**SIPRA-VR-RS07**

Enviar Notificaciones Automáticas a Dispositivos Móviles o Correos Electrónicos

RF07

|  |  |  |  |
| --- | --- | --- | --- |
| Responsable | Requisito | Versión | Fecha de Creación |
| Max Saavedra | Funcional | 1.0 | 06/04/2025 |

# **Historial de Cambios**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versión | Fecha | Secciones Modificadas | Descripción | Responsable |
| 1.0 | 06/04/2025 | Creación | Crear el documento | Max Saavedra |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Tabla de Contenidos**

[**Historial de Cambios** 1](#_Toc196685134)

[**1.** **Introducción** 2](#_Toc196685135)

[**1.1.** **Propósito** 2](#_Toc196685136)

[**1.2.** **Alcance** 2](#_Toc196685137)

[**1.3.** **Resumen** 2](#_Toc196685138)

[**2.** **Descripción General** 2](#_Toc196685139)

[**2.1.** **Descripción** 2](#_Toc196685140)

[**2.2.** **Diagrama de Casos de Uso** 3](#_Toc196685141)

[2.2.1. Descripción del CU 3](#_Toc196685142)

[**2.3.** **Diagrama de Secuencia** 3](#_Toc196685143)

[2.3.1. Descripción de la Secuencia 4](#_Toc196685144)

[**2.4.** **Prototipo** 4](#_Toc196685145)

[**2.5.** **Condiciones** 5](#_Toc196685146)

[2.5.1. Precondiciones 5](#_Toc196685147)

[2.5.2. Poscondiciones 5](#_Toc196685148)

[**2.6.** **Flujo Básico** 6](#_Toc196685149)

[**2.7.** **Excepciones** 6](#_Toc196685150)

# **Introducción**

## **Propósito**

Este documento tiene como finalidad describir el requisito funcional que permitirá al sistema enviar notificaciones automáticas a los dispositivos móviles o correos electrónicos del personal de seguridad y operadores. Este mecanismo de alerta tiene el objetivo de garantizar una respuesta inmediata ante situaciones de riesgo detectadas en espacios públicos.

## **Alcance**

Este requisito abarca la generación automática de notificaciones en tiempo real cuando se detecta un evento clasificado como riesgo moderado o alto. Las notificaciones incluirán información esencial como tipo de evento, ubicación geográfica y nivel de criticidad, y serán entregadas mediante servicios de correo electrónico y mensajería móvil.

## **Resumen**

Al ocurrir un evento crítico, el sistema backend será responsable de componer y enviar automáticamente notificaciones a las personas responsables registradas, asegurando la entrega rápida de información vital para una actuación oportuna.

# **Descripción General**

## **Descripción**

Cuando el sistema detecte un evento relevante, deberá generar una notificación estructurada que incluya los siguientes datos:

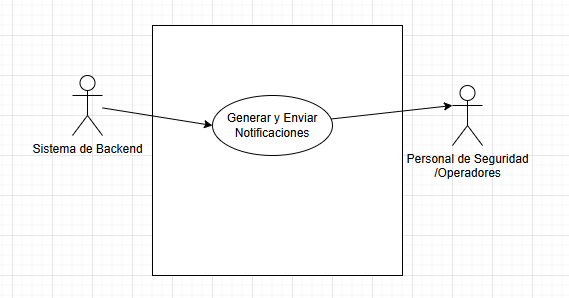
* Tipo de evento detectado (por ejemplo: caída, incendio, objeto sospechoso).
* Ubicación exacta del evento.
* Nivel de riesgo asignado (leve, moderado, alto).
* Hora y fecha del evento.

La notificación será enviada por dos vías:

* **Correo electrónico**, utilizando servicios SMTP o APIs de correo electrónico.
* **Mensaje Push** a aplicaciones móviles, utilizando servicios como Firebase Cloud Messaging (FCM) o equivalentes.

## **Diagrama de Casos de Uso**

Figura 1: Diagrama de Caso de Uso 7



Nota: *El personal de seguridad recibe una notificación de alerta*

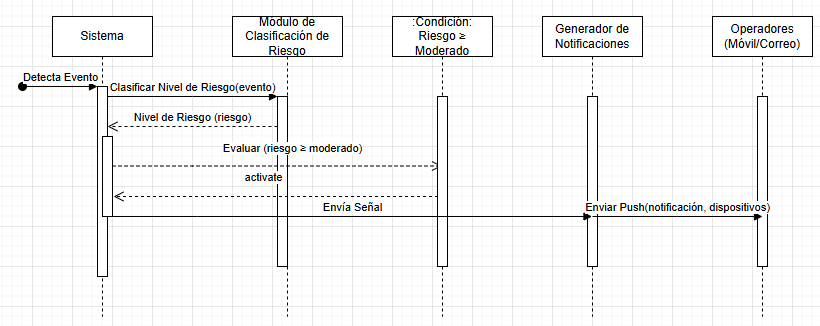
* **Actor principal**: Sistema de Backend
* **Caso de uso**: Generar y enviar notificaciones

### Descripción del CU

* **Sistema Backend:** Responsable de generar y despachar la notificación tras la detección del evento.
* **Personal de Seguridad/Operadores**: Usuarios que reciben las notificaciones y actúan en consecuencia.

## **Diagrama de Secuencia**

Figura 2: Diagrama de Secuencia



Nota: *Inicio de sesión para usuarios autorizados*

* Detección de evento → Clasificación → Generación de notificación → Envío a móvil/correo → Confirmación de entrega

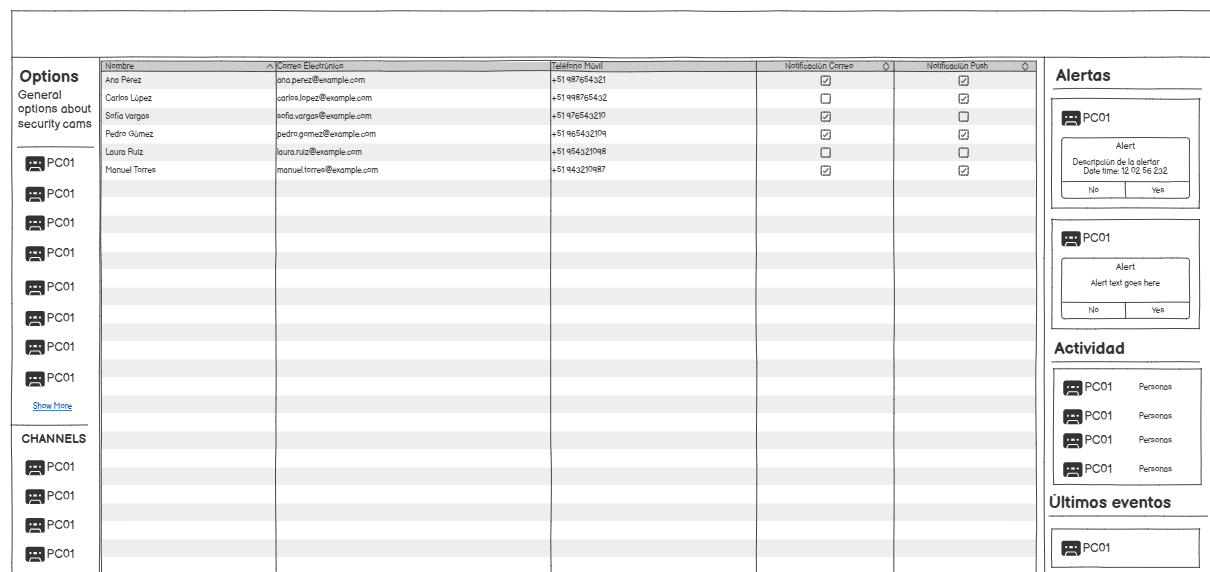
### Descripción de la Secuencia

El sistema detecta un evento relevante y lo clasifica. Si cumple con el criterio de riesgo moderado o alto, el backend genera automáticamente una notificación estructurada. Esta notificación es transmitida por los canales configurados (correo electrónico o servicio de mensajería móvil) a todos los operadores asignados. La confirmación de la entrega será registrada en los logs del sistema para auditoría.

## **Prototipo**

En la interfaz del dashboard, existirá una sección de configuración de notificaciones, donde se podrá gestionar la lista de destinatarios, activar o desactivar los métodos de notificación y visualizar el historial de alertas enviadas.

Figura 3: Prototipo de la interfaz principal



Nota: *Lista de operadores en una tabla.*

## **Condiciones**

### Precondiciones

* El evento debe haber sido detectado y clasificado como moderado o alto.
* Los correos electrónicos y dispositivos móviles de los usuarios deben estar registrados y activos en el sistema.
* El servicio de mensajería y/o correo debe estar configurado correctamente.

### Poscondiciones

* Se habrá enviado una notificación automática a los destinatarios configurados.
* La notificación quedará registrada en el historial del sistema.

## **Flujo Básico**

1. El sistema detecta un evento en el espacio público.
2. Se clasifica el evento como de riesgo moderado o alto.
3. El backend genera una notificación detallada con la información del evento.
4. La notificación se envía automáticamente por correo electrónico y/o push móvil.
5. El destinatario recibe la alerta y puede actuar en consecuencia.
6. El sistema registra el envío exitoso en su base de datos.

## **Excepciones**

* **Error de conexión al servicio de correo o mensajería**: El sistema intentará reenviar la notificación hasta tres veces antes de generar un error registrado.
* **Datos incompletos del destinatario**: Si no existe información de contacto válida para algún usuario, el sistema lo reportará como alerta de configuración pendiente.
* **Retraso en la entrega de mensajes**: Si el servicio de mensajería presenta retrasos por alta demanda, el sistema mostrará un aviso en el panel de administración.