

# Análisis y Planificación: Severidad

## Severidad

En el contexto del análisis y planificación de pruebas en el testing manual, la "severidad" se refiere a la medida en que un defecto o error en el software afecta el funcionamiento del sistema y la experiencia del usuario. La severidad se utiliza para clasificar la gravedad o importancia de un defecto y determinar la prioridad de su corrección.

Es muy probable que cada empresa tenga sus definiciones y nomenclaturas internas para identificar la severidad de los defectos, pero te proporcionamos las categorías más comunes utilizadas en el rubro:

- **Severidad Crítica (Critical):** Generalmente son defectos que causan un fallo total del sistema o impiden el uso fundamental de la aplicación. Pueden estar relacionados con funciones esenciales o cuestiones de seguridad.
- **Severidad Alta (Mayor):** Defectos que afectan la funcionalidad, pero no impiden el uso total del sistema. Pueden generar inconvenientes significativos o reducir la eficacia de ciertas características.
- **Severidad Baja (Minor):** Defectos que no afectan a todos los usuarios o a un proceso o aspecto clave. Si bien afecta un área clave, hay alternativas de llevar a cabo el mismo proceso o de completar la tarea.
- **Severidad Muy baja (Nominal / Trivial):** Defectos que en términos del sistema no afectan ni impide ninguno de sus aspectos principales.

Cabe mencionar, que las definiciones y límites concretos entre la clasificación de severidad pueden variar, pero es trabajo del tester asignar una severidad a los defectos detectados para proporcionar una guía clara al equipo de desarrollo sobre la importancia relativa de corregir cada problema.

A continuación te ofrecemos algunas preguntas que podrían serte útil para identificar la severidad de cada defecto:

- ¿Afecta a todos los usuarios del sistema? ¿A todos los usuarios de un Rol o tipo? ¿a un usuario específico?
- ¿Sucedde siempre? ¿Sucedde solamente a veces o de manera aleatoria? ¿Sucedió una única vez? ¿Cuándo?
- ¿Bloquea algún proceso clave del negocio / para los usuarios finales?
- ¿Se puede mitigar con alguna manera alternativa?

Estas preguntas son esenciales para comprender la severidad de cada defecto, independientemente de la terminología utilizada. Las respuestas a estas interrogantes serán valiosas para el análisis detallado del defecto.

Por ejemplo, si un comportamiento inesperado afecta solo a usuarios con un rol específico, podrías investigar los permisos asignados a ese rol. Si el comportamiento inesperado ocurrió una sola vez en una fecha y hora específicas, podrías examinar eventos relacionados con el rendimiento del sistema en ese momento.