UNIVERSIDAD NACIONAL DE COLOMBIA

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

CU06: CAMBIAR CONTRASEÑA

ACTORES	**REQUERIMIENTO**
● Usuario autenticado ● Sistema FortiFile	RF-08 – El sistema debe permitir cambiar la contraseña actual, solicitando la contraseña anterior

DESCRIPCIÓN

Este caso de uso permite al usuario autenticado modificar su contraseña actual en FortiFile, previa validación de la contraseña existente y asegurando que la nueva cumpla con los criterios de seguridad establecidos. El objetivo es garantizar que solo el propietario de la cuenta pueda cambiarla y que la nueva contraseña refuerce la seguridad del sistema .

PRECONDICIONES

- El usuario debe tener una sesión activa en FortiFile (estar autenticado).
- El usuario conoce su contraseña actual.
- El sistema está en ejecución y es capaz de acceder al almacenamiento de credenciales para validar la contraseña existente.
- La interfaz debe mostrar la opción “Cambiar contraseña” dentro del perfil o menú de configuración de la cuenta.

FLUJO NORMAL

1. El usuario selecciona la opción “Cambiar contraseña” desde la interfaz de FortiFile.
2. El sistema muestra un formulario solicitando la contraseña actual.
3. El usuario ingresa la contraseña actual.
4. El sistema verifica que la contraseña ingresada coincide con la almacenada (comparación mediante bcrypt/ hash seguro).
   4.1. Si la contraseña actual es incorrecta, el sistema muestra un mensaje de error indicando “Contraseña actual incorrecta” y permite reintentar hasta un número de intentos razonable (ver Flujo Alternativo).
5. Si la contraseña actual es correcta, el sistema muestra campos para ingresar la nueva contraseña y su confirmación.
6. El usuario ingresa la nueva contraseña y la confirma.
7. El sistema valida que la nueva contraseña cumpla los criterios de seguridad

definidos en RN-03 (p. ej., mínimo 8 caracteres, al menos una mayúscula, un número y un símbolo) .

7.1. Si no cumple los criterios, el sistema muestra un mensaje específico indicando los requisitos faltantes (“La nueva contraseña debe tener al menos 8 caracteres, incluir una mayúscula, un número y un símbolo”) y permite reingresar.

8. Si la nueva contraseña cumple los requisitos, el sistema solicita confirmación final (por ejemplo, un botón “Confirmar cambio de contraseña”).

9. El usuario confirma la acción.

10. El sistema realiza las siguientes tareas:

    - Almacena la nueva contraseña de forma segura (hash bcrypt + sal, siguiendo PEP8 y patrones de Clean Code).

    - Invalida temporalmente cualquier credencial en memoria vinculada a la contraseña anterior si aplica (por ejemplo, tokens de sesión), de modo que se use la nueva contraseña en futuras validaciones.

    - Registra el evento “Cambio de contraseña” en la bitácora local, con timestamp y detalles mínimos necesarios (sin exponer la contraseña) .

11. El sistema muestra un mensaje de éxito: “Contraseña cambiada correctamente”.

12. El usuario permanece autenticado tras el cambio o, dependiendo de la política de seguridad, puede requerirse reingreso de la nueva contraseña para continuar (opcional, pero en este proyecto se mantiene la sesión activa para usabilidad).

13. Fin del caso de uso.

FLUJOS ALTERNATIVOS

- **4.a Intentos de contraseña actual fallidos**:

    - El sistema permite un número limitado de reintentos (por ejemplo, 3) para validar la contraseña actual.

    - Si se supera el límite:

        - Se muestra mensaje: “Demasiados intentos fallidos. Por favor, inténtelo más tarde.”

        - Opcionalmente, se podría requerir re-login completo o bloquear temporalmente la función de cambio de contraseña según política de seguridad local.

        - Se registra el evento de intentos fallidos en la bitácora.

        - Se termina el caso de uso sin cambiar la contraseña.

- **7.a Nueva contraseña no coincide en confirmación**:

    - Si la confirmación no coincide con la nueva contraseña ingresada, el

sistema indica “Las contraseñas no coinciden” y vuelve al paso de ingreso de nueva contraseña.

- **Usuario cancela**:
    - En cualquier punto antes de la confirmación final, el usuario puede cancelar; el sistema abandona el cambio y retorna a la pantalla previa sin modificar la contraseña ni registrar evento de éxito.
- **Error de sistema o almacenamiento**:
    - Si al intentar guardar la nueva contraseña ocurre un error interno (p. ej., fallo en acceso a base de datos SQLite), el sistema muestra “Error al cambiar contraseña. Intente de nuevo más tarde” y registra el error en log de incidentes. Se puede ofrecer volver a intentar o contactar soporte.

POSTCONDICIONES

- La contraseña del usuario ha sido actualizada en el sistema de forma segura.
- Cualquier clave o token dependiente de la contraseña anterior ha sido invalidado si procede.
- Se ha registrado el evento de cambio de contraseña en la bitácora local .
- El usuario continúa con sesión activa (o, si la política requiere reautenticación, se redirige a ingresar la nueva contraseña).
- La nueva contraseña se utilizará para futuros inicios de sesión y validaciones.

NOTAS

- **Reglas de negocio relevantes**:
    - RN-04 – Verificación de contraseña en cambios: se exige la contraseña anterior para autorizar el cambio .
    - RN-03 – Contraseña segura obligatoria: la nueva debe cumplir con criterios de complejidad y longitud .
    - RN-09 – Registro de eventos críticos: debe registrarse el cambio exitoso y los intentos fallidos de validación .
    - RN-07 – Acceso exclusivo: solo el usuario autenticado puede invocar este caso de uso.
- **Consideraciones de seguridad**:
    - No mostrar la contraseña en texto claro en la interfaz (usar campos enmascarados).
    - Limitar la exposición de información sobre si la contraseña anterior es correcta o no de forma detallada a fin de evitar enumeración.

    - Gestionar bloqueo temporal si hay múltiples intentos fallidos para mitigar ataques por fuerza bruta.

    - Asegurar que el almacenamiento de la nueva contraseña use bcrypt + sal y que se siga PEP8 y principios de Clean Code en la implementación.

- **Interfaz y retroalimentación visual**:

    - Mensajes claros para cada error o éxito, indicando qué se requiere o informando del resultado.

    - Incluir indicadores de fortaleza de contraseña en el formulario para ayudar al usuario a elegir una contraseña robusta.

- **Interacción con otras funcionalidades**:

    - Después de cambiar contraseña, si existen procesos en segundo plano ligados a la cuenta (por ejemplo, cifrado/descifrado en curso), garantizar que no haya inconsistencias al validar credenciales en curso.

    - Considerar si se notifica al log de eventos sobre la necesidad de reingresar credenciales para operaciones críticas posteriores.

- **Referencias de plantilla**: La estructura de este caso de uso sigue la Plantilla de la asignatura de Ingeniería de Software 1