**SISTEMA DE GESTIÓN DE DONANTES DE SANGRE**

**Especificación de Requisito:**

**SGDS-06**

**Seguridad de la información**

**Lima, abril del 2023**

**ÍNDICE**

[**1. Introducción 3**](#_heading=h.1fob9te)

[1.1 Propósito 3](#_heading=h.3znysh7)

[1.2 Alcance 3](#_heading=h.tyjcwt)

[1.3 Resumen 3](#_heading=h.1t3h5sf)

[**2. Descripción General 4**](#_heading=h.2s8eyo1)

[2.1 Diagrama de Casos de Usos 4](#_heading=h.17dp8vu)

[2.2 Descripción 4](#_heading=h.26in1rg)

[2.3 Actores 4](#_heading=h.35nkun2)

[2.4 Precondiciones 5](#_heading=h.2jxsxqh)

[2.5 Pos Condiciones 5](#_heading=h.1y810tw)

[2.6 Flujo Básico 5](#_heading=h.1ci93xb)

[2.7 Excepciones 6](#_heading=h.ihv636)

# Introducción

## Propósito

El propósito del requisito "SEGURIDAD DE LA INFORMACIÓN" es garantizar la protección de la información de los usuarios donantes y hospitales registrados en el sistema de donación de sangre en línea. El requisito busca asegurar que la información personal y médica de los usuarios sea manejada de manera segura y confidencial, evitando cualquier tipo de vulneración o uso inapropiado de la información.

## Alcance

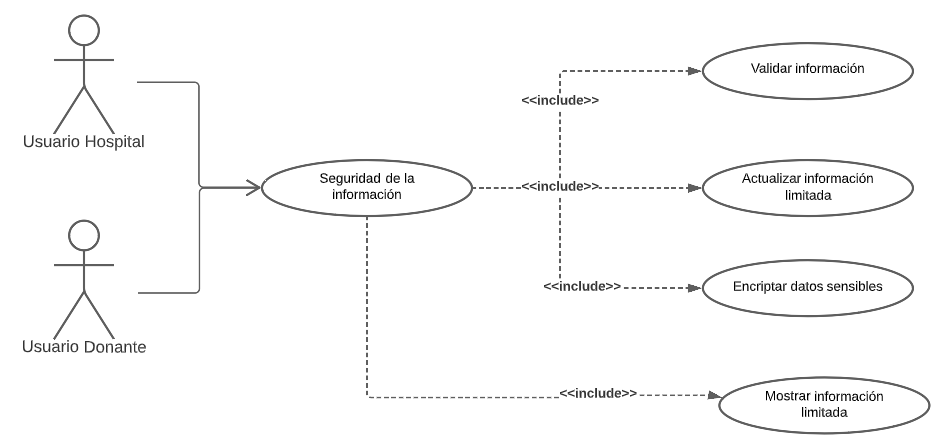
El requisito "SEGURIDAD DE LA INFORMACIÓN" se aplica a todos los datos almacenados en la base de datos del sistema de donación de sangre en línea, incluyendo la información personal y médica de los usuarios donantes y hospitales, así como cualquier otra información generada por el uso del sistema.

## Resumen

El requisito "SEGURIDAD DE LA INFORMACIÓN" se enfoca en garantizar la protección de la información de los usuarios del sistema de donación de sangre en línea. Para ello, se establecen medidas de seguridad para la gestión de la información, como la encriptación de datos, la gestión de contraseñas y el acceso limitado a la información.

# Descripción General

## Diagrama de Casos de Usos



**Figura 1. Prototipo del Caso de uso: CU007- Registro de Hospitales**

## Descripción

El requisito "SEGURIDAD DE LA INFORMACIÓN" establece medidas para proteger la información personal y médica de los usuarios donantes y hospitales registrados en el sistema de donación de sangre. Para ello, se deben establecer procedimientos de seguridad para la gestión de la información, como la encriptación de datos, la gestión de contraseñas y el acceso limitado a la información. Además, se deben establecer medidas para prevenir la pérdida, corrupción o alteración de la información almacenada en el sistema.

## Actores

* Usuario Donante: persona que accede al sistema para programar sus citas de donación de sangre y registrar sus datos personales y médicos.
* Usuario Hospital: entidad médica que accede al sistema para validar, gestionar y recompensar la donación de sangre y registrar la información correspondiente.

## Precondiciones

* El sistema de donación de sangre debe estar operativo y tener acceso a la base de datos.
* Los usuarios donantes y hospitales deben estar registrados en el sistema y contar con un perfil de usuario.

## Pos Condiciones

* La información personal y médica de los usuarios donantes y hospitales se encuentra protegida y segura.
* Se han establecido medidas de seguridad para prevenir la pérdida, corrupción o alteración de la información almacenada en el sistema.

## Flujo Básico

1. El sistema recibe la solicitud de registro de un Usuario Donante o Usuario Hospital.
2. El sistema valida la información proporcionada por el usuario para asegurarse de que cumple con los requisitos mínimos para el registro.
3. El sistema almacena la información del usuario en la base de datos, encriptando los datos sensibles (por ejemplo, contraseña) con técnicas de encriptación seguras.
4. El Usuario Donante o Usuario Hospital inicia sesión en el sistema.
5. El sistema verifica las credenciales del usuario y le concede acceso a las funciones correspondientes.
6. El Usuario Donante o Usuario Hospital puede ingresar, actualizar y eliminar su información personal.
7. El Usuario Donante puede programar una cita para la donación de sangre.
8. El Usuario Hospital puede validar y registrar la donación de sangre del Usuario Donante y entregar el beneficio correspondiente.
9. El sistema monitorea el acceso a los datos y registra todas las transacciones realizadas en la base de datos.
10. En caso de una violación de seguridad o intento de acceso no autorizado, el sistema notifica al administrador del sistema (desarrolladores).

## Excepciones

* EX[1]: Si un usuario no autorizado intenta acceder al sistema, se mostrará un mensaje de error y se registrará el intento en el registro de acceso del sistema.
* EX[2]: Si se produce una pérdida de datos debido a un fallo del sistema, se debe implementar un plan de contingencia para recuperar los datos perdidos y minimizar los daños.