Desactivar restricción de Windows para instalar certificados raíz

1. Ingresar a secpol.msc desde windows



2. En la sección izquierda de la ventana, seleccionar "Directivas de clave pública"



3. Luego, en la sección derecha de la ventana, seleccionar "Configuración de validación de rutas de certificados"

🚡 Directiva de seguridad local		-		×
<u>A</u> rchivo A <u>c</u> ción <u>V</u> er Ay <u>u</u> da				
🗢 🄿 🙍 📷 🖼 🖬				
Configuración de seguridad Configuración de seguridad Directivas de cuenta Windows Defender Firewall con segur Directivas de Adaministrador de listas of Directivas de clave públical Directivas de control de aplicaciones Directivas de control de aplicaciones Configuración de directiva de auditor	Tipo de objeto Sistema de cifrado de archivos (EFS) Cirtado de unidad BitLocker Cliente de Servicios de servidor de certificados - Directiva de inscrip Configuración de validación de rutas de certificados Cliente de Servicios de servidor de certificados - Inscripción automá	ción de certif	icados	

4. Para que el equipo permita instalar certificado raíz, debe tener las siguientes opciones habilitadas:

Propiedade	s de Configuración de	validación de rutas d	e certificados	?	×				
Almacenes	Editores de confianza	Recuperación de red	Revocación						
Especifiq raíz (CA)	ue reglas para la confian y certificados de confian	za del usuario con respe za del mismo nivel.	ecto a certificados de entidade	s de certificación					
<u> </u>	r esta configuración de d	lirectiva							
Almace	nes de certificados por u	suario							
⊠ <mark>Pe</mark> va	rmitir el uso de <u>e</u> ntidade lidar certificados (recom	s de certificación raíz de endado)	e confianza para						
Pe ⊠ce (n	ermitir que los usuarios co rtificados de confianza d ecomendado)	onfien en lel <u>m</u> ismo nivel	Seleccionar propósitos del ce	ertificado					
Almace	nes de certificados raíz -								
Entid	odes de certificación raiz	en las que pueden con: A raíz de empresa (rec	nar los equipos cliente:						
Ċ) Solo CA raíz de empres	a	Sinch ddoly						
Para realizar una autenticación de usuarios y equipos basada en certificados, los equipos cliente deben usar CA registradas en Active Directory. Las CA también deben ser compatibles con las restricciones de nombre principal del <u>u</u> suario (no recomendado)									
			Aceptar Can	celar Apli <u>c</u>	<u>a</u> r				