Plan de Pruebas de testing

Fase 1: Pruebas unitarias de cada módulo

- **Objetivo**: Validar la funcionalidad de cada módulo individualmente, asegurando que cada componente básico (Reporte, Usuario, Publicación) funcione conforme a los requisitos sin dependencias de otros módulos.
- **Actividades**:
    - **Creación**: Verificar que se pueda crear un nuevo registro en cada módulo, con pruebas específicas para campos obligatorios y opcionales.
    - **Lectura**: Comprobar que los datos almacenados en cada módulo puedan ser consultados y devueltos correctamente, validando la exactitud y consistencia de la información.
    - **Actualización**: Probar la capacidad de actualizar registros existentes, asegurando que los cambios se reflejan adecuadamente sin afectar otros datos.
    - **Eliminación**: Confirmar que los registros puedan eliminarse sin dejar referencias inconsistentes en la base de datos.
    - **Validación de campos**: Realizar pruebas específicas para validar que cada campo cumple con las restricciones establecidas (por ejemplo, validaciones de tipo, longitud, y valores permitidos).

Fase 2: Pruebas de integración para verificar interacciones

- **Objetivo**: Asegurar que los módulos Reporte, Usuario y Publicación interactúen correctamente entre sí, manteniendo consistencia y exactitud en la información compartida entre estos componentes.
- **Actividades**:
    - **Asociación de reportes**: Verificar que los reportes asociados a publicaciones y usuarios se actualicen correctamente en todos los

módulos, afectando campos como reportsCount y lastReportDate en el módulo de Publicación y Usuario.

- **Consistencia de datos**: Comprobar que las actualizaciones o eliminaciones en el módulo de Reporte se reflejan adecuadamente en Usuario y Publicación, especialmente cuando un reporte es sobre una publicación o usuario específico.
- **Flujo de reportes y estado de cuenta**: Validar que el módulo de Usuario refleja correctamente cambios en accountStatus según la cantidad de reportes recibidos, probando el bloqueo o limitación de funciones para cuentas con estados suspendidos o baneados.
- **Simulación de interacciones comunes**: Realizar pruebas de flujo en las que un usuario reporta una publicación o usuario y confirmar que estas interacciones mantienen integridad en todos los módulos afectados.

Fase 3: Pruebas de sistema para evaluar el comportamiento general

- **Objetivo**: Evaluar el sistema como un todo, asegurando que cada módulo y su funcionalidad trabajan en armonía en un entorno similar a producción.
- **Actividades**:
  - **Validación del flujo completo**: Ejecutar casos de uso completos que simulen escenarios reales, como un usuario que crea una publicación, otro usuario que reporta dicha publicación, y un administrador que revisa y resuelve el reporte.
  - **Pruebas de acceso y usabilidad**: Asegurar que los flujos de usuario son intuitivos y que cada rol (usuario común, administrador) tiene el acceso y las restricciones apropiadas según el estado de cuenta.
  - **Pruebas de visualización y permisos**: Probar que la visibilidad de publicaciones funciona correctamente y que los usuarios acceden o quedan limitados según su accountStatus o configuración de visibility en publicaciones.
  - **Evaluación de registros de auditoría**: Verificar que las acciones importantes (como la creación de reportes, cambios de estado en

usuarios) son registradas adecuadamente en los logs, facilitando la auditoría y rastreo.

Fase 4: Pruebas de rendimiento y seguridad

- **Objetivo**: Asegurar que el sistema mantiene un rendimiento adecuado y protege la información ante accesos no autorizados.
- **Actividades**:
    - **Pruebas de carga**: Simular un alto volumen de solicitudes para validar que el sistema responde eficientemente bajo diferentes niveles de demanda, enfocándose en operaciones intensivas como creación y consulta de reportes.
    - **Pruebas de escalabilidad**: Evaluar cómo el sistema se comporta al aumentar la cantidad de usuarios, publicaciones y reportes, midiendo tiempos de respuesta y consumo de recursos.
    - **Pruebas de seguridad**:
        - **Autenticación y autorización**: Verificar que solo usuarios autenticados y con permisos adecuados puedan acceder, crear, actualizar o eliminar reportes, usuarios y publicaciones.
        - **Protección contra vulnerabilidades**: Realizar pruebas de seguridad para detectar y prevenir amenazas como inyecciones de código, ataques de fuerza bruta, y otras vulnerabilidades conocidas.
        - **Cifrado de datos sensibles**: Asegurar que la información sensible, como contraseñas y datos de identificación, esté adecuadamente cifrada tanto en tránsito como en reposo.
    - **Monitoreo y recuperación**: Evaluar la capacidad del sistema para monitorear actividades y recuperarse de fallos, incluyendo la implementación de alertas y medidas de recuperación ante errores críticos o intentos de acceso no autorizado.

ID	Modulo	Caso de Prueba	Precondiciones	Entradas	Resultados Esperados.
TC01	Reporte	Crear reporte con todos los datos	Usuario autenticado	Reportad, reporterUserld, reporterUserld, postld, reportReason	Reporte creado exitosamente
TC02	Usuario	Cambiar estado de cuenta a “suspendida”	Usuario con permisos de administrador	Userld, accountStatus: suspendida	Estado actualizado, usuario limitado
TC03	Publicación	Crear publicación publica	Usuario autenticado	Postld, authorld, content, Visibility: Publica	Publicación accesible para todos los usuarios
TC04	Reporte	Verificar duplicados de reportes en 24h	Reporte creado en las últimas 24h	reporterUserld, reportedUserld, postld	Rechazar creación duplicada del reporte
TC05	Usuario	Verificar recuento de reportes recibidos	-	reportsReceived, lastReportDate	Contador de reportes actualizado correctamente.