**Pruebas (Evaluación de los prototipos y probadores)**

Para asegurarnos de que la solución de seguridad para taquillas funciona bien, hemos diseñado un plan de pruebas.

Primero, hacemos pruebas de resistencia y durabilidad, sometiendo la cerradura a miles de aperturas y cierres seguidos. Queremos comprobar que aguanta hasta 500,000 usos sin fallar. También la probamos en condiciones difíciles, como humedad, temperaturas extremas y vibraciones.

En la parte electrónica, usamos equipos automáticos para revisar que los circuitos y sensores funcionen bien en situaciones reales. Además, hacemos pruebas de interferencias para evitar problemas con otros dispositivos.

Las pruebas funcionales nos ayudan a comprobar que la cerradura se conecta bien con el software, gestionando accesos, monitoreo remoto y diferentes tipos de comunicación (RS-485, NFC, Bluetooth® y OSDP). También analizamos su seguridad frente a intentos de hackeo o manipulación física.

Por último, probamos el sistema con usuarios reales en gimnasios, oficinas y otros lugares. Así obtenemos comentarios y hacemos mejoras antes de lanzarlo al mercado.

Para definir las interacciones entre los distintos actores del sistema de seguridad de taquillas, hemos creado un diagrama de casos de uso UML que representa las funciones principales del sistema.

**Diagrama de Casos de uso**

1. Actores del Sistema
2. Usuario (Empleado/Cliente): Persona que utiliza la taquilla y necesita autenticarse para acceder a ella.
3. Administrador del Sistema: Responsable de la gestión de usuarios, configuración de credenciales y supervisión del sistema.
4. API de Terceros: Sistemas externos que pueden controlar accesos mediante la API REST.
5. Casos de Uso Identificados:
   1. Casos de Uso del Usuario:
      1. Autenticarse en la taquilla: El usuario se identifica con una tarjeta RFID, biometría o su dispositivo móvil.
      2. Abrir taquilla: Si la autenticación es válida, el sistema desbloquea la cerradura.
      3. Cerrar taquilla: El usuario puede cerrar la taquilla tras su uso, registrando el evento en el sistema.
      4. Solicitar soporte: En caso de problemas con el acceso, el usuario puede pedir asistencia.
   2. Casos de Uso del Administrador:
      1. Gestionar usuarios: Dar de alta o baja a los usuarios en la plataforma.
      2. Asignar credenciales: Configurar tarjetas RFID, datos biométricos o credenciales móviles.
      3. Monitorear accesos: Consultar registros de apertura/cierre y detectar posibles incidencias.
      4. Configurar horarios: Establecer horarios de acceso y restricciones según políticas de seguridad.
      5. Consultar bloqueos: Revisar taquillas bloqueadas o accesos fallidos por intentos no autorizados.
   3. Casos de Uso del API:
      1. Validar credenciales: Comprobar la autenticidad de los datos de acceso.
      2. Registrar eventos: Guardar en la base de datos cada apertura y cierre.
      3. Enviar alertas: Notificar al administrador en caso de intentos de acceso fallidos o actividades sospechosas.
      4. Actualizar cerraduras: Aplicar nuevas configuraciones de software y firmware a los dispositivos.

