# Aviso legal

## Descargo de responsabilidad legal

Esta guía y su contenido (la «Guía») son proporcionados por NXGEN. Todos los derechos sobre la Guía y sobre la propiedad intelectual incorporada en ella — incluidos, entre otros, marcas, nombres comerciales, logotipos y signos similares que figuren en la Guía — están protegidos por la ley. Todos los derechos, títulos e intereses sobre la Guía y sobre los derechos de propiedad intelectual relacionados pertenecen y permanecen con NXGEN y sus licenciantes.

La Guía se proporciona de forma gratuita, «tal cual» y únicamente con fines informativos, sin garantía de ningún tipo. No está destinada ni es adecuada para establecer relación jurídica alguna entre el lector y NXGEN o sus filiales, incluidas, entre otras, obligaciones de NXGEN o de sus filiales frente al lector.

Las obligaciones de NXGEN y de sus filiales respecto de los productos o servicios de NXGEN adquiridos por un cliente se rigen exclusivamente por los términos del contrato en virtud del cual se adquirieron dichos productos o servicios.

## Para mayor claridad

El lector asume todo el riesgo en cuanto al uso, los resultados y el rendimiento de la Guía. En la máxima medida permitida por la ley aplicable, NXGEN rechaza y excluye todas las garantías, ya sean legales, expresas o implícitas — incluidas, entre otras, las garantías implícitas de comerciabilidad, idoneidad para un fin determinado, titularidad y no infracción de derechos de terceros — así como cualquier responsabilidad o garantía derivada de sugerencias, especificaciones o muestras relacionadas con la Guía.

# Desbordamiento de eventos

Updated 2 September 2026

## Qué hace el desbordamiento de eventos

Event Overflow es una salvaguardia de estabilidad en toda la plataforma en GCXONE que protege automáticamente el sistema de ser inundado por un dispositivo defectuoso o mal configurado. Sin esta protección, un único sensor ruidoso podría enviar miles de alarmas en minutos, potencialmente sobrecargando toda la infraestructura de procesamiento de alarmas e impactando todos los clientes de la plataforma.

## Por qué es importante

Sin protección de Event Overflow, un único sensor ruidoso podría inundar toda la plataforma — impactando no solo a un cliente sino a cada cliente que comparte la infraestructura. El sistema de umbral garantiza que un dispositivo mal configurado no pueda derribar el procesamiento de alarmas para todos los demás.

## Cómo funciona

### GCXONE — Nivel de dispositivo

GCXONE opera un valor predeterminado en toda la plataforma para evitar el agotamiento de recursos. El sistema supervisa las alarmas entrantes a nivel de dispositivo/sensor individual:

- Umbral: Si un único dispositivo envía más de 25 alarmas dentro de cualquier ventana de 5 minutos, se supera el umbral de desbordamiento.
- Tipo de alarma: El sistema genera un tipo de alarma interno llamado event.overflow para registrar e indicar el incidente.

- Supresión: Todas las alarmas posteriores de ese sensor específico se descartan durante el resto de la ventana de 5 minutos.
- Recurrencia: El sistema vuelve a verificar al inicio de cada nueva ventana de 5 minutos. Si la tasa de alarma permanece por encima del umbral, se genera otro event.overflow y la supresión continúa.

### Talos (CMS) — Nivel de sitio

Incluso si los recuentos de alarmas de dispositivos individuales se abren paso a través de GCXONE, aún pueden ser bloqueados en el nivel del CMS (Evalink Talos), que aplica lógica de desbordamiento a nivel de sitio — en todos los dispositivos de un sitio:

- Umbral a nivel de sitio: Talos agrega alarmas en todos los sensores de un sitio. Por ejemplo, si dos dispositivos cada uno envían 15 alarmas (por debajo del umbral de GCXONE por dispositivo de 25), GCXONE los permite individualmente — pero Talos ve 30 alarmas totales para el sitio y los bloquea.
- Código de error: En Talos, esto aparece como el código de error Límite de alarma excedido.

## Capacidades clave

### Configuración y personalización

Los umbrales predeterminados están diseñados para la seguridad general de la plataforma. Para inquilinos con requisitos legítimos de alarmas de alto volumen, estos umbrales se pueden ajustar usando Propiedades personalizadas:

- Umbrales configurables: Para inquilinos específicos de alta prioridad, el límite predeterminado de 25 alarmas se puede aumentar (por ejemplo, a 50 o 100). Esto se establece a nivel de inquilino o proveedor de servicios.
- Nombre de propiedad personalizada: El parámetro utilizado para ajustar esto es style.overflow.threshold.

- Duración de aislamiento: El defaultIsolationDuration (establecido a nivel de Proveedor de servicios, en minutos) se puede configurar si un cliente requiere un comportamiento diferente de supresión de notificaciones.

Nota importante para los gerentes de éxito del cliente — Los cambios de umbral deben coordinarse con el equipo de I+D y solo deben aplicarse después de confirmar que el alto volumen de alarmas es legítimo (por ejemplo, sitios industriales con alta actividad de sensores) y no es el resultado de un dispositivo mal configurado.

## Mejores prácticas

Recordatorio clave — Event Overflow es una característica protectora — no un error. Cuando se activa, significa que el sistema está funcionando como se diseñó para proteger la plataforma. La prioridad siempre es identificar y corregir la configuración del dispositivo subyacente que está generando un volumen excesivo de alarmas.

- Cambiar de detección de movimiento básica a eventos inteligentes (IVS) — La detección de cruce de línea y la detección de intrusión se dirigen a eventos reales solo, eliminando la causa raíz de la mayoría de los incidentes de desbordamiento.
- Ejecute el cliente de prueba del fabricante antes de escalar al equipo de la plataforma — si también se desborda, el problema se confirma que es el dispositivo, no GCXONE.
- Coordine con el equipo de I+D antes de ajustar los umbrales — aumente los límites solo después de confirmar que el volumen de alarmas alto es legítimo y no es el resultado de un dispositivo mal configurado.
- Notifique al cliente cuando el desbordamiento esté activo — infórmele que las alarmas se están descartando para que pueda decidir si desea ser notificado inmediatamente o preferir una ventana de supresión cronometrada.

# Detalles adicionales

## Resolución de problemas — Identificar la causa

Cuando un dispositivo se bloquea debido a desbordamiento, casi nunca es un error de la plataforma. La causa raíz es casi siempre un problema de configuración a nivel de sitio físico.

1. Paso 1 — Abra el panel de control de GCXONE y busque sensores que muestren un estado de bloqueado o entradas de registro event.overflow.
2. Paso 2 — Acceda a los registros del NVR o cámara físicos para verificar si realmente está produciendo una avalancha de eventos.
3. Paso 3 — Ejecute el cliente de prueba del fabricante (por ejemplo, cliente de prueba de Hikvision, herramienta de configuración de Dahua). Si el cliente de prueba también se desborda, el problema es el dispositivo — no la plataforma.

## Soluciones recomendadas

Una vez que se identifica la causa, utilice los siguientes enfoques de remediación:

Recomendado: Cambiar a eventos inteligentes (IVS) — La causa raíz más común de desbordamiento es el uso de detección de movimiento básica, que se activa en cualquier cambio de píxel — viento, lluvia, reflejos, insectos. Recomendamos encarecidamente cambiar a eventos del Sistema de vídeo inteligente (IVS):

- Detección de cruce de línea — se activa solo cuando un objeto cruza una línea definida.
- Detección de intrusión — se activa solo cuando un objeto entra en una zona definida.
- Filtros de humano/vehículo — aplica IA en el borde para ignorar el movimiento no humano/no vehicular antes de enviar cualquier señal.

## Opciones adicionales de mitigación

- Reducir la sensibilidad de detección de movimiento: Reduzca la configuración de sensibilidad en la cámara o NVR, o aumente el umbral de tamaño mínimo del objeto, para que cambios ambientales menores no desencadenen alarmas.
- Ajustar tiempo de umbral: Configure el dispositivo para requerir una duración de detección sostenida (por ejemplo, 2 segundos de movimiento continuo) antes de enviar una alarma — esto filtra los activadores fugaces y que no son una amenaza.
- Notifique al cliente: Si un dispositivo entra en desbordamiento durante un período de monitoreo activo, informe al cliente que las alarmas se están descartando. Deben decidir si desean ser notificados inmediatamente cuando comienza el desbordamiento, o preferir una ventana de supresión cronometrada.