Requisitos para Plataforma SaaS de Historias Clínicas Electrónicas

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

Descripción: Garantizar la confidencialidad de los datos médicos mediante cifrado fuerte tanto en almacenamiento como en transmisión. Se recomienda el uso de AES-256 para datos en reposo y TLS 1.3 para comunicaciones.

Criterios de Aceptación:

- Implementación de cifrado AES-256 para datos almacenados.
- Uso de TLS 1.3 para la transmisión de datos.
- Claves de cifrado almacenadas de forma segura y accesibles solo para sistemas autorizados.

Justificación:

Garantiza la seguridad de la información médica, reduciendo riesgos de acceso no autorizado o exfiltración de datos.

Prioridad: Alta

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

SEG-002 - Autenticación Multifactor (MFA)

Descripción: El acceso a la plataforma por parte de personal médico y administrativo debe requerir autenticación multifactor para mitigar riesgos de accesos no autorizados.

Criterios de Aceptación:

- Implementación de MFA con al menos dos factores (contraseña + OTP/SMS/biometría).
- Aplicación obligatoria para usuarios con privilegios elevados.
- Opcional para pacientes, con la posibilidad de activarlo.

Justificación:

Evita accesos indebidos y fortalece la seguridad en la gestión de información clínica.

Prioridad: Alta

Fuente/Norma Aplicable: ISO 27001, ENS, RGPD Art. 25

SEG-003 - Registro de Auditoría de Accesos y Modificaciones

Descripción: Se debe registrar cada acceso y modificación de expedientes médicos, indicando el usuario, la fecha, la IP de acceso y la acción realizada.

Criterios de Aceptación:

- Implementación de un sistema de logs inmutables.
- Accesible solo por administradores de seguridad.
- Retención mínima de 2 años.

Justificación:

Facilita el rastreo de accesos y refuerza la trazabilidad de las modificaciones.

Prioridad: Alta

Fuente/Norma Aplicable: ENS, ISO 27001, LOPDGDD Art. 32

PRIV-001 - Obtención de Consentimiento Explícito

Descripción: Antes de procesar datos personales de pacientes, se debe obtener su consentimiento explícito, informando sobre el uso y almacenamiento de los datos.

Criterios de Aceptación:

- Interfaz de aceptación con opción de revocación.

- Registro de consentimiento con fecha y hora.

Justificación:

Cumple con la normativa de protección de datos personales en la UE.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD Art. 6 y 7, LOPDGDD

PRIV-002 - Derecho al Olvido y Eliminación de Datos

Descripción: La plataforma debe permitir a los pacientes solicitar la eliminación de sus datos médicos cuando estos ya no sean necesarios para la prestación del servicio.

Criterios de Aceptación:

- Implementación de interfaz para solicitud de eliminación.
- Eliminación segura y certificada de datos médicos.

Justificación:

Cumple con el derecho de los pacientes a eliminar su información.

Prioridad: Alta

Fuente/Norma Aplicable: RGPD Art. 17, LOPDGDD

ACC-001 - Control de Acceso Basado en Roles (RBAC)

Descripción: El acceso a los datos de la plataforma debe estar segmentado según perfiles de usuario (médico, administrativo, paciente).

Criterios de Aceptación:

- Definición clara de permisos por tipo de usuario.
- Restricción de acceso a datos sensibles solo a perfiles autorizados.

Justificación:

Minimiza riesgos de exposición innecesaria de información médica.

Prioridad: Alta

Fuente/Norma Aplicable: ENS, ISO 27001

ACC-002 - Sesiones Seguras y Políticas de Expiración

Descripción: Las sesiones de usuario deben expirar tras un tiempo de inactividad y requerir reautenticación.

Criterios de Aceptación:

- Expiración automática tras 15 minutos de inactividad.
- Cierre de sesión automático en todos los dispositivos en caso de cambio de credenciales.

Justificación:

Protege la sesión contra accesos no autorizados.

Prioridad: Media

Fuente/Norma Aplicable: ISO 27001, ENS

INT-001 - API para Integración con Otros Sistemas

Descripción: La plataforma debe contar con una API REST que permita la integración con sistemas de facturación, recetas electrónicas y bases de datos hospitalarias.

Criterios de Aceptación:

- Implementación de API con autenticación segura.
- Soporte para estándares HL7/FHIR para datos médicos.

Justificación:

Facilita la interoperabilidad con otros sistemas sanitarios.

Prioridad: Alta

Fuente/Norma Aplicable: IEEE 29148-2018

DISP-001 - Alta Disponibilidad y Respaldo Automático

Descripción: La plataforma debe garantizar 99.9% de disponibilidad con mecanismos de respaldo automático y redundancia de datos.

Criterios de Aceptación:

- Replicación de datos en múltiples servidores.
- Pruebas de restauración de datos periódicas.

Justificación:

Asegura la continuidad del servicio en caso de fallos.

Prioridad: Alta

Fuente/Norma Aplicable: ISO 27001, ENS