|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre del caso de uso**  Registro de usuario | **Priority Level:**  Alta | | **Id:** 001 | **Version: 1.0** | |
| **Actores:**  Registro de usuario (usuario final) | | | | | |
| **Description:**  El usuario se registra proporcionando nombre, correo, contraseña con el propósito de crear una cuenta única para acceso y privacidad | | | | | |
| **Preconditions:**   * El usuario no debe estar registrado previamente en el sistema * El sistema debe estar operativo | | | | | |
| **Main Flow:**   1. El usuario accede a la página de registro 2. Ingresa su nombre, correo electrónico y contraseña 3. El sistema valida que el correo no exista previamente 4. El sistema almacena los datos y crea la cuenta 5. El sistema muestra un mensaje de confirmación de registro exitoso | | | | | |
| **Alternative Flow:**   * Si el correo ya existe el sistema notifica al usuario y solicita un correo diferente * Si hay un error de conexión el sistema muestra un mensaje de error y solicita entrar más tarde | | | | | |
| **Postconditions:**   * La cuenta del usuario queda creada y habilitada * El usuario puede iniciar sesión en el sistema | | | | | |
| **Business Rules:**  La contraseña debe cumplir políticas de seguridad  El correo debe ser único en la base de datos | | | | | |
| **Written by:**  Software Development Team | | **Responsible:**  Pedro Hernández López | | | **Date: 10/03/2025** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre del caso de uso**  gestión del sistema y mantenimiento de seguridad | **Nivel de Prioridad:**  Alta | | **Identificador:** 1 | **Versión:** 2.0 | |
| **Actores:**  Administrador del sistema | | | | | |
| **Descripción:**  El administrador monitorea la salud del sistema, realiza backups, maneja la seguridad y gestiona las actualizaciones | | | | | |
| **Precondiciones:**   1. El administrador debe estar autenticado en el sistema con permisos elevados 2. El sistema debe estar en funcionamiento para realizar acciones administrativas | | | | | |
| **Flujo Principal:**   1. El administrador inicia sesión en el panel de administración 2. Revisa los logs del sistema y el estado de los sensores conectados. 3. Realiza tareas de mantenimiento: limpieza de logs, revisión de espacio en la base de datos, actualizaciones 4. Programa y realiza copias de seguridad de la base de datos. 5. Revisa y aplica actualizaciones de seguridad. 6. Documenta las acciones realizadas para futuras auditorías. | | | | | |
| **Flujo Alternativo:**   * Si se detecta una vulnerabilidad critica, el administrador activa los protocolos de emergencia y notifica a los usuarios de posibles interrupciones * Si la copia de seguridad falla, se intenta de nuevo y se documenta el incidente | | | | | |
| **Postcondiciones:**   1. El sistema queda actualizado, con copias de seguridad recientes y funcionando correctamente 2. Los incidentes se documentan para control de calidad y auditoria | | | | | |
| **Reglas de Negocio:**   1. Las copias de seguridad se deben realizar al menos cada 24 horas 2. Las actualizaciones críticas de seguridad deben aplicarse de inmediato 3. Se deben mantener logs de actividad | | | | | |
| **Redactado por:**  Equipo de Desarrollo de Software | | **Responsable:**  Pedro Hernández López | | | **Fecha: 10/03/2025** |