



# ELICITACIÓN INICIAL DE REQUISITOS

## Descripción breve

En este documento podrá encontrar todos los requisitos iniciales detectados, además de un conjunto de preguntas respecto a ciertos requisitos que han ido surgiendo en su elicitación.

Equipo de Desarrolladores

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

ID	Tipo	Descripción	Prioridad
RF01	Funcional	El sistema debe permitir el registro seguro de usuarios (validaciones, verificación por email, captcha/antiexploit).	A
RF02	Funcional	El sistema debe permitir la autenticación de usuarios mediante usuario y contraseña, aplicando el patrón RBAC (roles: administrador, creador, VIP, estándar).	A
RF03	Funcional	El sistema debe aplicar una política de contraseñas seguras ( $\geq 8$ caracteres, blacklist, evitar datos personales, verificación en brechas, no reutilizar últimas 5).	A
RF04	Funcional	El sistema debe incluir un mecanismo de recuperación de contraseñas seguro (token hashado, caducidad 10 min).	A
RF05	Funcional	El sistema debe soportar autenticación multifactor (2FA y 3FA). La 3FA será obligatoria para administradores y creadores, opcional para usuarios VIP y estándar.	A
RF06	Funcional	El sistema debe defenderse contra ataques de diccionario y credential stuffing mediante rate limiting adaptativo, backoff exponencial y verificación de contraseñas filtradas.	A
RF07	Funcional	El sistema debe almacenar las contraseñas aplicando hashing seguro (Argon2id/bcrypt + pepper) y comparación constante.	A
RF08	Funcional	Los usuarios deben poder gestionar su perfil personal (nombre, avatar, preferencias, controles parentales).	M
RF09	Funcional	Los usuarios deben poder gestionar su suscripción (alta, baja, cambio a VIP/Estándar, historial).	M
RF10	Funcional	Los usuarios deben poder reproducir contenidos multimedia en streaming seguro.	A

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

<b>RF11</b>	Funcional	Los usuarios deben poder valorar los contenidos (una valoración por título, editable).	M
<b>RF12</b>	Funcional	Los usuarios deben poder crear y gestionar listas de reproducción.	A
<b>RF13</b>	Funcional	Los usuarios deben poder marcar contenidos como favoritos.	M
<b>RF14</b>	Funcional	Los administradores deben poder modificar, consultar, bloquear/desbloquear y eliminar usuarios.	A
<b>RF15</b>	Funcional	Sólo los administradores deben poder crear otros administradores.	M
<b>RF16</b>	Funcional	Los administradores deben tener acceso en modo “solo lectura” a los contenidos gestionados por los creadores.	B
<b>RF17</b>	Funcional	Los creadores de contenido deben poder cargar y gestionar archivos multimedia (validación MIME, límite de tamaño, escaneo antivirus opcional).	A
<b>RF18</b>	Funcional	Los creadores de contenido deben poder gestionar la disponibilidad de los contenidos (fechas, regiones, tipo de usuario).	A
<b>RF19</b>	Funcional	Los creadores de contenido deben poder consultar estadísticas de reproducción.	M
<b>RF20</b>	Funcional	Los creadores de contenido deben poder consultar las valoraciones de los usuarios.	M
<b>RF21</b>	Funcional	El sistema debe incluir un módulo de gestión de usuarios accesible únicamente por administradores.	A
<b>RF22</b>	Funcional	El sistema debe registrar y auditar los eventos críticos (login, cambios de permisos, cargas de contenido).	A
<b>RF23</b>	Funcional	El sistema debe implementar mecanismos de gestión y control de sesión: cookies seguras (HttpOnly, Secure, SameSite), rotación tras login o privilegios, idle timeout (15–30 min) y absolute timeout (6–12 h).	A

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

<b>RF24</b>	Funcional	El sistema debe endurecer frontend y backend aplicando validación de entrada, codificación de salida, gestión de errores genéricos y rate limiting en endpoints sensibles.	A
<b>RF25</b>	Funcional	El sistema debe proporcionar un sistema de recomendaciones y alertas de contenido según las preferencias del usuario.	B
<b>RF26</b>	Funcional	El sistema debe estar disponible en versión móvil (nativa o PWA).	A
<b>RNF01</b>	No Funcional	El sistema debe desarrollarse en Java usando Spring Framework.	A
<b>RNF02</b>	No Funcional	El sistema debe utilizar MongoDB como gestor de base de datos.	A
<b>RNF03</b>	No Funcional	El proyecto debe gestionarse siguiendo la metodología Scrum.	A
<b>RNF04</b>	No Funcional	Las tareas deben planificarse en Azure DevOps.	M
<b>RNF05</b>	No Funcional	El sistema debe gestionarse con control de versiones en Git.	A
<b>RNF06</b>	No Funcional	El sistema debe desarrollarse aplicando TDD (Test Driven Development).	M
<b>RNF07</b>	No Funcional	El sistema debe asegurar las comunicaciones mediante HTTPS (TLS 1.2+).	A
<b>RNF08</b>	No Funcional	La información sensible almacenada en la BBDD debe estar protegida mediante cifrado en reposo y técnicas adicionales (field-level encryption, masking).	A
<b>RNF09</b>	No Funcional	La base de datos debe aplicar medidas de seguridad específicas: autenticación SCRAM-SHA-256, roles mínimos, cifrado TLS, prohibición de \$where.	A
<b>RNF10</b>	No Funcional	El sistema debe ser accesible desde cualquier navegador moderno.	A
<b>RNF11</b>	No Funcional	El sistema debe ser seguro y escalable, alcanzando al menos un 99.5% de disponibilidad.	A

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

<b>RNF12</b>	No Funcional	El sistema debe identificar y gestionar riesgos de seguridad siguiendo la norma ISO 27001:2022 (AGR con MARISMA).	M
<b>RNF13</b>	No Funcional	El sistema debe garantizar que el número de vulnerabilidades bloqueantes o críticas sea igual a 0.	A
<b>RNF14</b>	No Funcional	El sistema debe garantizar que la cobertura de pruebas sea superior al 60%.	A
<b>RNF15</b>	No Funcional	El sistema no debe contener código no utilizado.	A
<b>RNF16</b>	No Funcional	El sistema debe mantener la duplicidad de código por debajo del 10%.	A
<b>RNF17</b>	No Funcional	El sistema debe justificar la existencia de métodos con complejidad ciclomática elevada.	M
<b>RNF18</b>	No Funcional	El sistema debe proporcionar una matriz de trazabilidad entre casos de prueba e historias de usuario.	A
<b>RNF19</b>	No Funcional	El sistema no debe contener defectos críticos o bloqueantes en el código.	A
<b>RNF20</b>	No Funcional	El sistema debe asegurar que la calidad alcanzada en el Sprint 1 no empeore en los siguientes.	M
<b>RNF21</b>	No Funcional	El sistema debe verificar la calidad del código utilizando SonarQube y SonarLint.	A
<b>RNF22</b>	No Funcional	El sistema debe cumplir con las guías de seguridad CCN-CERT BP/28 y las buenas prácticas vistas en clase.	A
<b>RNF23</b>	No Funcional	El sistema debe cumplir con el RGPD (consentimiento, derecho de baja, anonimización de logs, exportación de datos).	A
<b>RNF24</b>	No Funcional	El sistema debe gestionar de forma segura los secretos y claves de la aplicación.	A

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

## **Lista de preguntas para entrevista con profesores**

<b>Requisito relacionado</b>	<b>Duda detectada</b>	<b>Pregunta para profesores</b>
RF09 Suscripciones	Diferencias poco claras entre usuarios VIP y estándar.	¿Qué diferencias exactas existirán entre usuarios VIP y estándar?
RF09 Suscripciones	Gestión de planes no detallada.	¿Cómo se gestionarán los planes de suscripción?
RF08 Perfil	Control parental mencionado, pero no definido.	¿El control parental será obligatorio? ¿Qué nivel de filtros debe incluir?
RF05 Autenticación 3FA	Tercer factor ambiguo (OTP email, CAPTCHA...).	¿Debe implementarse un conjunto fijo de factores o basta con habilitar varias opciones configurables?
RF05 Autenticación 3FA	Política para usuarios estándar no clara.	¿Es suficiente con 2FA (contraseña+TOTP) para usuarios normales o deben soportar también el tercer factor?
RF03 Contraseñas	Caducidad 30 días discutida.	¿La caducidad de contraseñas es obligatoria o solo una recomendación?
RF03/RF06 Contraseñas seguras	Verificación de contraseñas filtradas.	¿Se debe usar un diccionario local o un servicio externo?
RF23 Sesiones	Timeouts expresados como rangos (15–30 min / 6–12h).	¿Qué valores exactos deben aplicarse por rol, o basta con hacerlos configurables?
RF23 Sesiones	Rotación de sesión solo en login y credenciales.	¿Debe aplicarse también al cambiar de rol (ej. estándar→VIP)?
RF17 Gestión contenidos	Subida real o simulada no definido.	¿El sistema debe gestionar subida real de archivos multimedia o basta con simularla?

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

RF17 Gestión contenidos	Almacenamiento no definido.	¿Habría límite de almacenamiento por creador de contenido?
RF17/RF24 Seguridad uploads	Muchas medidas listadas (MIME, sandbox, antivirus, URLs firmadas).	¿Cuáles de estas medidas son obligatorias y cuáles se consideran opcionales en la práctica?
RF10 Reproducción	Streaming adaptativo (HLS/DASH) no definido.	¿Debe implementarse de forma real o basta con reproducir ficheros de vídeo de ejemplo?
RF25 Recomendaciones	Evolutivo o MVP no claro.	¿El sistema de recomendaciones es obligatorio en la primera entrega o parte del mantenimiento evolutivo?
RF25 Recomendaciones	Criterios no definidos.	¿Qué criterios debe seguir el motor de recomendaciones?
RF26 Móvil	Tipo de app no definido.	¿La versión móvil debe ser nativa (Android/iOS) o basta con una PWA adaptada?  NOTA: PWA = Aplicación Web Progresiva, es una aplicación web común (HTML, CSS, Javascript...), pero que ofrece una experiencia de usuario similar a la de un app nativa
RF26 Móvil	Alcance funcional no definido.	En caso de app nativa, ¿debe cubrir toda la funcionalidad o solo consumo básico de contenido?
RNF11 Escalabilidad	Concurrencia no definida.	¿El sistema debe estar preparado para soportar muchos usuarios concurrentes o solo un uso de laboratorio reducido?
RNF11 Escalabilidad	Rendimiento no concretado.	¿Existe un SLO de rendimiento definido (tiempo de inicio de reproducción, latencia máxima)?
RNF12 AGR ISO27001	Nivel de detalle de análisis no definido.	¿Se espera un documento formal MARISMA completo o una versión reducida adaptada a la práctica?

**Nombre:** Elicitación de Requisitos Inicial

**Versión:** 1.1

**Fecha:** 17/09/2025

**Fecha Última Actualización:** 18/02/2025

RNF23 RGPD	Alcance incompleto.	¿El cumplimiento RGPD incluye solo consentimiento y derecho de baja o también exportación/portabilidad de datos?
RNF21 Sonar/SonarLint	Forma de entrega no definida.	¿Deben entregarse informes de Sonar/SonarLint en cada sprint o basta con usarlos internamente?
RNF17 Complejidad ciclomática	Umbral no especificado.	¿Cuál es el umbral exacto a partir del cual se debe justificar un método por complejidad excesiva?
RNF14 Cobertura de pruebas	Ámbito de medición no definido.	¿La cobertura >60% se mide sobre todo el sistema (backend+frontend) o solo sobre el backend en Spring?
RNF14 Cobertura de pruebas	Tipo de pruebas no especificado.	¿Qué tipos de pruebas son obligatorias (unitarias, integración, end-to-end)?
RNF10 El sistema debe ser accesible desde cualquier navegador moderno.	Accesibilidad desde navegador no realista.	¿Bastaría con hacerlo en dos navegadores contemplando solo sus últimas dos versiones?