



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid

Bastionado active directory

Héctor Ramírez López.

Índice

1. Introducción	3
2. Bastionado de Identidades	9
3. Políticas de grupo.....	10
4. Deshabilitar SMB1	12
5. Auditoria.....	13

1. Introducción

Antes de promover el servidor a Controlador de Dominio debemos de actualizar el equipo desde windows update para aplicar los últimos parches de seguridad.

Windows Update

* La organización administra algunos valores de configuración

[Directivas de actualización de vista configurada](#)



Actualizaciones disponibles

Última comprobación: hoy, 19:49

Faltan correcciones importantes de seguridad y calidad en tu dispositivo.

Actualización de inteligencia de seguridad para Microsoft Defender Antivirus - KB2267602 (versión 1.443.19.0) - Canal actual (ampliado)

Estado: Descargando - 40%

Herramienta de eliminación de software malintencionado de Windows x64, v5.138 (KB890830)

Estado: Descarga pendiente

2025-12 Actualización acumulativa para Windows Server 2019 (1809) para sistemas basados en x64 (KB5071544)

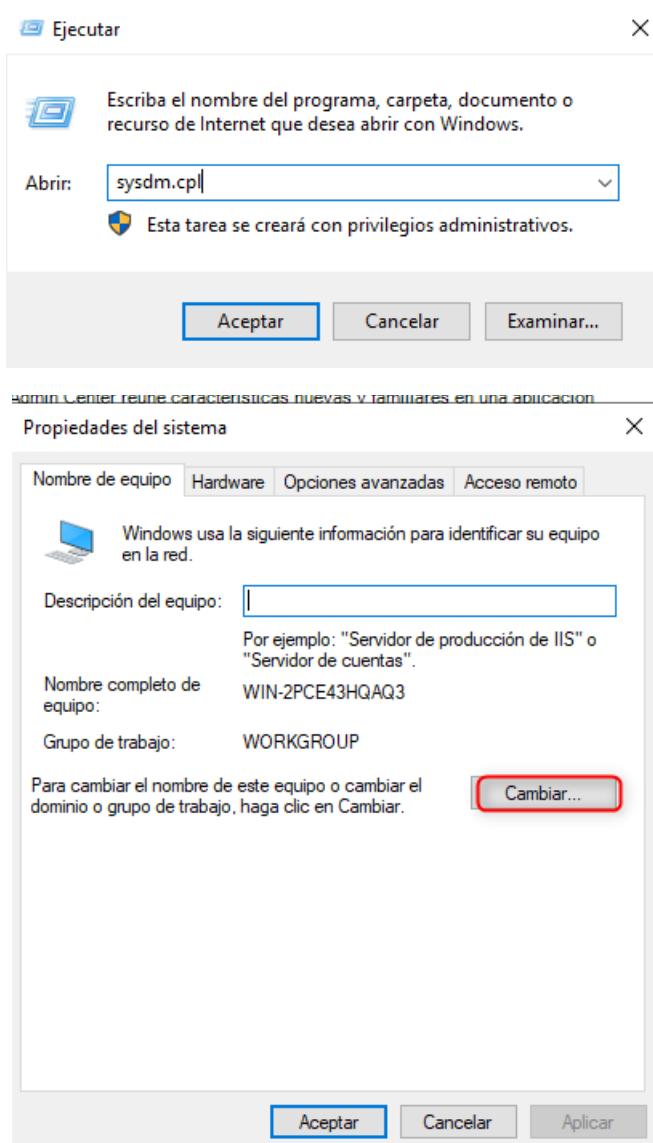
Estado: Descarga pendiente

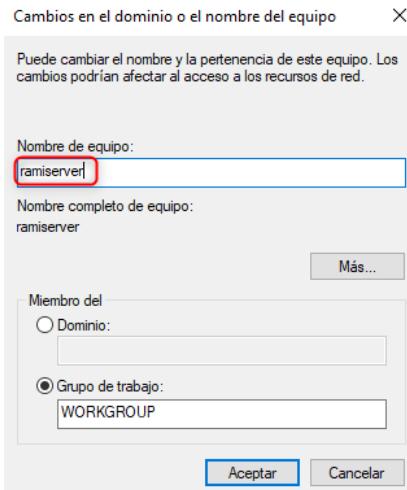
2025-10 Actualización acumulativa de .NET Framework 3.5, 4.7.2 y 4.8 para Windows Server 2019 para x64 (KB5066738)

Estado: Descarga pendiente

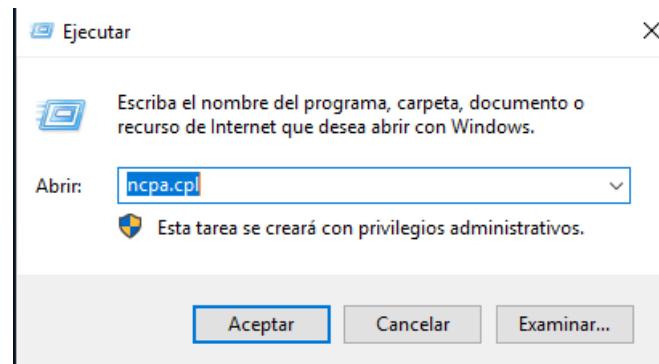
Lo siguiente sera cambiar el nombre del equipo y establecer un ip estatica.

Para cambiar el nombre abriremos ejecutar y escribimos el siguiente comando, le damos a cambiar y ponemos el nombre que queramos.

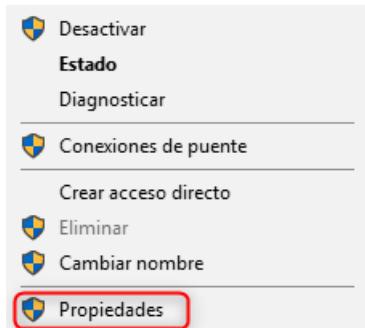




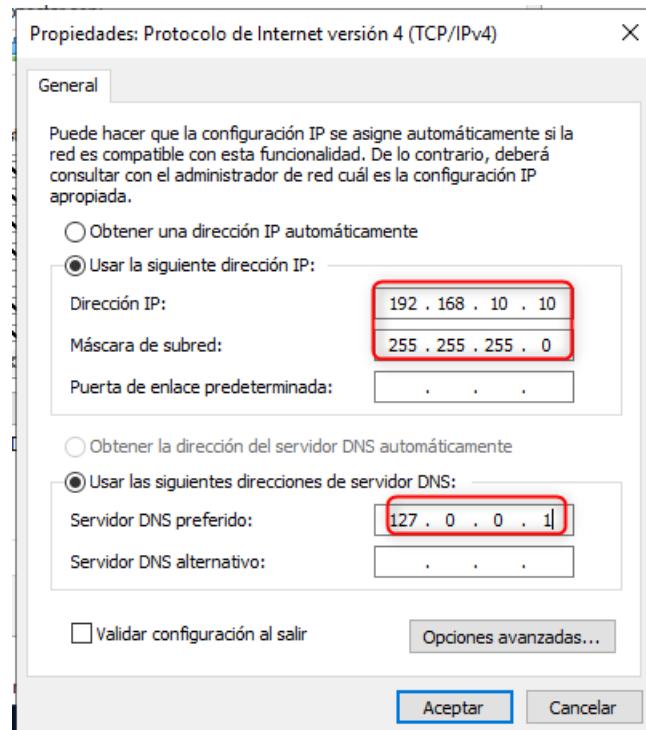
Para establecer una ip estática abrimos ejecutar y ponemos el siguiente comando.



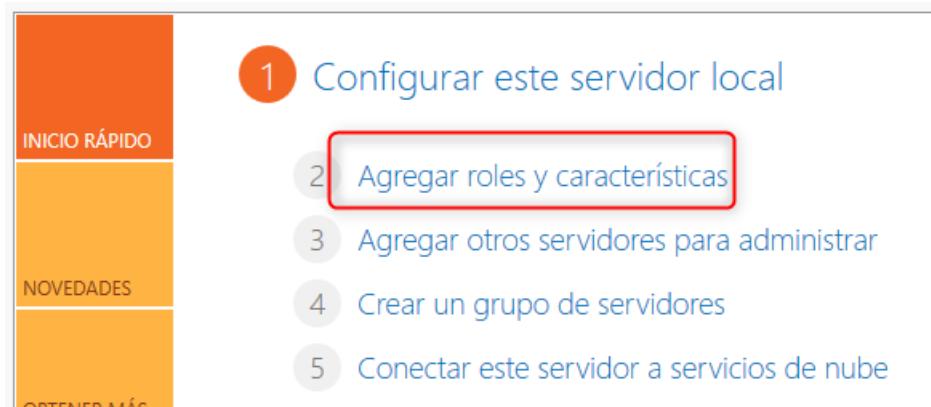
Le daremos clic derecho en el adaptador de red y nos iremos a propiedades.



Pondremos la siguiente dirección ip mascara de red y dns.



Ahora ya podremos promover el servidor a controlador de dominio abrimos el administrador del servidor y agregar roles y características, seleccionamos servicios de dominio y active directory.





Asistente para agregar roles y características

Seleccionar roles de servidor

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

AD DS

Confirmación

Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

Roles

- Acceso remoto
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Atestación de mantenimiento del dispositivo
- Controladora de red
- Hyper-V
- Servicio de protección de host
- Servicios de acceso y directivas de redes
- Servicios de archivos y almacenamiento (1 de 12 instalados)
- Servicios de certificados de Active Directory
- Servicios de dominio de Active Directory**
- Servicios de Escritorio remoto
- Servicios de federación de Active Directory
- Servicios de implementación de Windows
- Servicios de impresión y documentos
- Servidor de fax
- Servidor DHCP
- Servidor DNS
- Servidor web (IIS)

Agregamos un nuevo bosque con el nombre que queramos para nuestro active directory.

Configuración de implementación

Configuración de implementación...

Opciones del controlador...

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requis...

Instalación

Resultado

Seleccionar la operación de implementación

Agregar un controlador de dominio a un dominio existente

Agregar un nuevo dominio a un bosque existente

Agregar un nuevo bosque

Especificar la información de dominio para esta operación

Nombre de dominio raíz: rami.local

Nos pedira una contraseña para poder restaurar el directorio en caso de que haya problemas.

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2016

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio

Servidor de Sistema de nombres de dominio (DNS)

Catálogo global (GC)

Controlador de dominio de solo lectura (RODC)

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña: *****

Confirmar contraseña: *****

2. Bastionado de Identidades

No se debería trabajar con el usuario admin por defecto, vamos a crear uno nuevo para ello abrimos usuario y equipo de active directory creamos el usuario en la ou users.

The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree structure of organizational units (OU) under 'rami.local'. The 'Users' OU is selected. The right pane is a table listing existing users and groups. A new user account, 'hector ramirez', is visible at the bottom of the list, highlighted with a red rectangular box. The table columns are 'Nombre' (Name), 'Tipo' (Type), and 'Descripción' (Description). Other entries include 'Administradores' (Administrators) group, 'Controlador' (Controller) group, and 'Invitado' (Guest) user.

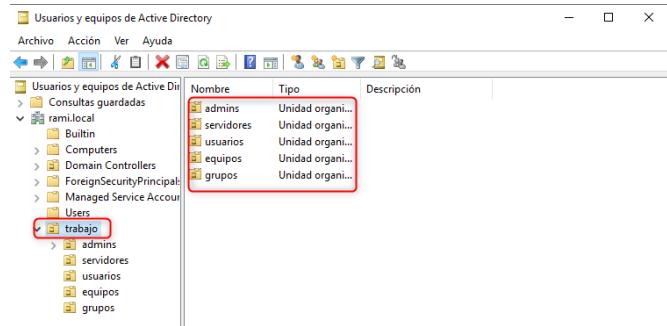
Nombre	Tipo	Descripción
Administradores	Grupo de segu...	Administradores design...
Administradores	Grupo de segu...	Administradores design...
Admins. del ...	Grupo de segu...	Administradores design...
Controlador...	Grupo de segu...	Todos los controladores ...
Controlador...	Grupo de segu...	Se pueden clonar los mi...
Controlador...	Grupo de segu...	Los miembros de este gr...
DnsAdmins	Grupo de segu...	Grupo de administrador...
DnsUpdateP...	Grupo de segu...	Clientes DNS que tienen...
Enterprise D...	Grupo de segu...	Los miembros de este gr...
Equipos del ...	Grupo de segu...	Todas los servidores y es...
Grupo de re...	Grupo de segu...	Los miembros de este gr...
Grupo de re...	Grupo de segu...	Los miembros de este gr...
hector ramirez	Usuario	
Invitado	Usuario	Cuenta integrada para el...

Renombraremos la cuenta de admin que venía por defecto.

The screenshot shows the 'Administradores' group in the Active Directory Users and Computers interface. The table lists a single member, 'sys log', which is highlighted with a red rectangular box. The table has columns for 'Nombre' (Name), 'Tipo' (Type), and 'Descripción' (Description).

Nombre	Tipo	Descripción
sys log	Usuario	Cuenta integrada para la...

Vamos a crear una OU llamada trabajo y dentro vamos a crear las ou's admins servidores, equipos, usuarios y grupos.



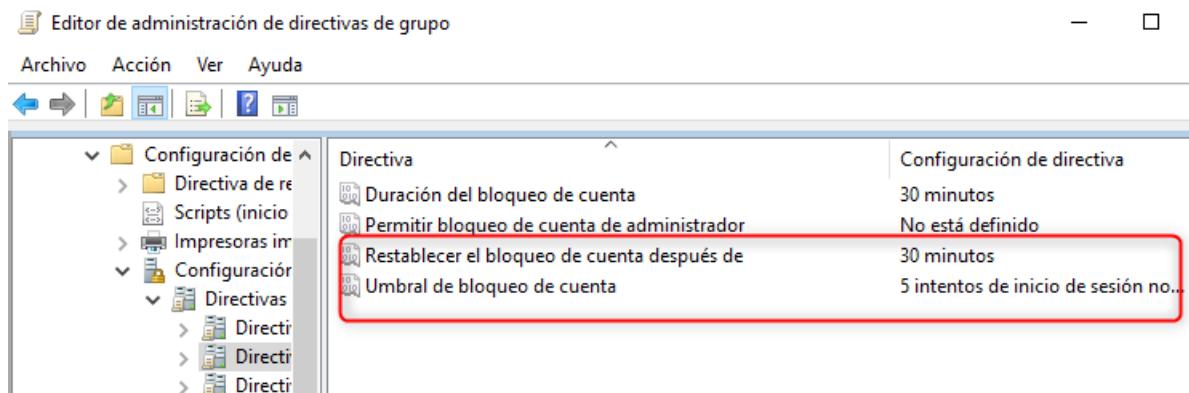
3. Políticas de grupo

Ahora vamos a crear políticas de grupo para ello abrimos ejecutar y escribimos gpmc.msc. Y en directivas de contraseña pondremos longitud minima de contraseña 14 caracteres.

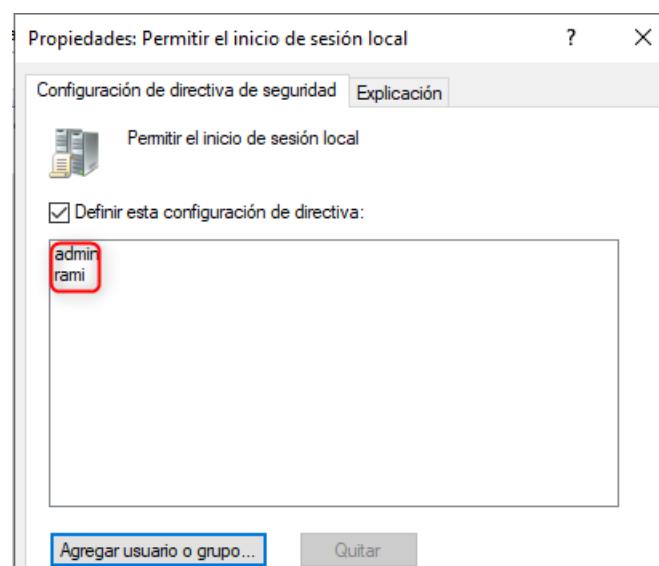
The screenshot shows the 'Editor de administración de directivas de grupo' (Group Policy Management Editor). The left pane shows a tree structure with 'Configuración de grupo' expanded, and 'Directivas' selected. The right pane displays a table of group policy settings. One setting, 'Longitud mínima de la contraseña' (Minimum password length), is highlighted with a blue selection bar. Its value is set to '14 caracteres' (14 characters).

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	Deshabilitada
Auditoría de longitud mínima de contraseña	No está definido
Exigir historial de contraseñas	24 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	14 caracteres
Vigencia máxima de la contraseña	42 días
Vigencia mínima de la contraseña	1 días

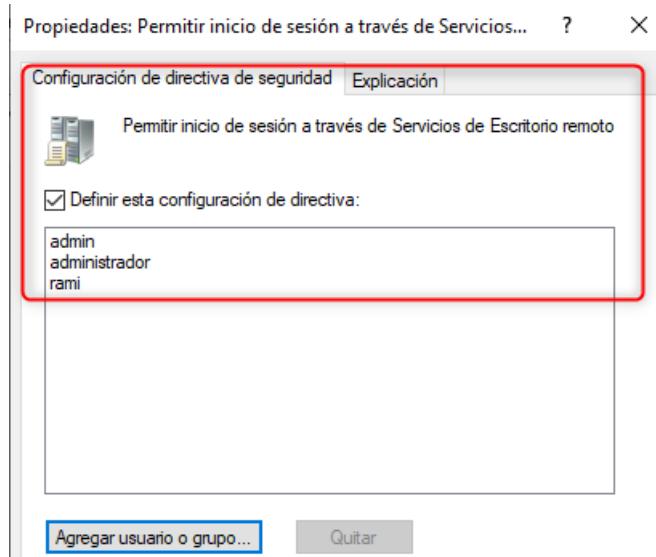
Ahora iremos a directivas de bloqueo de contraseñas y lo estableceremos en 5 intentos y que se reste el bloqueo despues de 30 minutos.



Ahora evitaremos que cualquier usuario inicie sesión en el servidor vamos a configuración del equipo, directivas, configuración de windows, configuración de seguridad, directivas locales y asignación de derechos de usuario. Ahí dentro nos vamos a permitir el inicio de sesión local y solo dejamos el usuario que sea administrador.



Y en permitir inicio de sesión por escritorio remoto creamos lo mismo.



4. Deshabilitar SMB1

Para deshabilitar SMB1 abrimos PowerShell y ejecutamos el siguiente comando.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
PS C:\Users\Administrador>
```

Para comprobar que ya no está activo ejecutaremos el siguiente comando y debería devolver false.

```
PS C:\Users\Administrador> Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
PS C:\Users\Administrador> Get-SmbServerConfiguration | Select EnableSMB1Protocol

EnableSMB1Protocol
-----
False

PS C:\Users\Administrador>
```

5. Auditoria

Primero activaremos la auditoria avanzada en la gpo de controladores de dominio y en inicio y cierre de sesión habilitamos inicio de sesión así registraremos los intentos de intrusión.

Subcategoría	Auditar eventos
[01] Auditar derechos de acceso	No configurada
[01] Auditar bloqueo de cuentas	No configurada
[01] Notificaciones de usuario o dispositivo de auditoria	No configurada
[01] Auditoría de pertenencia a grupos	No configurada
[01] Auditar modo extendido de IPsec	No configurada
[01] Auditar modo principal de IPsec	No configurada
[01] Auditar modo rápido de IPsec	No configurada
[01] Auditar cierre de sesión	No configurada
[01] Auditar inicio de sesión	Errores
[01] Auditar Servidor de directivas de redes	No configurada
[01] Auditar otros eventos de inicio y cierre de sesión	No configurada
[01] Auditar inicio de sesión especial	No configurada

Por último instalaremos pingcastle y nos escaneara nuestro active directory y nos dira como es de seguro y que podemos mejorar.

Una vez abierto seleccionamos la opción 1 healthcheck.

```
C:\Users\Administrador\Desktop\PingCastle_3.4.1.38\PingCastle.exe
*****
***** Netwrix PingCastle (Version 3.4.1.38)
*** **** Get Active Directory Security at 80% in 20% of the time
*   ##### End of support: 2027-01-10.
***** #####
***** ##### To find out more about PingCastle, visit https://www.pingcastle.com
###*****% ## For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
#### For support and questions:
***** ** - Open-source community, visit https://github.com/netwrix/pingcastle/issues
***** %** - Customers, visit https://www.netwrix.com/support.html
what do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-azuread -Score the risk of AzureAD
3-conso -Aggregate multiple reports into a single one
4-carto -Build a map of all interconnected domains
5-scanner -Perform specific security checks on workstations
6-export -Export users or computers
7-advanced -Open the advanced menu
0-Exit
=====
This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

Una vez termine nos dejara un archivo html en la carpeta donde hallamos descargado la herramienta.

TOSHIBA EXT (D:) > PingCastle_3.4.1.38				
	Nombre	Fecha de modificación	Tipo	Tamaño
ido	Active_Directory_Security_Self_Assessme...	16/07/2025 15:03	Firefox PDF Docu...	2.739 KB
s	ad_hc_rami.local.html	03/12/2025 18:09	Firefox HTML Doc...	1.561 KB
---	changelog.txt	16/07/2025 15:03	Documento de tex...	37 KB

Al abrir ese archivo nos dará una puntuación y según vayamos corrigiendo cosas nos bajará la puntuación, lo mejor es cuanto más baja este.

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Como podemos ver tenemos un 25 de 100 la idea es ir haciendo las cosas que no propone para bajar el riesgo a 0 o lo más cercano.

Anomalies rule details [13 rules matched on a total of 73]

LAPS doesn't seem to be installed	+ 15 Point(s)
-----------------------------------	---------------



Universidad
Francisco de
Vitoria
Centro de
Documentación
Europea
UFV Madrid