

	<b>DEPARTAMENTO INFORMÁTICA</b>	
	<b>2º ASIR - ASO</b>	
	<b>CONSULTAS LDAP en Power Shell</b>	

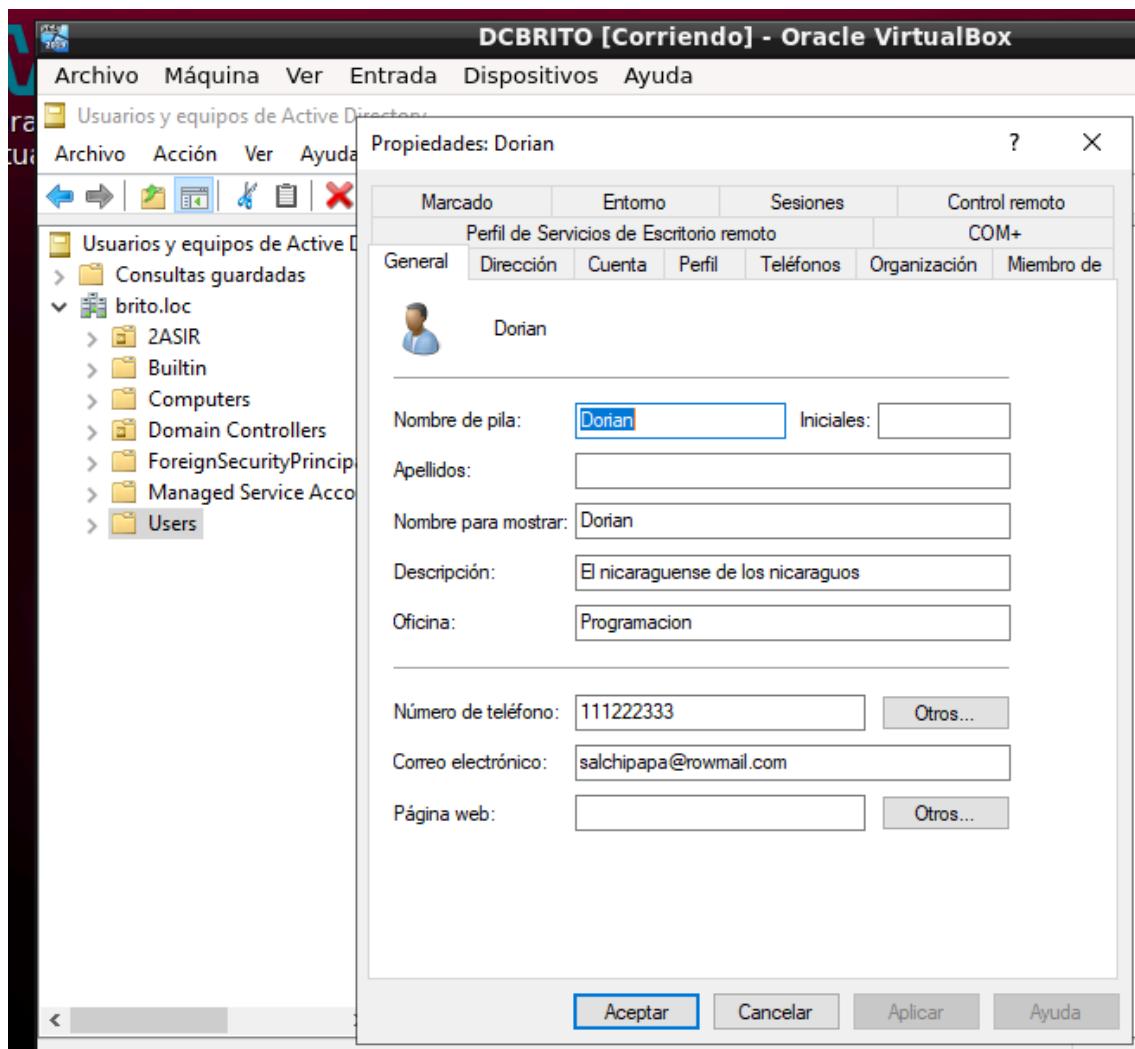
## 0. OBJETIVOS

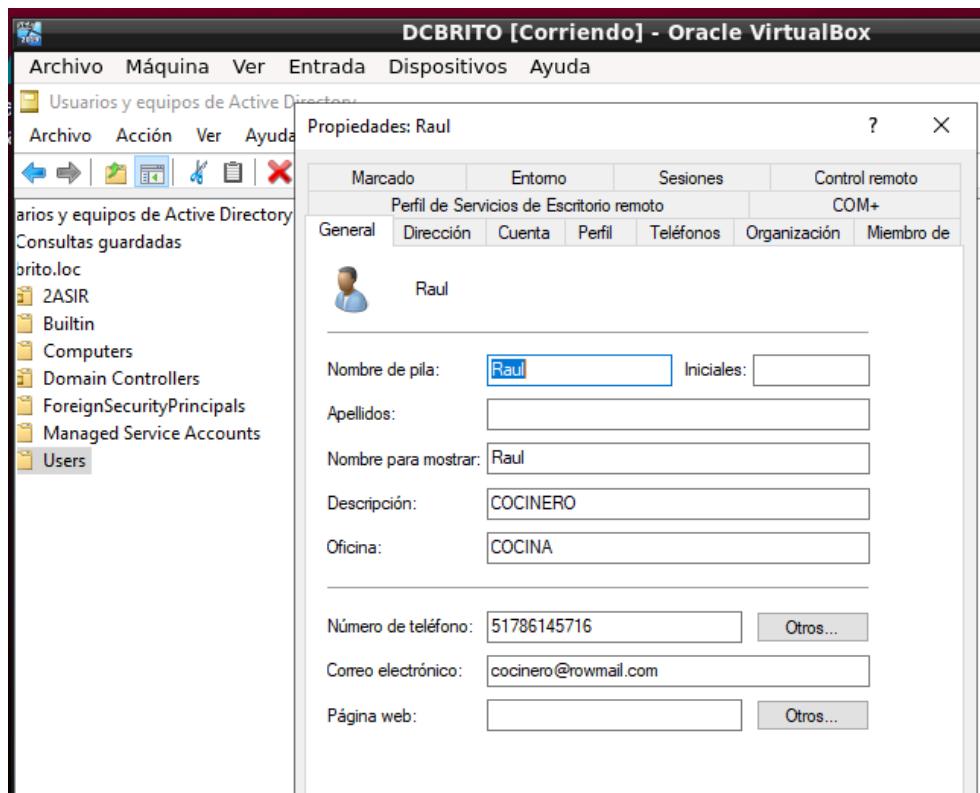
- Realizar consultas LDAP mediante POWER SHELL

## 1. INICIO

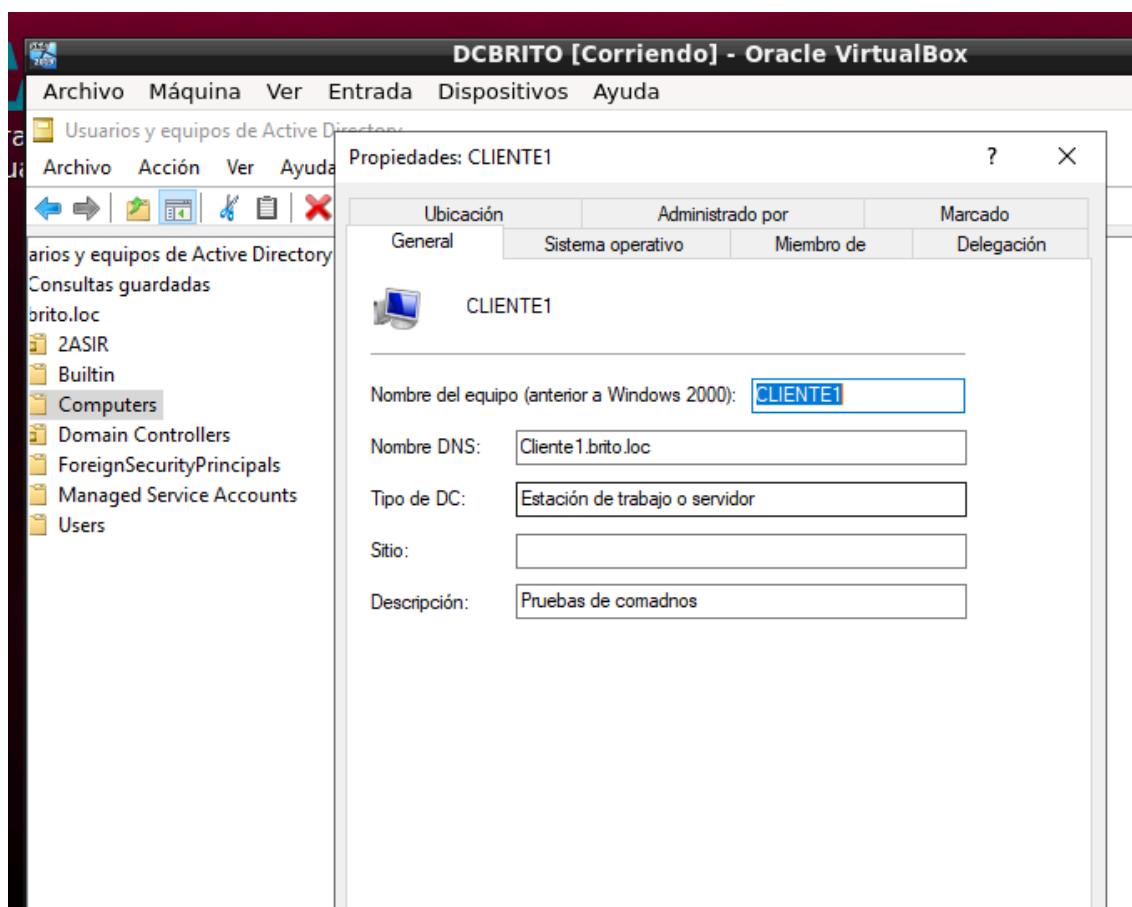
Con el objeto de obtener los máximos atributos debemos de completar mediante la herramienta de USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY toda información posible sobre **dos usuarios ya creados y sobre un equipo cliente**.

USUARIO: Sobre las fichas General – dirección y organización.





EQUIPO: solamente nos permite la descripción – rellenar.



## 2. Get-ADUser

Para poder utilizar los comandos relacionados con AD es necesario instalar el módulo de código para el entorno de active directory. Normalmente en un DC viene cargado.

Buscar la instrucción para cargarlo en caso de un equipo cliente.

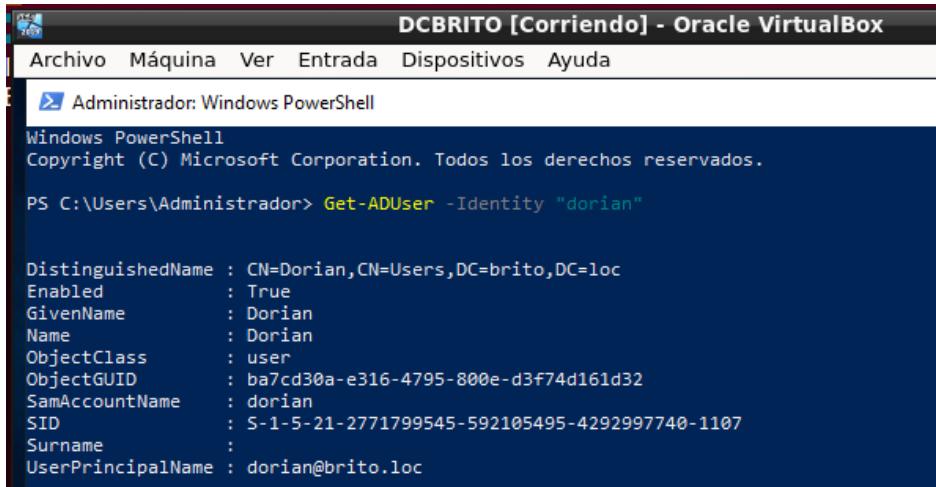
En un equipo cliente (como Windows 10 pro), el módulo no viene instalado. Habrá que instalar las RSAT (Remote Server Administration Tools). Con el comando

```
Get-WindowsCapability -Name RSAT.ActiveDirectory* -Online |  
Add-WindowsCapability -Online.
```

## USUARIO 1

Utilizar el cmdlet Get-ADUser para obtener los atributos principales de un usuario, nombre, nombre distinguido, nombre de cuenta sam, nombre usuario principal UPN, SID,

### Atributos Principales:

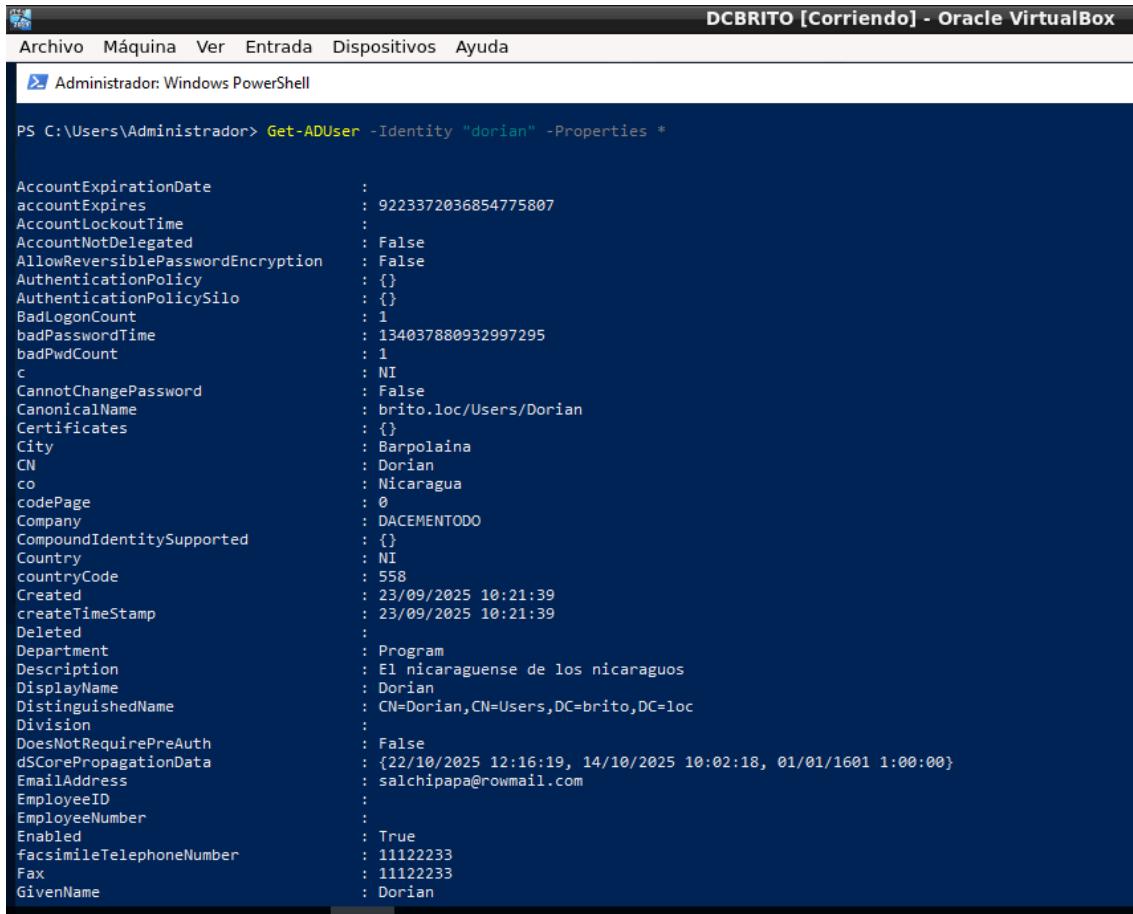


```
PS C:\Users\Administrador> Get-ADUser -Identity "dorian"

DistinguishedName : CN=Dorian,CN=Users,DC=brito,DC=loc
Enabled          : True
GivenName        : Dorian
Name             : Dorian
ObjectClass      : user
ObjectGUID       : ba7cd30a-e316-4795-800e-d3f74d161d32
SamAccountName   : dorian
SID              : S-1-5-21-2771799545-592105495-4292997740-1107
Surname          :
UserPrincipalName : dorian@brito.loc
```

Utilizar el mismo cmdlet para conseguir todos los atributos del usuario.

### Todos los Atributos:

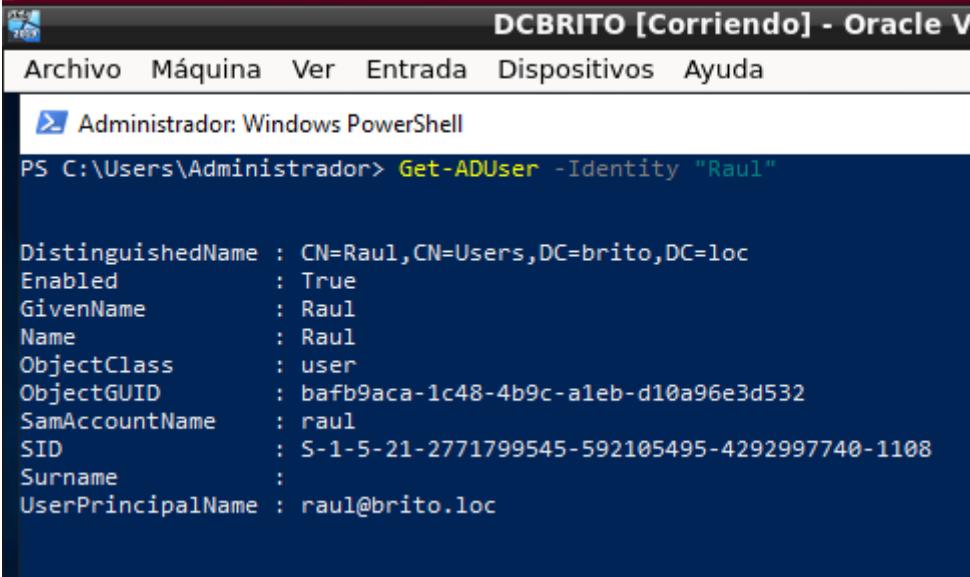


```
PS C:\Users\Administrador> Get-ADUser -Identity "dorian" -Properties *

AccountExpirationDate      :
accountExpires            : 9223372036854775807
AccountLockoutTime         :
AccountNotDelegated       : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy       : {}
AuthenticationPolicySilo   : {}
BadLogonCount              : 1
badPasswordTime            : 134037880932997295
badPwdCount                : 1
c                           : NI
CannotChangePassword       : False
CanonicalName              : brito.loc/Users/Dorian
Certificates               : {}
City                        : Barpolaina
CN                          : Dorian
co                          : Nicaragua
codePage                   : 0
Company                    : DACEMENTODO
CompoundIdentitySupported  : {}
Country                     : NI
countryCode                : 558
Created                    : 23/09/2025 10:21:39
createTimeStamp             : 23/09/2025 10:21:39
Deleted                    :
Department                 : Program
Description                : El nicaraguense de los nicaraguanos
DisplayName                : Dorian
DistinguishedName          : CN=Dorian,CN=Users,DC=brito,DC=loc
Division                   :
DoesNotRequirePreAuth     : False
dSCorePropagationData     : {22/10/2025 12:16:19, 14/10/2025 10:02:18, 01/01/1601 1:00:00}
EmailAddress               : salchipapa@rowmail.com
EmployeeID                 :
EmployeeNumber              :
Enabled                    : True
facsimileTelephoneNumber  : 11122233
Fax                        : 11122233
GivenName                  : Dorian
```

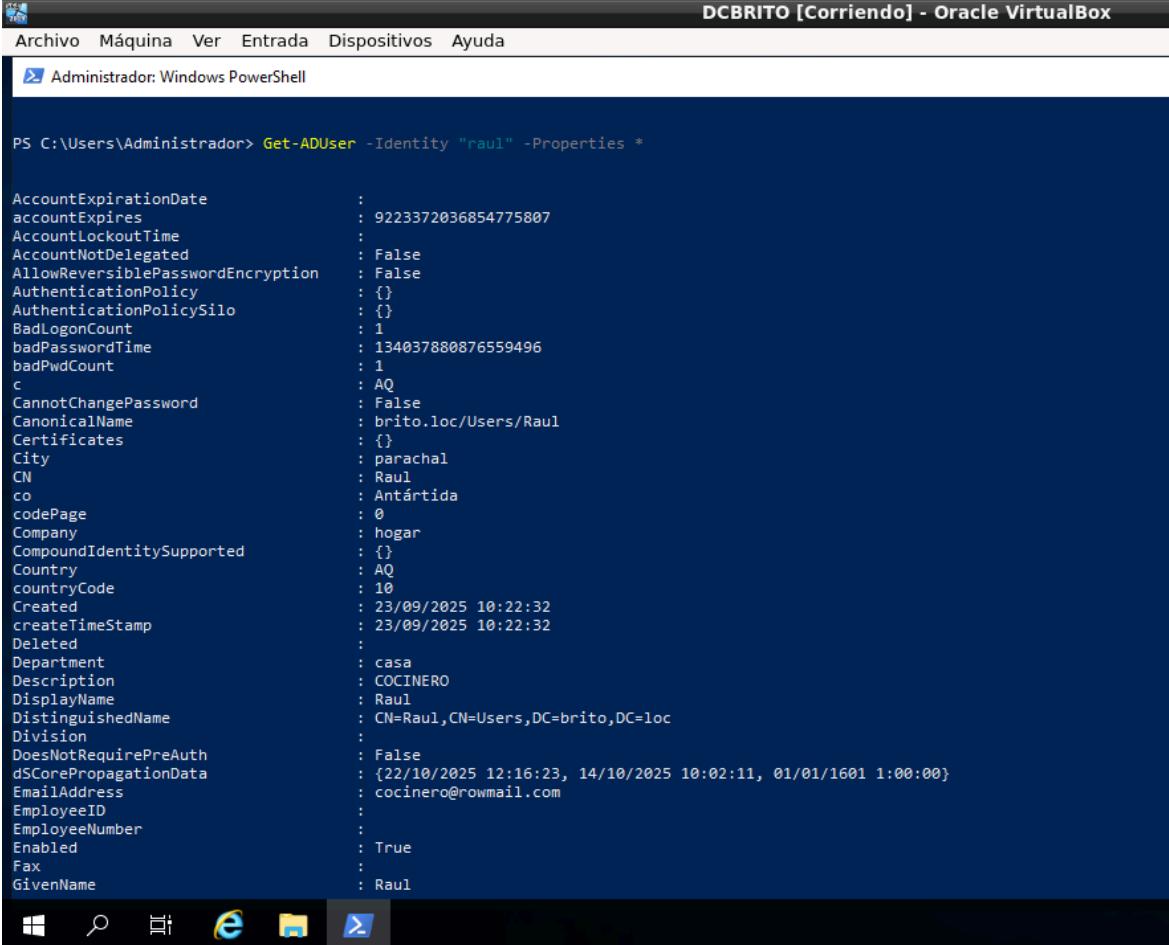
## USUARIO 2

Lo mismo



```
PS C:\Users\Administrador> Get-ADUser -Identity "Raul"

DistinguishedName : CN=Raul,CN=Users,DC=brito,DC=loc
Enabled          : True
GivenName        : Raul
Name             : Raul
ObjectClass      : user
ObjectGUID       : bafb9aca-1c48-4b9c-a1eb-d10a96e3d532
SamAccountName   : raul
SID              : S-1-5-21-2771799545-592105495-4292997740-1108
Surname          :
UserPrincipalName : raul@brito.loc
```

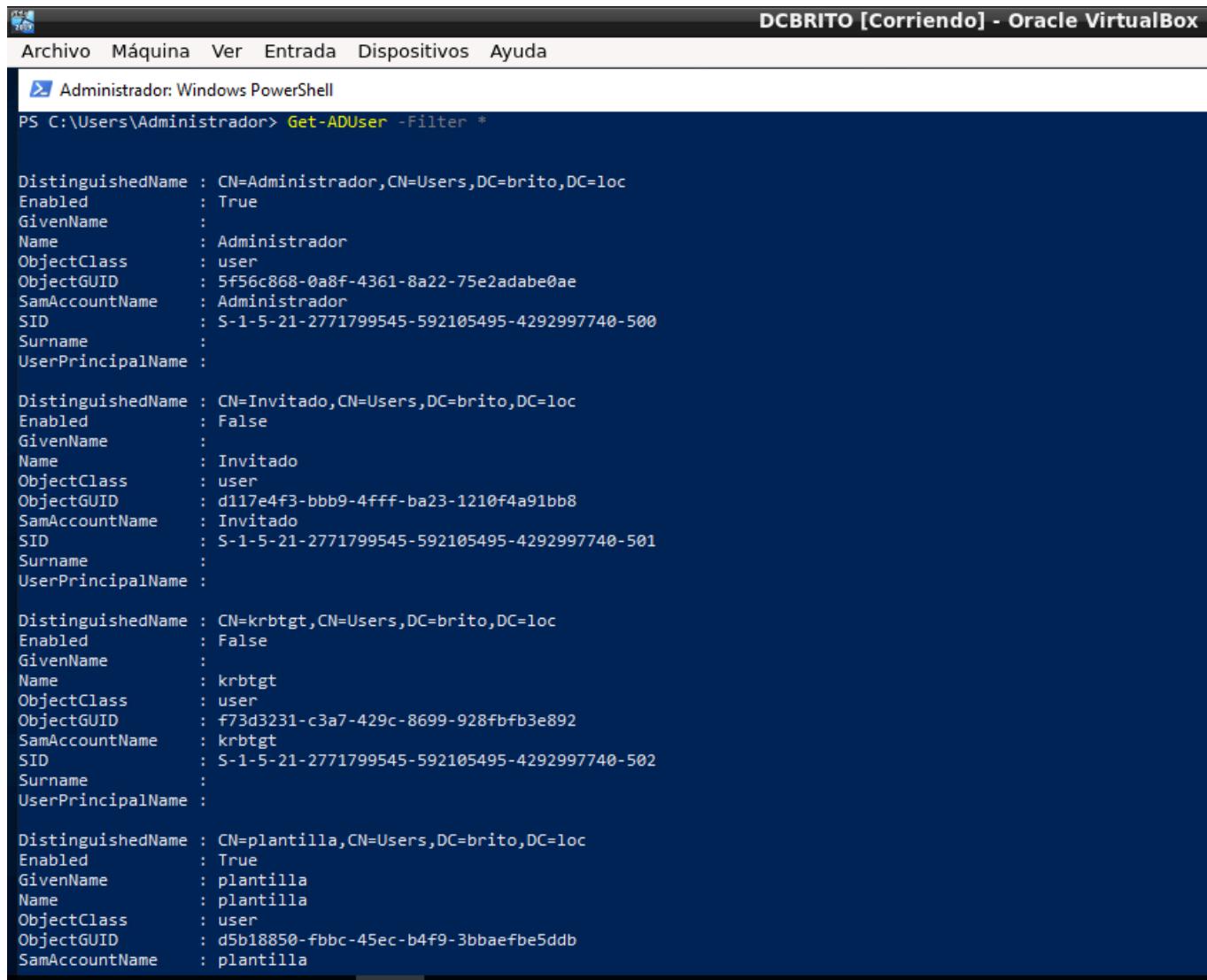


```
PS C:\Users\Administrador> Get-ADUser -Identity "raul" -Properties *

AccountExpirationDate      :
accountExpires            : 9223372036854775807
AccountLockoutTime         :
AccountNotDelegated        : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy       : {}
AuthenticationPolicySilo   : {}
BadLogonCount              : 1
badPasswordTime            : 134037880876559496
badPwdCount                : 1
c                           : AQ
CannotChangePassword       : False
CanonicalName              : brito.loc/Users/Raul
Certificates               : {}
City                        : parachal
CN                          : Raul
co                          : Antártida
codePage                   : 0
Company                    : hogar
CompoundIdentitySupported  : {}
Country                     : AQ
countryCode                : 10
Created                    : 23/09/2025 10:22:32
createTimeStamp             : 23/09/2025 10:22:32
Deleted                    :
Department                 : casa
Description                : COCINERO
DisplayName                : Raul
DistinguishedName          : CN=Raul,CN=Users,DC=brito,DC=loc
Division                   :
DoesNotRequirePreAuth     : False
dSCorePropagationData     : {22/10/2025 12:16:23, 14/10/2025 10:02:11, 01/01/1601 1:00:00}
EmailAddress               : cocinero@rowmail.com
EmployeeID                 :
EmployeeNumber              :
Enabled                    : True
Fax                        :
GivenName                  : Raul
```

### 3. OTROS

Obtener la lista de usuarios del dominio.



The screenshot shows a Windows PowerShell window titled "Administrador: Windows PowerShell" running on a virtual machine named "DCBRITO [Corriendo]". The command "Get-ADUser -Filter \*" is being run, and the output lists several users from the Active Directory:

```
PS C:\Users\Administrador> Get-ADUser -Filter *

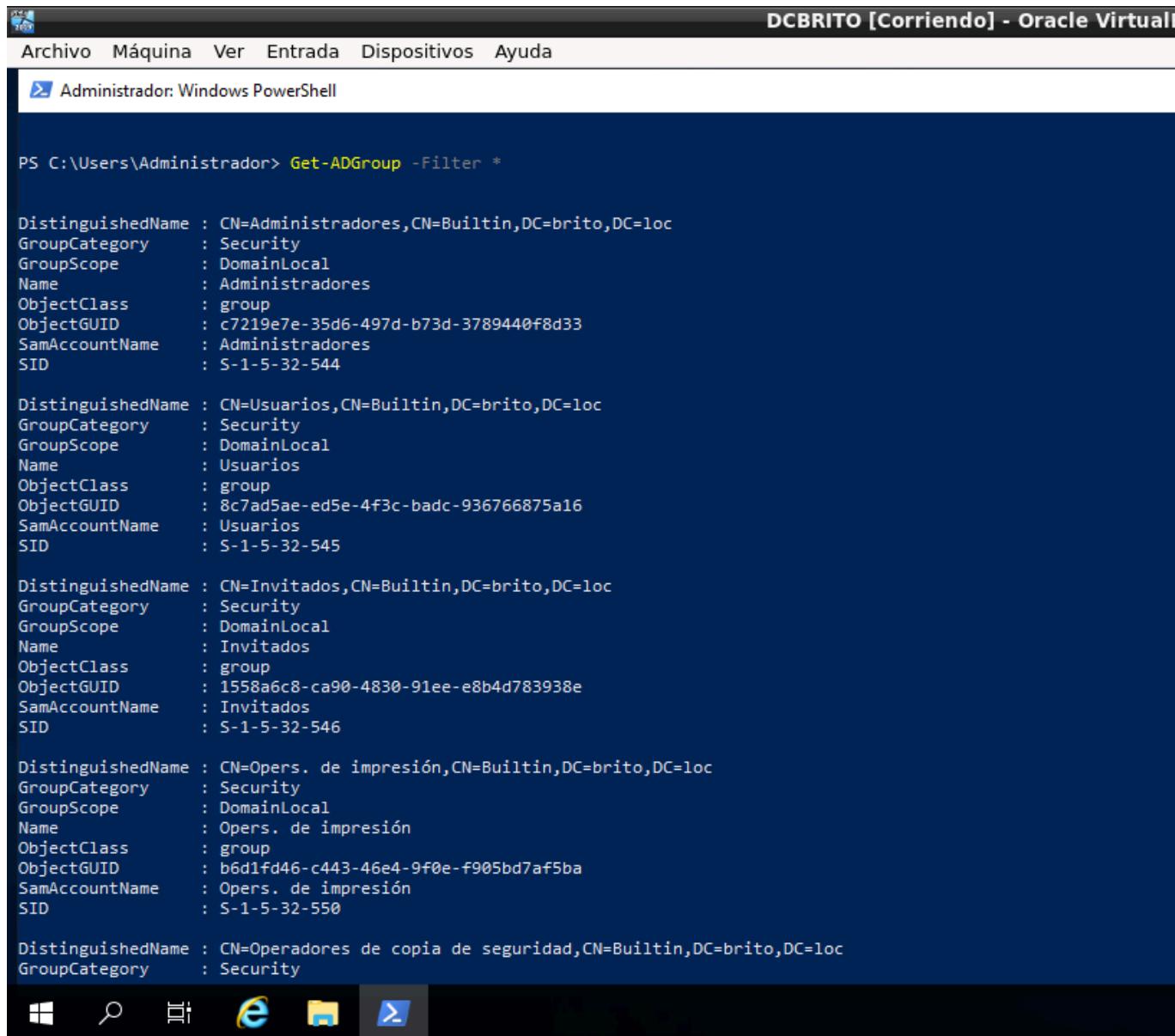
DistinguishedName : CN=Administrador,CN=Users,DC=brito,DC=loc
Enabled          : True
GivenName        :
Name             :
ObjectClass      : user
ObjectGUID       : 5f56c868-0a8f-4361-8a22-75e2adabe0ae
SamAccountName   : Administrador
SID              : S-1-5-21-2771799545-592105495-4292997740-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=Invitado,CN=Users,DC=brito,DC=loc
Enabled          : False
GivenName        :
Name             :
ObjectClass      : user
ObjectGUID       : d117e4f3-bbb9-4fff-ba23-1210f4a91bb8
SamAccountName   : Invitado
SID              : S-1-5-21-2771799545-592105495-4292997740-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=krbtgt,CN=Users,DC=brito,DC=loc
Enabled          : False
GivenName        :
Name             :
ObjectClass      : user
ObjectGUID       : f73d3231-c3a7-429c-8699-928fbfb3e892
SamAccountName   : krbtgt
SID              : S-1-5-21-2771799545-592105495-4292997740-502
Surname          :
UserPrincipalName :

DistinguishedName : CN=plantilla,CN=Users,DC=brito,DC=loc
Enabled          : True
GivenName        : plantilla
Name             : plantilla
ObjectClass      : user
ObjectGUID       : d5b18850-fbbc-45ec-b4f9-3bbaefbe5ddb
SamAccountName   : plantilla
```

Obtener la lista de grupos del dominio.



The screenshot shows a Windows PowerShell window titled "Administrador: Windows PowerShell" running on a virtual machine named "DCBRITO [Corriendo] - Oracle VirtualBox". The command "Get-ADGroup -Filter \*" is being run, and the output lists five built-in groups in the domain:

```
PS C:\Users\Administrador> Get-ADGroup -Filter *

DistinguishedName : CN=Administradores,CN=BuiltIn,DC=brito,DC=loc
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Administradores
ObjectClass       : group
ObjectGUID        : c7219e7e-35d6-497d-b73d-3789440f8d33
SamAccountName   : Administradores
SID               : S-1-5-32-544

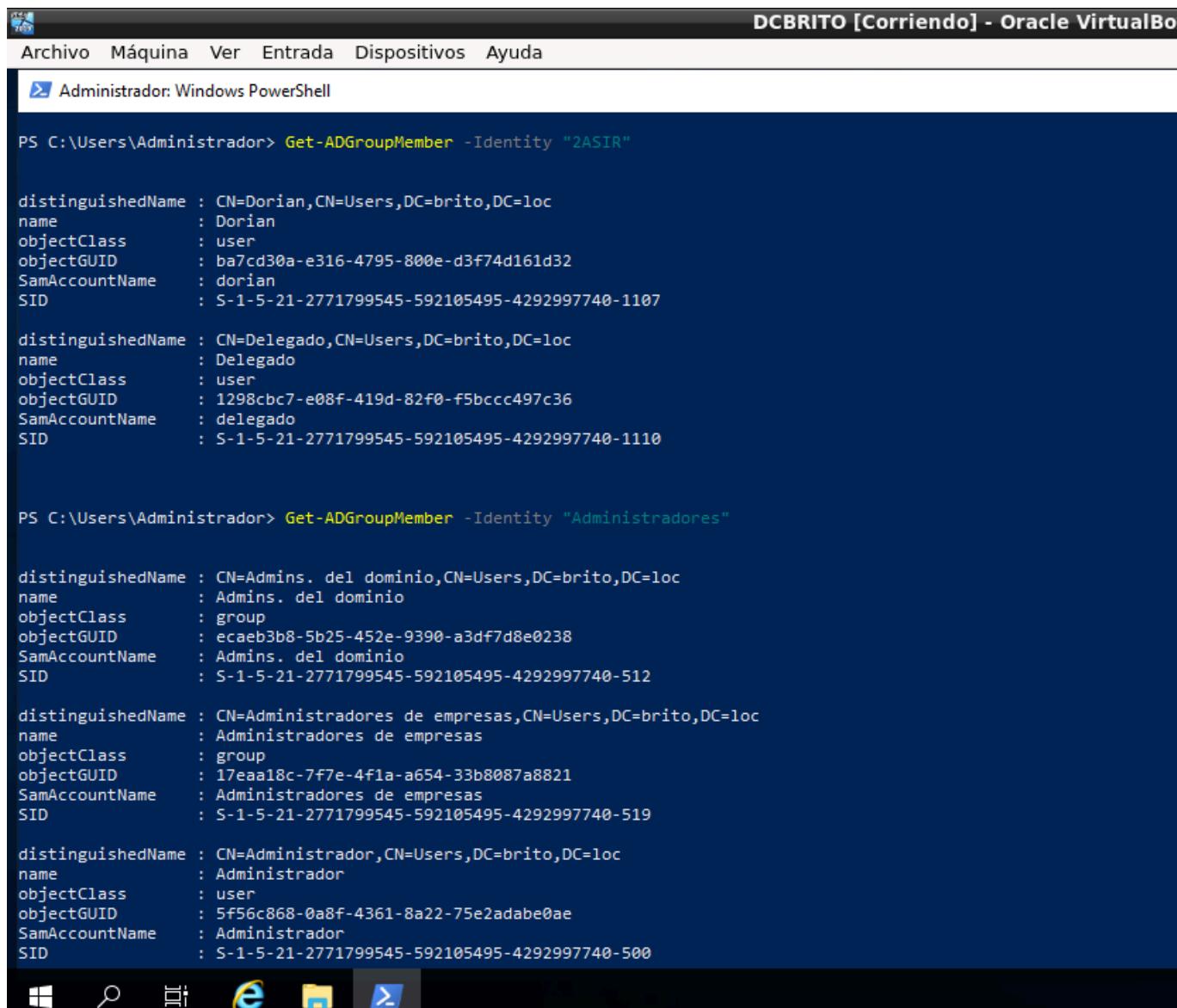
DistinguishedName : CN=Usuarios,CN=BuiltIn,DC=brito,DC=loc
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Usuarios
ObjectClass       : group
ObjectGUID        : 8c7ad5ae-ed5e-4f3c-badc-936766875a16
SamAccountName   : Usuarios
SID               : S-1-5-32-545

DistinguishedName : CN=Invitados,CN=BuiltIn,DC=brito,DC=loc
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Invitados
ObjectClass       : group
ObjectGUID        : 1558a6c8-ca90-4830-91ee-e8b4d783938e
SamAccountName   : Invitados
SID               : S-1-5-32-546

DistinguishedName : CN=Oper. de impresión,CN=BuiltIn,DC=brito,DC=loc
GroupCategory     : Security
GroupScope        : DomainLocal
Name              : Oper. de impresión
ObjectClass       : group
ObjectGUID        : b6d1fd46-c443-46e4-9f0e-f905bd7af5ba
SamAccountName   : Oper. de impresión
SID               : S-1-5-32-550

DistinguishedName : CN=Operadores de copia de seguridad,CN=BuiltIn,DC=brito,DC=loc
GroupCategory     : Security
```

Obtener de un grupo de seguridad sus usuarios.



The screenshot shows a Windows PowerShell window titled "DCBRITO [Corriendo] - Oracle VirtualBox". The window title bar includes the text "DCBRITO [Corriendo] - Oracle VirtualBox". The menu bar contains "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The command prompt shows two Get-ADGroupMember commands. The first command retrieves users from the group "2ASIR", and the second retrieves users from the group "Administradores". Both commands output a list of users with their distinguished names, names, object classes, object GUIDs, Sam account names, and SIDs.

```
PS C:\Users\Administrador> Get-ADGroupMember -Identity "2ASIR"

distinguishedName : CN=Dorian,CN=Users,DC=brito,DC=loc
name : Dorian
objectClass : user
objectGUID : ba7cd30a-e316-4795-800e-d3f74d161d32
SamAccountName : dorian
SID : S-1-5-21-2771799545-592105495-4292997740-1107

distinguishedName : CN=Delegado,CN=Users,DC=brito,DC=loc
name : Delegado
objectClass : user
objectGUID : 1298cbc7-e08f-419d-82f0-f5bcc497c36
SamAccountName : delegado
SID : S-1-5-21-2771799545-592105495-4292997740-1110

PS C:\Users\Administrador> Get-ADGroupMember -Identity "Administradores"

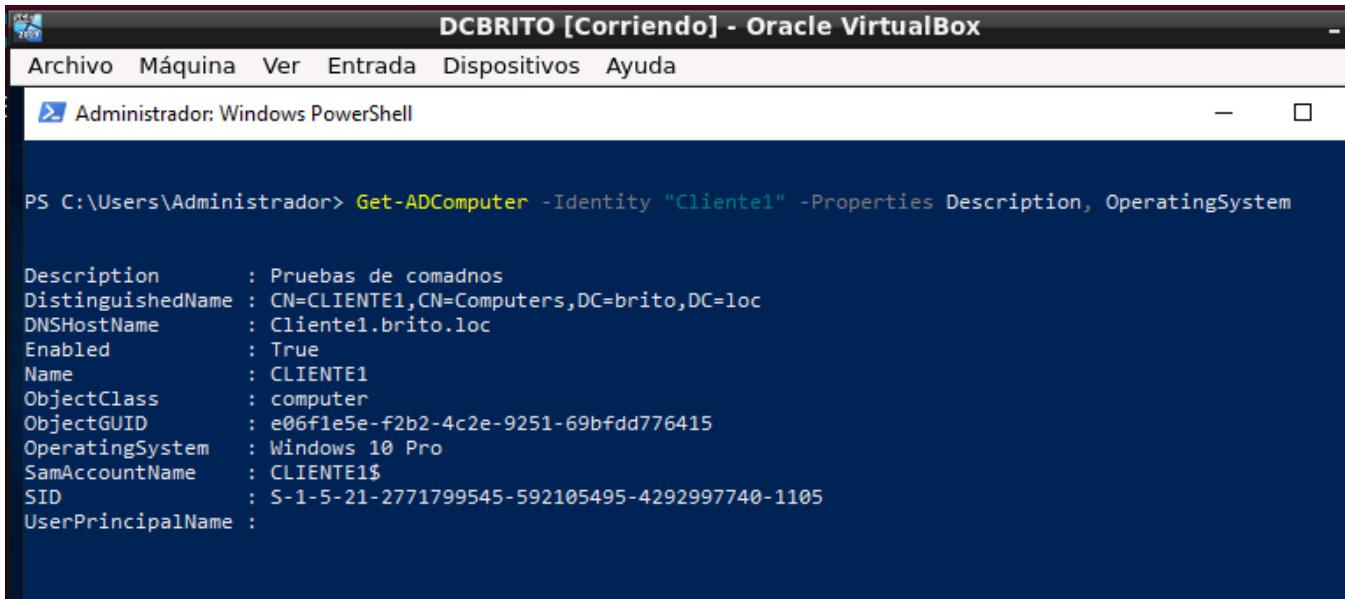
distinguishedName : CN=Admins. del dominio,CN=Users,DC=brito,DC=loc
name : Admins. del dominio
objectClass : group
objectGUID : ecaeb3b8-5b25-452e-9390-a3df7d8e0238
SamAccountName : Admins. del dominio
SID : S-1-5-21-2771799545-592105495-4292997740-512

distinguishedName : CN=Administradores de empresas,CN=Users,DC=brito,DC=loc
name : Administradores de empresas
objectClass : group
objectGUID : 17eaa18c-7f7e-4f1a-a654-33b8087a8821
SamAccountName : Administradores de empresas
SID : S-1-5-21-2771799545-592105495-4292997740-519

distinguishedName : CN=Administrador,CN=Users,DC=brito,DC=loc
name : Administrador
objectClass : user
objectGUID : 5f56c868-0a8f-4361-8a22-75e2adabe0ae
SamAccountName : Administrador
SID : S-1-5-21-2771799545-592105495-4292997740-500
```

## 4. Get-ADComputer

Obtener la información esencial de un equipo cliente.

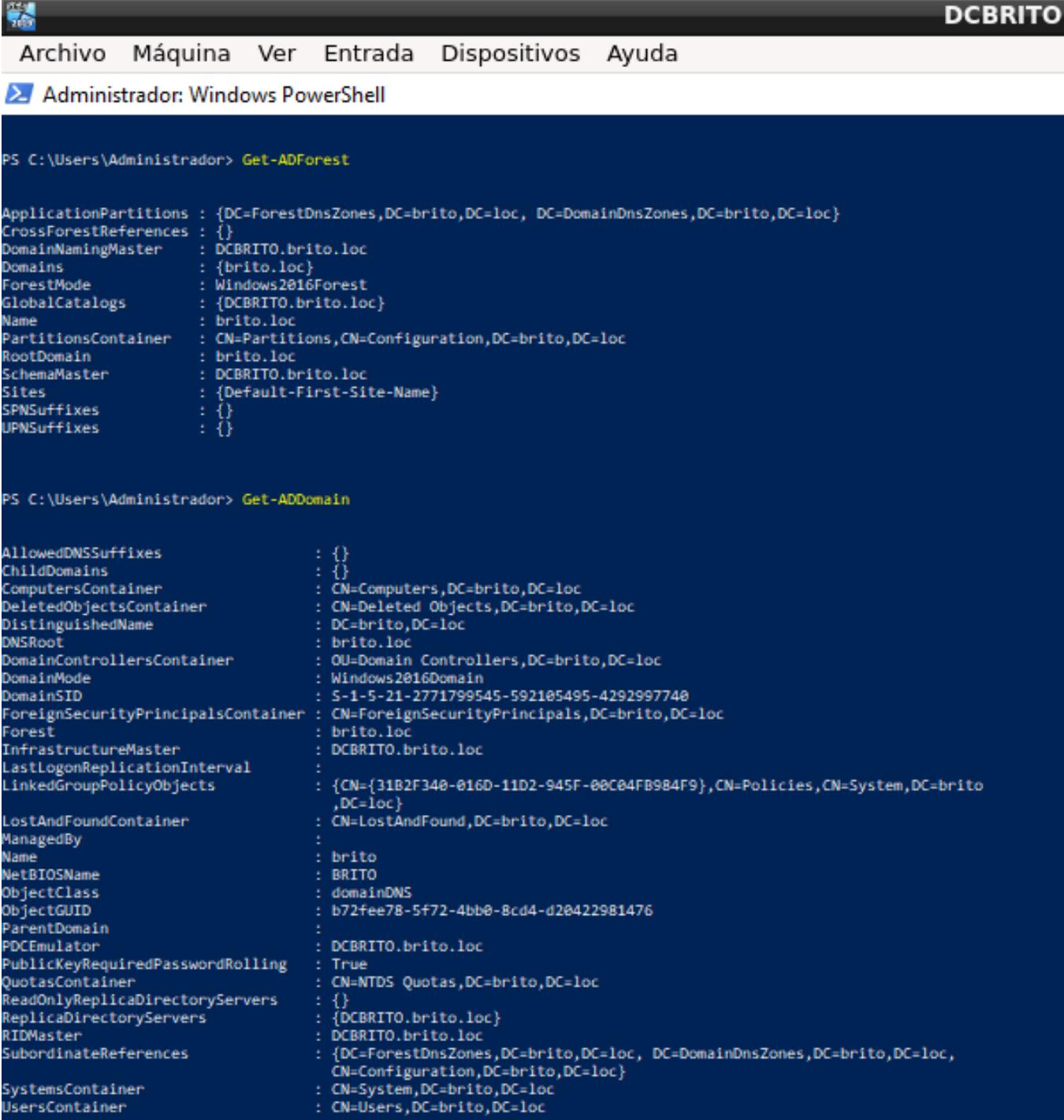


```
PS C:\Users\Administrador> Get-ADComputer -Identity "Cliente1" -Properties Description, OperatingSystem

Description      : Pruebas de comadnos
DistinguishedName : CN=CLIENTE1,CN=Computers,DC=brito,DC=loc
DNSHostName     : Cliente1.brito.loc
Enabled         : True
Name            : CLIENTE1
ObjectClass     : computer
ObjectGUID       : e06f1e5e-f2b2-4c2e-9251-69bfdd776415
OperatingSystem   : Windows 10 Pro
SamAccountName   : CLIENTE1$
SID              : S-1-5-21-2771799545-592105495-4292997740-1105
UserPrincipalName :
```

## 5. Get-ADForest y Get-ADDomain

Para obtener la información sobre el bosque y/o sobre un dominio en concreto.



The screenshot shows a Windows PowerShell window titled "Administrador: Windows PowerShell". The title bar includes the text "DCBRITO". The command PS C:\Users\Administrador> Get-ADForest is run, displaying properties like ApplicationPartitions, CrossForestReferences, DomainNamingMaster, Domains, ForestMode, GlobalCatalogs, Name, PartitionsContainer, RootDomain, SchemaMaster, Sites, SPNSuffixes, and UPNSuffixes. The command PS C:\Users\Administrador> Get-ADDomain is run, displaying properties like AllowedDNSSuffixes, ChildDomains, ComputersContainer, DeletedObjectsContainer, DistinguishedName, DNSRoot, DomainControllersContainer, DomainMode, DomainSID, ForeignSecurityPrincipalsContainer, Forest, InfrastructureMaster, LastLogonReplicationInterval, LinkedGroupPolicyObjects, LostAndFoundContainer, ManagedBy, Name, NetBIOSName, ObjectClass, ObjectGUID, ParentDomain, PDCEmulator, PublicKeyRequiredPasswordRolling, QuotasContainer, ReadOnlyReplicaDirectoryServers, ReplicaDirectoryServers, RIDMaster, SubordinateReferences, SystemsContainer, and UsersContainer.

```
PS C:\Users\Administrador> Get-ADForest

ApplicationPartitions : {DC=ForestDnsZones,DC=brito,DC=loc, DC=DomainDnsZones,DC=brito,DC=loc}
CrossForestReferences : {}
DomainNamingMaster   : DCBRITO.brito.loc
Domains              : {brito.loc}
ForestMode            : Windows2016Forest
GlobalCatalogs       : {DCBRITO.brito.loc}
Name                 : brito.loc
PartitionsContainer : CN=Partitions,CN=Configuration,DC=brito,DC=loc
RootDomain           : brito.loc
SchemaMaster         : DCBRITO.brito.loc
Sites                : {Default-First-Site-Name}
SPNSuffixes          : {}
UPNSuffixes          : {}

PS C:\Users\Administrador> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains             : {}
ComputersContainer       : CN=Computers,DC=brito,DC=loc
DeletedObjectsContainer : CN=Deleted Objects,DC=brito,DC=loc
DistinguishedName       : DC=brito,DC=loc
DNSRoot                 : brito.loc
DomainControllersContainer : OU=Domain Controllers,DC=brito,DC=loc
DomainMode               : Windows2016Domain
DomainSID                : S-1-5-21-2771799545-592105495-4292997740
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=brito,DC=loc
Forest                  : brito.loc
InfrastructureMaster     : DCBRITO.brito.loc
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-0160-11D2-945F-00C04FB9B4F9},CN=Policies,CN=System,DC=brito,DC=loc}
LostAndFoundContainer    : CN=LostAndFound,DC=brito,DC=loc
ManagedBy                : 
Name                     : brito
NetBIOSName              : BRITO
ObjectClass               : domainDNS
ObjectGUID                : b72fee78-5f72-4bb0-8cd4-d28422981476
ParentDomain              : 
PDCEmulator              : DCBRITO.brito.loc
PublicKeyRequiredPasswordRolling : True
QuotasContainer           : CN=NTDS Quotas,DC=brito,DC=loc
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers   : {DCBRITO.brito.loc}
RIDMaster                 : DCBRITO.brito.loc
SubordinateReferences    : {DC=ForestDnsZones,DC=brito,DC=loc, DC=DomainDnsZones,DC=brito,DC=loc, CN=Configuration,DC=brito,DC=loc}
SystemsContainer           : CN=System,DC=brito,DC=loc
UsersContainer             : CN=Users,DC=brito,DC=loc
```

Ejecuta e investiga cada objeto /atributo que se obtiene.

## **ANÁLISIS DE GET-ADFOREST**

Este comando te da información sobre toda la estructura de Active Directory, que en mi caso se llama brito.loc.

**- . Name / RootDomain:** brito.loc

Este es el nombre DNS completo del bosque. Es el primer dominio que se creó y es la raíz de todo.

**- . ForestMode:** Windows2016Forest

Este es el Nivel Funcional del Bosque. Determina las características de AD disponibles en todo el bosque. Un nivel de 2016 significa que todos los Controladores de Dominio (DC) en todos los dominios de tu bosque deben ser, como mínimo, Windows Server 2016.

**- . DomainNamingMaster:** DCBRITO.brito.loc

Este rol es único en todo el bosque. El servidor DCBRITO es el único que tiene la autoridad para agregar o quitar nuevos dominios al bosque.

**- . SchemaMaster:** DCBRITO.brito.loc

Este es el segundo Rol FSMO único en el bosque. El DCBRITO es el único servidor que puede realizar cambios en el "esquema" (la plantilla o "blueprint" de Active Directory). Por ejemplo, si instalas un programa como Microsoft Exchange, este necesita añadir nuevos atributos a los usuarios (como "buzón de correo"), y solo puede hacerlo contactando con el Schema Master.

**- . GlobalCatalogs:** DCBRITO.brito.loc

Esto indica qué servidores son Catálogos Globales (GC). Un GC almacena una copia completa de su propio dominio y una copia parcial de todos los demás dominios del bosque. Es esencial para búsquedas rápidas y para los inicios de sesión de usuarios en dominios diferentes.

## **ANÁLISIS DE GET-ADDOMAIN**

Este comando te da información específica sobre tu dominio (que también es brito.loc, ya que solo tienes uno).

### **- . NetBIOSName: BRITO**

Este es el nombre "corto" o "pre-Windows 2000" de tu dominio. Es el que se usa para iniciar sesión con el formato DOMINIO\usuario (ej. BRITO\Administrator).

### **- . DomainMode: Windows2016Domain**

Este es el Nivel Funcional del Dominio. A diferencia del nivel de bosque, este controla las características dentro de este dominio específico. Debe ser igual o superior al nivel del bosque.

### **- . DomainSID: S-1-5-21-27...**

Este es el Security Identifier (SID) único para tu dominio. Cada objeto (usuario, grupo, equipo) en tu dominio tendrá un SID que comienza con este número, seguido de su propio ID único (RID).

### **- . PDCEmulator: DCBRITO.brito.loc**

Este es el tercer Rol FSMO (único por dominio). Es uno de los más importantes. Se encarga de:

- Sincronizar la hora de todos los equipos del dominio.
- Gestionar los cambios de contraseña (se replican a él primero).
- Ser el servidor al que se conecta la herramienta de Administración de GPOs.

### **- . RIDMaster: DCBRITO.brito.loc**

Este es el cuarto Rol FSMO (único por dominio). El "Maestro RID" es el responsable de dar "paquetes" de RIDs (Relative IDs) a cada DC. Cuando creas un usuario, el DC local le asigna un RID de su paquete para formar el SID completo. Si un DC se queda sin RIDs, le pide más a este maestro.

### **- . InfrastructureMaster: DCBRITO.brito.loc**

Este es el quinto y último Rol FSMO (único por dominio). Se encarga de actualizar las referencias de objetos entre dominios (por ejemplo, si un usuario del Dominio A está en un grupo del Dominio B).

**- . ComputersContainer / UsersContainer: CN=Computers... / CN=Users...**

Estos son los contenedores por defecto donde se crean los nuevos equipos y usuarios. Es importante notar que son "Contenedores" (CN) y no "Unidades Organizativas" (OU), lo que significa que no puedes aplicarles GPOs directamente. Por eso es una buena práctica redirigirlos a OUs personalizadas.