



UNIVERSIDAD
NACIONAL
DE COLOMBIA

Universidad Nacional de Colombia - sede Bogotá
Facultad de Ingeniería
Departamento de Sistemas e Industrial
Curso: Ingeniería de Software 1 (2016701)

<CIFRAR CONTRASEÑAS DE USUARIO>

ACTORES

Sistema de gestion de usuarios

REQUISITO

RNF-05.2: El sistema debe cifrar la contraseña de cada nuevo usuario creado antes de almacenarlos en la base de datos, con el fin de evitar que usuarios malintencionados puedan obtener de manera directa esta información.

DESCRIPCIÓN

Este caso de uso describe el comportamiento del sistema de gestión de usuarios al momento de registrar una nueva cuenta. Antes de guardar la información del usuario en la base de datos, el sistema cifra la contraseña utilizando un algoritmo seguro (por ejemplo, SHA-256 o bcrypt). De esta manera, se garantiza la confidencialidad y protección de las credenciales de acceso ante posibles vulneraciones o accesos no autorizados.

PRECONDICIONES

- El usuario debe haber sido registrado correctamente en el sistema.
- El sistema debe tener implementado un módulo de cifrado activo.
- La base de datos debe estar disponible y operativa para registrar los datos del nuevo usuario.

FLUJO NORMAL

1. El sistema recibe los datos del nuevo usuario desde el formulario de registro (nombre, documento, correo electrónico, contraseña, etc.).
2. El sistema valida los campos ingresados, incluyendo el formato y longitud de la contraseña.
3. Antes de almacenar los datos, el sistema aplica un algoritmo de cifrado a la contraseña ingresada.
4. El sistema reemplaza el valor original de la contraseña por su versión cifrada (hash).
5. El sistema guarda los datos del nuevo usuario en la base de datos.
6. El sistema registra en el log la creación del usuario (sin almacenar la contraseña ni su hash).
7. El sistema confirma que el registro fue exitoso.

POSTCONDICIONES

- La contraseña del usuario se ha almacenado cifrada en la base de datos.
- Ningún usuario ni administrador puede visualizar contraseñas en texto plano.

- Se garantiza la integridad y confidencialidad de la información sensible

NOTAS

- El sistema no debe almacenar ni mostrar contraseñas en texto plano bajo ninguna circunstancia.
- El proceso de cifrado debe ser irreversible.
- Si el registro del usuario falla antes del cifrado, no debe guardarse ninguna información parcial en la base de datos.
- Este caso de uso se ejecuta de forma automática e interna cada vez que se crea un nuevo usuario.

MOCKUP

N/A