UNIVERSIDAD NACIONAL DE COLOMBIA

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

CU04: BLOQUEAR ACCESO TRAS INTENTOS FALLIDOS	
ACTORES ● Usuario visitante ● Sistema FortiFile	**REQUERIMIENTO** RN-05 – Si se introducen 5 contraseñas incorrectas consecutivas al iniciar sesión, el sistema debe bloquear temporalmente el acceso.

DESCRIPCIÓN

Este caso de uso describe el mecanismo de seguridad que aplica FortiFile cuando un usuario registrado intenta iniciar sesión con credenciales incorrectas en múltiples ocasiones consecutivas. El sistema lleva un registro de intentos fallidos y, al alcanzar el límite definido, activa un bloqueo temporal para prevenir accesos no autorizados.

PRECONDICIONES

- Debe existir una cuenta registrada en el sistema.
- El usuario ha intentado iniciar sesión sin éxito previamente.

FLUJO NORMAL

1. El usuario intenta iniciar sesión ingresando credenciales incorrectas.
2. El sistema verifica las credenciales y determina que no son válidas.
3. El sistema incrementa el contador de intentos fallidos.
4. El sistema muestra un mensaje de error e informa cuántos intentos fallidos van acumulados.
5. Si el contador llega a 5 intentos fallidos consecutivos:
    - El sistema bloquea temporalmente el acceso al formulario de inicio de sesión.
    - Muestra un mensaje indicando que el sistema está bloqueado por seguridad.
    - Se inicia una cuenta regresiva o se establece un tiempo de espera (por ejemplo, 5 minutos).

6. Una vez transcurrido el tiempo de bloqueo, el sistema habilita nuevamente el formulario de inicio de sesión.

7. El contador de intentos fallidos se reinicia.

POSTCONDICIONES

- El sistema queda temporalmente bloqueado si se superó el número de intentos permitidos.
- El evento de bloqueo se registra en el log del sistema.
- El contador se reinicia al completarse el periodo de espera o tras un inicio de sesión exitoso posterior

NOTAS

- El tiempo de bloqueo puede ser definido por configuración del sistema (por ejemplo, 5 o 10 minutos).
- Esta medida está diseñada para mitigar ataques de fuerza bruta locales.
- No se permite recuperación de contraseña en esta versión, por lo que el usuario debe recordar su clave

REGISTRAR NUEVO USUARIO

ACTORES	**REQUERIMIENTO**
Usuario visitante Sistema de gestión de usuarios	RF_01 – El sistema debe permitir a un usuario no registrado crear una cuenta ingresando sus datos personales y de acceso.

DESCRIPCIÓN

Este caso de uso permite que un usuario no registrado cree una cuenta nueva en el sistema. El proceso implica la recopilación de información básica y la validación de los datos ingresados, incluyendo correo electrónico y contraseña. Una vez completado, el sistema almacena los datos y envía un mensaje de confirmación.

PRECONDICIONES

- El usuario no debe tener una sesión activa en el sistema o El sistema debe estar disponible y con acceso al módulo de gestión de usuarios.

FLUJO NORMAL

1. El usuario accede a la opción "Registrarse" desde la pantalla principal.
2. El sistema muestra el formulario de registro.
3. El usuario completa los campos requeridos: nombre, correo electrónico, y contraseña como mínimo, los demás campos son opcionales.
4. El sistema valida los datos ingresados.
    a. Si el usuario deja campos obligatorios sin completar, el sistema muestra un mensaje de error indicando qué campos faltan y no permite continuar.
    → Vuelve a punto 3
5. El sistema verifica que el correo electrónico no esté previamente registrado.
    a. Si el correo electrónico ingresado ya está registrado, el sistema muestra un mensaje de advertencia y ofrece la opción de **{ Recuperar contraseña }**.
6. **{ Validar formato de campos }**.
7. El sistema guarda la nueva cuenta en la base de datos.
8. El sistema envía un correo de verificación.
9. El sistema informa al usuario que debe verificar su cuenta.
10. **{ Confirmar cuenta por correo electrónico }**

POSTCONDICIONES

Se ha creado un nuevo usuario en estado “pendiente de verificación”.
Se ha enviado un correo electrónico con el enlace de activación.
Se ha registrado la transacción en el log de usuarios.

NOTAS

- El correo electrónico es el identificador único del usuario en el sistema.
- Este caso de uso se puede invocar desde diferentes puntos, como el flujo de compra si el usuario intenta realizar una acción que requiere autenticación.
- La contraseña debe cumplir con los requisitos definidos por el área de seguridad. Adjunto documento de especificaciones