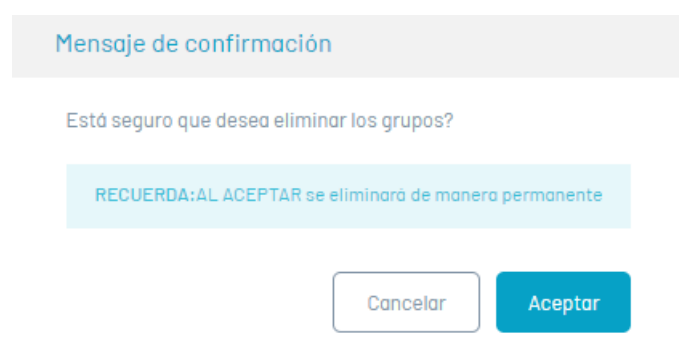
Grupo	Dispositivos del grupo
001 backup	2
002 browser	0
003 firewall	1
004 bkp.browser.firewall	1
ASEC CHROME	1
Default group	0
DEMO	0
DEMO TESTS	1

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**.



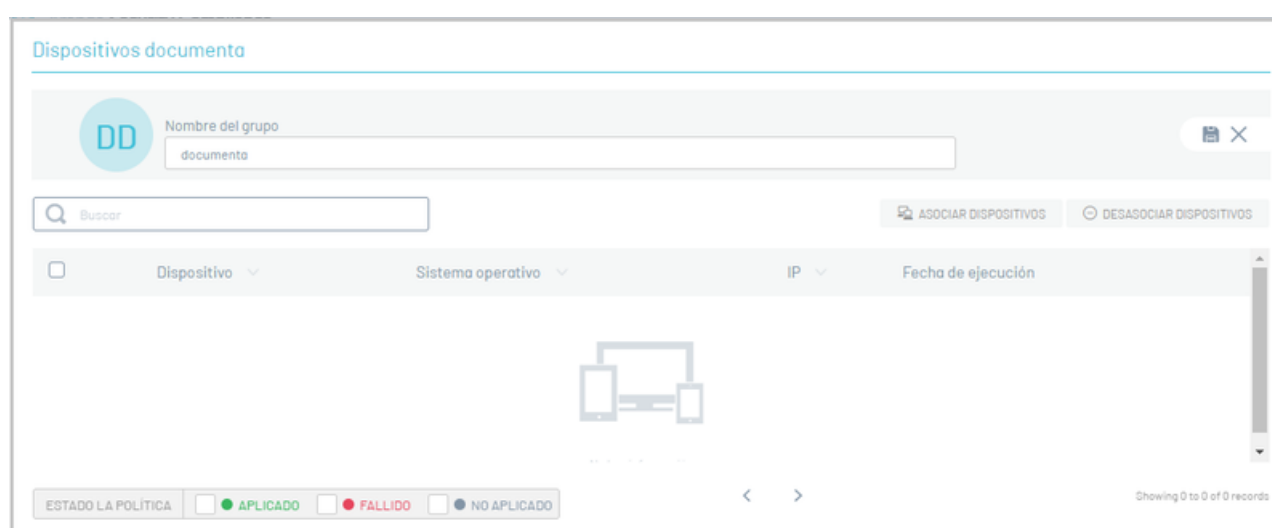
En la ventana que se habilita podrá confirmar o denegar la acción de eliminar el grupo.



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**.

Dispositivos DevGroup

Nombre del grupo: DevGroup

Buscar

ASOCIAR DISPOSITIVOS DESASOCIAR DISPOSITIVOS

Dispositivo	Sistema operativo	IP	Fecha de ejecución
<input checked="" type="checkbox"/> BG-D-JPEDRAZAD1	Microsoft Windows 10 Pro	172.22.112.1; 192.168.1.53...	23/10/2023 9:32:37 am
<input checked="" type="checkbox"/> BG-D-WPENAO1	Microsoft Windows 10 Pro	192.168.0.147; fe80::fd28...	23/10/2023 4:23:15 pm
<input type="checkbox"/> DESKTOP-CBTU79I	Microsoft Windows 11 En...	172.27.208.1; 192.168.50....	10/10/2023 11:42:25 pm
<input type="checkbox"/> JCTREJOSI	Microsoft Windows 11 Ho...	192.168.1.2; fe80::8527.3...	23/10/2023 6:22:43 am

ESTADO LA POLÍTICA: APLICADO FALLIDO NO APLICADO

Showing 1 to 8 of 8 records

\\n## Configuración General – title: Configuración General chapter: “configuracion_general” –

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



1. Administrar usuarios y asignar Roles

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 siguientes roles:

- Administrador.
- Especialista

2. Configurar Servidores de Correo

Esta sección 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).

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.

4. Servicios de Directorio

Configurar los servicios de directorio que pueden ser usados en la aplicación de Aranda Security, como el protocolo ligero de acceso a directorio&DAP, que permite configurar la conexión con otros directorios empresariales o el servicio de directorios Azure Active Directory

5. Configurar Proveedores de Autenticación

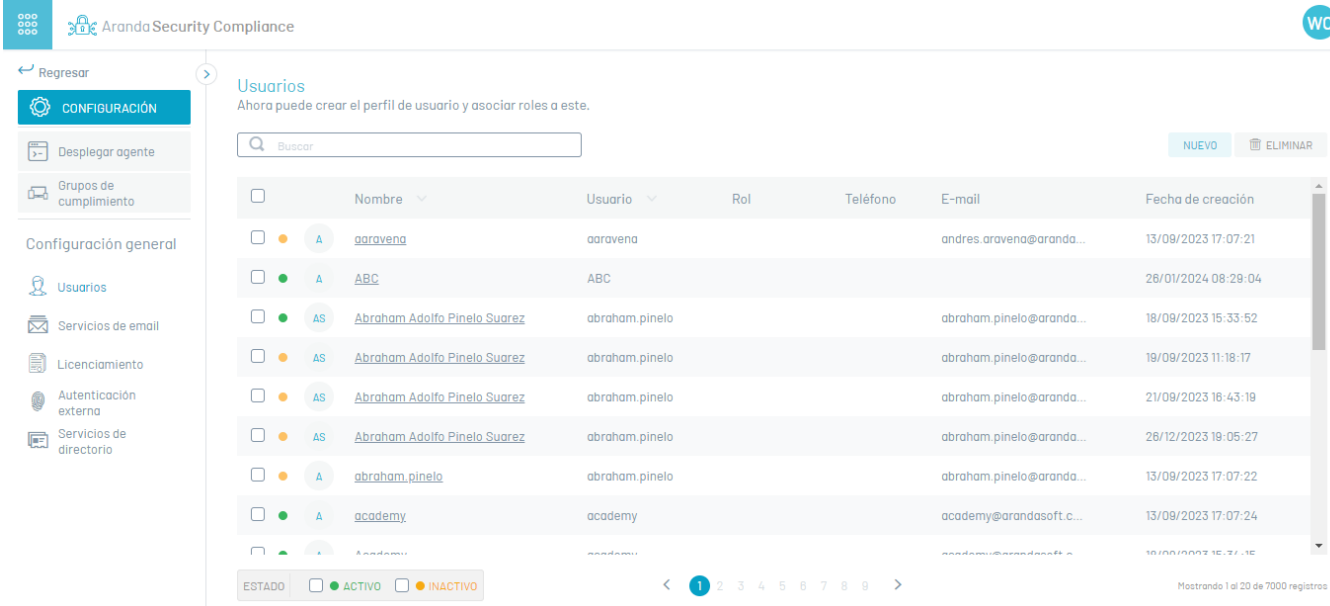
Aranda Security Compliance permite utilizar proveedores de autenticación externa, que siguen el estandar SAML (Security Assertion Markup Language) para realizar la autenticación del usuario en la aplicación.

– title: “Usuarios” chapter: “configuracion_general” –

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

Visualizar Usuarios

1. Ingrese a la consola de Aranda Security con rol de administrador, en la sección de Configuración general del menú principal, seleccione la opción Usuarios. En la vista de información se despliega el listado de usuarios disponibles. La información de los usuarios está agrupada por nombre, usuario, rol, correo y fecha de creación.



2. En la vista de información de los usuarios, tendrá habilitadas acciones de gestión y organización de la información. [Vista de Información en Entorno Web ASEC](#)

Crear Usuarios

3. Para crear usuarios, en la vista de información de usuarios seleccione el botón **Nuevo**; se habilita el formulario para ingresar la información básica del usuario, establecer el estado del usuario (activo, inactivo) y definir los siguientes roles de acceso:

4. En la ventana que se habilita ingrese la información solicitada del usuario:

Dato	Obligatorio	Descripción
Nombre	Si	Nombre con el cual se identifica el usuario.
Nombre de usuario	Si	Nombre usado por el usuario para acceder a la aplicación.
Contraseña	Si	Clave utilizada por el usuario para acceder a la aplicación.
Teléfono	No	Número de teléfono para comunicarse con el usuario.
Correo electrónico	Si	Correo registrado por el usuario para recibir información.
Estado	NA	Indica si el usuario se encuentra activo o inactivo.

Nota Cada uno de los campos del usuario deben tener en cuenta las [especificaciones para campos ASEC](#)

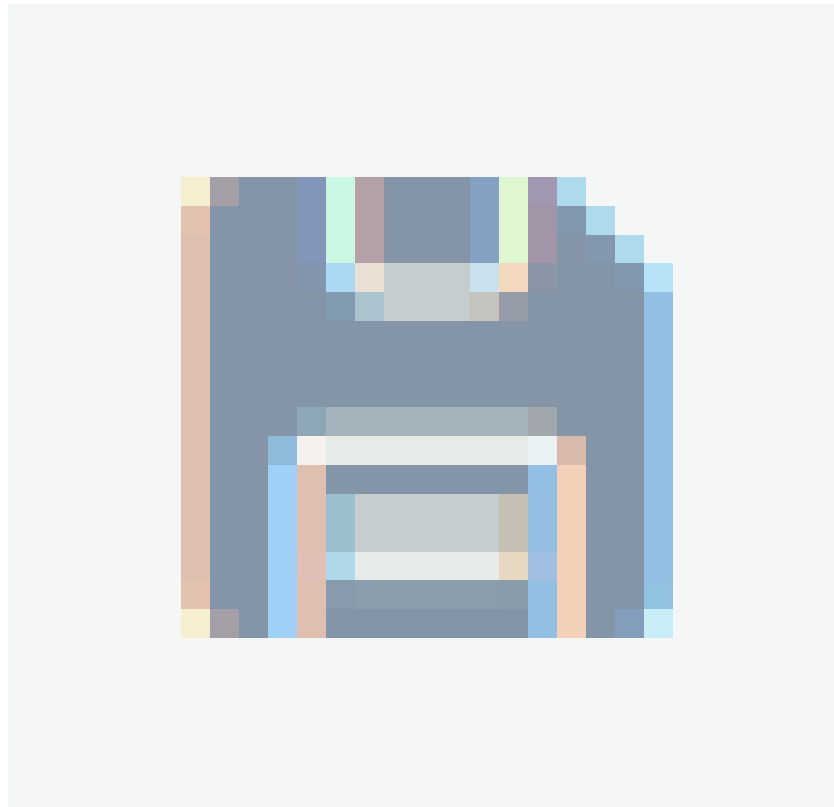
Roles

Un rol es el conjunto de permisos que puede tener un usuario para utilizar la aplicación de Aranda Security Compliance. Al usuario se le podrán autorizar uno o varios permisos de acuerdo a su rol y a las funciones que desempeñe en la aplicación ASEC.

Para facilitar la gestión se han definido roles preconfigurados con los permisos más utilizados en la aplicación, los cuales son:

- [Administrador General](#)
- [Especialista](#)

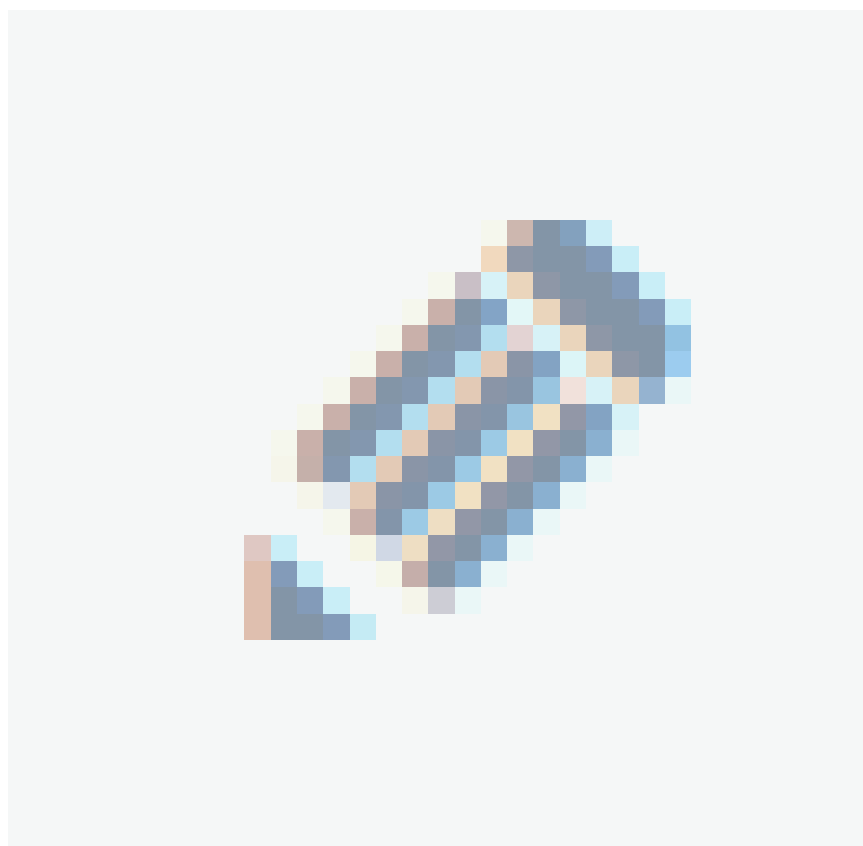
5. Al terminar de configurar la información del usuario y asignar los roles, haga clic en el icono **Guardar**



para confirmar los cambios realizados.

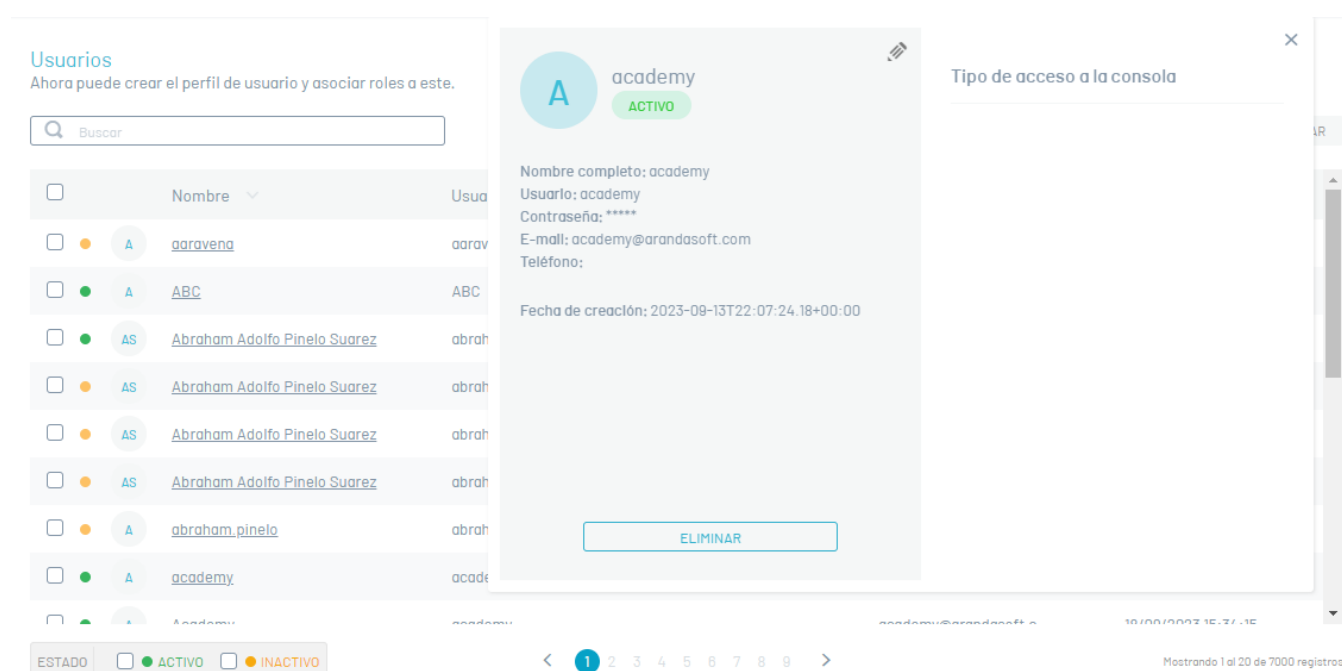
Editan Usuarios

6. Una vez creado el nuevo usuario, este se incluirá en el listado de la consola de Aranda Security. Al seleccionar el nombre del usuario, se despliega el formulario con el detalle. Haga clic en el icono de **editar**



para activar el modo de edición y modificar la información requerida.

7. Para confirmar los cambios, presione el icono de **Guardar**, para regresar al modo de lectura.



Usuarios
Ahora puede crear el perfil de usuario y asociar roles a este.

Buscar

<input type="checkbox"/>	Nombre	Usua
<input type="checkbox"/>	garaveng	garav
<input type="checkbox"/>	ABC	ABC
<input type="checkbox"/>	Abraham Adolfo Pinelo Suarez	abrah
<input type="checkbox"/>	Abraham Adolfo Pinelo Suarez	abrah
<input type="checkbox"/>	Abraham Adolfo Pinelo Suarez	abrah
<input type="checkbox"/>	Abraham Adolfo Pinelo Suarez	abrah
<input type="checkbox"/>	abraham_pinelo	abrah
<input type="checkbox"/>	academy	acade

academy ACTIVO

Nombre completo: academy
Usuario: academy
Contraseña: ****
E-mail: academy@arandasoft.com
Teléfono:

Fecha de creación: 2023-09-13T22:07:24.18+00:00

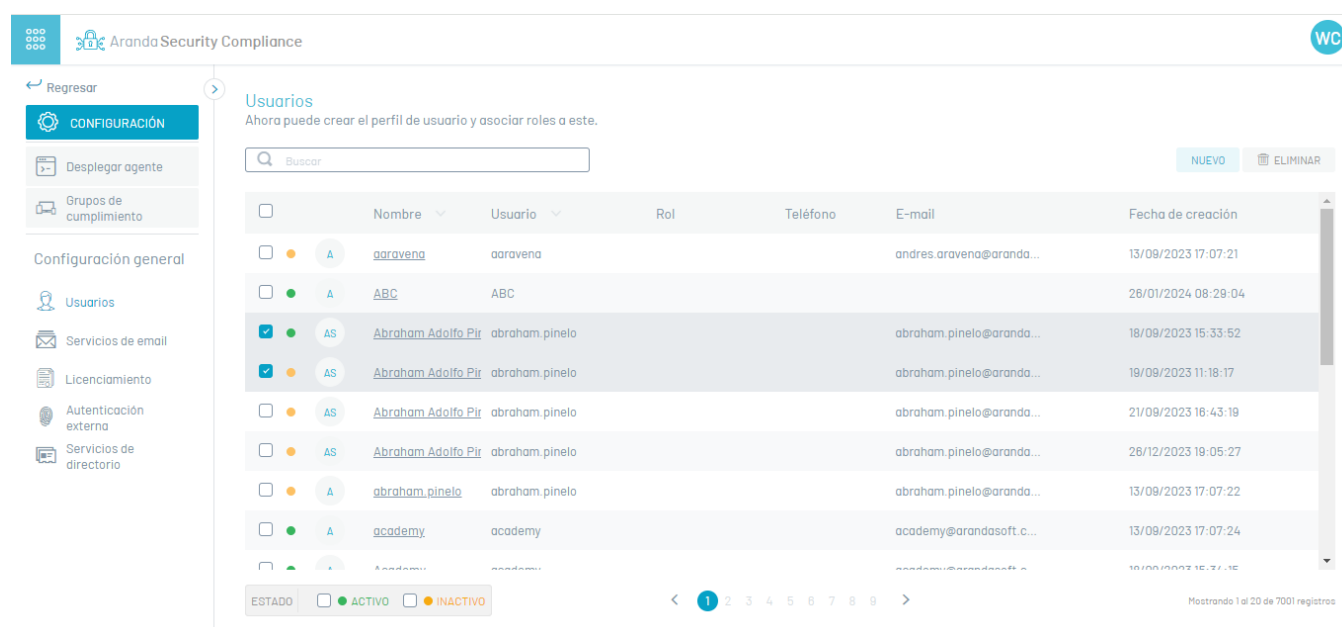
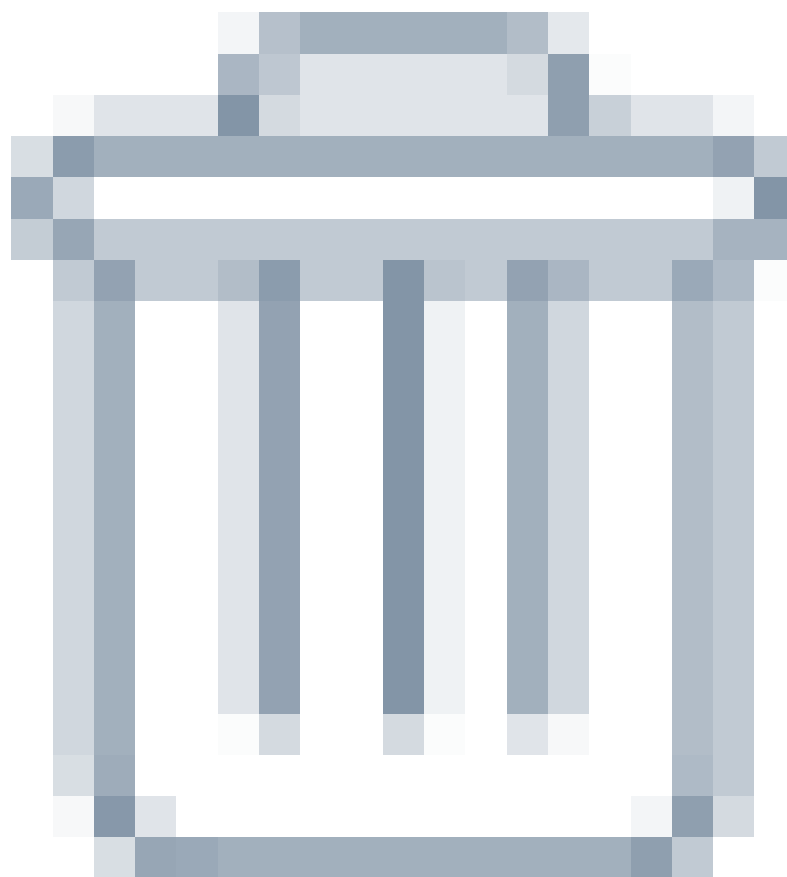
ELIMINAR

Tipo de acceso a la consola

Mostrando 1 de 20 de 7000 registros

Eliminar Usuarios

8. Para eliminar usuarios, en la vista de información seleccione uno o varios registros del listado de usuarios existentes que quiere borrar y presione el botón Eliminar



The screenshot shows the 'Usuarios' (Users) management page in the Aranda Security Compliance application. The page includes a search bar, a 'NUEVO' (New) button, and an 'ELIMINAR' (Delete) button. A table lists users with columns for selection, name, user ID, role, phone, email, and creation date. Two users are selected with checkboxes. The table data is as follows:

	Nombre	Usuario	Rol	Teléfono	E-mail	Fecha de creación
<input type="checkbox"/>	A aravena	aravena			andres.aravena@aranda...	13/09/2023 17:07:21
<input type="checkbox"/>	A ABC	ABC				26/01/2024 08:29:04
<input checked="" type="checkbox"/>	AS Abraham Adolfo Pir	abraham.pinelo			abraham.pinelo@aranda...	18/09/2023 16:33:52
<input checked="" type="checkbox"/>	AS Abraham Adolfo Pir	abraham.pinelo			abraham.pinelo@aranda...	19/09/2023 11:18:17
<input type="checkbox"/>	AS Abraham Adolfo Pir	abraham.pinelo			abraham.pinelo@aranda...	21/09/2023 16:43:19
<input type="checkbox"/>	AS Abraham Adolfo Pir	abraham.pinelo			abraham.pinelo@aranda...	26/12/2023 19:05:27
<input type="checkbox"/>	A abraham.pinelo	abraham.pinelo			abraham.pinelo@aranda...	13/09/2023 17:07:22
<input type="checkbox"/>	A academy	academy			academy@arandasoft.c...	13/09/2023 17:07:24
<input type="checkbox"/>	A academy	academy			academy@arandasoft.c...	18/09/2023 16:33:52

At the bottom, there is a legend for 'ESTADO' (Status) with 'ACTIVO' (Active) and 'INACTIVO' (Inactive) options, and a pagination indicator showing 'Mostrando 1 al 20 de 7001 registros'.

- Notas:**
- 1. Al eliminar un usuario podrá visualizar un mensaje de error en la parte inferior de la consola.
 - 2. Tenga en cuenta que sólo puede modificar los usuarios del proveedor Aranda. No podrá realizar ediciones para aquellos que han sido sincronizados desde proveedores externos como LDAP. Para usuarios sincronizados solo podrá asignarles un rol en la aplicación.

\n## Servidor de Correo – title: “Servidor de Correo” chapter: “configuracion_general” –

Visualizar Servidores

1. Ingrese a la consola de Aranda Security con rol de administrador, en la sección de Configuración general del menú principal, seleccione la opción Servidor de Correo. En la vista de información se despliega el listado de servidores disponibles.

Aranda Security Compliance

Regresar

CONFIGURACIÓN

Desplegar agente

Grupos de cumplimiento

Configuración general

Usuarios

Servicios de email

Licenciamiento

Autenticación externa

Servicios de directorio

Servidor de correo
Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

NUEVO ELIMINAR

Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
DE Default	pruebasayu	Oauth	sayu	pruebasayu@yahoo.com
DE Default	outlook.44	Basic	astrid	nidia@yahoo.com
NU nuevo	nuevo	Basic	nuevo	nuevo@gmail
NO Notificaciones ASEC	outlook.office365.com	Basic	Notificaciones ASEC	walter.berdugo@arandasoft.com
AO AOMMailProvider052023	smtp.office365.com	Basic	Aranda Query Manager	store@arandasoft.com
DE Default	abigail.org	Basic	Jody Powlowski	Ally_Stanton81@hotmail.com
DE Default	outlook.office365.com	Oauth	AEMM OAUTH	diana.cortes@arandasoft.com
AM AEMM Mail Server	outlook.office365.com	Basic	Pruebas AEMM Basic	miguel.jimenez@arandasoft.com
AF AFLS DEFAULT MAIL	smtp.office365.com	Oauth	Pruebas QA3	julieth.mancera@arandasoft.com
DE Default	outlook.office365.com	Basic	sangle	sangle.pinzon@arandasoft.com

2. En la vista de información de los servidores, tendrá habilitadas acciones de gestión y organización de la información. [Vista de Información en Entorno Web ASEC](#)

Crear Servidores de Correo

3. Para crear servidores de correo, en la sección de Configuración del menú principal, seleccione la opción Servidor de Correo. En la vista de información seleccione el botón Nuevo y en la vista detalle se habilita la ventana de propiedades del servidor donde podrá completar la información requerida:

Nombre

✕

Tipo de autenticación

Selección del tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

➤ Para finalizar la configuración envíe el correo de prueba

* Campos obligatorios

Basica
 Oauth

Requiere autenticación NO

*Nombre del correo

*Servidor

*Puerto

Nombre del remitente

Correo del remitente

Establecer correo por defecto NO

Habilitar SSL NO

Parámetro	Descripción
Nombre	Nombre del servidor que permite el transporte del correo.
Servidor	Nombre DNS del servidor de correo
Puerto	Puerto de operación del servicio TCP
Nombre remitente	Nombre del remitente de la notificación de los correos
Correo del remitente	Dirección de correo del remitente
Establecer predeterminado	Indica si desea que ese proveedor sea el único autorizado para enviar correos en AES
Habilitar SSL	Indica si su conexión usa protocolo seguro

4. En la sección Tipo de Autenticación, podrá establecer las opciones disponibles por tipo de proveedor:

- Autenticación Básica
- Autenticación Oauth

Autenticación Básica

5. Para la autenticación básica ingrese el usuario de acceso al servidor de correo y la contraseña si se requiere.

Autenticación OAuth (Open Authorization)

6. Para la autenticación OAuth Solicita los campos obligatorios

Parámetro	Descripción
ID Cliente	Identificador de cliente dada por su proveedor OAuth
Clave Secreta	Contraseña
Url Autorización	Dirección url para poder realizar la autorización
Url Token	Dirección url para la generacion de token de autorización

7. Configure la información relevante al proveedor de correo OAuth en el portal de Azure [Configuración para la autenticación moderna OAuth 2.0](#). Este proceso genera los parámetros que son requeridos en el formulario de configuración correo OAuth en Aranda Security.

Parámetro	Descripción
Token de Acceso	Este será generado durante el proceso de generación de credenciales
Refresh Token	Este será generado durante el proceso de generación de credenciales

N Nombre

*Nombre del correo

*Servidor

*Puerto

Nombre del remitente

Correo del remitente

Establecer correo por defecto NO

Habilitar SSL NO

Tipo de autenticación

Selección del tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Para finalizar la configuración envíe el correo de prueba

* Campos obligatorios

Básica OAuth

*ID Cliente

*Secreto del cliente (contraseña)

*URL de autorización

*URL de token

*Token de actualización

Nombre

*Nombre del correo

Tipo de autenticación

Selección del tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Para finalizar la configuración envíe el correo de prueba

*Servidor

* Campos obligatorios

Basica Oauth

*Puerto

*Token de actualización

Nombre del remitente

*Token de acceso

Correo del remitente

Establecer correo por defecto NO

Habilitar SSL NO

8. Al terminar de configurar el servidor de correo, haga clic en el ícono **Guardar** para confirmar los cambios realizados.

Nota: Si ha creado más de una configuración de servidor de correo, sólo una de ellas puede estar marcada como configuración **Por defecto**.

Editar un Servidor de Correo

9. Para editar un registro de servidor de correo, en la vista de información, seleccione el nombre del proveedor del listado disponible.

Aranda Security Compliance

Regresar

CONFIGURACIÓN

Desplegar agente

Grupos de cumplimiento

Configuración general

Usuarios

Servicios de email

Licenciamiento

Autenticación externa

Servicios de directorio

Servidor de correo

Ahora puede configurar el servidor de correos, asignarles un servidor y establecer el tipo de correo a manejar

Buscar todos los conceptos

NUEVO ELIMINAR

<input type="checkbox"/>	Nombre	Servidor	Tipo	Nombre del remitente	Correo del remitente
<input type="checkbox"/>	DE Default	andreeanne.biz	Basic	Percy Oultzon DVM	Margarette35@yahoo.com
<input type="checkbox"/>	DE Default	zachariah.net	Basic	Derrick Howe	Chet_Sporer@gmail.com
<input type="checkbox"/>	DE Default	ignatius.name	Basic	Sheryl Lebsack	Anika73@hotmail.com
<input type="checkbox"/>	DE Default	maryam.biz	Basic	Constance McClure I	Darran.Langosh@yahoo.com
<input type="checkbox"/>	DE Default	celia.name	Basic	Mario Rowe	Eloisa.Feil88@yahoo.com
<input type="checkbox"/>	DE Default	outlook.office365.com	Oauth	Nidia	nidia.alejo@arandasoft.com
<input type="checkbox"/>	AT atest	outlook.office365.com	Basic	testAsec	fredy.cardenas@arandasoft.com
<input checked="" type="checkbox"/>	WA wapl1989@hotmail.com	wapl1989@hotmail.com	Basic	wapl1989@hotmail.com	wapl1989@hotmail.com
<input type="checkbox"/>	NO nombreCorreoss	smtp.live.com	Basic	William	wapl1989@hotmail.com
<input type="checkbox"/>	A0 A0MOAuthProvider042023	smtp.office365.com	Oauth	Aranda Query Manager	store@arandasoft.com

10. Se habilita la ventana de propiedades del servidor, donde podrá modificar los datos del servidor o del tipo de autenticación.

office.out320.com

Servidor: office.out320.com
Puerto: 587
Nombre del remitente: ASEC
Correo del remitente: demo@arandasoft.com

Establecer correo por defecto

Habilitar SSL

ELIMINAR

Tipo de autenticación

Selección del tipo de autenticación para este servidor de correo.

Requiere autenticación NO

11. Al terminar los ajustes del servidor de correo, haga clic en el icono Guardar para confirmar los cambios realizados.

office.out320.com

*Nombre del correo
demo@arandasoft.com

*Servidor
office.out320.com

*Puerto
587

Nombre del remitente
ASEC

Correo del remitente
demo@arandasoft.com

Establecer correo por defecto SI

Hab

La modificación fué exitosa

Tipo de autenticación

Selección del tipo de autenticación para este servidor de correo. Pruebe la conexión antes de guardar

Para finalizar la configuración envíe el correo de prueba

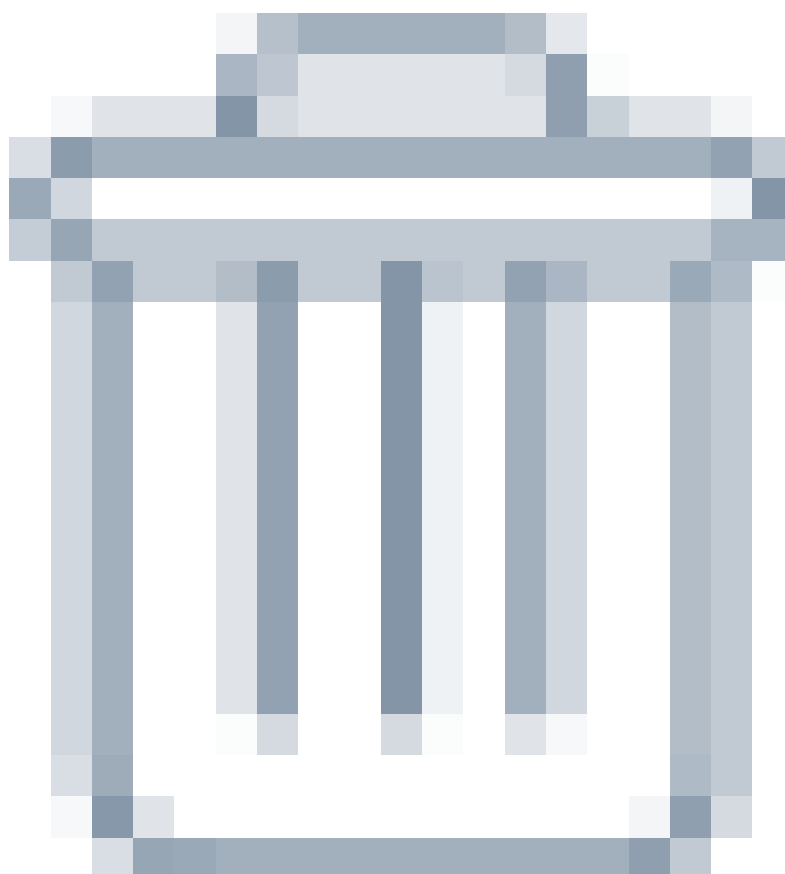
* Campos obligatorios

Basica Oauth

Requiere autenticación NO

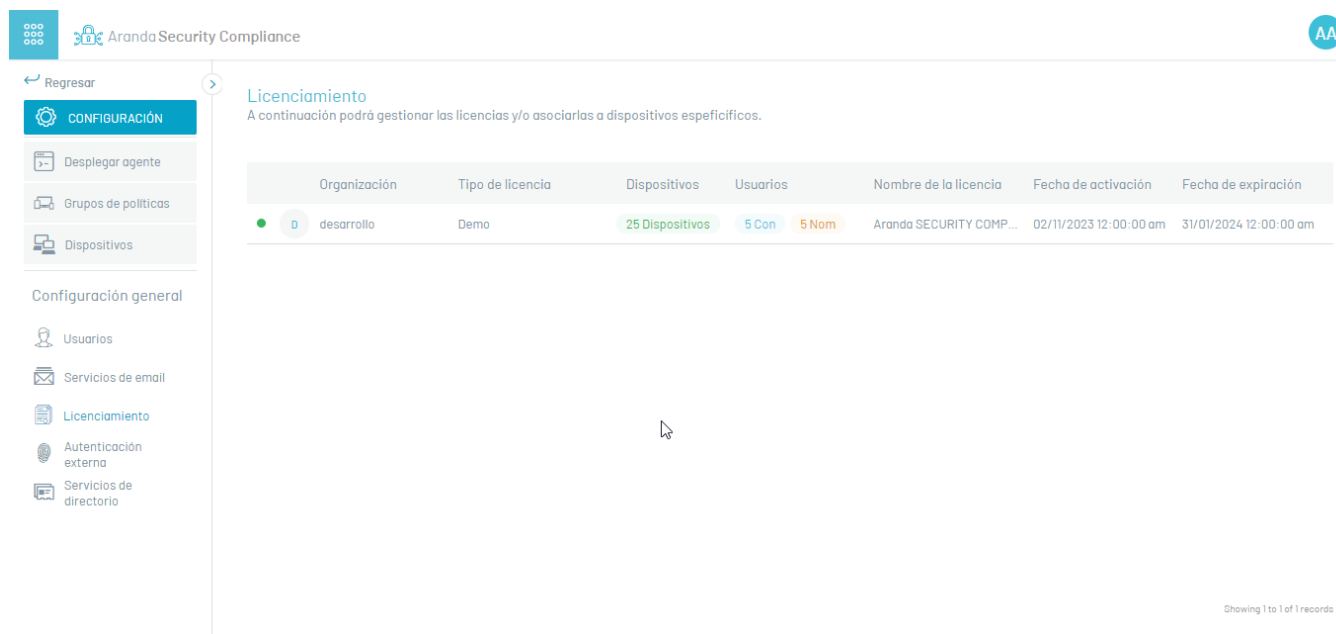
Eliminar Servidores

12. Para eliminar Servidores, en la vista de información seleccione uno o varios registros del listado de servidores configurados que quiere borrar y presione el botón Eliminar



Visualizar la información de las licencias

1. Ingrese a la consola de Aranda Security Compliance con un usuario con rol de administrador , en la sección de **Configuración general** del menú principal, seleccione la opción **Licenciamiento**. En la vista de información se podrá visualizar el listado de licencias disponibles agrupadas con datos como:

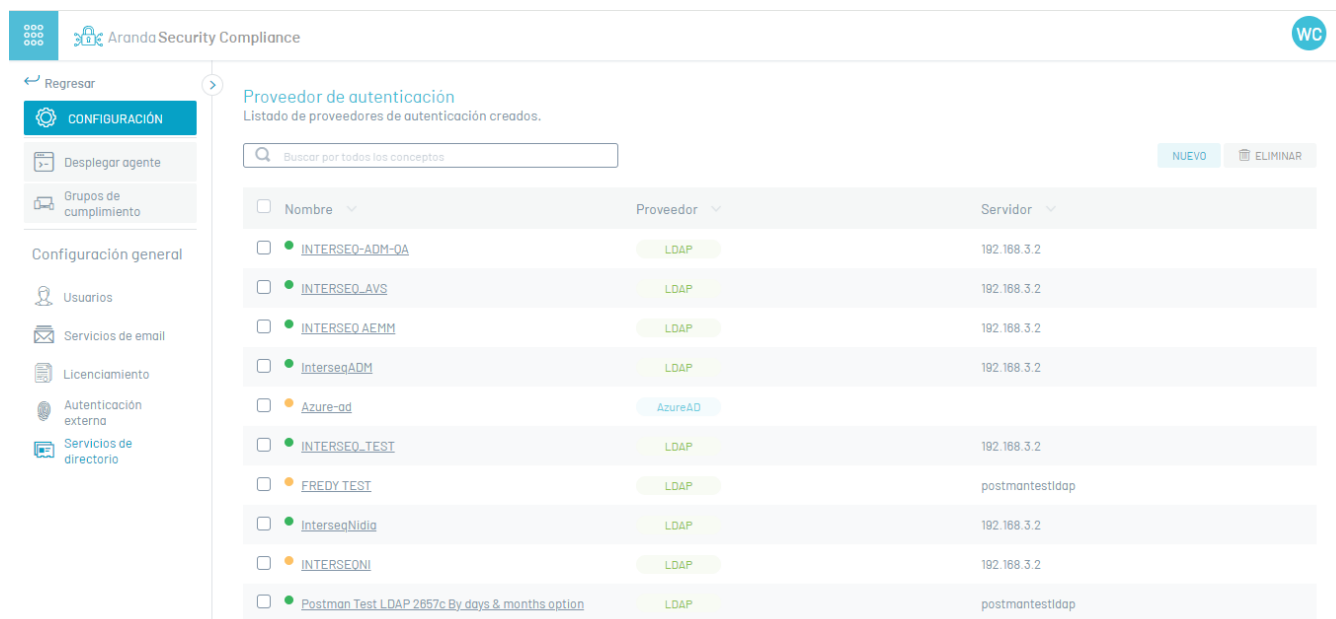


Columna	Descripción
Nombre	Es el nombre asignado a la licencia.
Tipo	Tipo de licencia.
Dispositivos	Número de estaciones de trabajo concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Usuarios	Número de usuarios concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Organización	Empresa dueña de la licencia
Fecha de activación	Fecha en la que son activadas las licencias.
Fecha de expiración	Fecha de caducidad de las licencias.

Servicios de directorio

Configuración de tipo de proveedor LDAP

1. Ingrese a la consola de Aranda Security con rol de administrador, en la sección de **Configuración general** del menú principal, seleccione la opción **Servicios de Directorio**. En la vista de información se despliega el listado de proveedores de autenticación.



2. En la vista de información de los proveedores, tendrá habilitadas acciones de gestión y organización de la información. [Vista de Información en Entorno Web ASEC](#)

Crear Proveedores

3. En la vista de información de servidores de directorios, seleccione el botón **Nuevo** y complete la información básica requerida para establecer la conexión con su servidor de directorio:

El formulario muestra un encabezado con 'NC' y 'Nombre completo' (INACTIVO). Los campos obligatorios (*Nombre completo, *Servidor LDAP, *Puerto, *Tipo de autenticación, *Formato de usuario) están acompañados de iconos de advertencia. El estado 'Estado' tiene un interruptor desactivado. A la derecha, 'Seleccione el tipo de autenticación' ofrece 'LDAP' (seleccionado) y 'Azure AD'. Los checkboxes 'Utilizar proveedor por defecto', 'Usar distinción de nombre DS' y 'Habilitar SSL' están desactivados. Un botón 'Modificar' está ubicado en la parte inferior derecha.

Campo	Descripción
Nombre completo	Nombre que le desea asignar a su directorio.
Servidor LDAP	DNS o IP del servidor del directorio.
Puerto	Puerto TCP para establecer comunicación con el servidor del directorio.
Tipo de autenticación	Modo de autenticación a través del cual se permiten las conexiones.
Formato de usuario	Podrá elegir entre 3 formatos de usuario: UserNameOnly, FullyQualifiedDomainName y UserPrincipalName .
Estado	Para la creación del directorio debe seleccionar el estado activo.
Proveedor de autenticación	Podrá elegir entre dos proveedores LDAP o Azure AD.
Utilizar proveedor por defecto	Se activa esta opción para que el tipo de autenticación que aparezca por defecto, sea el creado (LDAP o Azure AD) al ingresar al sitio de AVS.
Usar distinción de nombre DS	Esta opción se activa cuando el servidor de directorios es OpenLDAP y debe enviar el nombre distintivo para el inicio de sesión (No se utiliza el nombre de usuario).
Habilitar SSL	Indica si aplica protocolo de seguridad.

4. En la sección **Tipo de Autenticación**, podrá establecer el tipo de proveedor para la autenticación:

- **LDAP**: Es un protocolo de aplicación estándar para consultas, que puede almacenar, gestionar, proteger y autenticar la información de los usuarios, como el nombre de usuario y la contraseña.
- **Azure**: Servicio de administración de identidades basado en el cloud de Microsoft.

Proveedor LDAP

5. En la vista detalle del proveedor, haga clic en el botón **Modificar**; se habilita la ventana **Importar** donde podrá ingresar los datos necesarios para la sincronización. En la información básica del directorio empresarial LDAP, ingrese los datos usuario y contraseña.

En la pestaña **Mapeo de Usuarios** los campos obligatorios a registrar son: Filtro de usuario para tener en cuenta en la importación, identificador único y nombre de usuario.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

INTERSE0-ADM-0A
AzureAD

*URL de autoridad *Identificador del cliente *Secreto del cliente

Mapeo de usuarios Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la Importación *Identificador único
(&(objectCategory=person)) objectGUID

*Nombre de usuario	Correo electrónico	Nombre completo	Jefe Inmediato
sAMAccountName	mail	name	
Identificación	País	Departamento	Ciudad
Teléfono	Teléfono oficina	Teléfono oficina 2	Fax
mobile			

6. Al registrar los campos haga clic en el botón **Probar conexión**




. Si la conexión fue exitosa podrá visualizar el mensaje: **La información quedó completa ya puedes finalizar la importación** y se autoriza la continuación del proceso.

7. Al terminar de registrar la información, haga clic en el botón **desincronizar**




y en la ventana que se habilita active la sincronización.

 **Última sincronización**
2023-12-28T20:18:01.253+00:00 Activo

Programar sincronización
Seleccione la fecha y la hora en la que quiere hacer la programación

Ejecutar ahora Programar

8. La sincronización puede ser manual (de inmediato) o se puede programar automáticamente una única vez o cada cierto número de horas para actualizar los nuevos usuarios. Después de seleccionar el tipo de sincronización y realizar la configuración, haga clic en el botón **Confirmar sincronización**.

 **Última sincronización**
2023-12-28T20:18:01.253+00:00 Activo

Programar sincronización
Seleccione la fecha y la hora en la que quiere hacer la programación

Ejecutar ahora Programar

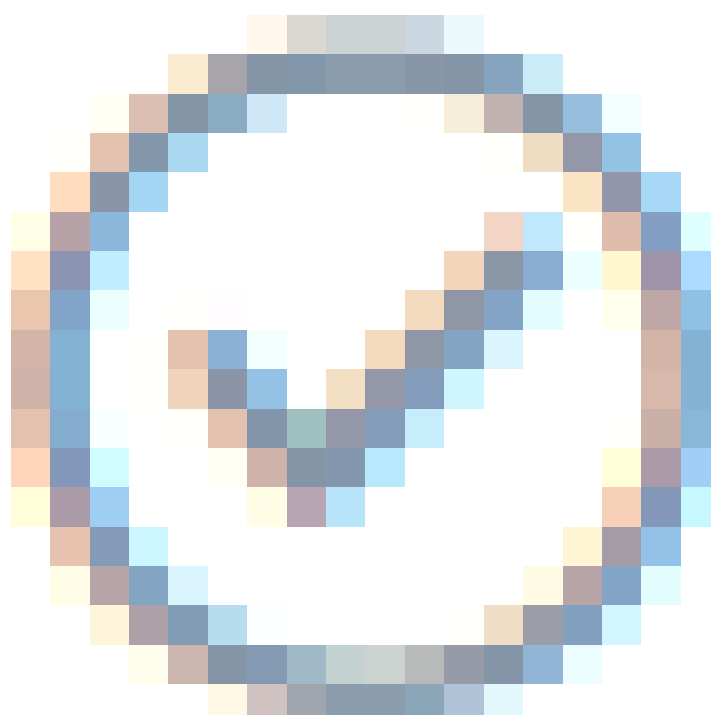
Periodicidad

Una Vez Por Hora

Iniciar en:

Repetir cada: Hora(s)

9. Al terminar la configuración del directorio LDAP, en la ventana Importar, haga clic en el botón **deconfirmación**



y en la ventana de configuración básica de LDAP haga clic en **Guardar**



INTERSEQ_TEST ACTIVO

*Nombre completo
INTERSEQ_TEST

*Servidor LDAP
192.168.3.2

*Puerto
0

*Tipo de autenticación
Negotiate

*Formato de usuario
UserNameOnly

Estado Activo

Seleccione el tipo de autenticación

Seleccione el proveedor por el que va crear el tipo de autenticación

LDAP
Cree uno o varios directorios empresariales.

Azure AD
Importar usuario de office 365.

Utilizar proveedor por defecto
 Usar distinción de nombre DS
 Habilitar SSL

Modificar

10. Terminada la sincronización, el administrador podrá asignar los roles respectivos a los usuarios sincronizados.

Proveedor Azure AD

1. En la vista detalle del proveedor, ingrese el nombre completo del directorio de Azure que desea sincronizar y haga clic en el botón **Modificar**; se habilita la ventana **Importar** donde podrá ingresar los datos necesarios para la sincronización. En la información básica del directorio Azure, ingrese los datos URL de autoridad, el identificador del cliente y el secreto del cliente suministrado por Azure.

En la pestaña **Mapeo de Usuarios** los campos obligatorios a registrar son: Filtro de usuario para la importación, identificador único y Nombre de usuario.

Importar
Seleccione el tipo de proveedor de autenticación para importar.

INTERSEQ-ADM-OA
AzureAD

*URL de autoridad

*Identificador del cliente

*Secreto del cliente

Mapeo de usuarios | Mapeo de grupos

*Ingrese el filtro de usuario para tener en cuenta en la Importación

*Identificador único

*Nombre de usuario <input type="text" value="sAMAccountName"/>	Correo electrónico <input type="text" value="mail"/>	Nombre completo <input type="text" value="name"/>	Jefe Inmediato <input type="text"/>
Identificación <input type="text"/>	País <input type="text"/>	Departamento <input type="text"/>	Ciudad <input type="text"/>
Teléfono <input type="text" value="mobile"/>	Teléfono oficina <input type="text"/>	Teléfono oficina 2 <input type="text"/>	Fax <input type="text"/>

6. Al registrar los campos haga clic en el botón **Probar conexión**




. Si la conexión fue exitosa podrá visualizar el mensaje: **La información quedó completa ya puedes finalizar la importación y se autoriza la continuación del proceso.**

7. Al terminar de registrar la información, haga clic en el botón **desincronizar**



y en la ventana que se habilita active la sincronización.

 **Última sincronización** 2023-12-28T20:18:01.253+00:00 Activo

Programar sincronización
Seleccione la fecha y la hora en la que quiere hacer la programación

Ejecutar ahora Programar

Periodicidad

Una Vez Por Hora

Iniciar en:

8. La sincronización puede ser manual (de inmediato) o se puede programar automáticamente una única vez o cada cierto número de horas. Después de seleccionar el tipo de sincronización y realizar la configuración, haga clic en el botón **Confirmar sincronización**.



Última sincronización

2023-12-28T20:18:01.253+00:00

Activo

Programar sincronización

Seleccione la fecha y la hora en la que quiere hacer la programación

Ejecutar ahora Programar

Periodicidad

Una Vez Por Hora

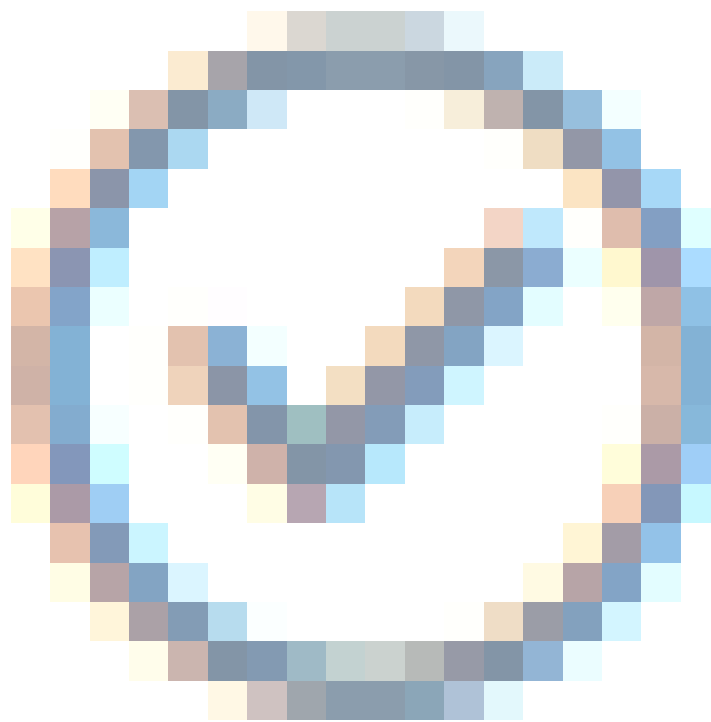
Iniciar en:

Repetir cada: Hora(s)

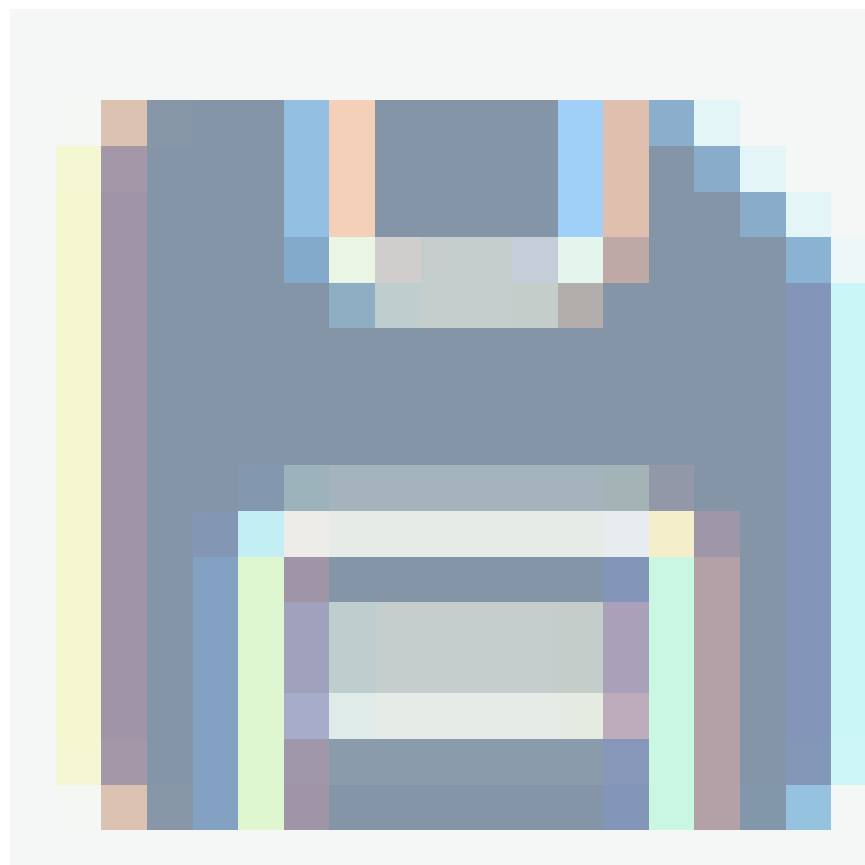
CANCELAR

CONFIRMAR SINCRONIZACIÓN

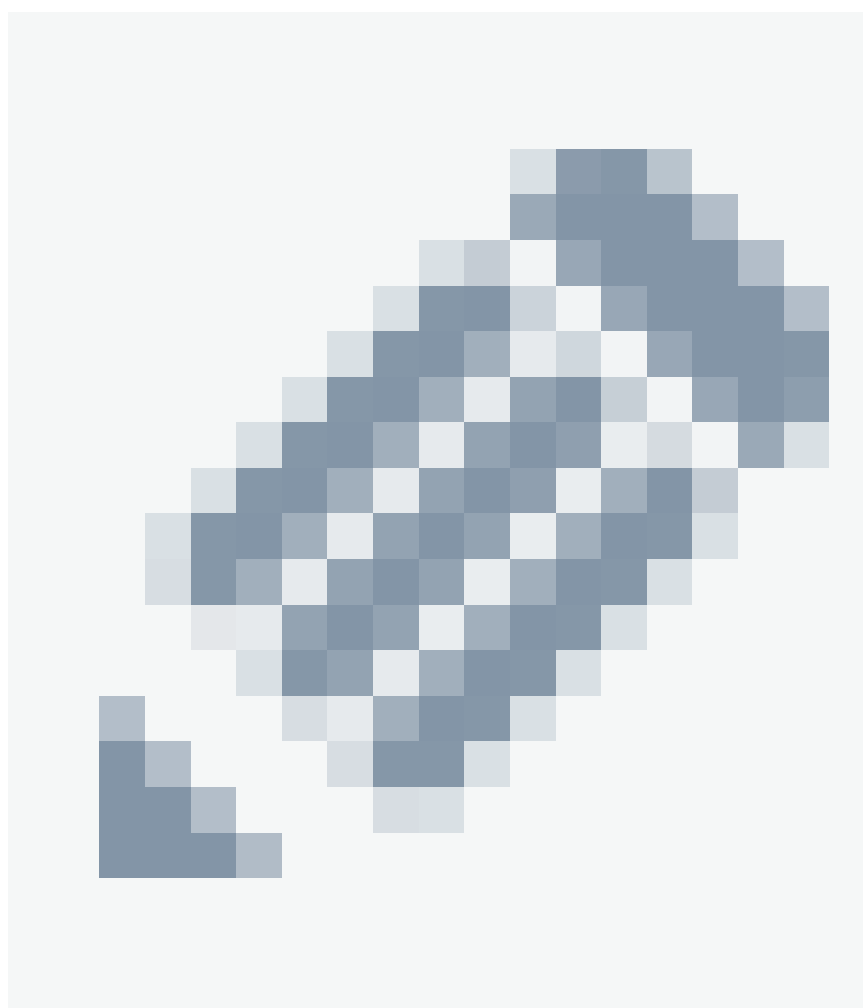
9. Al terminar la configuración del directorio de Azure AD en la ventana Importar, haga clic en el botón de confirmación



y en la ventana de configuración básica de Azure AD haga clic en Guardar



1. Para editar un directorio o proveedor de autenticación, en la vista de información de servicios de directorios de la consola web de ASEC, seleccione un registro del listado de servicios de directorios y en la vista detalle haga clic en el ícono de editar



para modificar la información requerida.

compliance

Proveedor de autenticación

Listado de proveedores de autenticación creados.

Nombre	Proveedor
<input type="checkbox"/> INTERSEQ-ADM-OA	LDAP
<input type="checkbox"/> INTERSEQ-AVS	LDAP
<input type="checkbox"/> INTERSEQ-AEMM	LDAP
<input type="checkbox"/> InterseqADM	LDAP
<input type="checkbox"/> Azure-ad	AzureA
<input type="checkbox"/> INTERSEQ_TEST	LDAP
<input type="checkbox"/> FREDY_TEST	LDAP
<input type="checkbox"/> InterseqNidla	LDAP 192.168.3.2
<input type="checkbox"/> INTERSEQNI	LDAP 192.168.3.2
<input type="checkbox"/> Postman Test LDAP 2857c By days & months option	LDAP postmantestidap

INTERSEQ_TEST

ACTIVO

Nombre completo: INTERSEQ_TEST
Servidor LDAP: 192.168.3.2
Puerto: 0

Tipo de autenticación: Negociada
Formato de usuario: Sólo nombre de usuario (usuario)

ELIMINAR

Tipo de autenticación

Proveedor seleccionado

LDAP

Proveedor por defecto

Sincronización

Edite la sincronización de la importación.

Última sincronización
25/01/2024 17:07

Eliminar un proveedor de autenticación

La eliminación de los registros de servicios de directorios se puede realizar de dos formas:

1. Seleccione un registro del listado de servicios de directorios o proveedores de autenticación y en la vista de detalle haga clic en el botón **Eliminar**.
2. Seleccione el checkbox del registro que desea eliminar y haga clic en el botón **Eliminar**



del listado de registros. En ambos casos recibirá una pregunta de confirmación antes de realizar la eliminación.

Proveedor de autenticación
Listado de proveedores de autenticación creados.

Buscar por todos los conceptos

NUEVO ELIMINAR

<input type="checkbox"/>	Nombre	Proveedor	Servidor
<input type="checkbox"/>	INTERSEQ-ADM-OA	LDAP	192.168.3.2
<input type="checkbox"/>	INTERSEQ_AVS	LDAP	192.168.3.2
<input checked="" type="checkbox"/>	INTERSEQ AEMM	LDAP	192.168.3.2
<input type="checkbox"/>	InterseqADM	LDAP	192.168.3.2
<input type="checkbox"/>	Azure-od	AzureAD	
<input type="checkbox"/>	INTERSEQ_TEST	LDAP	192.168.3.2
<input type="checkbox"/>	FREDDY TEST	LDAP	postmantestldap
<input type="checkbox"/>	InterseqNidia	LDAP	192.168.3.2
<input type="checkbox"/>	INTERSEQNI	LDAP	192.168.3.2
<input type="checkbox"/>	Postman Test LDAP 2657c By days & months option	LDAP	postmantestldap

Autenticación externa – title: “Autenticación externa” chapter: “configuracion_general” –

Visualizar Proveedores

1. Ingrese a la consola de Aranda Security con rol de administrador, en la sección de **Configuración general** del menú principal, seleccione la opción **Autenticación Externa**. En la vista de información se despliega el listado de proveedores creados.

Aranda Security Compliance

Autenticación externa
Listado de proveedores de autenticación creados.

Buscar por nombre

NUEVO ELIMINAR

<input type="checkbox"/>	Nombre	Consola para la autenticación	Url de la consola
<input type="checkbox"/>	prueba1	ASEC ExternalProviders	https://releaseqa3.arandasoft.com/asec
<input type="checkbox"/>	TestProveedor	ASEC ExternalProviders	https://releaseqa3.arandasoft.com/asec

ESTADO ACTIVO INACTIVO

Mostrando 1 al 2 de 2 registros

2. En la vista de información de los servidores, tendrá habilitadas acciones de gestión y organización de la información. [Vista de Información en Entorno Web ASEC](#)

Crear Proveedor Externo

1. Para crear proveedores externos, en la sección de **Configuración** del menú principal, seleccione la opción **Autenticación Externa**. En la vista de información

seleccione el botón **Nuevo** y en la lista detalle se habilita la ventana de propiedades del proveedor donde podrá completar la información requerida de producto y proveedor:

Nombre de proveedor
INACTIVO

Nombre de proveedor

URL de la consola

URL Inicio de sesión

URL cerrar sesión

Estado Inactivo

Icono y texto del proveedor

Texto corto
Nombre que aparece al lado del icono

Seleccionar Icono
Icono (Tamaño 20x20 pixeles png, jpg)

Información del proveedor
Complete la información para la creación del proveedor de autenticación.

Identificador de Identidad
Ingrese url donde se configura la identidad.

URL Inicio sesión
Ingrese la url con la que va iniciar sesión.

URL Cerrar sesión
Ingrese la url con la que va a cerrar sesión.

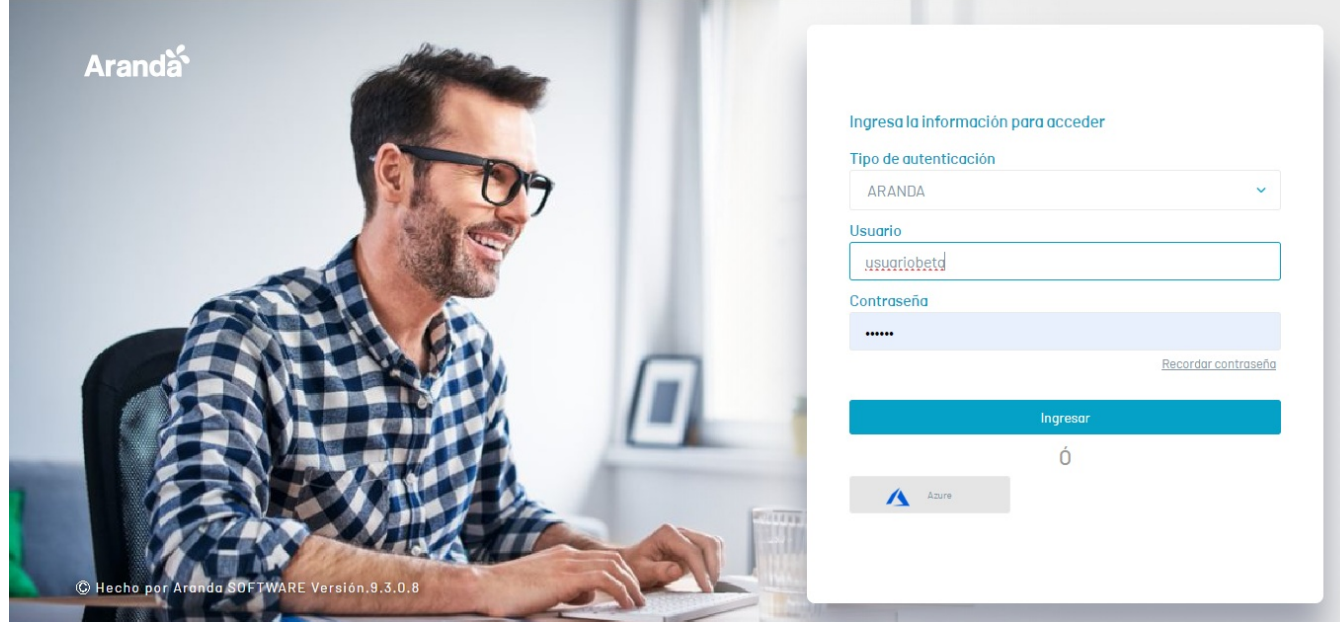
Información de producto

Campo	Descripción
Nombre de proveedor	Nombre que le desea asignar a su directorio.
URL de la consola	URL de la consola web de AVS.
URL inicio de sesión	URL de inicio de sesión de AVS, se genera automáticamente después del ingreso de la URL de la consola.
URL cerrar sesión	URL de cierre de sesión de AVS, se genera automáticamente.
Texto corto	Nombre que aparecerá al realizar el login, al lado del ícono .
Estado	El directorio debe colocarlo en estado activo.
Seleccionar ícono	Imagen de tamaño 20X20 píxeles, que se verá en el login de la aplicación de AVS.

Información del proveedor

Campo	Descripción
Identificador de identidad	URL donde se configura la identidad del proveedor.
URL inicio sesión	URL de inicio de sesión del proveedor.
URL cerrar sesión	URL de cierre de sesión del proveedor.

3. Al terminar de configurar la autenticación de proveedores, haga clic en el botón de **Guardar**. Si la configuración es exitosa, en la pantalla de inicio podrá visualizar el icono con el nombre dado al proveedor externo.

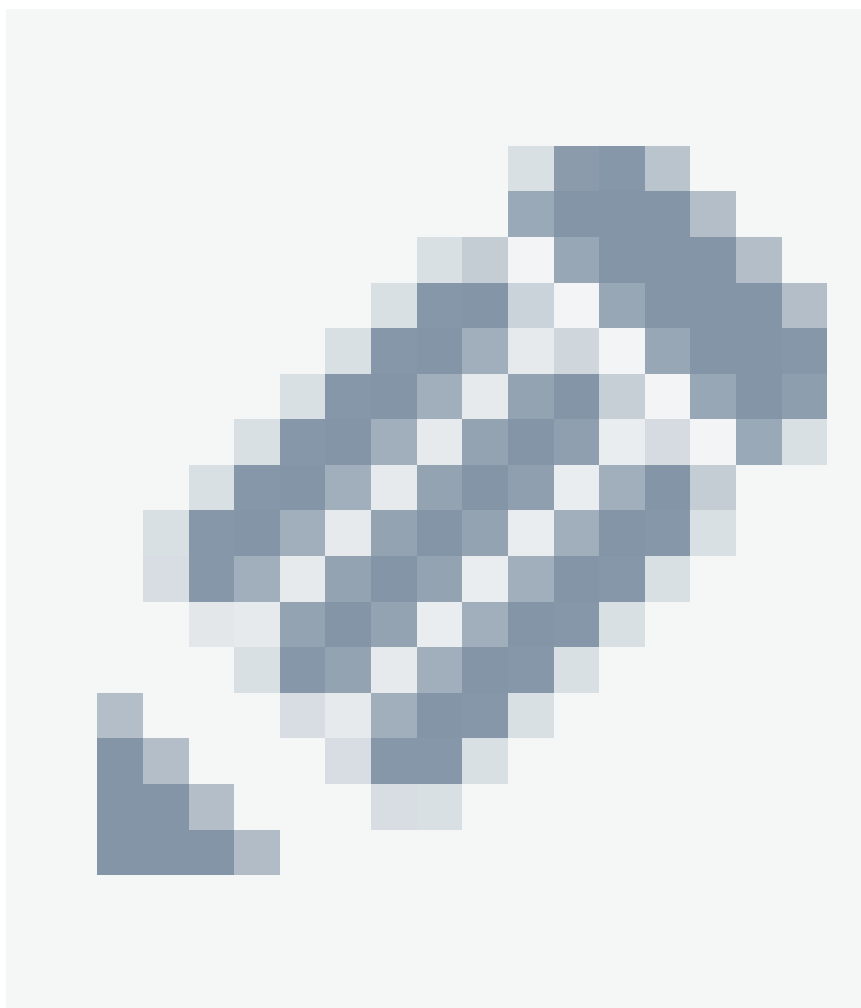


Nota:

- El correo con el que se realiza la autenticación desde el proveedor externo es utilizado como la identificación del usuario y debe estar registrado en la aplicación de AVS.
- Para que la consola pueda autenticar al usuario, este debe ser importado o creado antes de realizar la configuración de autenticación externa.

Editar proveedor Externo

1. Para editar proveedor externo, en la vista de información de autenticación externa de la consola web de ASEC, seleccione un registro del listado de proveedores y en la vista detalle haga clic en el icono de editar



para modificar la información requerida.

Compliance

Autenticación externa
Listado de proveedores de autenticación creados.

Buscar por nombre

Nombre	Consola para
prueba1	ASEC.Extern
TestProveedor	ASEC.Extern

ESTADO ACTIVO INACTIVO

Mostrando 1 al 2 de 2 registros

Eliminar proveedor externo

La eliminación de los registros de servicios de directorios se puede realizar de dos formas:

1. Seleccione un registro del listado de proveedores y en la vista de detalle haga clic en el botón **Eliminar**.
2. Seleccione el checkbox del registro que desea eliminar y haga clic en el botón **Eliminar**



del listado de registros. En ambos casos recibirá una pregunta de confirmación antes de realizar la eliminación.