

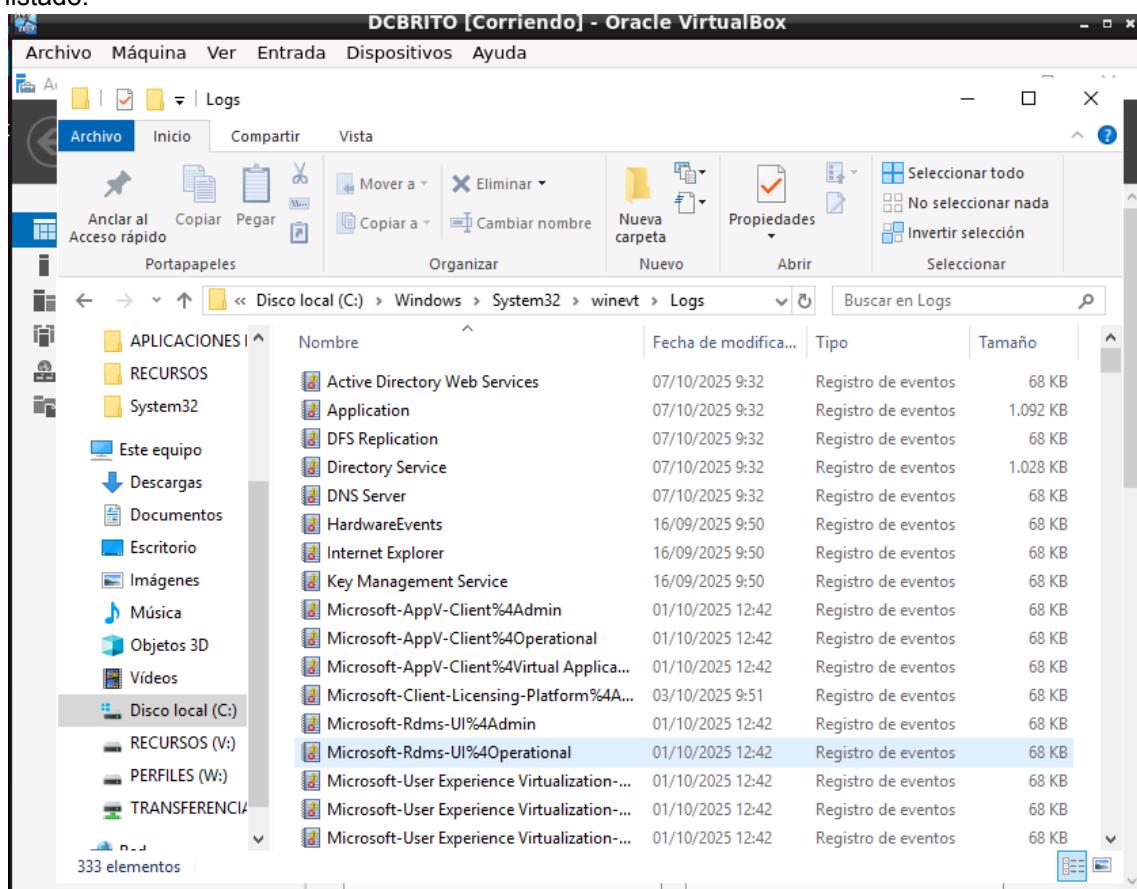
	DEPARTAMENTO INFORMÁTICA	
	2º ASIR - ASO	
	TALLER VISOR DE EVENTOS	

0. OBJETIVOS

- Manejar con destreza el visor de eventos de un controlador de Dominio.

1. PREVIO.

Navegar hasta la carpeta que contiene todos los registros de eventos. Pegar una imagen con el listado.



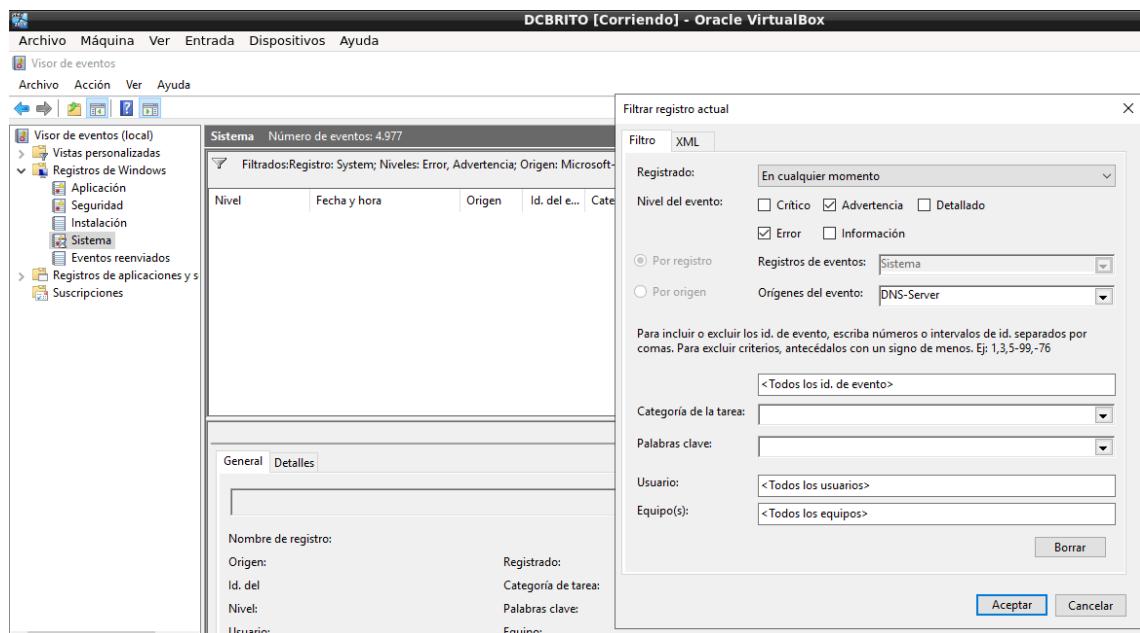
Desde el Administrador del Servidor configura alguno de los Roles para que se active la alerta (quede en rojo) ante cualquier evento. Luego deshaz la configuración y vuelve a dejarla solamente para Críticos.

2. Visor de Eventos. Nivel Básico

1. Explorar registros del sistema:

- o En el servidor DC, ve al **Visor de eventos**.
- o Navega a **Registros de Windows** y luego a **Sistema**.
- o Identifica y filtra por eventos de "Advertencia" o "Error" que tengan como origen "DNS Server" o "NTDS General" o cualquier servicio.

- No salieron



- o Borrar el filtro para volver a la situación inicial.

Tarea: Configurar un filtro de Advertencia para todos los orígenes. Registra al menos 3 eventos, incluyendo su ID y una breve descripción.

The screenshot shows the Windows Event Viewer interface titled "DCBRITO [Corriendo] - Oracle VirtualBox". The main pane displays a table of events under the "Sistema" category, with a filter applied: "Filtrados: Registro: System; Nivel: Advertencia; Orígenes: .NET Runtime, .NET Runtime". The table has columns: Nivel (Level), Fecha y hora (Date and Time), Origen (Source), Id. del e... (Event ID), and Categor... (Category). There are 12 entries, all marked as "Advertencia" (Warning) with source "Time-S." (Time-Service) and ID 12. The right pane, titled "Acciones" (Actions), lists various options like "Abrir registro..." (Open registry...) and "Importar vista..." (Import view...).

Nivel	Fecha y hora	Origen	Id. del e...	Categor...
Advertencia	07/10/2025 9:31:41	Time-S...	12	Ninguno
Advertencia	07/10/2025 9:31:41	Windo...	10154	Ninguno
Advertencia	07/10/2025 9:31:13	DNS Cli...	1014	(1014)
Advertencia	07/10/2025 9:31:09	Disk	34	Ninguno
Advertencia	07/10/2025 9:31:09	Disk	34	Ninguno
Advertencia	07/10/2025 9:31:09	Disk	34	Ninguno
Advertencia	06/10/2025 11:07:40	Time-S...	12	Ninguno
Advertencia	06/10/2025 11:07:40	Windo...	10154	Ninguno
Advertencia	06/10/2025 11:07:07	DNS Cli...	1014	(1014)
Advertencia	06/10/2025 11:07:04	Disk	34	Ninguno

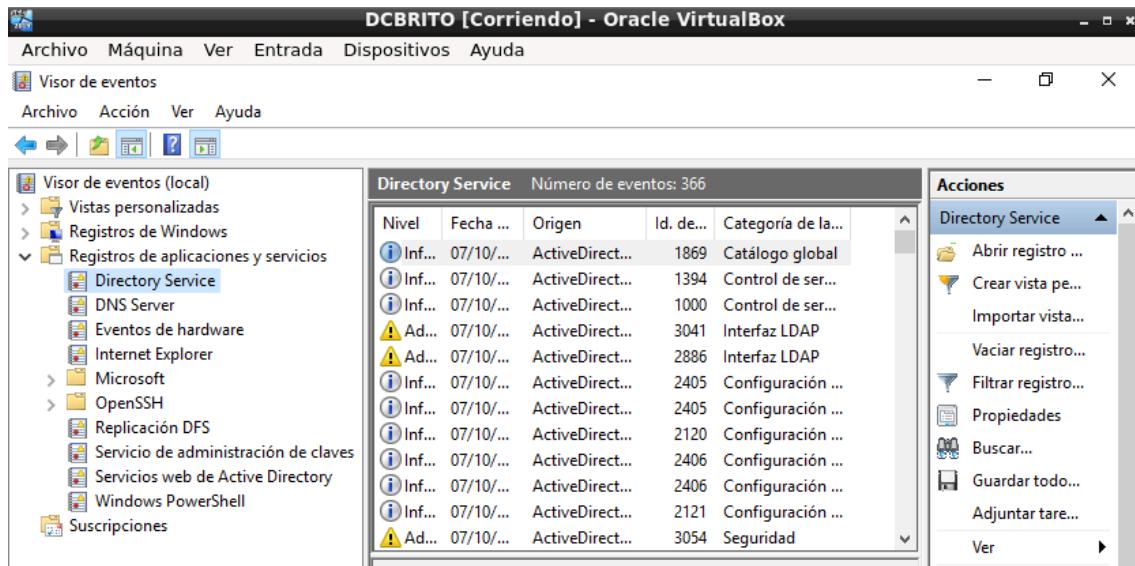
- Advertencia de Origen Time-Service (ID 12): Este evento de advertencia indica que el servicio de hora de Windows no pudo sincronizar la hora del sistema con el origen de tiempo configurado. Esto puede deberse a problemas de conectividad de red o a que el origen de tiempo no está disponible.

- Advertencia de Origen DNS Client (ID 1014): Esta advertencia muestra que el cliente DNS no pudo resolver un nombre. Es un indicativo de que la configuración de DNS podría tener un problema o que el servidor DNS al que se está intentando conectar no está respondiendo.

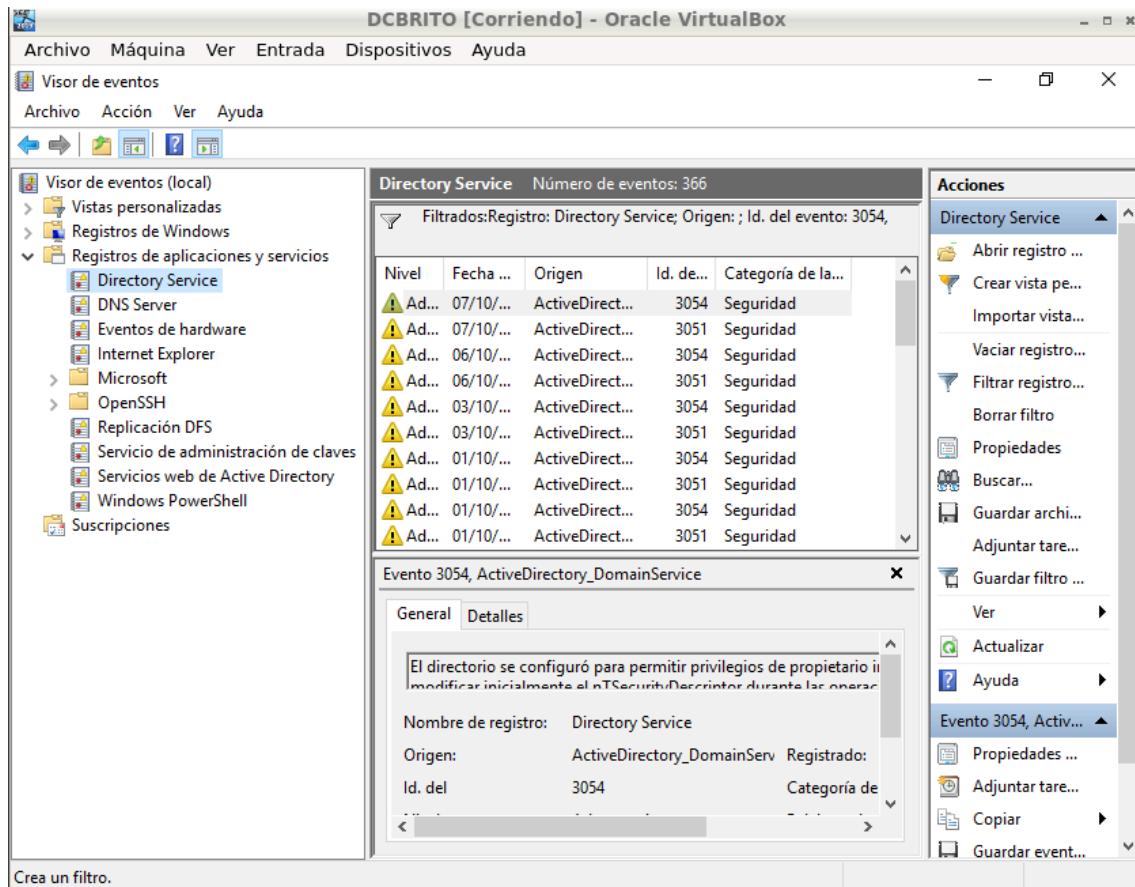
- Advertencia de Origen Disk (ID 34): Este evento generalmente se relaciona con problemas en un disco físico o en una partición. Podría ser una señal de que el disco está a punto de fallar o de que se han encontrado errores de escritura o lectura.

2. Verificar la replicación de AD:

- o En el servidor DC, revisa el registro de **Servicio de directorio**.



- o Filtra por eventos que tengan como origen **NTDS General** y el ID **3054** y **3051**..



Tarea: Sobre el Servicio de Directorio, anota dos advertencias con su origen y definición.

- Advertencia de origen ActiveDirectory_WebServices (Id. de evento 3054): Esta advertencia indica que el Servicio Web de Active Directory (ADWS) no pudo contactar con un servidor del catálogo global. Esto puede causar problemas con aplicaciones o servicios que dependen de la conectividad de ADWS para funcionar correctamente.
- Advertencia de origen ActiveDirectory_WebServices (Id. de evento 3051): Esta advertencia indica que el Servicio Web de Active Directory (ADWS) no pudo conectarse al servicio de directorio en un servidor en particular. Esto a menudo se debe a problemas de red, como la falta de conectividad o una configuración incorrecta, lo que podría afectar la capacidad de los clientes para comunicarse con Active Directory.

3. Auditoría de inicio de sesión:

- o En el servidor DC, navega a **Registros de Windows** y luego a **Seguridad**.

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	07/10/2025 9:55:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:55:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:55:44	Microsoft Windows sec...	4672	Special Logon
Auditoría correcta	07/10/2025 9:54:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:54:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:54:44	Microsoft Windows sec...	4672	Special Logon
Auditoría correcta	07/10/2025 9:53:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:53:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:53:44	Microsoft Windows sec...	4672	Special Logon
Auditoría correcta	07/10/2025 9:52:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:52:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:52:44	Microsoft Windows sec...	4672	Special Logon
Auditoría correcta	07/10/2025 9:52:05	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4624	Logon

- o Filtra los eventos con el ID **4624** (inicio de sesión exitoso) **4634 4625** (inicio de sesión fallido).

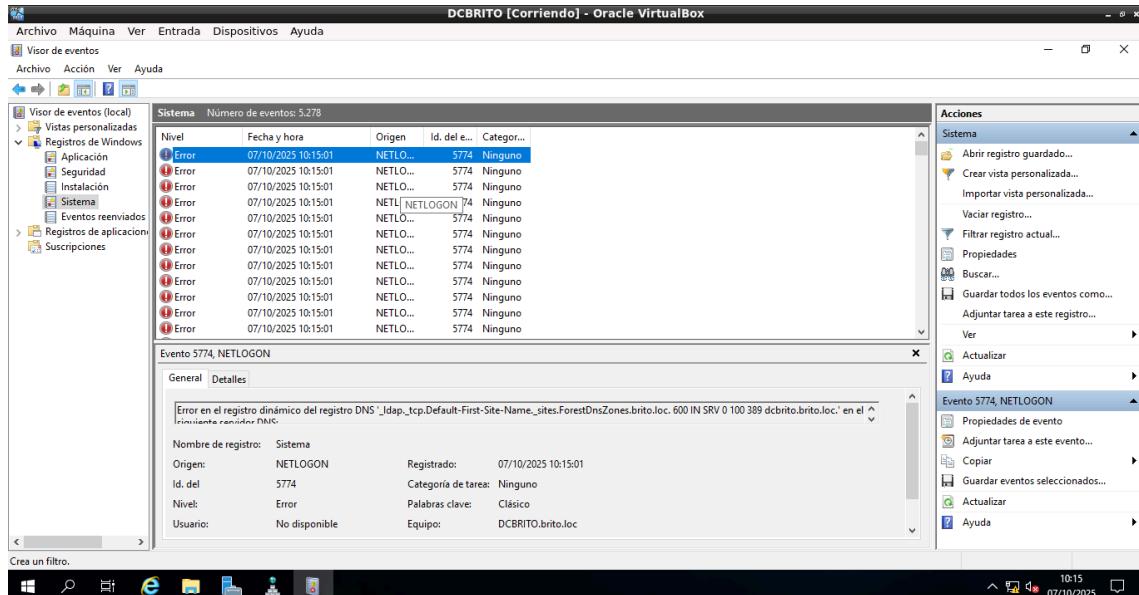
Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	07/10/2025 9:54:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:54:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:53:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:53:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:52:44	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:52:44	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:52:05	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4634	Logoff
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4624	Logon
Auditoría correcta	07/10/2025 9:51:54	Microsoft Windows sec...	4624	Logon

3. Nivel Intermedio: Diagnóstico

1. Resolver un problema de servicio:

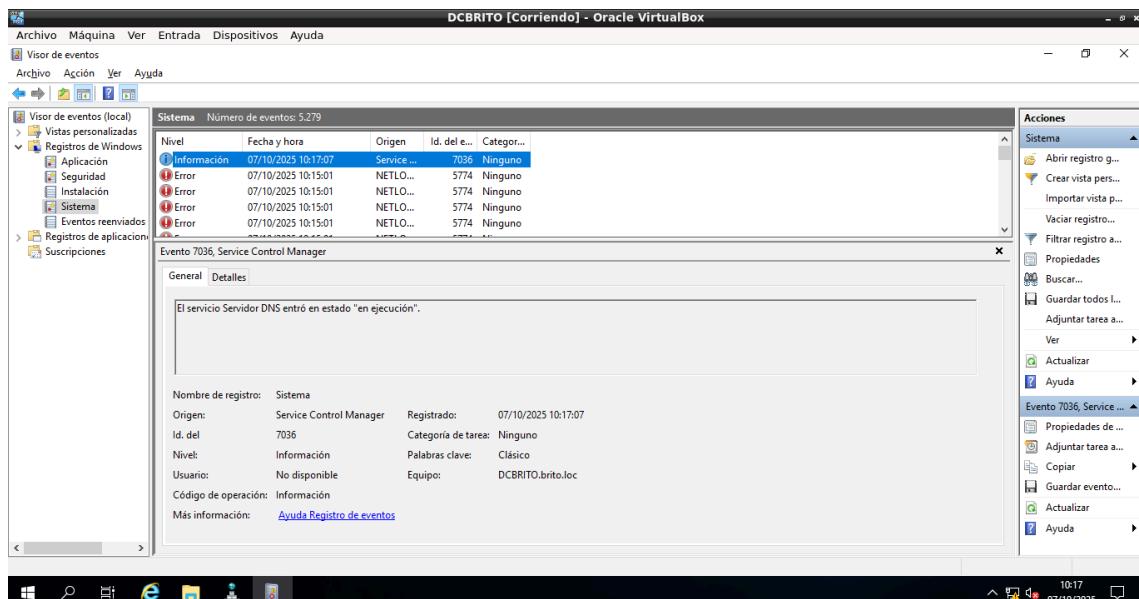
- o En el servidor DC, crea un problema intencionado. Por ejemplo, detén el servicio de servidor DNS (desde **services.msc**).
- o Vuelve al Visor de eventos, en el registro **Sistema**, y busca el evento de error generado por la detención del servicio. El origen será **Service Control Manager**.

id 5774



Tarea: Identifica el evento y anota su ID. Luego, reinicia el servicio y verifica en el Visor de eventos que se haya registrado un evento de "Información" indicando que el servicio se ha iniciado correctamente.

id 7036



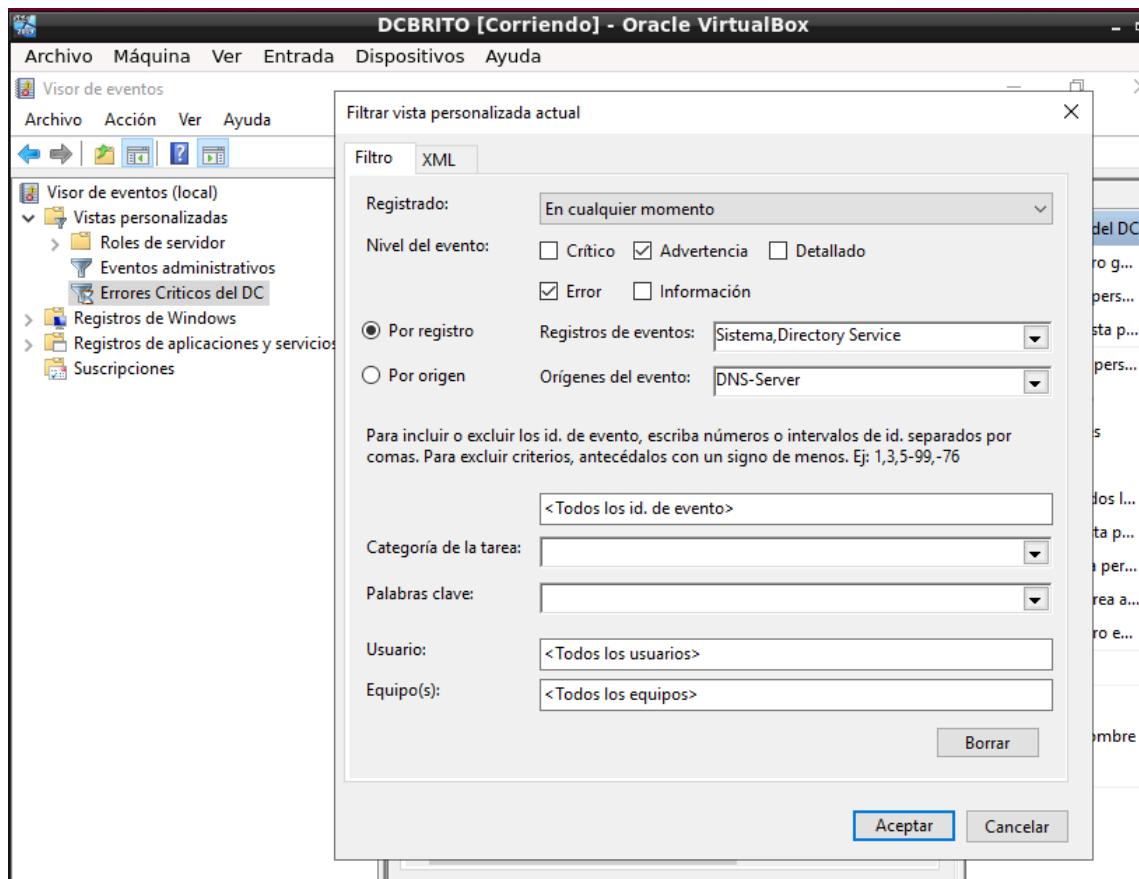
4. Nivel Avanzado: Gestión y Mantenimiento

1. Crear una vista personalizada:

- o En el servidor DC, en el panel del Visor de eventos, haz clic en **Crear vista personalizada**.
- o Configura la vista para que muestre solo eventos de "Advertencia" y "Error" de los registros **Sistema** y **Servicio de directorio** con los orígenes más relevantes para tu escenario (como **DNS Server**, **NTDS General** y **Kerberos**).

Tarea: Guarda la vista con el nombre "**Errores Críticos del DC**". Úsala para realizar un seguimiento rápido y diario de los problemas más importantes.

- No aparece NTDS General ni Kerberos



- He agregado el SERVICE CONTROL MANAGER

