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

CU07: ELIMINAR CUENTA Y REINICIAR FORTIFILE

ACTORES

- Usuario autenticado

REQUERIMIENTO

RF-10 – El sistema debe permitir eliminar la cuenta local, previo ingreso de la contraseña actual.

RF-13 – El sistema debe permitir restablecer FortiFile a su estado inicial eliminando usuario, archivos y configuraciones.

RN-02 – Al eliminar la cuenta, también se eliminan todos los archivos, configuraciones y registros asociados.
Estos requerimientos y reglas de negocio se detallan en la especificación del proyecto FortiFile

DESCRIPCIÓN

Este caso de uso permite al usuario autenticado eliminar permanentemente su cuenta en FortiFile, lo cual implica borrar todas las claves, credenciales, archivos cifrados, registros y configuraciones asociadas, dejando la aplicación en su estado inicial (sin cuenta registrada). Antes de proceder, se solicita al usuario confirmar la operación mediante la contraseña actual, garantizando que solo el propietario de la cuenta pueda realizar esta acción irreversible. Tras la eliminación, FortiFile se comporta como en una instalación nueva, permitiendo registrar una nueva cuenta si así se desea

PRECONDICIONES

- El usuario debe tener una sesión activa en FortiFile (estar autenticado).
- El sistema debe disponer del mecanismo para validar la contraseña actual contra la almacenada de forma segura (bcrypt + hash).
- La aplicación debe estar en estado en que existe una cuenta registrada localmente.
- No deben existir procesos críticos en curso que impidan la eliminación inmediata de datos (o, en caso de existir, el sistema debe manejar su cancelación o finalizar de forma segura).

FLUJO NORMAL

1. El usuario accede a la opción “Eliminar cuenta” o “Reiniciar FortiFile” desde la interfaz de configuración o menú de usuario.

2. El sistema muestra un mensaje de advertencia clara sobre la acción irreversible: “Eliminar cuenta borrará todos los archivos cifrados, configuraciones y registros. Esta acción no se puede deshacer. ¿Desea continuar?”

3. El usuario confirma que desea continuar.

4. El sistema solicita la contraseña actual para confirmar la identidad del usuario.

5. El usuario ingresa su contraseña actual.

6. El sistema valida la contraseña:

   6.1. Si la contraseña es incorrecta, se muestra “Contraseña incorrecta” y se permite reintentar hasta un número limitado de intentos (ver flujo alternativo).

7. Si la contraseña es correcta, el sistema solicita confirmación final (por ejemplo, escribiendo “ELIMINAR” o pulsando un botón de confirmación definitiva).

8. El usuario confirma la acción irreversible.

9. El sistema realiza las siguientes tareas en secuencia:

   - Invalida la sesión actual del usuario.

   - Elimina de la base de datos SQLite todas las entradas relacionadas con la cuenta (credenciales, metadatos).

   - Borra permanentemente del sistema de archivos todos los archivos cifrados y temporales asociados a la cuenta.

   - Elimina configuraciones y registros (bitácora local) asociados a esta cuenta.

   - Registra (antes de borrarse) en la bitácora local un evento de “Eliminación de cuenta” con timestamp, sin incluir datos sensibles (la bitácora puede almacenarse temporalmente hasta guardarse en un log externo si se requiere, o bien omitirse tras la eliminación completa, según política; pero el evento debe registrarse según RN-09 antes de la eliminación física) .

   - Restablece el estado interno de la aplicación a valores iniciales: sin usuario registrado, con base de datos limpia o recreada según diseño.

10. El sistema muestra la pantalla inicial de FortiFile, indicando que la cuenta y todos los datos han sido eliminados y que puede registrarse una nueva cuenta.

11. Fin del caso de uso.

FLUJOS ALTERNATIVOS

- **6.a Intentos de contraseña incorrectos**:

  - El sistema permite un número limitado de reintentos (por ejemplo, 3 intentos).

  - Si se supera el límite:

        - Se muestra mensaje: “Demasiados intentos fallidos. Operación cancelada.”
        - Se registra el evento de intentos fallidos en la bitácora local (sin revelar contraseña).
        - El caso de uso termina sin eliminar la cuenta y retorna a la pantalla previa.

- **2.a Usuario cancela en advertencia inicial**:
    - Si, tras ver la advertencia, el usuario decide no continuar, el sistema abandona la operación y retorna a la pantalla anterior sin cambios.
- **8.a Usuario cancela en confirmación final**:
    - Si el usuario no confirma definitivamente (por ejemplo, no escribe la palabra “ELIMINAR” o cancela), se detiene el proceso y no se elimina nada.
- **Procesos críticos en curso**:
    - Si existen operaciones en curso (p. ej., cifrado/descifrado activo, transferencia o respaldo temporal), el sistema notifica al usuario y ofrece:
        - Esperar a que terminen con éxito o cancelarlos de forma segura.
        - Solo tras resolverse estos, proceder con la eliminación.
    - Si el usuario opta por cancelar dichos procesos, el sistema los finaliza de forma segura y continua con el flujo de eliminación.
    - Si el usuario decide no cancelar procesos, el caso de uso se aborta.
- **Error de sistema al eliminar datos**:
    - Si al intentar borrar archivos o entradas en la base de datos ocurre un error (p. ej., fallo I/O o corrupción de base), el sistema muestra “Error al eliminar datos. Intente de nuevo más tarde o contacte soporte.”
    - Registra el error detallado en bitácora de incidentes.
    - Dependiendo de la gravedad, puede quedar en un estado intermedio: en ese caso, el sistema debe intentar restaurar consistencia o, si no es posible, informar claramente al usuario y bloquear parcialmente la aplicación hasta resolución manual.

POSTCONDICIONES

- No existe cuenta registrada en FortiFile.
- Todos los datos asociados (archivos cifrados, configuraciones, registros) han sido borrados permanentemente.

- La base de datos SQLite se ha reiniciado o recreado en estado inicial vacío.
- La sesión del usuario ha sido invalidada.
- El sistema inicia en pantalla de registro de nueva cuenta, listo para operación como instalación limpia.
- Se ha registrado el evento de eliminación de cuenta (antes de la eliminación física), cumpliendo RN-02 y RN-09

NOTAS

- **Reglas de negocio**:
    - RN-01: Solo una cuenta por instalación; tras eliminación, se permite crear otra.
    - RN-02: Eliminación de cuenta reinicia el sistema, eliminando todos los datos asociados .
    - RN-11: No se permite editar nombre de usuario; en este caso, se elimina por completo si el usuario así lo desea.
    - RN-09: Antes de borrar el log completo, registrar el evento de eliminación.
- **Seguridad**:
    - Asegurar que la contraseña se verifica mediante hash seguro (bcrypt) sin exponer datos.
    - Confirmaciones claras para evitar eliminaciones accidentales.
    - No dejar datos residuales en caché o temporales tras la operación.
- **Usabilidad**:
    - Mensajes claros en la interfaz sobre la irreversibilidad de la operación.
    - Posibilidad de guiar al usuario con pasos intermedios si hay procesos en curso.
- **Implementación técnica**:
    - La eliminación de archivos cifrados debe usar métodos seguros de borrado si el SO lo permite, o bien sobrescribir antes de borrar, según política de seguridad local.
    - La base de datos SQLite puede descartarse y recrearse o bien vaciar tablas clave; se recomienda recrear para evitar inconsistencias.
    - Manejar excepciones I/O y asegurar consistencia en caso de fallos parciales.
- **Interacción con otros casos de uso**:

    - Tras eliminación, se deshabilitan temporalmente funcionalidades de gestión de archivos hasta que se registre nueva cuenta (pasar a CU01).
    - Cualquier proceso programado para respaldo local, cifrado o limpieza debe cancelarse o reiniciarse tras la eliminación.

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