Requerimientos No Funcionales – User Story: Autenticación de Usuarios

Seguridad

• Contraseñas con hash fuerte (Argon2id o bcrypt ≥ cost 12).
• Transporte cifrado: TLS 1.2+ (ideal 1.3).
• Protección CSRF/XSS: Cookies HttpOnly/Secure/SameSite.
• Gestión de sesión: Idle timeout 30 min, absolute timeout 8 h.
• Rate limit: máximo 5 intentos/min/IP.
• No guardar tokens sensibles en LocalStorage.
• Auditoría sin PII y con trazabilidad (traceId).

Privacidad

• Retención de datos de intentos fallidos ≤ 90 días.
• Cumplimiento de políticas internas y legislación aplicable.

Disponibilidad

• Uptime del servicio de autenticación ≥ 99.9% mensual.

Rendimiento

• Latencia de login P95 ≤ 300 ms; P99 ≤ 600 ms.

Escalabilidad

• Soportar al menos 200 solicitudes/segundo sin degradación.

Usabilidad

• Mensajes claros sin revelar si el correo existe.

Accesibilidad

• Cumplir WCAG 2.1 AA (contraste, teclado, ARIA).

Compatibilidad

• Navegadores: últimas 2 versiones de Chrome, Edge, Firefox, Safari; móviles iOS/Android.

Observabilidad

• Métricas: tasa de éxito/fallo, latencia P95/P99; alertas configuradas.

Mantenibilidad

• Coverage ≥ 80%, linters sin errores críticos, OWASP Top 10 verificado.

Interoperabilidad

• Endpoints preparados para OAuth 2.1 / OIDC en el futuro.

Recuperación

• RTO ≤ 15 min, RPO ≤ 5 min para servicio de autenticación.

Configuración

• Secrets almacenados en Vault/KMS; nunca en repositorios.

CORS

• Política restrictiva: sin comodín (*) en producción.