REQUISITOS PARA LA PLATAFORMA WEB SaaS DE GESTIÓN DE HISTORIAS CLÍNICAS ELECTRÓNICAS

1. Seguridad de la Información

SEG-001: Cifrado de Datos en Reposo y en Tránsito

Descripción: Los datos médicos deben ser cifrados mediante AES-256 en reposo y TLS 1.2/1.3 en tránsito.

Criterios de Aceptación:

- Cifrado AES-256 para almacenamiento de datos.
- Uso de TLS 1.2 o superior para la transmisión.
- Certificados digitales actualizados.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD (Art. 32), ISO 27001, ENS

SEG-002: Autenticación Multifactor (MFA)

Descripción: Se implementará MFA para usuarios con acceso privilegiado (médicos, administradores).

Criterios de Aceptación:

- Implementación de MFA para cuentas privilegiadas.
- Generación y validación de OTP o biometría.
- Configuración de políticas de autenticación.

Prioridad: Alta

Fuente/Norma Aplicable: ENS, ISO 27001

SEG-003: Registro de Auditoría de Accesos y Modificaciones

Descripción: El sistema almacenará registros detallados de accesos y modificaciones en los historiales médicos.

Criterios de Aceptación:

- Registro detallado de accesos, modificaciones y eliminaciones.
- Identificación del usuario, fecha y hora.
- Protección de logs contra alteraciones.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD (Art. 30, 32), ENS, ISO 27001

2. Protección de Datos y Privacidad

PRIV-001: Consentimiento Explícito para el Tratamiento de Datos Médicos

Descripción: Se solicitará y registrará el consentimiento del paciente antes de procesar su información médica.

Criterios de Aceptación:

- Sistema para capturar consentimiento.
- Registro de fecha, hora y tipo de consentimiento.
- Posibilidad de revocación del consentimiento.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD (Art. 6, 7, 9), LOPDGDD

PRIV-002: Derecho de Acceso y Portabilidad de Datos Médicos

Descripción: Los pacientes podrán acceder a su historial médico y descargarlo en formatos interoperables.

Criterios de Aceptación:

- Exportación de datos en formato estructurado y legible.
- Validación de identidad antes de conceder acceso.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD (Art. 15, 20), LOPDGDD

PRIV-003: Derecho al Olvido y Eliminación de Datos Médicos

Descripción: Se permitirá a los pacientes solicitar la eliminación de sus datos personales.

Criterios de Aceptación:

- Implementación de un mecanismo de solicitud de eliminación.
- Eliminación segura de datos tras el tiempo legal requerido.
- Notificación de confirmación al paciente tras la eliminación.

Prioridad: Media

Fuente/Norma Aplicable: RGPD (Art. 17), LOPDGDD

3. Accesibilidad y Funcionalidad

FUNC-001: Control de Acceso Basado en Roles (RBAC)

Descripción: La plataforma permitirá la asignación de roles y permisos específicos para cada usuario.

Criterios de Aceptación:

- Definición de roles y permisos diferenciados.
- Restricción de acceso según rol asignado.
- Registro de intentos de acceso no autorizados.

Prioridad: Alta

Fuente/Norma Aplicable: ISO 27001, ENS

FUNC-002: Firma Digital de Documentos Médicos

Descripción: Los médicos deben poder firmar electrónicamente documentos clínicos mediante una firma digital avanzada.

Criterios de Aceptación:

- Implementación de firma electrónica basada en certificados digitales.
- Validación de identidad antes de firmar un documento.
- Verificabilidad de la firma sin alteraciones.

Prioridad: Alta

Fuente/Norma Aplicable: eIDAS, ENS

FUNC-003: Respaldo Automático y Alta Disponibilidad

Descripción: La plataforma debe contar con mecanismos de respaldo automático y estrategias de alta disponibilidad.

Criterios de Aceptación:

- Copias de seguridad periódicas cifradas.
- Sistema de recuperación ante desastres.
- Infraestructura con redundancia de servidores.

Prioridad: Alta

Fuente/Norma Aplicable: ISO 27001, ENS