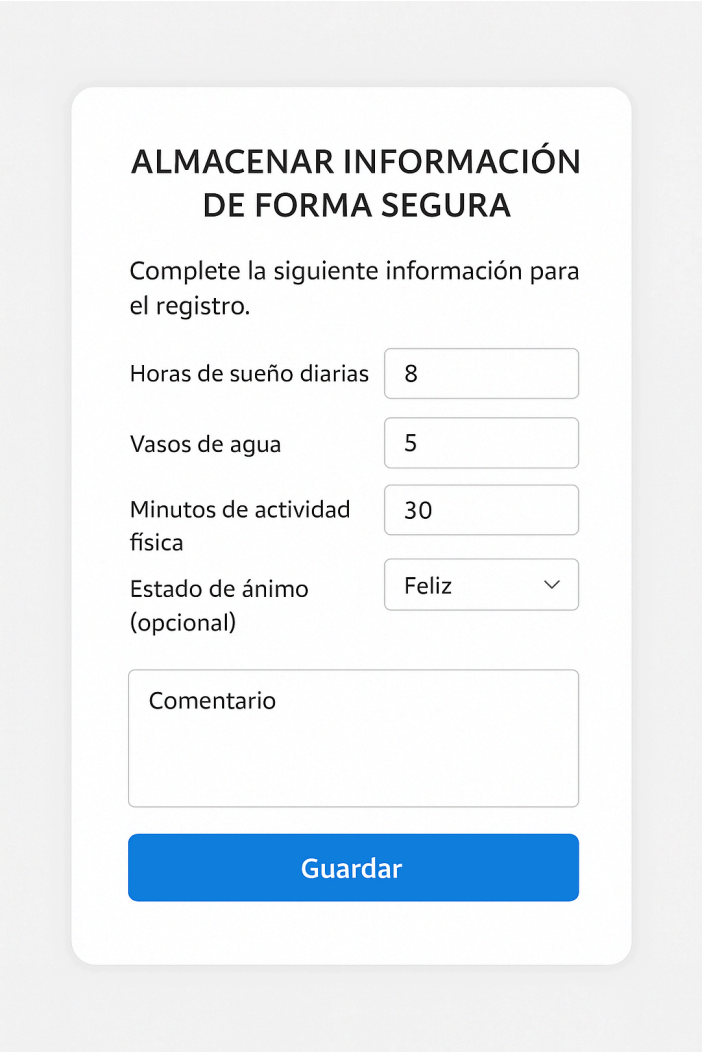
Universidad Nacional de Colombia - sede Bogotá
Facultad de Ingeniería
Departamento de Sistemas e Industrial
Curso: Ingeniería de Software 1 (2016701)

ALMACENAR INFORMACIÓN DE FORMA SEGURA	
ACTORES ● Administrador ● Usuario final ● Sistema de Bases de Datos	**REQUISITO** ● RF_1 – Permite el acceso controlado previo al almacenamiento de información. ● RF_5 – Complementa la seguridad de la información almacenada (protege datos sensibles). ● RF_8 – Garantiza que la información almacenada pueda mantenerse íntegra y actual.
DESCRIPCIÓN En este caso de uso, se espera que el sistema procese y almacene de forma segura la información generada por los usuarios (como datos personales, hábitos y registros diarios) en una base de datos protegida. El sistema debe validar la autenticación del usuario antes de guardar cualquier dato, aplicar los mecanismos de cifrado definidos y confirmar que la información se haya almacenado correctamente, garantizando su confidencialidad e integridad.	
PRECONDICIONES ● El usuario debe estar autenticado en el sistema (sesión iniciada). ● La base de datos debe estar disponible y conectada. ● El sistema debe tener definidos los métodos de cifrado para los datos sensibles.	
FLUJO NORMAL ● Usuario: Usuario autenticado accede a la funcionalidad de envío/registro de datos (p. ej. guarda perfil o registra hábitos). ● Sistema: Verifica que la sesión del usuario sea válida (token/ sesión activa). ● Sistema: Comprueba la disponibilidad de la base de datos y abre una conexión/transacción. ● Usuario: Envía los datos a almacenar (campos correspondientes: personales, hábitos, comentario de estado de ánimo, etc.). ● Sistema: Valida formato y rangos de los datos recibidos (ej. horas 0–24, número entero para vasos, longitud máxima de texto). ● Sistema: Rechaza cualquier dato inválido; si todo es válido, procede. (en el caso feliz no ocurre rechazo) ● Sistema: Aplica transformaciones necesarias (normalización de texto, timestamp de registro, asociación al ID del usuario). ● Sistema: Para los datos sensibles (p. ej. contraseñas, información clasificable),	

genera salt/nonce y aplica el algoritmo de hashing/cifrado configurado (p. ej. bcrypt o Argon2 para contraseñas; cifrado simétrico si corresponde para otros campos).
- Sistema: Inserta/actualiza los registros dentro de la transacción en la base de datos (operación ACID).
- Sistema: Registra un evento de auditoría / log seguro que indique la operación realizada (usuario, tipo de operación, timestamp, resultado) sin almacenar datos sensibles en texto plano.
- Sistema: Confirma la persistencia exitosa (commit de la transacción).
- Sistema: Realiza acciones post-persistencia programadas: notificar subsistemas interesados (generador de reportes, indexador, cola para backups) y, si aplica, encolar copia para respaldo automático.
- Sistema: Envía confirmación al usuario (mensajería en UI y/o notificación), indicando que los datos fueron guardados correctamente.
- Sistema: Cierra la conexión de base de datos y libera recursos.
- Sistema (continuo): Copia de seguridad y/o replicación realiza su trabajo según el plan (backup/replicación configurada), garantizando disponibilidad y resiliencia.

POSTCONDICIONES
- La información del usuario se almacena correctamente en la base de datos.
- Los datos sensibles quedan cifrados y no pueden visualizarse en texto plano.
- Se registra (o se puede registrar) una confirmación de almacenamiento exitoso o un log del evento.

NOTAS
- Este caso de uso aplica a todos los módulos que impliquen persistencia de datos (registro, hábitos, contraseñas, comentarios, etc.).
- Las contraseñas nunca se almacenan en texto plano; deben cifrarse con un algoritmo de hashing seguro (p. ej. bcrypt o Argon2).
- La conexión entre el cliente y el servidor debe realizarse mediante protocolo HTTPS para proteger la transmisión de datos.
- En caso de error de conexión o pérdida de integridad, el sistema debe generar un log y mostrar un mensaje genérico al usuario (sin revelar detalles técnicos).
- La base de datos debe contar con copias de seguridad automáticas y control de acceso por roles.
- Este proceso puede invocar servicios internos de auditoría o monitoreo para registrar intentos de escritura y detectar anomalías.
- Si el almacenamiento falla, el sistema no debe confirmar éxito al usuario, y la transacción debe revertirse (rollback).


ALMACENAR INFORMACIÓN DE FORMA SEGURA
Complete la siguiente información para el registro.
Horas de sueño diarias
8
Vasos de agua
5
Minutos de actividad física
30
Estado de ánimo (opcional)
Feliz
Comentario
Guardar