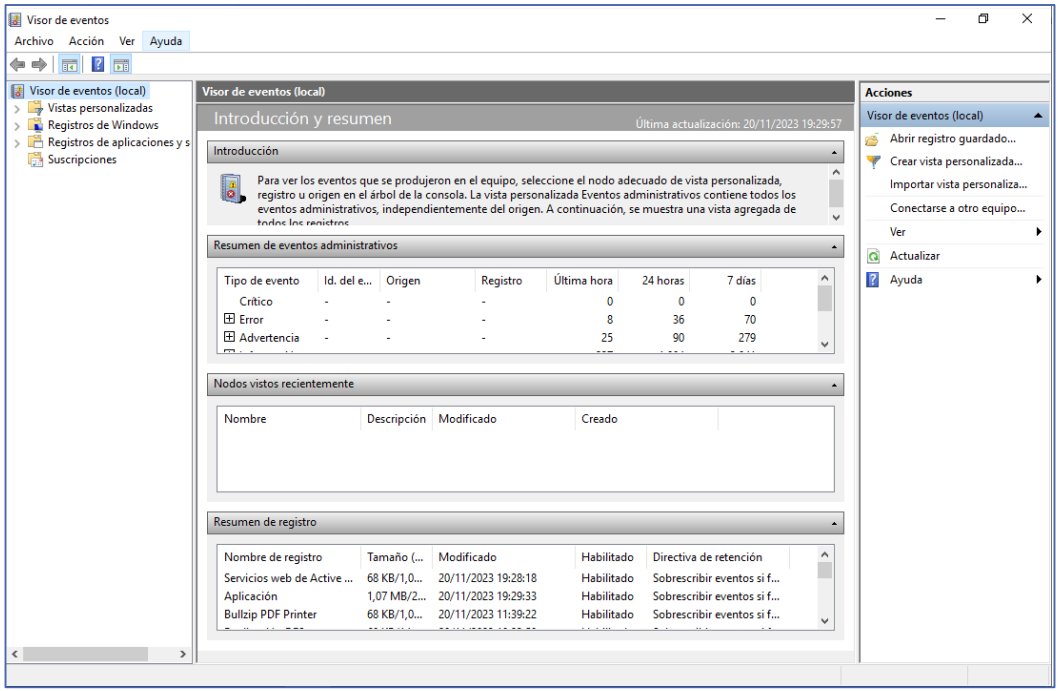
UD06
Visor de Eventos



Índice

Introducción

Introducción

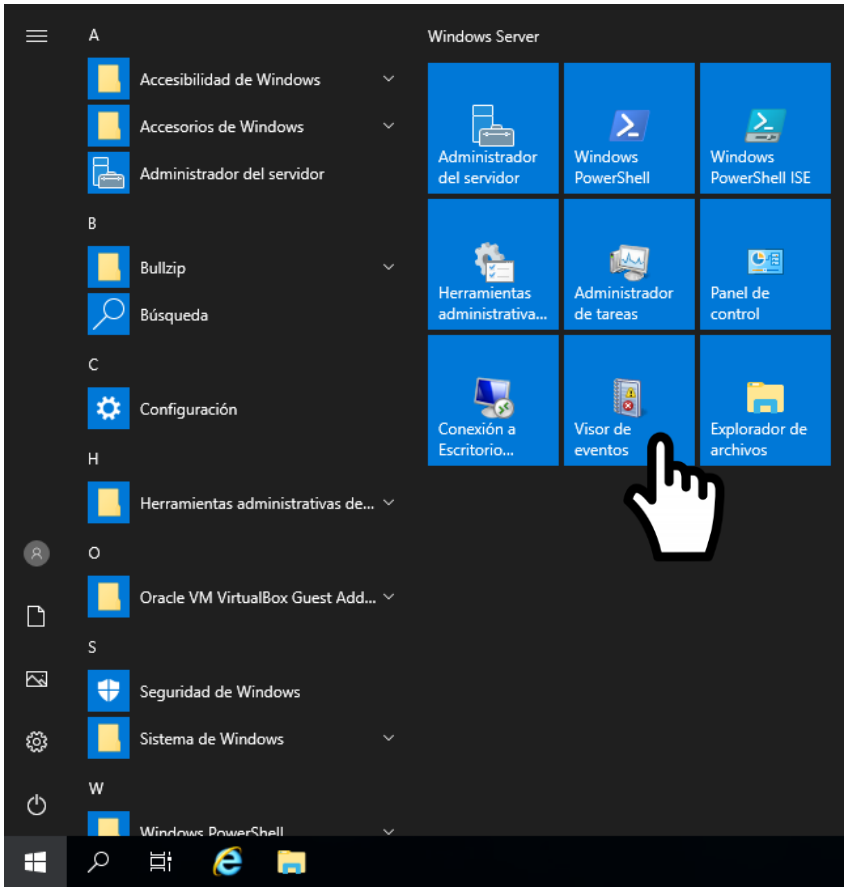
- El **administrador** del sistema necesita **saber** lo que ocurre en su sistema.
- Los **sistemas operativos**, y muchas de las **aplicaciones**, suelen **guardar detalles** de su funcionamiento en unos archivos especiales, llamados **registros de eventos** (también logs o bitácoras).
- Estos archivos 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**.

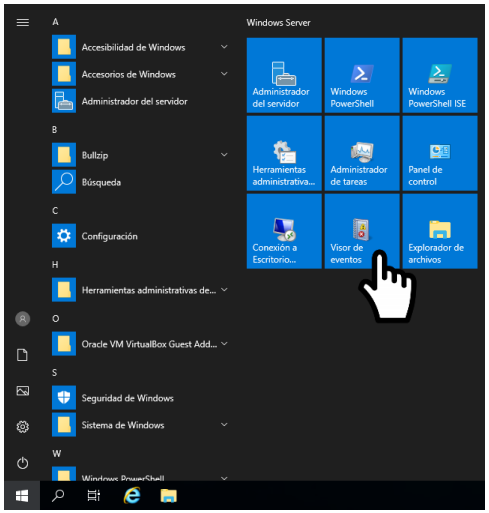
Visor de eventos

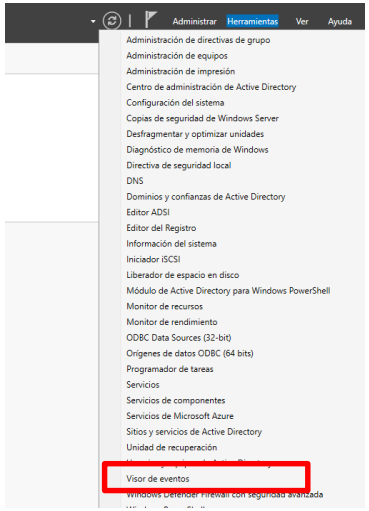
Abrir el Visor de Eventos

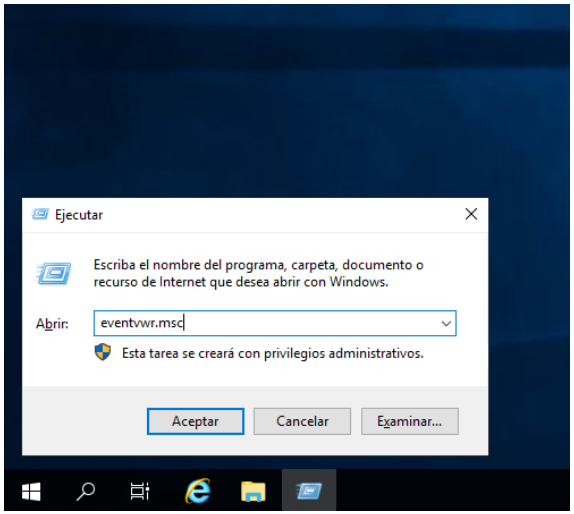


Abrir el Visor de Eventos

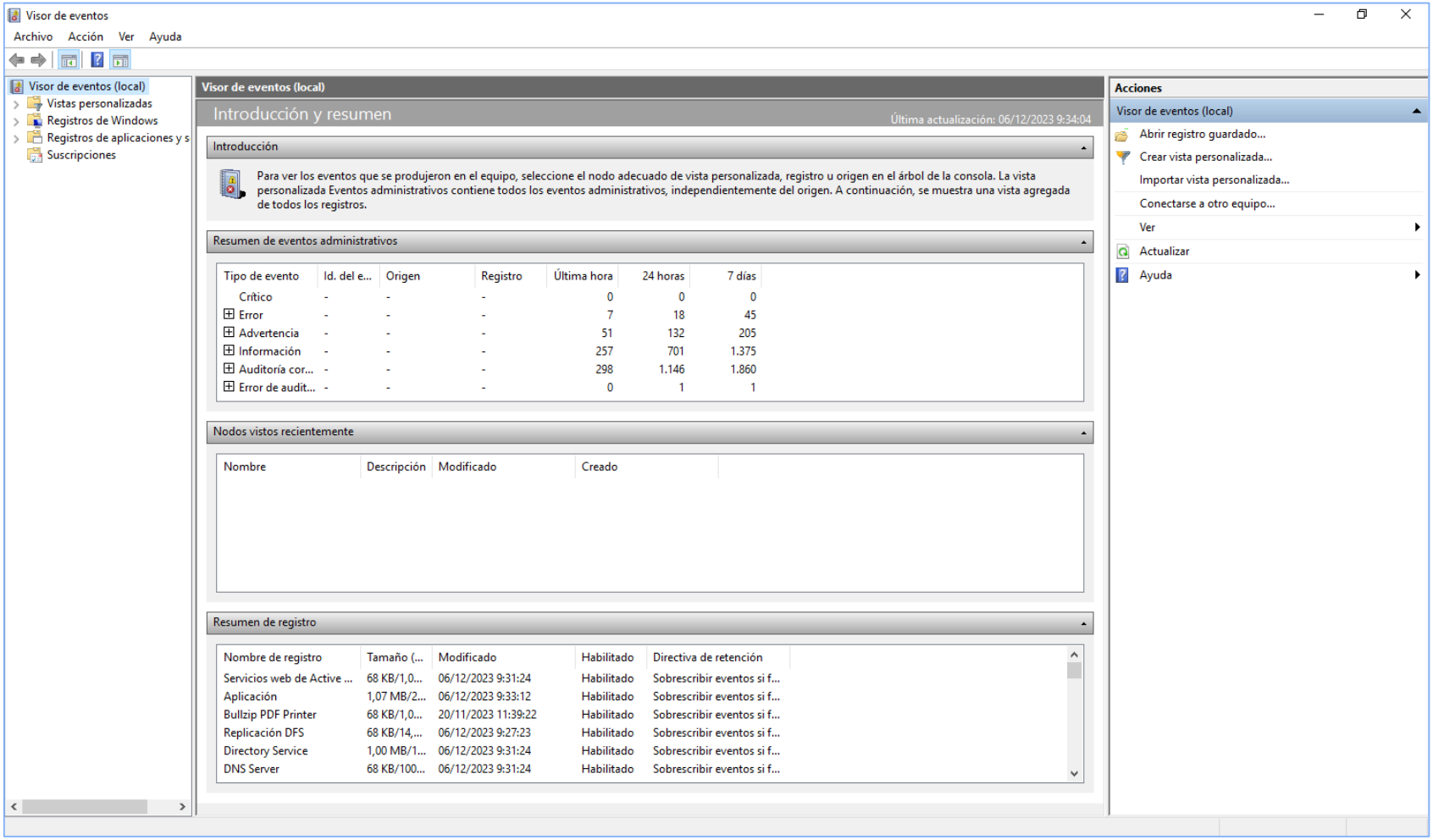
- Existen distintos modos de **abrir el visor de eventos**:
  - Inicio → **Herramientas administrativas** → Visor de eventos.
  - Directamente en el conjunto de **herramientas de Windows Server** que aparece al pulsar sobre Inicio.
  - Desde el **Administrador del Servidor** → Herramientas → Visor de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





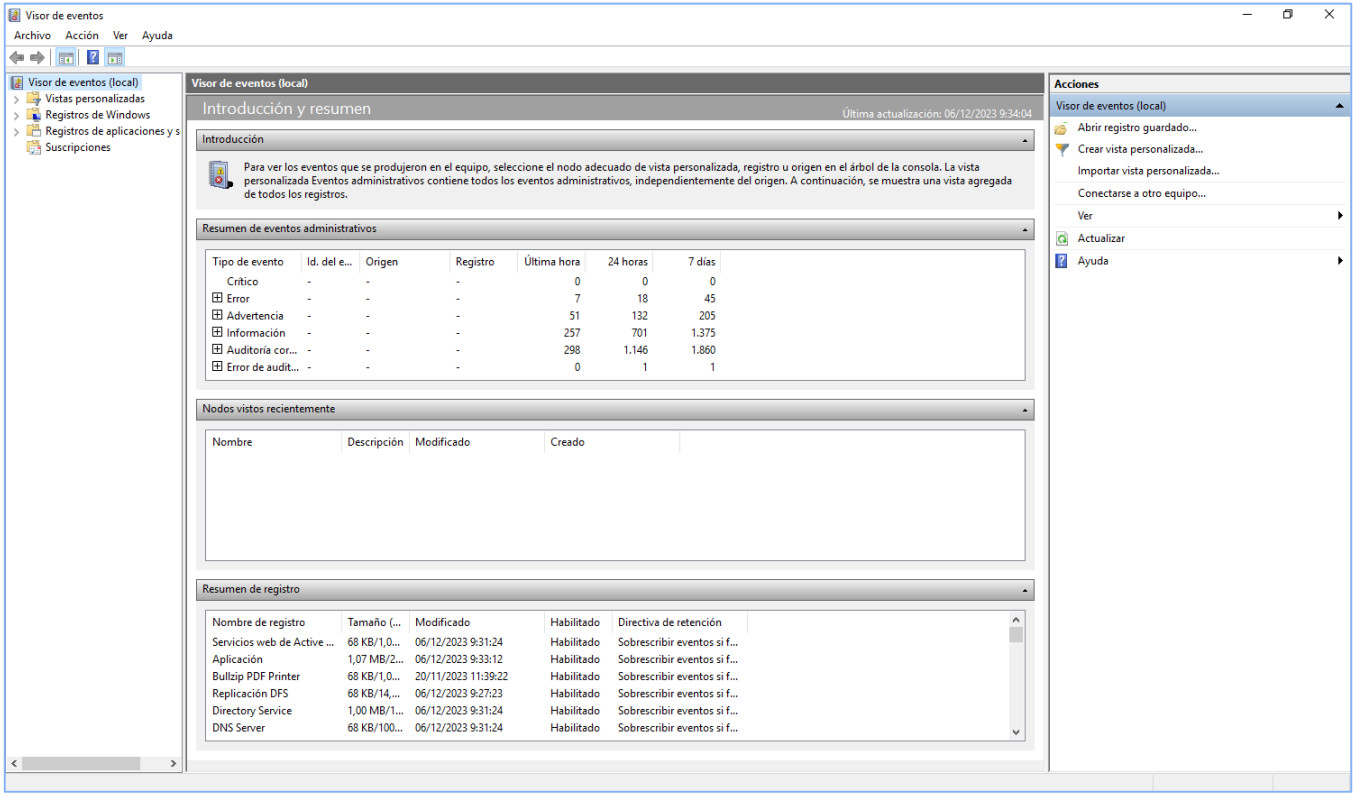


Abrir el Visor de Eventos



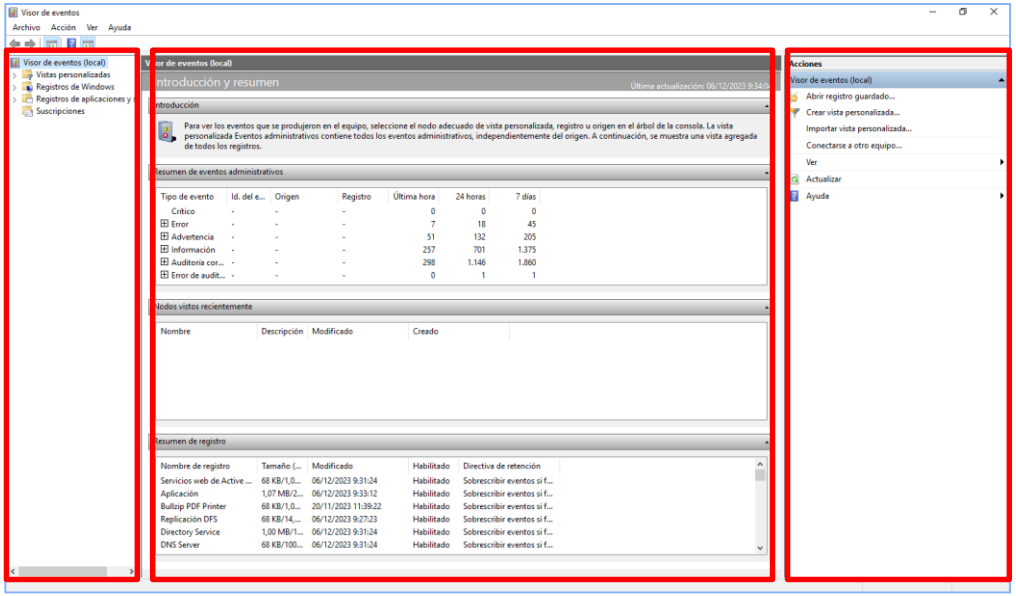
Visor de eventos

La ventana del Visor de Eventos



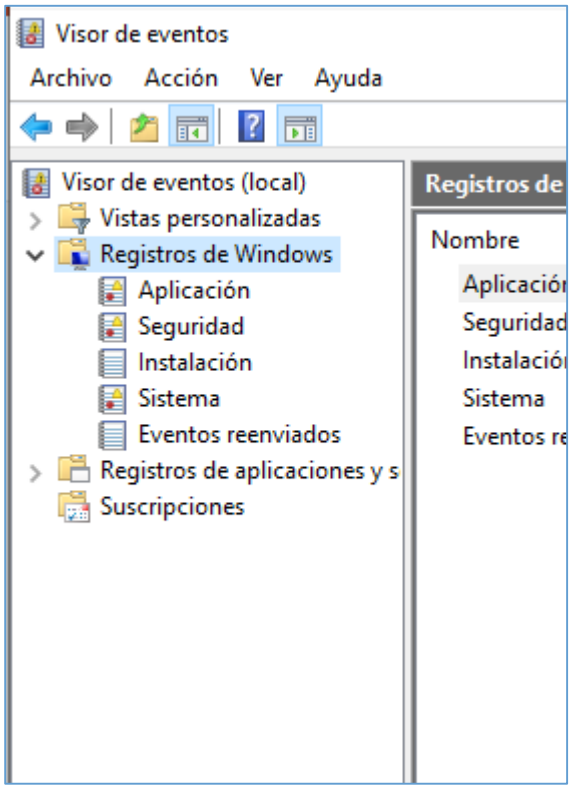
La ventana del Visor de Eventos

- 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

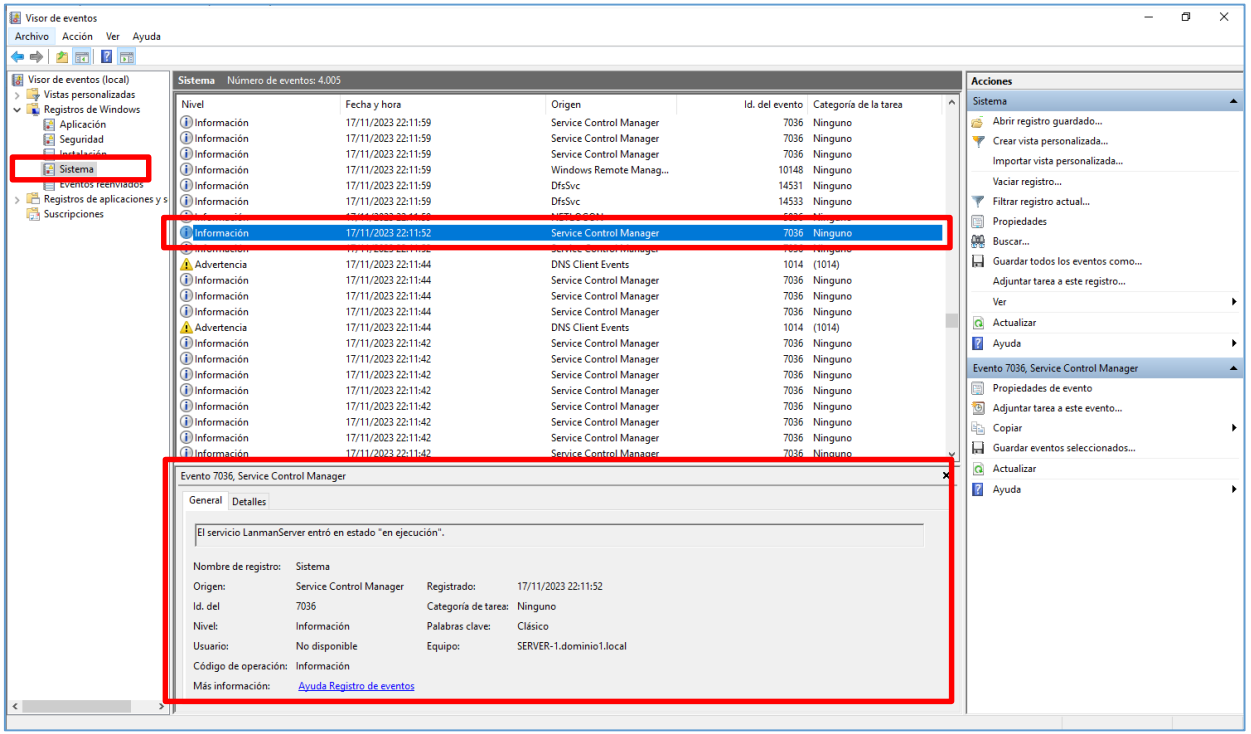
- Vamos a centrarnos en la **categoría Registros de Windows**, que contiene distintas **subcategorías**. Al seleccionar las diferentes subcategorías, la información mostrada en el **panel central variará**:
  - **Aplicación**: eventos de las aplicaciones y los servicios que no forman parte del sistema.
  - **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:



Consultar eventos

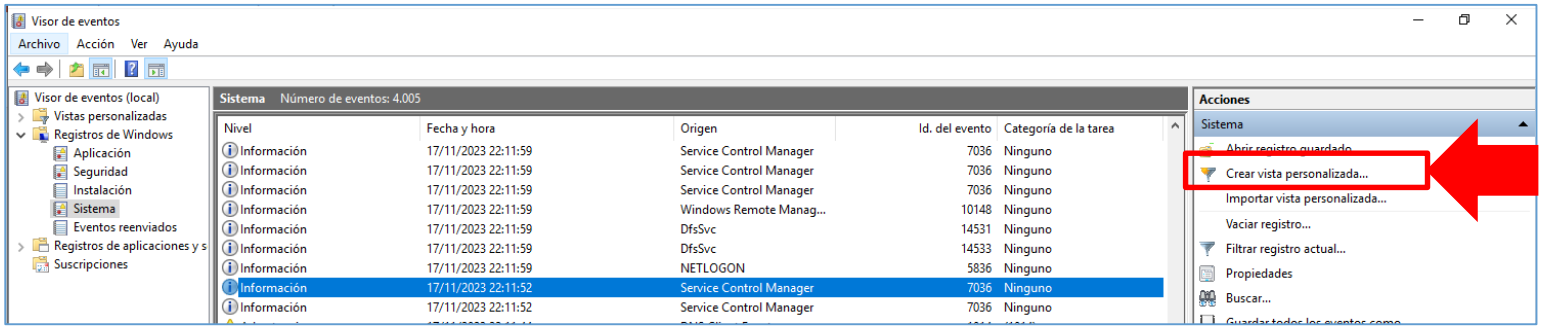
- La **información** sobre cada evento incluye:
  - Su **origen**.
  - Identificador de tipo de evento.
  - **Fecha y hora** en la que se produjo el evento.
  - **Equipo** en el que se ha producido el evento.
  - …

- 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

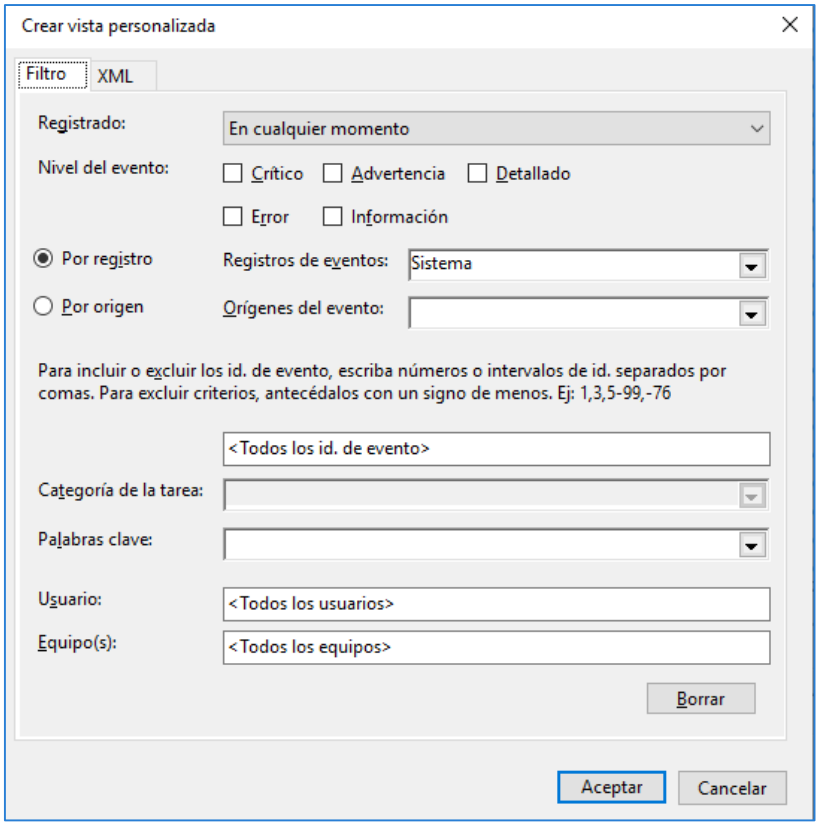
Vistas personalizadas

- 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.

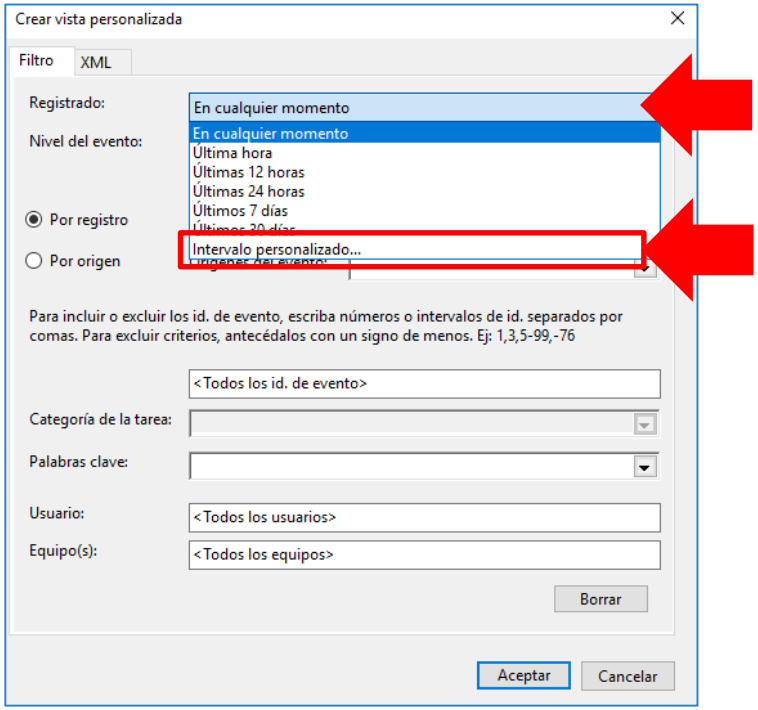


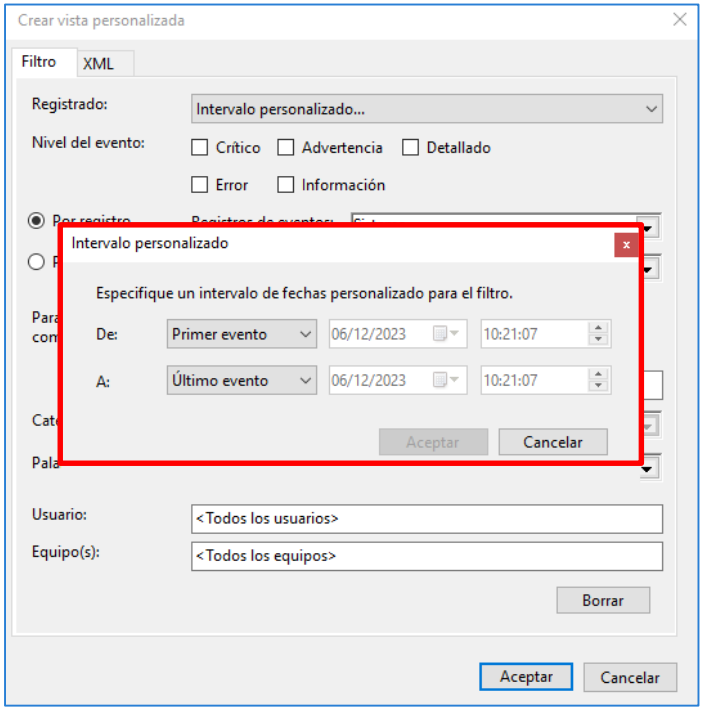
Vistas personalizadas
Configuración

- 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).

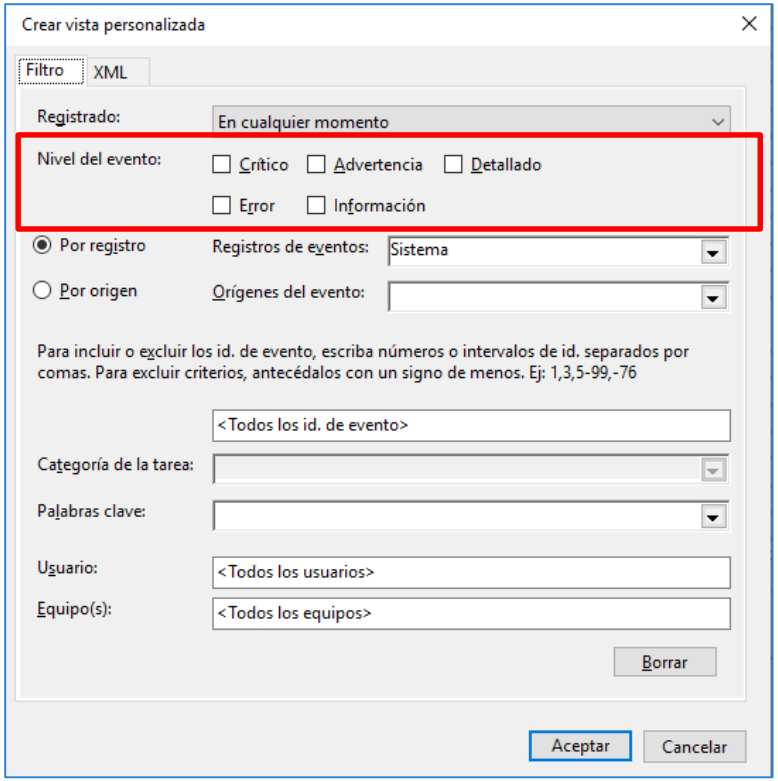




Vistas personalizadas
Configuración

- **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



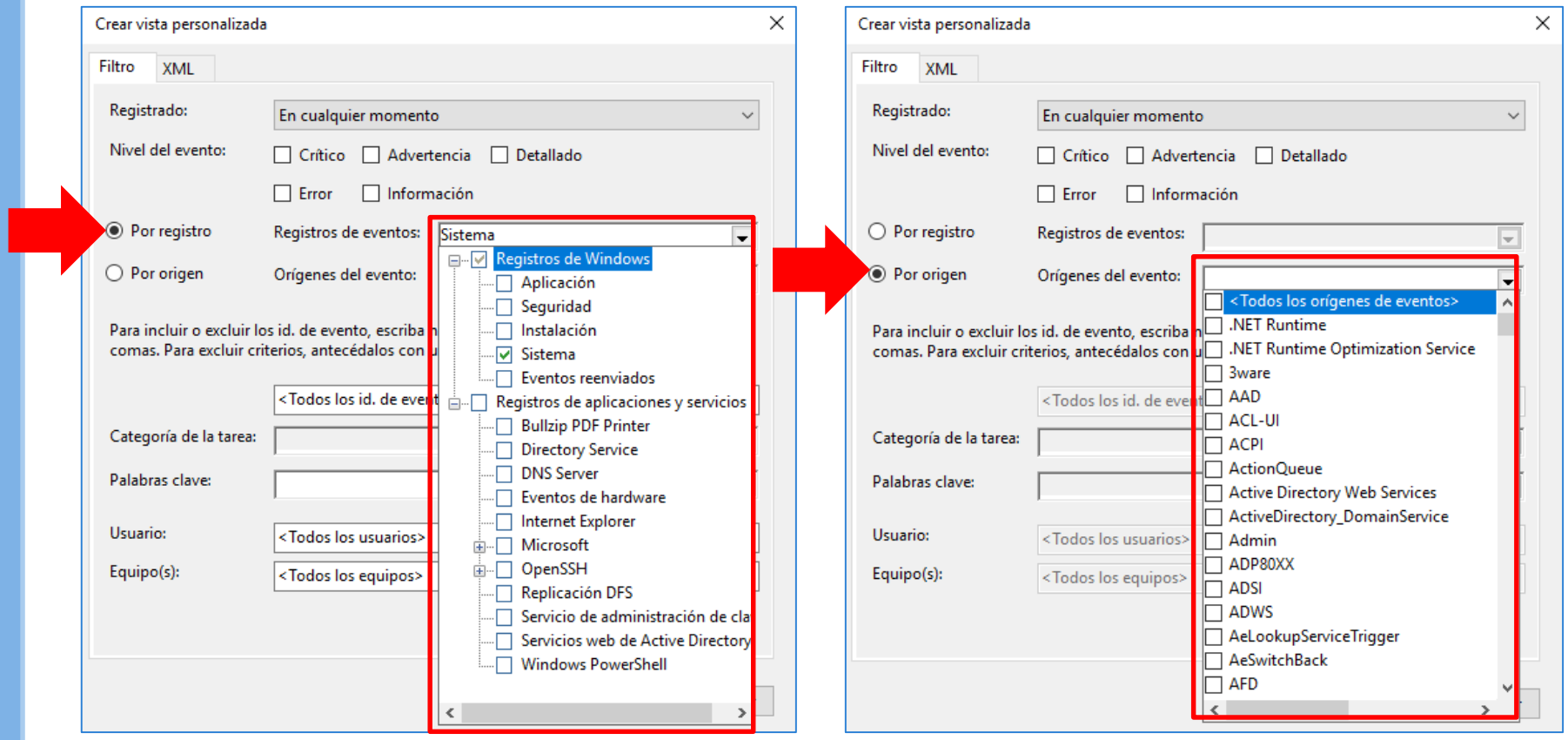
Nota: si no se selecciona ningún nivel, al contrario de lo que se podrían pensar, se incluirán todos los niveles.

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

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

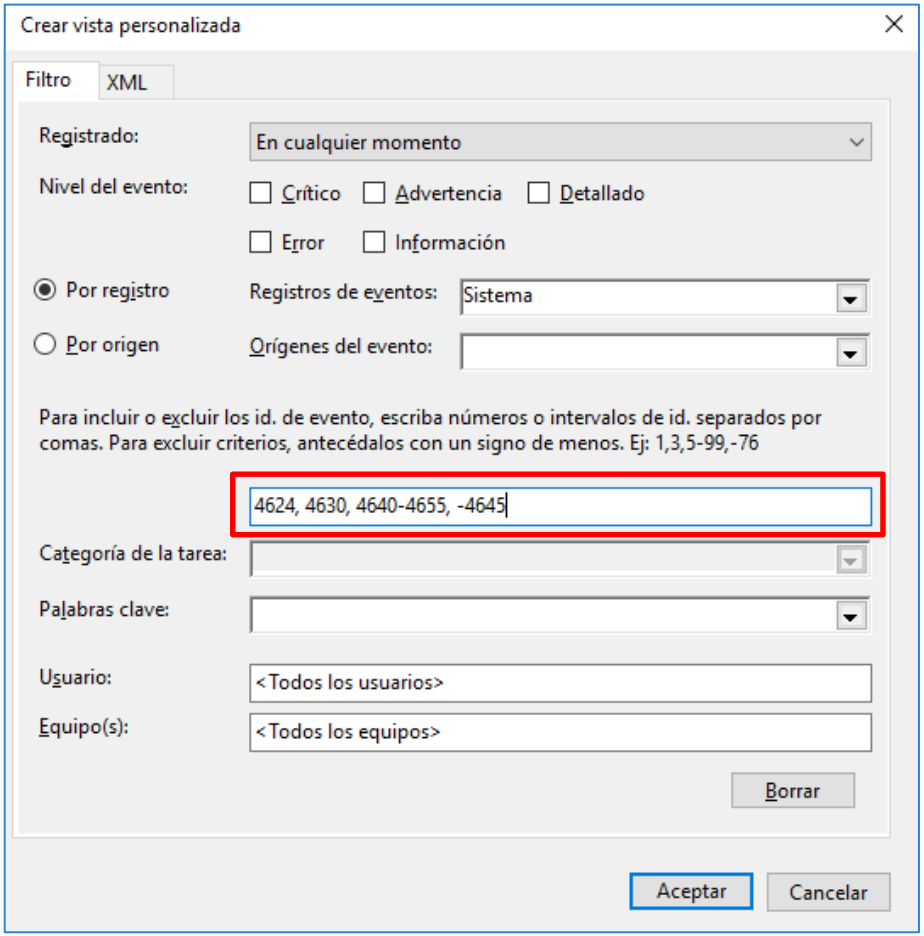


Vistas personalizadas
Configuración

- **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.

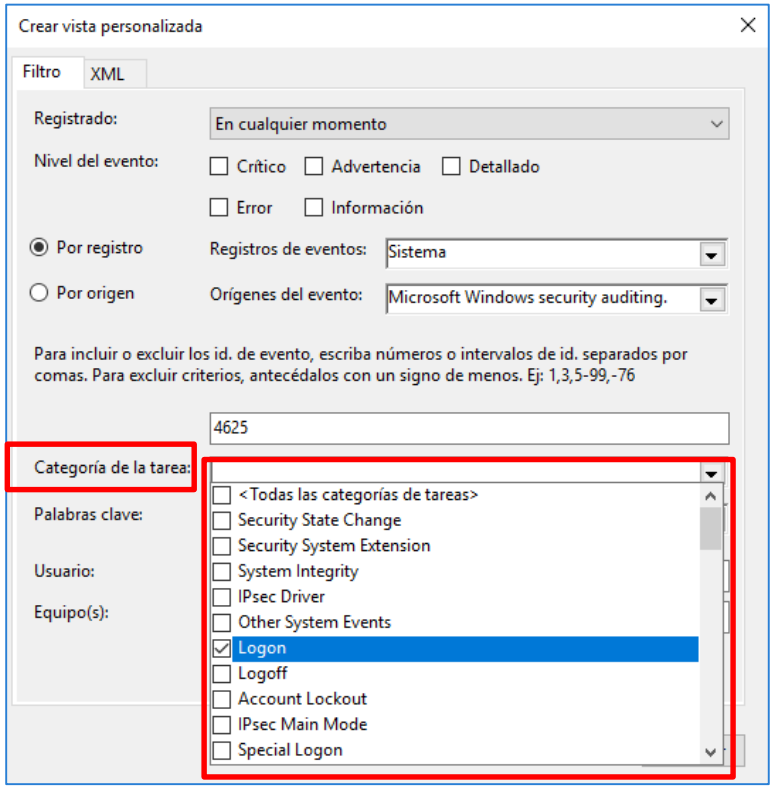
Vistas personalizadas

Configuración



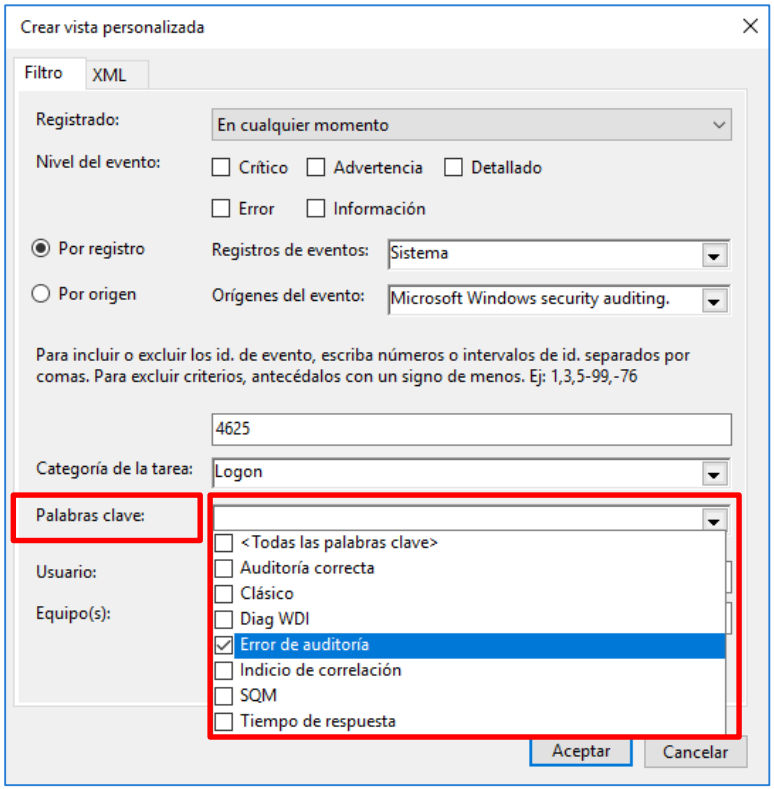
Vistas personalizadas
Configuración

- **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**.



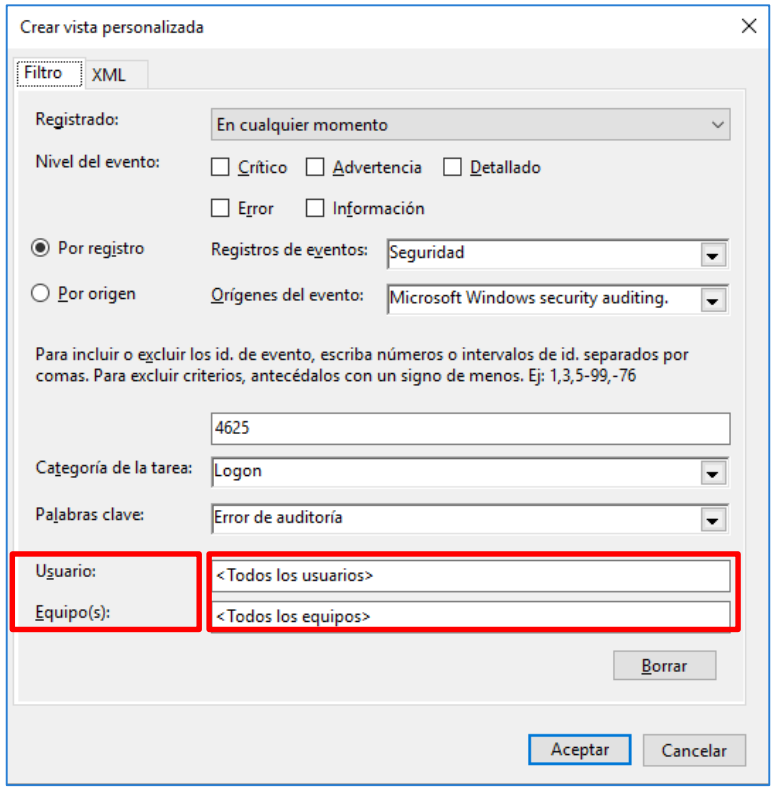
Vistas personalizadas
Configuración

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



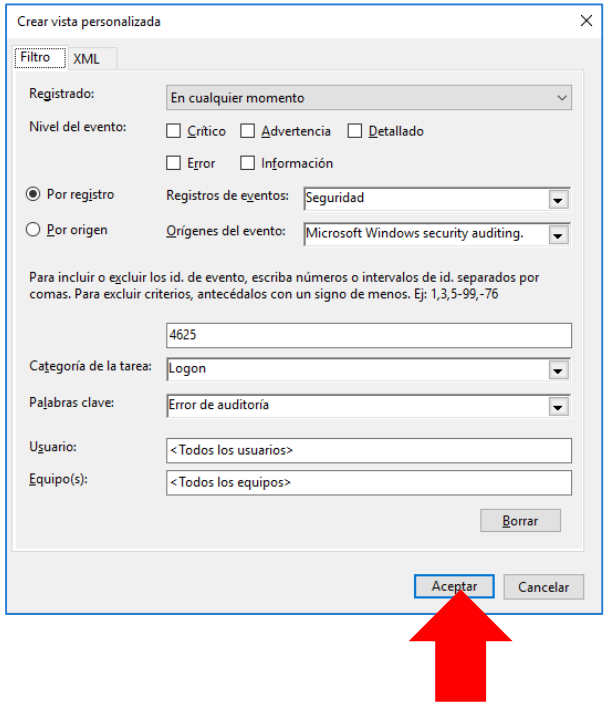
Vistas personalizadas
Configuración

- **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**.



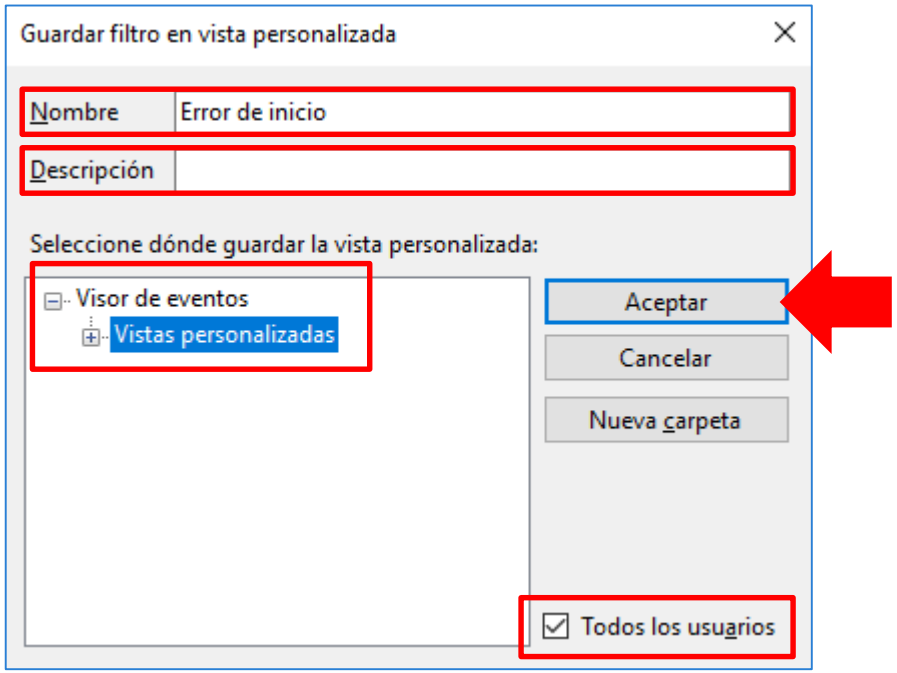
Nota: si hacemos clic en el botón Borrar, se eliminará la configuración realizada, quedando en blanco todos los apartados que hemos ido modificando.

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.

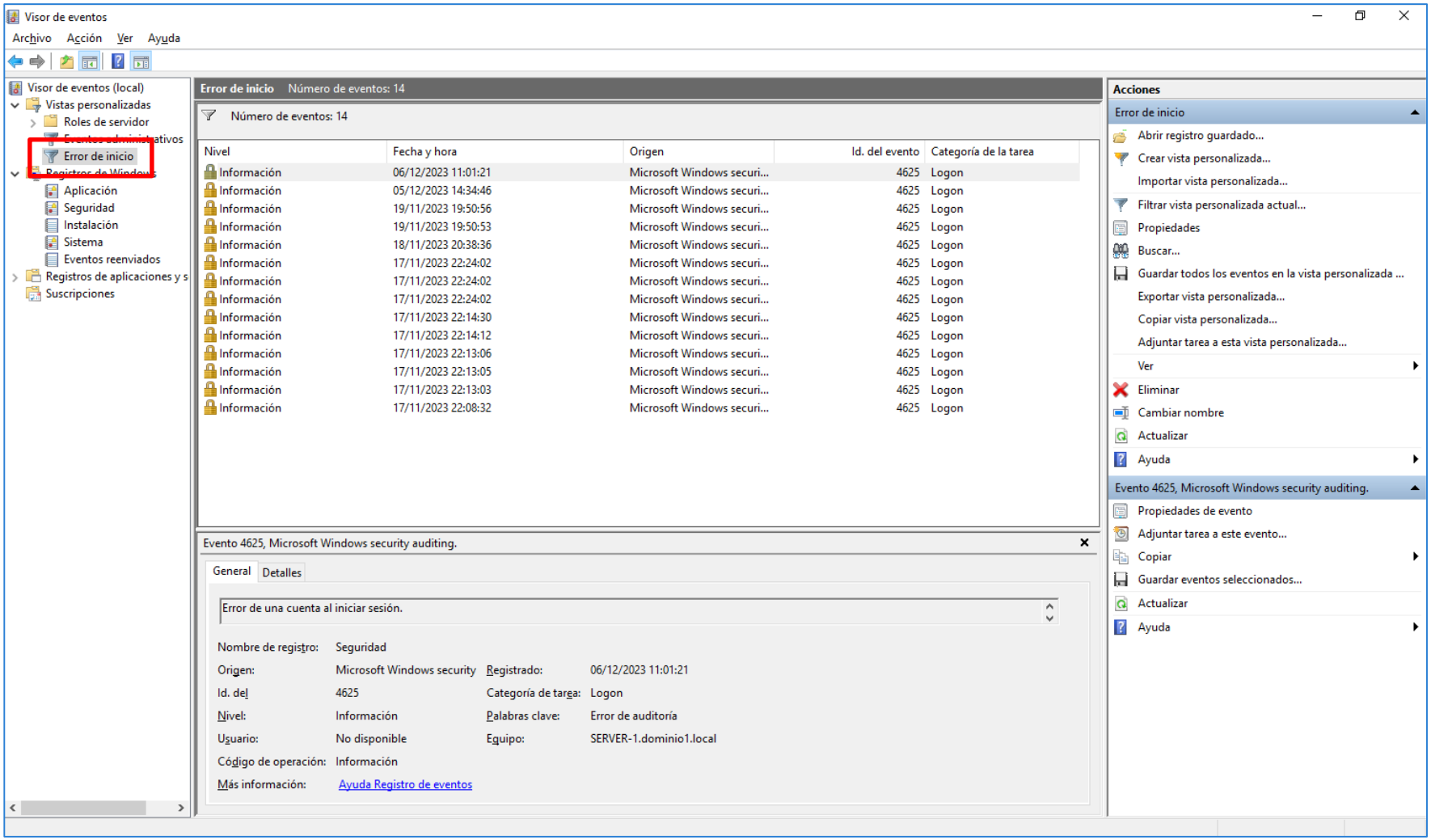
Vistas personalizadas

Guardar vista personalizada

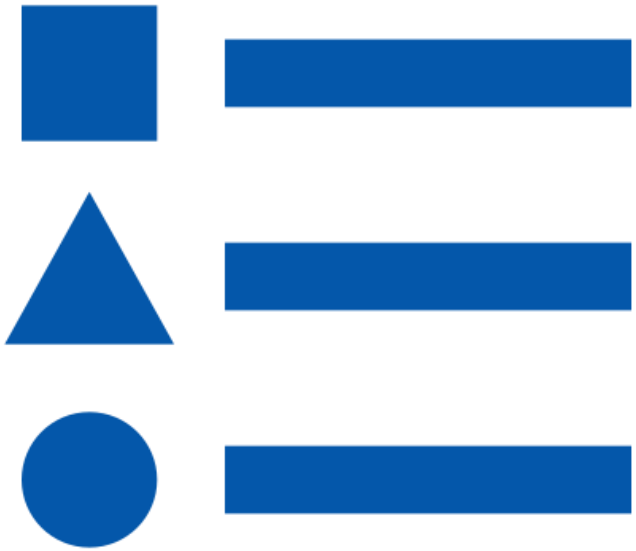


Vistas personalizadas

Guardar vista personalizada

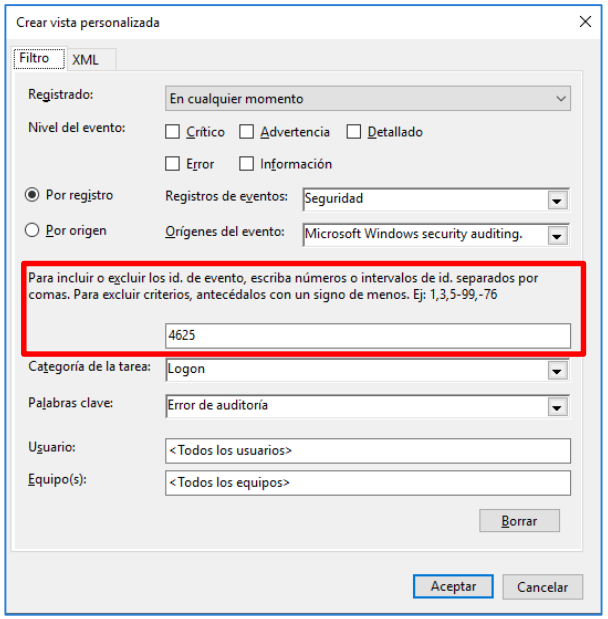


Identificador de tipo de evento



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.



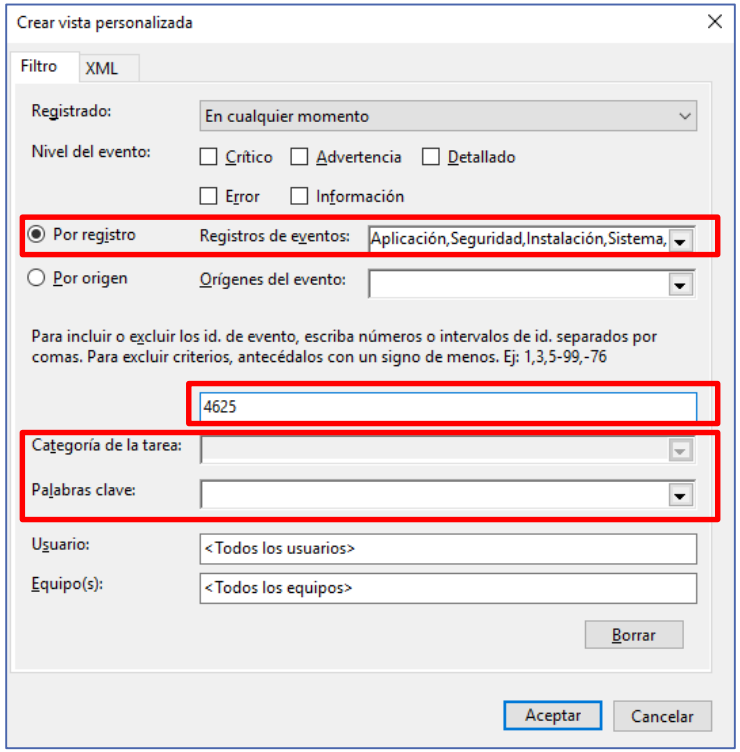
Identificador de tipo de evento

- 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 blando.
- Si no conocemos **palabras clave** asociadas al evento, podemos dejarlo en blanco.