



UNIVERSIDAD
NACIONAL
DE COLOMBIA

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

CU11 – DESCARGAR Y DESCIFRAR ARCHIVO

ACTORES

- Sistema FortFile
- Usuario Autenticado

REQUERIMIENTO

RF-06 – El sistema debe permitir al usuario descargar sus archivos y descifrarlos localmente de forma segura.

DESCRIPCIÓN

Este caso de uso describe el proceso por el cual un usuario puede recuperar uno de sus archivos previamente almacenados, aplicando un proceso de descifrado controlado que garantiza la confidencialidad y la integridad de la información. La funcionalidad se desarrolla en modo completamente local, sin depender de servicios externos, y está diseñada para ofrecer seguridad sin sacrificar la usabilidad.

PRECONDICIONES

- El usuario debe haber iniciado sesión correctamente.
- Debe existir al menos un archivo previamente cifrado y almacenado.
- La clave de descifrado del usuario debe estar disponible en memoria tras la autenticación.

FLUJO NORMAL

1. El usuario accede a la sección “Mis archivos” desde la interfaz principal.
2. El usuario selecciona uno de los archivos listados y elige la opción “Descargar”.
3. El sistema solicita una carpeta de destino en el dispositivo del usuario.
4. **Si el usuario elige una carpeta válida:**
 - a. El sistema recupera el archivo cifrado desde el almacenamiento interno.
 - b. Se accede a la clave de descifrado correspondiente al usuario actual (asociada desde su sesión).
 - c. El sistema aplica el algoritmo de descifrado (por ejemplo, AES) para convertir el archivo a su estado original.
 - d. El archivo descifrado se guarda en la ubicación seleccionada.
 - e. El sistema informa al usuario que la descarga ha finalizado exitosamente.
5. **Si el usuario cancela la selección de carpeta o esta no es válida:**
 - a. El sistema aborta la operación de descarga.
 - b. Se muestra un mensaje explicativo y se vuelve al listado de archivos.
6. **Si ocurre un error durante el proceso de descifrado (ej. clave corrupta, archivo dañado):**
 - a. El sistema notifica al usuario con un mensaje claro sobre la falla.
 - b. Se registra el error en el log de eventos para análisis posterior.
 - c. El sistema no guarda ningún archivo incompleto.

7. Tras completar el proceso (éxito o error), el sistema permanece disponible para nuevas acciones.

POSTCONDICIONES

- El archivo ha sido descifrado y descargado correctamente en el dispositivo del usuario, o la operación ha sido cancelada o fallida sin comprometer la seguridad.
- Se ha registrado la operación (exitosa o no) en el log del sistema.

NOTAS

- El archivo se descifra exclusivamente en memoria y solo se guarda una vez completado el proceso.
- El sistema no conserva versiones descifradas en segundo plano para evitar filtraciones accidentales.
- Todas las operaciones se realizan en entorno local y no dependen de conexión a internet ni servidores externos.
- El descifrado solo es posible durante una sesión activa y válida; fuera de ella, las claves no están disponibles.