Para lograr el objetivo de forma segura, se pueden establecer los siguientes mecanismos y estrategias:

**Seguridad de la información**: es importante garantizar la seguridad de la información de los usuarios y las transacciones. Para ello, se deben utilizar técnicas de encriptación y autenticación, así como establecer políticas de seguridad claras y medidas de protección contra ataques externos.

**Pruebas de seguridad**: es importante realizar pruebas de seguridad regulares para identificar posibles vulnerabilidades en el sistema. Estas pruebas deben incluir pruebas de penetración y pruebas de vulnerabilidad.

**Gestión de acceso**: es importante establecer políticas claras de gestión de acceso y autenticación para los usuarios y el personal interno. Esto incluye la gestión de contraseñas, la autenticación multifactorial y el control de acceso basado en roles.

**Respaldo y recuperación**: es importante establecer un plan de respaldo y recuperación para garantizar la disponibilidad del sistema en caso de fallas o desastres. Esto incluye la realización de copias de seguridad regulares y la implementación de medidas de recuperación ante desastres.

**Auditoría y monitoreo**: es importante realizar auditorías y monitoreo regulares para detectar posibles problemas de seguridad o rendimiento. Esto incluye el monitoreo de logs y la implementación de herramientas de análisis de seguridad.

**Actualizaciones y parches**: es importante mantener el sistema actualizado con las últimas versiones de software y parches de seguridad. Esto incluye la implementación de procesos regulares de actualización y parcheo.

**Cultura de seguridad**: es importante fomentar una cultura de seguridad en todo el equipo, incluyendo la capacitación regular sobre prácticas de seguridad y la promoción de buenas prácticas en el desarrollo y el uso del sistema.

En resumen, para lograr el objetivo de forma segura, es importante establecer políticas claras y medidas técnicas adecuadas para garantizar la seguridad, la disponibilidad y el rendimiento del sistema. Además, es importante fomentar una cultura de seguridad en todo el equipo para garantizar la protección de la información y los usuarios del sistema.