CIFRAR CONTRASEÑAS Y DATOS SENSIBLES	
ACTORES Sistema biUNestar Base de datos del sistema	**REQUERIMIENTO** RF_5 – El sistema deberá cifrar contraseñas y datos sensibles utilizando algoritmos criptográficos estándar (por ejemplo, SHA-256).

DESCRIPCIÓN

Este caso de uso describe el proceso mediante el cual el sistema protege la información sensible de los usuarios, asegurando que contraseñas, correos institucionales y datos personales sean almacenados de forma cifrada e inaccesible para terceros.

PRECONDICIONES

El usuario debe haber ingresado o actualizado información que incluya datos sensibles.
El sistema debe contar con el módulo de seguridad habilitado.

FLUJO NORMAL

1. El usuario ingresa una contraseña o dato sensible (por ejemplo, al registrarse o cambiar contraseña).
2. El sistema recibe el dato y lo somete al algoritmo de cifrado definido (SHA-256).
3. El sistema genera un hash cifrado del dato.
4. El sistema almacena únicamente el hash en la base de datos, sin conservar el valor original.
5. En futuras autenticaciones, el sistema compara el hash ingresado con el almacenado para validar el acceso.
6. Si coinciden, se concede el acceso o se confirma la operación.
7. El sistema registra la transacción en el log de seguridad.

POSTCONDICIONES

Los datos sensibles quedan protegidos mediante cifrado irreversible.
El sistema mantiene la integridad y confidencialidad de la información almacenada.

NOTAS

Se recomienda aplicar un “salting” único por usuario para fortalecer la seguridad.
El sistema debe cumplir con la política institucional de protección de datos personales.

Cifrar contraseñas y datos sensibles

Contraseña

••••••••••

La aplicación cifrará las contraseñas y datos sensibles antes de almacenarlos.

Cifrar datos