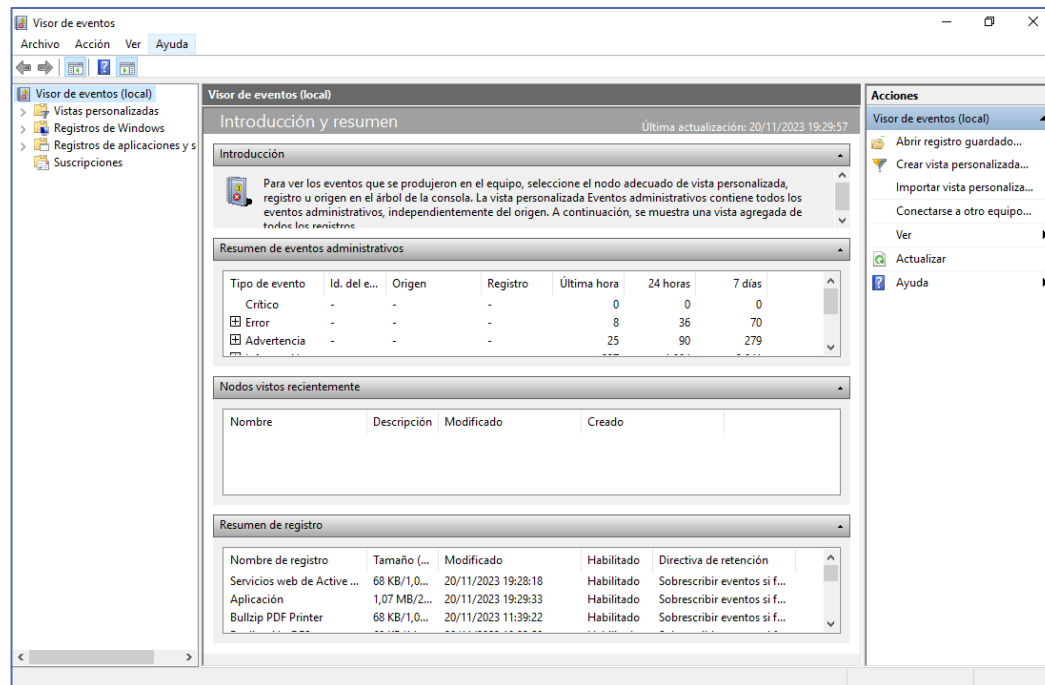


# UD06

## Visor de Eventos



# Índice

---

- Introducción.
- Abrir el Visor de Eventos.
- La ventana del Visor de Eventos.
- Consultar eventos.
- Vista personalizadas.
  - Configuración.
  - Guardar vista personalizada.
- Identificador de tipo de evento.



## Introducción



# Introducción



- El **administrador** del sistema necesita **saber** lo que ocurre en su sistema.
- Los **sistemas operativos**, y muchas de las **aplicaciones**, suelen **guardar detalles** de su funcionamiento en unos archivos especiales, llamados **registros de eventos** (también logs o bitácoras).
- Estos archivos guardan información **sobre el funcionamiento**, sobre las **anomalías** que surjan durante éste, o sobre **cualquier otro problema** o situación que deba ser reseñada a lo largo del tiempo.
- El Visor de eventos de Windows Server es un **complemento de Microsoft Management Console (MMC)** que permite **consultar y administrar** de forma centralizada la información contenida en los **múltiples registros de eventos** de las aplicaciones y servicios de Windows, por lo que resulta imprescindible **para supervisar** el funcionamiento del servidor **y resolver** cualquier incidencia.

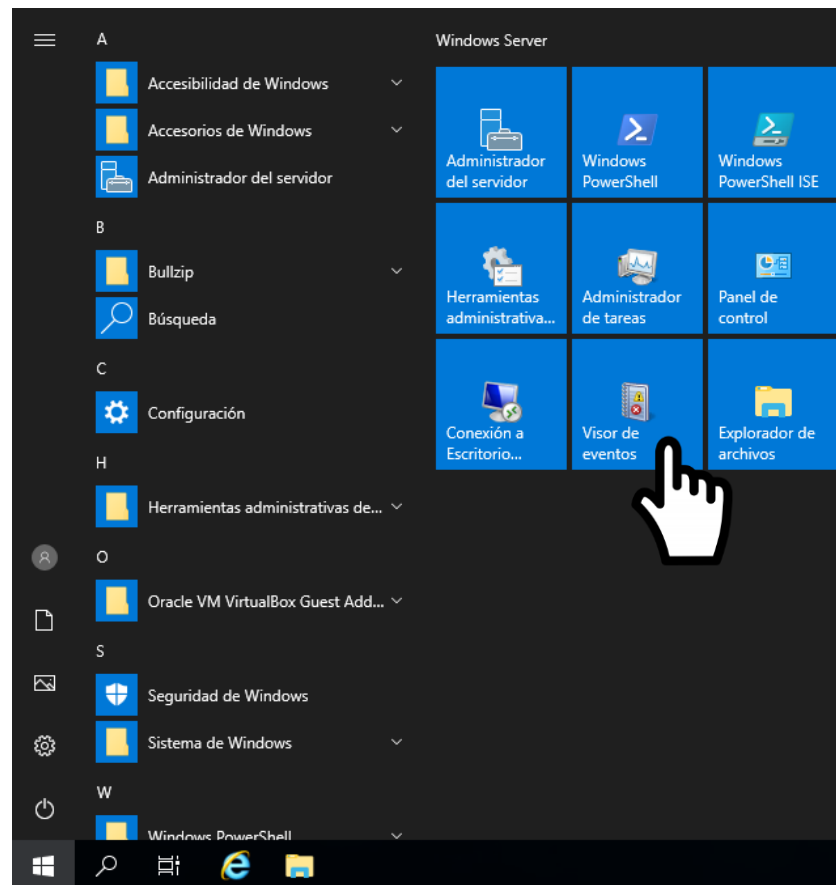
# Introducción



- Desde el Visor de eventos podremos realizar las siguientes **tareas**:
  - **Consultar** los eventos que se hayan producido.
  - **Crear filtros** para los eventos que más nos interesen y **almacenarlos** como **vistas personalizadas** que podemos volver a utilizar en cualquier momento.
  - **Programar una tarea** para que se ejecute en respuesta a una situación específica.
  - Establecer **suscripciones a determinados eventos**.



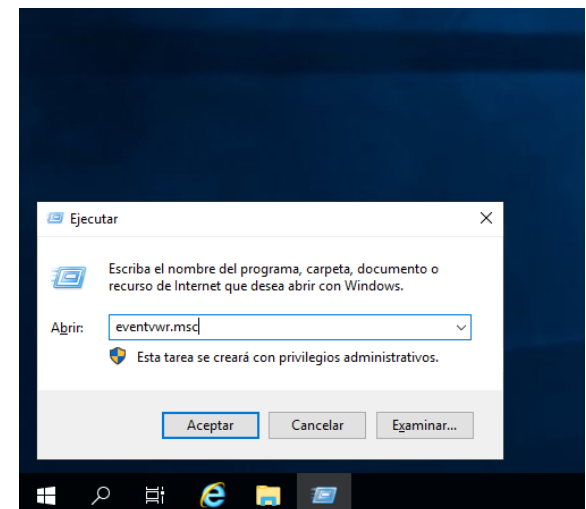
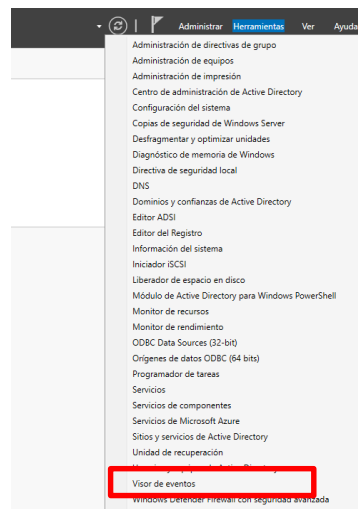
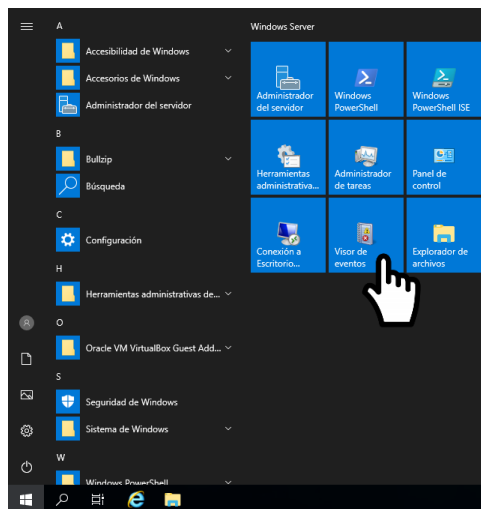
## Abrir el Visor de Eventos



# Abrir el Visor de Eventos



- Existen distintos modos de **abrir el visor de eventos**:
  - Inicio → **Herramientas administrativas** → Visor de eventos.
  - Directamente en el conjunto de **herramientas de Windows Server** que aparece al pulsar sobre Inicio.
  - Desde el **Administrador del Servidor** → Herramientas → Visor de Eventos.
  - Ejecutando (WIN + R) **eventvwr.msc**



# Abrir el Visor de Eventos



Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
- Registros de aplicaciones y servicios
- Suscripciones

Visor de eventos (local)

Introducción y resumen

Última actualización: 06/12/2023 9:34:04

Introducción

Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
Crítico	-	-	-	0	0	0
Error	-	-	-	7	18	45
Advertencia	-	-	-	51	132	205
Información	-	-	-	257	701	1.375
Auditoría cor...	-	-	-	298	1.146	1.860
Error de audit...	-	-	-	0	1	1

Nodos vistos recientemente

Nombre	Descripción	Modificado	Creado
--------	-------------	------------	--------

Resumen de registro

Nombre de registro	Tamaño (...)	Modificado	Habilitado	Directiva de retención
Servicios web de Active ...	68 KB/1,0...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...
Aplicación	1,07 MB/2...	06/12/2023 9:33:12	Habilitado	Sobrescribir eventos si f...
Bullzip PDF Printer	68 KB/1,0...	20/11/2023 11:39:22	Habilitado	Sobrescribir eventos si f...
Replicación DFS	68 KB/14,...	06/12/2023 9:27:23	Habilitado	Sobrescribir eventos si f...
Directory Service	1,00 MB/1...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...
DNS Server	68 KB/100...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...

Acciones

Visor de eventos (local)

- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Conectarse a otro equipo...
- Ver
- Actualizar
- Ayuda





## La ventana del Visor de Eventos

**Visor de eventos**

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
- Registros de aplicaciones y suscripciones

**Introducción y resumen** Última actualización: 06/12/2023 9:34:04

**Introducción**

Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.

**Resumen de eventos administrativos**

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
Crítico	-	-	-	0	0	0
Error	-	-	-	7	18	45
Advertencia	-	-	-	51	132	205
Información	-	-	-	257	701	1.375
Auditoría cor...	-	-	-	298	1.146	1.860
Error de audit...	-	-	-	0	1	1

**Nodos vistos recientemente**

Nombre	Descripción	Modificado	Creado
--------	-------------	------------	--------

**Resumen de registro**

Nombre de registro	Tamaño (...)	Modificado	Habilitado	Directiva de retención
Servicios web de Active ...	68 KB/1,0...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...
Aplicación	1,07 MB/2...	06/12/2023 9:33:12	Habilitado	Sobrescribir eventos si f...
Bullzip PDF Printer	68 KB/1,0...	20/11/2023 11:39:22	Habilitado	Sobrescribir eventos si f...
Replicación DFS	68 KB/14...	06/12/2023 9:27:23	Habilitado	Sobrescribir eventos si f...
Directory Service	1,00 MB/1...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...
DNS Server	68 KB/100...	06/12/2023 9:31:24	Habilitado	Sobrescribir eventos si f...

**Acciones**

Visor de eventos (local)

- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Conectarse a otro equipo...

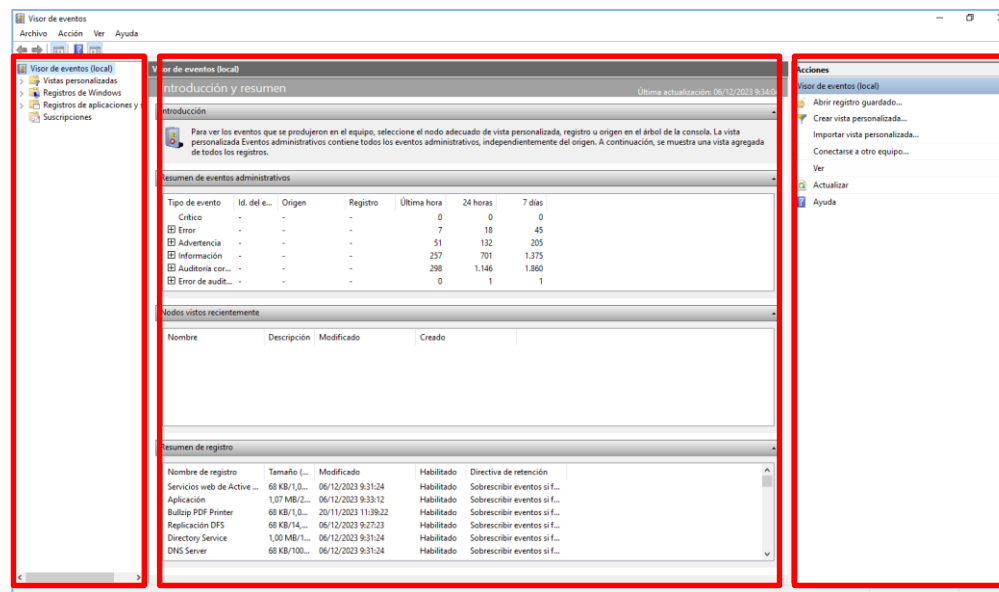
Ver

- Actualizar
- Ayuda

# La ventana del Visor de Eventos



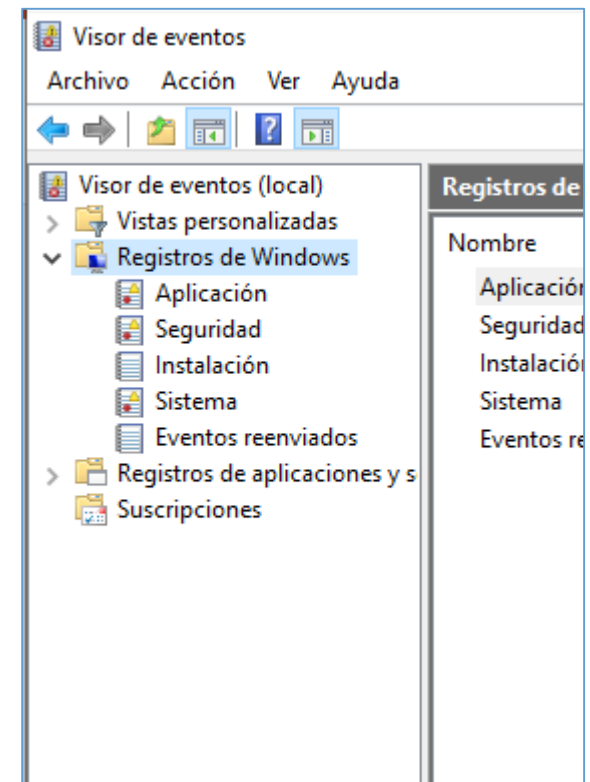
- La **ventana** del Visor de eventos aparecerá dividida en **tres paneles**:
  - El panel de la **izquierda** aparece organizado a modo de árbol. En él nos encontramos diferentes **categorías** que podemos ir desplegando.
  - En el panel **central** encontramos la **información** relacionada con los eventos.
  - En el panel de la **derecha** aparece un menú con distintas **acciones**.



# La ventana del Visor de Eventos



- Vamos a centrarnos en la **categoría Registros de Windows**, que contiene distintas **subcategorías**. Al seleccionar las diferentes subcategorías, la información mostrada en el **panel central variará**:
  - **Aplicación**: eventos de las aplicaciones y los servicios que no forman parte del sistema.
  - **Seguridad**: información de los eventos relacionados con la seguridad del sistema.
  - **Instalación**: información de los eventos relativos a la configuración de roles y características.
  - **Sistema**: información relativa a los eventos del sistema y de sus componentes.
  - **Eventos reenviados**: información reenviada por otros sistemas de la red.





## Consultar eventos



# Consultar eventos



- Para **consultar eventos**, seleccionamos la **categoría** en el panel de la izquierda y el **evento en concreto** en el panel central.
- En la **parte inferior del panel central** se muestra **información** detallada en relación al evento seleccionado:

Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema**
  - Eventos reiniciados
- Registros de aplicaciones y servicios
- Suscripciones

Sistema Número de eventos: 4.005

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	17/11/2023 22:11:59	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:59	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:59	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:59	Windows Remote Manag...	10148	Ninguno
Información	17/11/2023 22:11:59	DfsSvc	14531	Ninguno
Información	17/11/2023 22:11:59	DfsSvc	14533	Ninguno
Información	17/11/2023 22:11:52	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:44	Service Control Manager	7036	Ninguno
Advertencia	17/11/2023 22:11:44	DNS Client Events	1014	(1014)
Información	17/11/2023 22:11:44	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:44	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:44	Service Control Manager	7036	Ninguno
Advertencia	17/11/2023 22:11:44	DNS Client Events	1014	(1014)
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno
Información	17/11/2023 22:11:42	Service Control Manager	7036	Ninguno

Evento 7036, Service Control Manager

General Detalles

El servicio LanmanServer entró en estado "en ejecución".

Nombre de registro: Sistema

Origen: Service Control Manager Registrado: 17/11/2023 22:11:52

Id. del: 7036 Categoría de tarea: Ninguno

Nivel: Información Palabras clave: Clásico

Usuario: No disponible Equipo: SERVER-1.dominio1.local

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

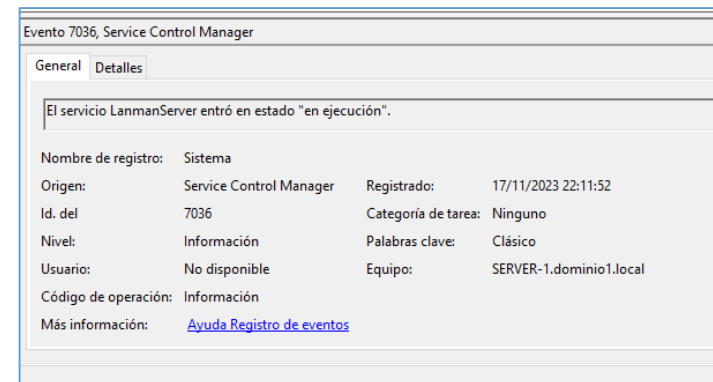
Acciones

- Sistema
  - Abrir registro guardado...
  - Crear vista personalizada...
  - Importar vista personalizada...
  - Vaciar registro...
  - Filtrar registro actual...
  - Propiedades
  - Buscar...
  - Guardar todos los eventos como...
  - Adjuntar tarea a este registro...
  - Ver
  - Actualizar
  - Ayuda
- Evento 7036, Service Control Manager
  - Propiedades de evento
  - Adjuntar tarea a este evento...
  - Copiar
  - Guardar eventos seleccionados...
  - Actualizar
  - Ayuda

# Consultar eventos



- La **información** sobre cada evento incluye:
  - Su **origen**.
  - Identificador de tipo de evento.
  - **Fecha y hora** en la que se produjo el evento.
  - **Equipo** en el que se ha producido el evento.
  - ...



- El **identificador del tipo** de evento nos permite **localizar** rápidamente todos los **eventos del mismo tipo** que se hayan producido.
- Además, podremos encontrar un **enlace**, que nos llevará a una página web de **Microsoft** con más **información sobre el tipo de evento**. Para obtener esta información es necesario **iniciar sesión** con una cuenta de Microsoft.



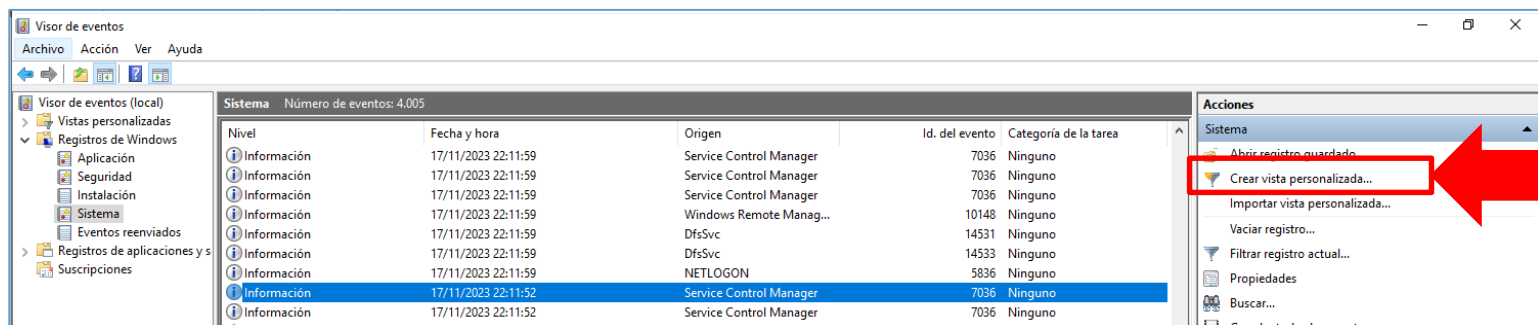
## Vista personalizadas



# Vistas personalizadas



- Cuando recurrimos al Visor de eventos, es muy frecuente que estemos **buscando un determinado tipo de evento** que, a su vez, está relacionado con un **problema en concreto**.
- Una de las principales ventajas del Visor de eventos es que nos permite **filtrar eventos específicos**, de manera **independiente a la categoría** concreta a la que pertenezcan.
- De esta forma, podremos **ver todos los eventos relacionados** con la situación que estamos investigando.
- Para ello creamos lo que denominamos **vistas personalizadas**.







# Vistas personalizadas

- Al hacer clic sobre la acción **Crear vista personalizada...**, que aparece en el panel de la derecha, aparecerá una **ventana donde debemos definir el tipo de evento** que estamos buscando.

The screenshot shows a dialog box titled "Crear vista personalizada" with a close button (X) in the top right corner. The dialog has two tabs: "Filtro" (selected) and "XML".

Under the "Filtro" tab, the following options are visible:

- Registrado:** A dropdown menu showing "En cualquier momento".
- Nivel del evento:** Four checkboxes: ☐ Critico, ☐ Advertencia, ☐ Detallado, ☐ Error, and ☐ Información.
- Por registro:** A radio button that is selected.
- Registros de eventos:** A dropdown menu showing "Sistema".
- Por origen:** A radio button that is not selected.
- Orígenes del evento:** A dropdown menu.

Below these options, there is a text instruction: "Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76".

Below the instruction, there are several input fields:

- A text field containing "<Todos los id. de evento>".
- Categoría de la tarea:** A dropdown menu.
- Palabras clave:** A dropdown menu.
- Usuario:** A text field containing "<Todos los usuarios>".
- Equipo(s):** A text field containing "<Todos los equipos>".

At the bottom right of the dialog, there is a "Borrar" button. At the very bottom, outside the dialog box, are "Aceptar" and "Cancelar" buttons.



# Vistas personalizadas

## Configuración

---

- La **configuración de la vista personalizada** la llevamos a cabo a través de la **ventana Crear vista personalizada**, donde contamos con múltiples **opciones**:
  - Registrado.
  - Nivel de evento.
  - Por registro/origen.
  - Eventos restringidos.
  - Categoría de la tarea.
  - Palabras clave.
  - Usuarios y equipos.



# Vistas personalizadas

## Configuración

- **Registrado:** desplegable que permite indicar el **periodo de tiempo en el que queremos centrar la búsqueda** (En cualquier momento, última hora, últimas 12 horas..., incluso un intervalo personalizado si seleccionamos la última opción).

Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: En cualquier momento

☒ Por registro

☐ Por origen

Intervalo personalizado...

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

<Todos los id. de evento>

Categoría de la tarea:

Palabras clave:

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar

Crear vista personalizada

Filtro XML

Registrado: Intervalo personalizado...

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado

☐ Error ☐ Información

☒ Por registro

Registros de eventos: 15

Intervalo personalizado

Especifique un intervalo de fechas personalizado para el filtro.

Para con De: Primer evento 06/12/2023 10:21:07

A: Último evento 06/12/2023 10:21:07

Aceptar Cancelar

Cat

Pal

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar



# Vistas personalizadas

## Configuración

---

- **Nivel del evento:** nos permite filtrar eventos en función del **nivel de gravedad**. Las posibles **opciones**, ordenadas de mayor e menor gravedad, son:
  - **Crítico:** por lo general **afectan a todo el sistema o alguna aplicación** y requieren la **intervención inmediata** del administrador del sistema.
  - **Error:** indican algún **problema pero no requieren al intervención inmediata** del administrador del sistema.
  - **Advertencia:** indican que un **componentes o aplicación no se encuentra en su estado ideal** y que podría dar lugar a un error crítico.
  - **Información:** eventos que proporcionan **información no crítica** al administrador.
  - **Detallado:** mensajes de **progreso o de operación correcta**.



# Vistas personalizadas

## Configuración

Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro Registros de eventos: Sistema

☐ Por origen Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

< Todos los id. de evento >

Categoría de la tarea:

Palabras clave:

Usuario: < Todos los usuarios >

Equipo(s): < Todos los equipos >

Borrar

Aceptar Cancelar

**Nota: si no se selecciona ningún nivel, al contrario de lo que se podrían pensar, se incluirán todos los niveles.**

[https://learn.microsoft.com/es-es/previous-versions/office/developer/sharepoint-2010/ff604025\(v=office.14\)](https://learn.microsoft.com/es-es/previous-versions/office/developer/sharepoint-2010/ff604025(v=office.14))



# Vistas personalizadas

## Configuración

---

- **Por registro/origen:** indicaremos si buscamos eventos **en función del registro** en el que se encuentran **o según su origen**:
  - **Por registro:** podremos seleccionar las **subcategoría** a la que pertenece el evento, dentro de las categorías de **Registros de Windows y Registros de aplicaciones y servicios**.
  - **Por origen:** podemos especificar qué **parte del sistema que ha ocasionado el evento** (por ejemplo, el spooler de impresión). Al elegir el origen, se asigna de **forma automática el valor adecuado en la subcategoría Por registro**, sustituyendo a la que pudiéramos haber elegido en el punto anterior.

# Vistas personalizadas

## Configuración



Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro ☐ Por origen

Registros de eventos: Sistema

Orígenes del evento:

- ☒ Registros de Windows
  - ☐ Aplicación
  - ☐ Seguridad
  - ☐ Instalación
  - ☒ Sistema
  - ☐ Eventos reenviados
- ☐ Registros de aplicaciones y servicios
  - ☐ Bullzip PDF Printer
  - ☐ Directory Service
  - ☐ DNS Server
  - ☐ Eventos de hardware
  - ☐ Internet Explorer
  - ☐ Microsoft
  - ☐ OpenSSH
  - ☐ Replicación DFS
  - ☐ Servicio de administración de cla
  - ☐ Servicios web de Active Directory
  - ☐ Windows PowerShell

Para incluir o excluir los id. de evento, escriba en las casillas de texto y presione Enter. Para excluir criterios, antecédalos con una tilde (~).

Categoría de la tarea: <Todos los id. de evento>

Palabras clave: <Todos los id. de evento>

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☐ Por registro ☒ Por origen

Registros de eventos:

Orígenes del evento:

- ☒ <Todos los orígenes de eventos>
- ☐ .NET Runtime
- ☐ .NET Runtime Optimization Service
- ☐ 3ware
- ☐ AAD
- ☐ ACL-UI
- ☐ ACPI
- ☐ ActionQueue
- ☐ Active Directory Web Services
- ☐ ActiveDirectory\_DomainService
- ☐ Admin
- ☐ ADP80XX
- ☐ ADSI
- ☐ ADWS
- ☐ AeLookupServiceTrigger
- ☐ AeSwitchBack
- ☐ AFD

Para incluir o excluir los id. de evento, escriba en las casillas de texto y presione Enter. Para excluir criterios, antecédalos con una tilde (~).

Categoría de la tarea: <Todos los id. de evento>

Palabras clave: <Todos los id. de evento>

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>



# Vistas personalizadas

## Configuración

---

- **Eventos restringidos:** podemos hacer una **búsqueda de determinados tipos de eventos**, representados por su identificador. Existen distintas opciones:
  - **Un solo tipo de evento:** escribimos su identificador, por ejemplo: 4624
  - **Varios tipos de evento:** escribimos sus identificadores, separamos por comas, por ejemplo: 4624, 4655
  - **Un rango de tipos de eventos:** escribimos el primero y el último de los identificadores que necesitamos incluir, separados por un guion, por ejemplo: 4624-4655
  - **Eliminar un tipo en particular, de un rango dado:** simplemente se precederá de un signo menos, por ejemplo: 4624-4655, -4645.
  - **Combinar todo lo anterior:** escribimos identificadores individuales separados por comas y rangos especificados con guiones, por ejemplo: 4624, 4630, 4640-4655, -4645.



# Vistas personalizadas

## Configuración



Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro    Registros de eventos: Sistema

☐ Por origen    Orígenes del evento:

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

4624, 4630, 4640-4655, -4645

Categoría de la tarea:

Palabras clave:

Usuario: <Todos los usuarios>

Equipo(s): <Todos los equipos>

Borrar

Aceptar Cancelar



# Vistas personalizadas

## Configuración

- **Categoría de la tarea:** también podemos filtrar por la categoría de la tarea, que indica la acción que fue realizada en el evento. Las posibles categorías seleccionables dependerán del tipo de evento.

Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro Registros de eventos: Sistema

☐ Por origen Orígenes del evento: Microsoft Windows security auditing.

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

4625

Categoría de la tarea:

- ☐ < Todas las categorías de tareas >
- ☐ Security State Change
- ☐ Security System Extension
- ☐ System Integrity
- ☐ IPsec Driver
- ☐ Other System Events
- ☒ Logon
- ☐ Logoff
- ☐ Account Lockout
- ☐ IPsec Main Mode
- ☐ Special Logon

Palabras clave:

Usuario:

Equipo(s):



# Vistas personalizadas

## Configuración

- **Palabras clave:** también podemos seleccionar las **palabras clave** que se desea filtrar desde el **origen de suceso** o de **registro**.

Crear vista personalizada

Filtro XML

Registrado: En cualquier momento

Nivel del evento: ☐ Crítico ☐ Advertencia ☐ Detallado  
☐ Error ☐ Información

☒ Por registro Registros de eventos: Sistema

☐ Por origen Orígenes del evento: Microsoft Windows security auditing.

Para incluir o excluir los id. de evento, escriba números o intervalos de id. separados por comas. Para excluir criterios, antecédalos con un signo de menos. Ej: 1,3,5-99,-76

4625

Categoría de la tarea: Logon

**Palabras clave:**

Usuario:

Equipo(s):

- ☐ <Todas las palabras clave>
- ☐ Auditoría correcta
- ☐ Clásico
- ☐ Diag WDI
- ☒ Error de auditoría
- ☐ Indicio de correlación
- ☐ SQM
- ☐ Tiempo de respuesta

Aceptar Cancelar



# Vistas personalizadas

## Configuración

- **Usuarios y equipos:** también podemos especificar solo eventos en relación a usuarios o equipos en concreto. Si queremos indicar varios usuarios, o varios equipos, debemos separarlos con comas.



# Vistas personalizadas

## Configuración

- Una vez **finalizada la configuración** de la vista personalizada del visor de eventos, haremos  **clic en el botón Aceptar**.

Nota: si hacemos clic en el botón Borrar, se eliminará la configuración realizada, quedando en blanco todos los apartados que hemos ido modificando.



# Vistas personalizadas

## Guardar vista personalizada

---

- Al hacer clic sobre el botón aceptar, aparecerá la ventana **Guardar filtro en vista personalizada**, en la cual debemos configurar los siguientes campos:
  - **Nombre:** nombre que queremos dar a la vista personalizada.
  - **Descripción:** podemos incluir una breve descripción del tipo de eventos que filtraremos con la vista personalizada. Este campo puede dejarse en blanco.
  - **Seleccionar donde guardar la vista personalizada:** indicaremos el lugar donde queremos guardar la vista personalizada. Podemos elegir:
    - **Vistas personalizadas**, del panel izquierdo del Visor de eventos
    - Cualquiera de las **subcarpetas** de la entrada Vistas personalizadas.
    - Crear una **nueva subcarpeta**, usando el botón Nueva Carpeta.
  - **Todos los usuarios:** podemos indicar si queremos que la vista personalizada que estamos creando esté disponible para todos los usuarios o sólo para el usuario que estamos utilizando en este momento.

# Vistas personalizadas

## Guardar vista personalizada



Guardar filtro en vista personalizada

Nombre: Error de inicio

Descripción:

Seleccione dónde guardar la vista personalizada:

- Visor de eventos
  - Vistas personalizadas

Aceptar

Cancelar

Nueva carpeta

☒ Todos los usuarios

# Vistas personalizadas

## Guardar vista personalizada



Visor de eventos

Archivo Acción Ver Ayuda

Visor de eventos (local)

- Vistas personalizadas
  - Roles de servidor
  - Error de inicio**
  - Registros de Windows
    - Aplicación
    - Seguridad
    - Instalación
    - Sistema
    - Eventos reenviados
  - Registros de aplicaciones y suscripciones

**Error de inicio** Número de eventos: 14

Número de eventos: 14

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	06/12/2023 11:01:21	Microsoft Windows securi...	4625	Logon
Información	05/12/2023 14:34:46	Microsoft Windows securi...	4625	Logon
Información	19/11/2023 19:50:56	Microsoft Windows securi...	4625	Logon
Información	19/11/2023 19:50:53	Microsoft Windows securi...	4625	Logon
Información	18/11/2023 20:38:36	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:24:02	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:24:02	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:24:02	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:14:30	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:14:12	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:13:06	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:13:05	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:13:03	Microsoft Windows securi...	4625	Logon
Información	17/11/2023 22:08:32	Microsoft Windows securi...	4625	Logon

**Acciones**

- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar vista personalizada actual...
- Propiedades
- Buscar...
- Guardar todos los eventos en la vista personalizada ...
- Exportar vista personalizada...
- Copiar vista personalizada...
- Adjuntar tarea a esta vista personalizada...
- Ver
- Eliminar
- Cambiar nombre
- Actualizar
- Ayuda

**Evento 4625, Microsoft Windows security auditing.**

General Detalles

Error de una cuenta al iniciar sesión.

Nombre de registro: Seguridad

Origen: Microsoft Windows security Registrado: 06/12/2023 11:01:21

Id. del: 4625 Categoría de tarea: Logon

Nivel: Información Palabras clave: Error de auditoría

Usuario: No disponible Equipo: SERVER-1.dominio1.local

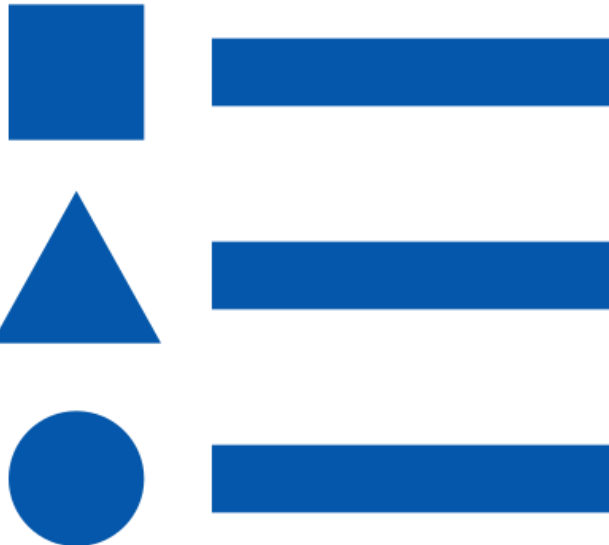
Código de operación: Información

Más información: [Ayuda Registro de eventos](#)





## Identificador de tipo de evento



# Identificador de tipo de evento



- Hemos visto como crear **vistas personalizadas** en el visor de eventos. Estas vistas personalizadas permiten al administrador tener una **visión rápida de algunos aspectos que desea supervisar**.
- Dentro de los parámetros que hemos utilizado para **filtrar eventos** al crear una vista personalizada se encuentra el **identificador de tipo de evento**.
- Al utilizar el **identificador de tipo** de evento podremos conocer de un **vistazo cuando se ha producido ese tipo** de evento, e **investigar** al respecto, si procede.
- También podemos **programar tareas relacionadas con dicho evento**, como puede ser, que el sistema nos envíe un **correo electrónico avisándonos** de que se ha producido dicho evento.



# Identificador de tipo de evento

- Por tanto, resulta interesante **conocer a qué evento corresponde cada código** de identificador de tipo de evento.
- En la siguiente **URL** puedes consultar el significado de cada código:  
<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>
- Algunos códigos de interés, relacionados con las **acciones comunes que hemos realizado con los sistemas en red** son:

Identificador	Descripción del evento
4608	Windows se está iniciando.
4609	Windows se está apagando.
4624	Se inició sesión correctamente en una cuenta.
4625	No se pudo iniciar sesión en una cuenta.
4720	Se creó una cuenta de usuario.
4727	Se creó un grupo global con seguridad habilitada.
4728	Se agregó un miembro a un grupo global con seguridad habilitada.
4729	Se quitó un miembro de un grupo global con seguridad habilitada.
4741	Se cambió una cuenta de equipo.
6005	Se inició el servicio de Registro de eventos.
6006	Se detuvo el servicio de Registro de eventos.



# Identificador de tipo de evento

- Conociendo que tipo de evento representa cada identificador, podemos crear, por ejemplo, una **vista personalizada del visor de evento** que permita al administrador saber **cuándo se ha producido un error al iniciar sesión**.

- Si no conocemos el **tipo de registro de evento**, podemos selección todos.
- Si no conocemos la **categoría de la tarea** asociada al evento, podemos dejarlo en blanco.
- Si no conocemos **palabras clave** asociadas al evento, podemos dejarlo en blanco.