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

Clasificación de categorías de Requisitos

1. **Protección de Datos Personales y Privacidad**
    - **Consentimiento y Bases Legales para el Tratamiento de Datos (RGPD, LOPDGDD)**
    - **Minimización de Datos (RGPD)**
    - **Derechos de los Titulares de los Datos (Acceso, Rectificación, Supresión, Oposición, Portabilidad)**
    - **Tratamiento de Datos Sensibles (Datos de Salud) y Limitaciones**
    - **Transferencia Internacional de Datos (RGPD)**
    - **Plazos de Conservación y Eliminación Segura de Datos (LOPDGDD)**
2. **Seguridad de la Información**
    - **Cifrado de Datos en Reposo y en Tránsito (ISO 27001, ENS)**
    - **Autenticación Multifactor (MFA) para Usuarios Sensibles (ENS, ISO 27001)**
    - **Registro de Auditoría y Trazabilidad de Accesos y Modificaciones (ENS, ISO 27001)**
    - **Control de Acceso Basado en Roles (RBAC) (ISO 27001)**
    - **Medidas de Protección contra Accesos No Autorizados y Amenazas Externas (ENS, ISO 27001)**
    - **Seguridad Física y Lógica de los Centros de Datos (ISO 27001)**
3. **Cumplimiento Legal y Normativo**
    - **Cumplimiento con el RGPD y LOPDGDD en el Tratamiento de Datos de Salud**
    - **Adopción del Esquema Nacional de Seguridad (ENS) para Protección de Datos Sensibles**
    - **Aplicación de la ISO/IEC 27001 para la Gestión de Seguridad de la Información**
    - **Gestión de Incidentes de Seguridad y Notificación a Autoridades (RGPD, ENS)**
4. **Continuidad del Negocio y Recuperación ante Desastres**
    - **Copias de Seguridad y Recuperación ante Fallos (ISO 27001)**

- **Planes de Continuidad del Negocio en Caso de Incidentes de Ciberseguridad (ENS)**
- **Alta Disponibilidad y Redundancia de los Datos (ISO 27001)**

5. Interoperabilidad y Transferencia de Datos

- **Compatibilidad con Estándares de Intercambio de Información Médica (FHIR, HL7)**
- **Integración Segura con Bases de Datos Hospitalarias y Sistemas Externos**
- **Exportación de Datos en Formatos Estándar**

6. Auditoría y Monitorización Continua

- **Registro de Eventos y Monitoreo de Actividades Críticas (ENS, ISO 27001)**
- **Realización de Auditorías de Seguridad Periódicas (ENS)**
- **Gestión de Vulnerabilidades y Aplicación de Parches de Seguridad (ISO 27001)**

Requisitos de Consentimiento y Bases Legales para el Tratamiento de Datos

1. Obtención de Consentimiento Explícito

- **Identificador único:** PRIV-001
- **Título:** Obtención de Consentimiento Explícito
- **Descripción:** De acuerdo con el Artículo 6 del **RGPD** y la **LOPDGDD**, el consentimiento explícito debe ser obtenido antes de procesar los datos personales del usuario. Este consentimiento debe ser libre, informado, específico e inequívoco.
- **Criterios de Aceptación:**
    - Presentación de un formulario de consentimiento previo a la recopilación de datos personales.
    - Posibilidad de revocar el consentimiento en cualquier momento.
    - Registro de fecha, hora y modalidad de otorgamiento del consentimiento.
- **Prioridad:** Alta
- **Categoría:** Consentimiento del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 6; LOPDGDD
- **Justificación:** Es fundamental para cumplir con la legalidad y evitar sanciones, además de garantizar que el tratamiento de datos personales de los pacientes se realice con pleno conocimiento y aceptación por parte de los mismos.

---

2. Consentimiento Diferenciado para Finalidades Específicas

- **Identificador único:** PRIV-002
- **Título:** Consentimiento Diferenciado por Tipo de Tratamiento
- **Descripción:** El **RGPD** establece que el consentimiento debe otorgarse de manera específica para cada finalidad del tratamiento. Esto significa que los pacientes deben poder aceptar o rechazar el uso de sus datos para diferentes propósitos (e.g., asistencia médica, investigación, marketing).
- **Criterios de Aceptación:**
    - Implementación de casillas independientes para cada finalidad del tratamiento en la interfaz de consentimiento.
    - Documentación clara y concisa sobre las finalidades del uso de los datos.
    - Posibilidad de modificar preferencias en cualquier momento desde la plataforma.
- **Prioridad:** Alta
- **Categoría:** Consentimiento del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 6 y 7
- **Justificación:** Este requisito evita el consentimiento genérico y mejora la transparencia, permitiendo que los usuarios controlen el uso de sus datos según su propia voluntad.

---

3. Registro y Almacenamiento del Consentimiento

- **Identificador único:** PRIV-003
- **Título:** Registro y Auditoría del Consentimiento
- **Descripción:** La plataforma debe garantizar que el consentimiento otorgado por los usuarios quede debidamente almacenado y accesible en caso de auditoría o reclamación legal.
- **Criterios de Aceptación:**
    - Almacenamiento de registros de consentimiento con sellado de tiempo.
    - Implementación de un sistema de auditoría para verificar cambios o revocaciones de consentimiento.
    - Capacidad de exportación de registros de consentimiento en formatos legibles.

- **Prioridad:** Alta
- **Categoría:** Consentimiento del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 7(1) y Art. 30; LOPDGDD
- **Justificación:** Este requisito asegura la trazabilidad del consentimiento y la protección de la organización en caso de disputas legales o auditorías por parte de autoridades regulatorias.

---

4. Excepciones al Requisito de Consentimiento

- **Identificador único:** PRIV-004
- **Título:** Tratamiento de Datos sin Consentimiento en Base a Interés Público o Legal
- **Descripción:** En situaciones específicas, el tratamiento de datos puede realizarse sin consentimiento expreso, siempre que se justifique en bases legales como el interés público, el cumplimiento de obligaciones legales o la prestación de servicios médicos esenciales.
- **Criterios de Aceptación:**
    - Definición clara de los casos en los que no es necesario el consentimiento.
    - Documentación de la base legal que justifica el tratamiento sin consentimiento.
    - Implementación de medidas de seguridad para garantizar el tratamiento adecuado de estos datos.
- **Prioridad:** Media
- **Categoría:** Bases Legales del Tratamiento
- **Fuente/Norma Aplicable:** RGPD, Art. 6(1)(c)(d)(e); LOPDGDD
- **Justificación:** Permite la operatividad del sistema en casos en los que obtener consentimiento no es viable, asegurando al mismo tiempo que el tratamiento se realice de forma legítima y conforme a la normativa vigente.

---

5. Revocación del Consentimiento

- **Identificador único:** PRIV-005
- **Título:** Mecanismo de Revocación del Consentimiento
- **Descripción:** Según el **RGPD**, los usuarios deben poder retirar su consentimiento en cualquier momento sin perjuicio de la legalidad del tratamiento previo. La plataforma debe permitir un mecanismo accesible para ejercer este derecho.

- **Criterios de Aceptación:**
    - Opción accesible en la plataforma para revocar el consentimiento en cualquier momento.
    - Eliminación o anonimización de los datos asociados tras la revocación, salvo que exista una base legal para su conservación.
    - Notificación al usuario de la efectividad de su revocación.
- **Prioridad:** Alta
- **Categoría:** Consentimiento del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 7(3)
- **Justificación:** Garantiza la autonomía del usuario en la gestión de sus datos personales y refuerza la confianza en la plataforma.

Requisitos de Minimización de Datos

1. Recopilación de Datos Estrictamente Necesarios

- **Identificador único:** PRIV-006
- **Título:** Recopilación Mínima de Datos
- **Descripción:** La plataforma solo debe solicitar y almacenar los datos personales que sean estrictamente necesarios para la prestación del servicio de gestión de historias clínicas electrónicas, evitando la recopilación excesiva o irrelevante.
- **Criterios de Aceptación:**
    - Evaluación previa de los datos requeridos para cada funcionalidad del sistema.
    - Justificación documental de la necesidad de cada tipo de dato recopilado.
    - Implementación de controles en los formularios para evitar la introducción de datos innecesarios.
- **Prioridad:** Alta
- **Categoría:** Minimización de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(c)
- **Justificación:** Reducir el volumen de datos recopilados disminuye los riesgos de exposición y el impacto de una posible brecha de seguridad.

---

2. Anonimización y Pseudonimización de Datos

- **Identificador único:** PRIV-007
- **Título:** Aplicación de Anonimización y Pseudonimización
- **Descripción:** Los datos personales deberán ser anonimizados o pseudonimizados cuando sea posible, especialmente en usos secundarios como la generación de informes y estadísticas.
- **Criterios de Aceptación:**
    - Implementación de técnicas de anonimización y pseudonimización en bases de datos.
    - Uso de identificadores en lugar de información directamente identificable en informes internos.
    - Restricción de acceso a la información original solo a usuarios autorizados.
- **Prioridad:** Alta
- **Categoría:** Minimización de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 32 y Art. 89(1)
- **Justificación:** Permite el uso de datos con menos riesgos para la privacidad, asegurando el cumplimiento de los principios de protección de datos.

---

3. Eliminación Automática de Datos Innecesarios

- **Identificador único:** PRIV-008
- **Título:** Mecanismo de Eliminación de Datos No Necesarios
- **Descripción:** El sistema deberá implementar procedimientos automáticos y manuales para eliminar datos personales que ya no sean necesarios para la finalidad para la que fueron recogidos.
- **Criterios de Aceptación:**
    - Configuración de plazos de retención para cada tipo de dato, con eliminación automática al vencer dichos plazos.
    - Notificación a usuarios antes de la eliminación de sus datos personales, cuando sea aplicable.
    - Generación de registros de auditoría sobre las eliminaciones efectuadas.
- **Prioridad:** Alta
- **Categoría:** Minimización de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(e)

- **Justificación:** Reduce el almacenamiento innecesario de datos personales, minimizando riesgos de exposición en caso de brecha de seguridad.

---

4. Control de Acceso a Datos Sensibles

- **Identificador único:** PRIV-009
- **Título:** Restricción de Acceso a Datos Específicos Según Rol
- **Descripción:** Solo los usuarios con funciones específicas dentro de la plataforma podrán acceder a determinados tipos de datos, asegurando que cada perfil solo visualice la información estrictamente necesaria para sus tareas.
- **Criterios de Aceptación:**
    - Implementación de un sistema de permisos basado en roles (RBAC).
    - Control de accesos diferenciado para médicos, administrativos y pacientes.
    - Registro de auditoría que almacene intentos de acceso no autorizados.
- **Prioridad:** Alta
- **Categoría:** Minimización de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(c), Art. 32
- **Justificación:** Limita la exposición de datos personales solo a quienes realmente los necesitan, reduciendo riesgos de acceso indebido.

---

5. Uso de Datos Agregados para Análisis

- **Identificador único:** PRIV-010
- **Título:** Generación de Informes con Datos Agregados
- **Descripción:** La plataforma deberá permitir la generación de informes y estadísticas utilizando datos anonimizados o agregados, evitando el uso de datos personales directos siempre que sea posible.
- **Criterios de Aceptación:**
    - Implementación de una opción para anonimizar datos en informes y estadísticas.
    - Restricción del acceso a datos individuales cuando no sea necesario.
    - Verificación de que los datos agregados no permitan la reidentificación de pacientes.
- **Prioridad:** Media

- **Categoría:** Minimización de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 25(2), Art. 89(1)
- **Justificación:** Facilita el análisis de datos médicos sin comprometer la privacidad de los pacientes.

Requisitos de Derechos de los Titulares de los Datos

1. Derecho de Acceso a los Datos Personales

- **Identificador único:** PRIV-011
- **Título:** Acceso a los Datos Personales
- **Descripción:** Los usuarios (pacientes y profesionales sanitarios) deben tener acceso a sus datos personales en la plataforma, incluyendo información sobre su historial clínico y registros de tratamiento. La plataforma debe proporcionar un mecanismo sencillo para que los titulares consulten qué datos están siendo almacenados y procesados.
- **Criterios de Aceptación:**
    - Opción en la plataforma para que el usuario visualice sus datos personales en un formato claro y estructurado.
    - Generación de un informe descargable en formato legible (e.g., PDF, JSON).
    - Registro de auditoría que almacene los accesos a la información personal.
- **Prioridad:** Alta
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 15
- **Justificación:** Garantiza la transparencia en el tratamiento de datos y permite a los usuarios verificar qué información suya está siendo almacenada y utilizada.

---

2. Derecho de Rectificación de Datos

- **Identificador único:** PRIV-012
- **Título:** Modificación y Corrección de Datos
- **Descripción:** Los usuarios tienen derecho a solicitar la corrección de datos personales inexactos o incompletos. La plataforma debe proporcionar un mecanismo para que los pacientes y profesionales puedan actualizar su información.

- **Criterios de Aceptación:**
    - Interfaz que permita solicitar la rectificación de datos personales incorrectos.
    - Validación por parte de personal autorizado antes de aplicar cambios críticos (e.g., información médica).
    - Registro de modificaciones realizadas en la historia clínica electrónica.
- **Prioridad:** Alta
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 16
- **Justificación:** Evita errores en los registros médicos y asegura que los datos almacenados sean precisos y actualizados.

---

3. Derecho de Supresión ("Derecho al Olvido")

- **Identificador único:** PRIV-013
- **Título:** Eliminación de Datos Personales a Petición del Usuario
- **Descripción:** Los usuarios tienen derecho a solicitar la eliminación de sus datos personales cuando estos ya no sean necesarios para la finalidad con la que fueron recogidos, salvo en los casos en los que exista una obligación legal de conservación (e.g., normativa sanitaria).
- **Criterios de Aceptación:**
    - Implementación de una opción en la plataforma para que los usuarios soliciten la eliminación de sus datos.
    - Evaluación automática de restricciones legales que impidan la supresión (e.g., datos de historias clínicas que deben conservarse por normativa).
    - Notificación al usuario sobre el estado de su solicitud de eliminación.
    - Eliminación segura y definitiva de los datos personales, salvo en los casos donde deban ser anonimizados para fines médicos o estadísticos.
- **Prioridad:** Alta
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 17
- **Justificación:** Proporciona control a los usuarios sobre su información personal y refuerza la confianza en la plataforma.

---

4. Derecho a la Limitación del Tratamiento

- **Identificador único:** PRIV-014
- **Título:** Restricción Temporal del Tratamiento de Datos
- **Descripción:** Los usuarios deben poder solicitar la restricción del tratamiento de sus datos en ciertos casos, como impugnaciones de exactitud de la información o procesos legales en curso. Durante la restricción, los datos solo podrán ser almacenados sin tratamiento activo.
- **Criterios de Aceptación:**
    - Opción en la plataforma para solicitar la restricción del tratamiento de datos.
    - Implementación de etiquetas de estado para indicar qué datos están restringidos.
    - Bloqueo temporal de la edición y uso de los datos mientras dure la restricción.
    - Notificación al usuario cuando se levante la restricción.
- **Prioridad:** Media
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 18
- **Justificación:** Permite a los usuarios controlar el uso de sus datos en situaciones específicas sin requerir su eliminación total.

---

5. Derecho a la Portabilidad de los Datos

- **Identificador único:** PRIV-015
- **Título:** Exportación de Datos Personales
- **Descripción:** Los usuarios deben poder solicitar una copia de sus datos personales en un formato estructurado, de uso común y lectura mecánica, para poder transferirlos a otro proveedor de servicios de salud.
- **Criterios de Aceptación:**
    - Implementación de un botón de descarga para que los usuarios exporten sus datos en formatos estándar (JSON, XML, FHIR).
    - Garantía de que los datos exportados incluyan toda la información relevante sin modificarla ni alterarla.
    - Posibilidad de enviar los datos directamente a otro proveedor de servicios de salud si el usuario lo solicita.

- **Prioridad:** Alta
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 20
- **Justificación:** Facilita la interoperabilidad y el derecho del usuario a controlar sus datos personales en diferentes plataformas de salud.

---

6. Derecho de Oposición al Tratamiento

- **Identificador único:** PRIV-016
- **Título:** Oposición al Uso de Datos para Finalidades Específicas
- **Descripción:** Los usuarios pueden oponerse al tratamiento de sus datos personales en ciertos casos, especialmente cuando estos se utilicen para finalidades distintas a la prestación de servicios médicos esenciales.
- **Criterios de Aceptación:**
    - Opción en la plataforma para que los usuarios gestionen su oposición a ciertos tratamientos de datos.
    - Restricción automática del uso de los datos para las finalidades indicadas por el usuario.
    - Notificación al usuario sobre la aplicación de su oposición y sus consecuencias.
- **Prioridad:** Media
- **Categoría:** Derechos del Usuario
- **Fuente/Norma Aplicable:** RGPD, Art. 21
- **Justificación:** Refuerza el derecho de los usuarios a decidir sobre el uso de su información personal más allá de lo estrictamente necesario.

Requisitos de Tratamiento de Datos Sensibles (Datos de Salud) y Limitaciones

1. Tratamiento Legítimo de Datos de Salud

- **Identificador único:** PRIV-017
- **Título:** Tratamiento Legítimo de Datos Sensibles
- **Descripción:** El tratamiento de datos de salud solo puede realizarse bajo una base legal válida, como el consentimiento explícito del paciente o la necesidad del tratamiento por razones médicas. La plataforma debe garantizar que estos datos sean utilizados exclusivamente para finalidades sanitarias.

- **Criterios de Aceptación:**
    - Implementación de un sistema que valide la base legal antes de procesar datos sensibles.
    - Restricción del tratamiento a personal médico autorizado.
    - Registro detallado de los accesos y usos de los datos de salud.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 9(2); LOPDGDD
- **Justificación:** Garantiza que los datos médicos solo se utilicen en contextos legítimos, evitando accesos indebidos o usos no autorizados.

---

2. Consentimiento Explícito para el Tratamiento de Datos de Salud

- **Identificador único:** PRIV-018
- **Título:** Consentimiento Expreso para Datos Sensibles
- **Descripción:** Cuando el tratamiento de datos de salud no esté amparado en la legislación sanitaria, se debe obtener un consentimiento explícito e informado del paciente antes de su procesamiento.
- **Criterios de Aceptación:**
    - Solicitud de consentimiento explícito antes de procesar información médica no obligatoria.
    - Registro de la fecha y hora del consentimiento en la base de datos.
    - Implementación de una opción para revocar el consentimiento en cualquier momento.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 9(2)(a); LOPDGDD
- **Justificación:** Asegura el respeto a la privacidad del paciente y el cumplimiento de la normativa de protección de datos.

---

3. Acceso Restringido a Datos Médicos

- **Identificador único:** PRIV-019
- **Título:** Control de Acceso a Datos de Salud

- **Descripción:** Solo los profesionales sanitarios autorizados deben tener acceso a los datos clínicos de los pacientes, con permisos diferenciados según el rol de cada usuario en la plataforma.
- **Criterios de Aceptación:**
    - Implementación de control de acceso basado en roles (RBAC).
    - Registro de auditoría de accesos y modificaciones realizadas en los expedientes médicos.
    - Aplicación de autenticación multifactor (MFA) para el acceso a datos de salud.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 32; ENS
- **Justificación:** Limita la exposición de datos médicos solo a quienes realmente los necesitan, reduciendo riesgos de accesos indebidos.

---

4. Cifrado de Datos Sensibles en Reposo y en Tránsito

- **Identificador único:** PRIV-020
- **Título:** Cifrado de Datos de Salud
- **Descripción:** Los datos médicos deben estar protegidos mediante cifrado robusto tanto en reposo como en tránsito para evitar accesos no autorizados.
- **Criterios de Aceptación:**
    - Cifrado de la base de datos con estándares AES-256 o superiores.
    - Uso de protocolos de seguridad en la transmisión de datos (TLS 1.2 o superior).
    - Implementación de mecanismos de desencriptación solo para usuarios autorizados.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 32; ENS; ISO 27001
- **Justificación:** Reduce el riesgo de exposición de datos médicos en caso de accesos no autorizados o filtraciones.

---

5. Anonimización y Pseudonimización de Datos Sensibles

- **Identificador único:** PRIV-021
- **Título:** Protección de Identidad en Datos de Salud
- **Descripción:** Cuando los datos de salud se utilicen para fines de análisis, investigación o mejora del sistema, deben ser anonimizados o pseudonimizados para evitar la identificación de pacientes.
- **Criterios de Aceptación:**
    - Implementación de algoritmos de anonimización o pseudonimización.
    - Restricción del acceso a los datos anonimizados a personal autorizado.
    - Verificación periódica de la eficacia del proceso de anonimización.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 25; ISO 27001
- **Justificación:** Protege la privacidad de los pacientes cuando sus datos se usan con fines secundarios.

---

6. Registro y Monitoreo de Accesos a Datos de Salud

- **Identificador único:** PRIV-022
- **Título:** Registro de Auditoría en el Acceso a Datos Médicos
- **Descripción:** La plataforma debe registrar cada acceso, modificación o eliminación de datos médicos, permitiendo auditorías de seguridad y detección de accesos indebidos.
- **Criterios de Aceptación:**
    - Generación automática de logs de acceso a información médica.
    - Almacenamiento seguro de registros de auditoría por un período definido.
    - Implementación de alertas para detectar accesos sospechosos o no autorizados.
- **Prioridad:** Alta
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 30 y 33; ENS; ISO 27001
- **Justificación:** Garantiza la trazabilidad del uso de datos médicos y permite la identificación de posibles brechas de seguridad.

---

7. Eliminación Segura de Datos Sensibles

- **Identificador único:** PRIV-023
- **Título:** Borrado Seguro de Información Clínica
- **Descripción:** Cuando los datos de salud ya no sean necesarios y puedan ser eliminados, la plataforma debe aplicar un proceso de eliminación segura que impida su recuperación.
- **Criterios de Aceptación:**
    - Implementación de métodos de eliminación segura (e.g., sobrescritura, borrado criptográfico).
    - Eliminación automática de datos tras expirar el período de retención definido por la normativa sanitaria.
    - Registro de auditoría de los datos eliminados.
- **Prioridad:** Media
- **Categoría:** Protección de Datos Sensibles
- **Fuente/Norma Aplicable:** RGPD, Art. 17 y 32; ENS
- **Justificación:** Reduce el riesgo de filtraciones al eliminar correctamente los datos médicos cuando ya no son necesarios.

Requisitos de Transferencia Internacional de Datos

1. Restricción de Transferencias a Países con Protección Inadecuada

- **Identificador único:** PRIV-024
- **Título:** Restricción de Transferencias a Países sin Nivel Adecuado de Protección
- **Descripción:** La plataforma solo permitirá la transferencia de datos personales fuera del Espacio Económico Europeo (EEE) si el país de destino cuenta con un nivel de protección adecuado reconocido por la Comisión Europea o si se implementan garantías adecuadas.
- **Criterios de Aceptación:**
    - Bloqueo automático de transferencias a países sin decisión de adecuación de la Comisión Europea.
    - Aplicación de cláusulas contractuales tipo (CCT) o normas corporativas vinculantes (BCR) cuando sea necesario.
    - Registro de todas las transferencias internacionales de datos y su justificación legal.

- **Prioridad:** Alta
- **Categoría:** Transferencias Internacionales
- **Fuente/Norma Aplicable:** RGPD, Art. 44-45
- **Justificación:** Evita transferencias ilegales de datos personales a jurisdicciones con niveles insuficientes de protección.

---

2. Implementación de Cláusulas Contractuales Tipo (CCT)

- **Identificador único:** PRIV-025
- **Título:** Uso de Cláusulas Contractuales Tipo para Transferencias Internacionales
- **Descripción:** Cuando los datos deban transferirse a un país sin decisión de adecuación, la plataforma debe establecer Cláusulas Contractuales Tipo aprobadas por la Comisión Europea con los destinatarios de los datos.
- **Criterios de Aceptación:**
    - Implementación de CCT en todos los contratos con proveedores de servicios fuera del EEE.
    - Supervisión del cumplimiento de las CCT mediante auditorías internas.
    - Registro de los contratos que contienen las CCT y su aplicación efectiva.
- **Prioridad:** Alta
- **Categoría:** Transferencias Internacionales
- **Fuente/Norma Aplicable:** RGPD, Art. 46
- **Justificación:** Asegura la protección de los datos personales cuando sean transferidos a países sin reconocimiento de adecuación.

---

3. Evaluación de Riesgos antes de la Transferencia de Datos

- **Identificador único:** PRIV-026
- **Título:** Análisis de Impacto en la Protección de Datos (AIPD) para Transferencias Internacionales
- **Descripción:** Antes de realizar cualquier transferencia internacional de datos, la plataforma debe evaluar los riesgos asociados y documentar medidas de mitigación.
- **Criterios de Aceptación:**

    - Realización de un **Análisis de Impacto en la Protección de Datos (AIPD)** cuando se transfieran datos a terceros países.
    - Registro de las medidas implementadas para reducir los riesgos identificados.
    - Supervisión y actualización del AIPD según cambios en la normativa internacional.
- **Prioridad:** Alta
- **Categoría:** Transferencias Internacionales
- **Fuente/Norma Aplicable:** RGPD, Art. 35, 46
- **Justificación:** Permite identificar riesgos en las transferencias y asegurar el cumplimiento con el RGPD.

---

4. Transferencias Basadas en el Consentimiento del Usuario

- **Identificador único:** PRIV-027
- **Título:** Consentimiento Específico para Transferencias Internacionales
- **Descripción:** En caso de que no existan otras bases legales para la transferencia internacional de datos, se deberá obtener el **consentimiento explícito e informado** del usuario.
- **Criterios de Aceptación:**
    - Implementación de una opción en la plataforma para que los usuarios otorguen su consentimiento explícito antes de la transferencia de sus datos a países sin nivel adecuado de protección.
    - Presentación de una advertencia clara sobre los riesgos de la transferencia antes de obtener el consentimiento.
    - Registro de la fecha, hora y detalles del consentimiento otorgado por el usuario.
- **Prioridad:** Media
- **Categoría:** Transferencias Internacionales
- **Fuente/Norma Aplicable:** RGPD, Art. 49(1)(a)
- **Justificación:** Garantiza que los usuarios tomen decisiones informadas sobre la transferencia de sus datos personales.

---

5. Uso de Normas Corporativas Vinculantes (BCR)

- **Identificador único:** PRIV-028
- **Título:** Normas Corporativas Vinculantes para Empresas del Mismo Grupo
- **Descripción:** Si la plataforma pertenece a un grupo empresarial con sedes fuera del EEE, las transferencias internas de datos deben regirse por **Normas Corporativas Vinculantes (BCR)** aprobadas por las autoridades de protección de datos.
- **Criterios de Aceptación:**
    - Desarrollo y aplicación de BCR conforme a las directrices del Comité Europeo de Protección de Datos (CEPD).
    - Obtención de la aprobación de las autoridades competentes antes de la implementación de las BCR.
    - Verificación periódica del cumplimiento de las BCR dentro del grupo empresarial.
- **Prioridad:** Media
- **Categoría:** Transferencias Internacionales
- **Fuente/Norma Aplicable:** RGPD, Art. 47
- **Justificación:** Proporciona una base legal robusta para transferencias dentro de una misma organización multinacional.

---

6. Registro de Transferencias Internacionales

- **Identificador único:** PRIV-029
- **Título:** Registro de Transferencias de Datos Personales fuera del EEE
- **Descripción:** La plataforma debe mantener un registro de todas las transferencias internacionales de datos, incluyendo la base legal utilizada y las medidas de protección adoptadas.
- **Criterios de Aceptación:**
    - Creación de un registro accesible que documente cada transferencia internacional de datos.
    - Inclusión de detalles como la entidad destinataria, el país de destino, la base legal y la fecha de la transferencia.
    - Mecanismo para auditar y revisar regularmente las transferencias internacionales registradas.
- **Prioridad:** Alta
- **Categoría:** Transferencias Internacionales

- **Fuente/Norma Aplicable:** RGPD, Art. 30
- **Justificación:** Asegura la trazabilidad y el control sobre la transferencia de datos fuera del EEE.

Requisitos de Plazos de Conservación y Eliminación Segura de Datos

1. Definición de Plazos de Conservación de Datos

- **Identificador único:** PRIV-030
- **Título:** Establecimiento de Plazos de Conservación de Datos Personales
- **Descripción:** La plataforma debe definir y documentar los períodos de conservación de los datos personales en función de su finalidad y las normativas aplicables.
- **Criterios de Aceptación:**
    - Configuración de plazos de retención específicos según el tipo de dato (historia clínica, registros administrativos, consentimientos, etc.).
    - Aplicación automática de reglas de eliminación o anonimización tras el vencimiento del plazo.
    - Registro de las fechas de recogida y eliminación de los datos en un sistema de auditoría.
- **Prioridad:** Alta
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(e); LOPDGDD
- **Justificación:** Evita el almacenamiento innecesario de datos personales y minimiza riesgos en caso de brechas de seguridad.

---

2. Eliminación Segura de Datos Personales

- **Identificador único:** PRIV-031
- **Título:** Borrado Seguro de Datos Personales
- **Descripción:** Los datos personales deben ser eliminados de forma irrecuperable al finalizar su período de retención, salvo que deban conservarse por obligaciones legales.
- **Criterios de Aceptación:**
    - Implementación de técnicas de eliminación segura (e.g., sobrescritura múltiple, borrado criptográfico).

    - Eliminación irreversible de datos personales de copias de seguridad, registros y sistemas activos.
    - Registro de auditoría con detalles sobre la eliminación de los datos.
- **Prioridad:** Alta
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(e); LOPDGDD
- **Justificación:** Reduce el riesgo de recuperación indebida de datos eliminados y protege la privacidad de los usuarios.

---

3. Conservación Obligatoria de Datos Clínicos

- **Identificador único:** PRIV-032
- **Título:** Conservación de Historias Clínicas según Normativa Sanitaria
- **Descripción:** La plataforma debe garantizar que los datos de salud se conserven durante el período legalmente establecido en la normativa sanitaria antes de su eliminación o anonimización.
- **Criterios de Aceptación:**
    - Aplicación de períodos de conservación obligatorios según la normativa vigente en España y la UE.
    - Protección de los datos durante el período de retención contra accesos no autorizados.
    - Eliminación segura o anonimización de los datos tras el período de conservación.
- **Prioridad:** Alta
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** LOPDGDD, Normativa Sanitaria Española
- **Justificación:** Garantiza el cumplimiento de las leyes sanitarias en la gestión de historias clínicas y protege la confidencialidad de los pacientes.

---

4. Mecanismo de Eliminación Automática de Datos

- **Identificador único:** PRIV-033
- **Título:** Automatización del Borrado de Datos Tras Expirar su Período de Retención

- **Descripción:** La plataforma debe implementar un sistema automatizado para la eliminación o anonimización de los datos personales cuando ya no sean necesarios.
- **Criterios de Aceptación:**
    - Implementación de un proceso de eliminación periódica de datos vencidos.
    - Notificación a los administradores antes de eliminar datos críticos.
    - Mecanismo de auditoría para revisar la correcta eliminación de los datos.
- **Prioridad:** Media
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(e); LOPDGDD
- **Justificación:** Evita la retención innecesaria de datos y reduce la carga operativa en la gestión de la información.

---

5. Anonimización de Datos para Uso Posterior

- **Identificador único:** PRIV-034
- **Título:** Conversión de Datos Personales en Datos Anonimizados
- **Descripción:** En lugar de eliminar ciertos datos personales, la plataforma debe ofrecer la opción de anonimización para su uso en análisis, estadísticas o investigación.
- **Criterios de Aceptación:**
    - Implementación de un mecanismo que transforme datos personales en información anónima.
    - Verificación de que los datos anonimizados no permitan la reidentificación de los usuarios.
    - Restricción del acceso a los datos anonimizados a usuarios con permisos específicos.
- **Prioridad:** Media
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 89(1); ISO 27001
- **Justificación:** Facilita el aprovechamiento de datos para análisis sin comprometer la privacidad de los usuarios.

---

6. Registro de Auditoría para Seguimiento de Eliminaciones

- **Identificador único:** PRIV-035
- **Título:** Registro de Eliminaciones de Datos para Auditoría
- **Descripción:** Cada eliminación de datos personales debe quedar registrada con detalles como la fecha, el responsable de la acción y el método de eliminación utilizado.
- **Criterios de Aceptación:**
    - Implementación de un sistema de auditoría para registrar eliminaciones de datos personales.
    - Posibilidad de generar informes de auditoría para supervisión y cumplimiento normativo.
    - Mecanismos de alerta en caso de intentos de eliminación indebidos.
- **Prioridad:** Alta
- **Categoría:** Conservación y Eliminación de Datos
- **Fuente/Norma Aplicable:** RGPD, Art. 30; ENS; ISO 27001
- **Justificación:** Asegura la trazabilidad de las eliminaciones y permite detectar posibles accesos indebidos o errores en la gestión de datos.

Requisitos de Cifrado de Datos en Reposo y en Tránsito

1. Cifrado de Datos en Reposo

- **Identificador único:** SEG-001
- **Título:** Cifrado de Datos Almacenados
- **Descripción:** Todos los datos almacenados en la plataforma, incluyendo historias clínicas electrónicas, credenciales de usuario y registros de auditoría, deben estar cifrados con algoritmos robustos.
- **Criterios de Aceptación:**
    - Implementación de cifrado AES-256 o superior para bases de datos y archivos sensibles.
    - Cifrado automático de datos antes de su almacenamiento.
    - Restricción del acceso a claves de cifrado únicamente a personal autorizado.
    - Auditoría periódica de la efectividad del cifrado.
- **Prioridad:** Alta

- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Reduce el riesgo de exposición de datos en caso de acceso no autorizado o brecha de seguridad.

---

2. Cifrado de Datos en Tránsito

- **Identificador único:** SEG-002
- **Título:** Protección de Datos Durante la Transmisión
- **Descripción:** Toda la comunicación entre la plataforma y los usuarios debe estar protegida con cifrado de extremo a extremo, evitando la interceptación de datos durante la transmisión.
- **Criterios de Aceptación:**
    - Implementación de **TLS 1.2 o superior** para todas las conexiones web y API.
    - Uso de certificados digitales válidos emitidos por una Autoridad de Certificación de confianza.
    - Bloqueo de conexiones HTTP no seguras y redirección automática a HTTPS.
    - Cifrado de correos electrónicos que contengan datos sensibles.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Evita la interceptación de datos sensibles por parte de atacantes en redes no seguras.

---

3. Gestión Segura de Claves de Cifrado

- **Identificador único:** SEG-003
- **Título:** Administración y Protección de Claves de Cifrado
- **Descripción:** La plataforma debe implementar una política estricta para la gestión y almacenamiento seguro de claves criptográficas utilizadas en el cifrado de datos.
- **Criterios de Aceptación:**

    - Uso de **Hardware Security Modules (HSM)** o sistemas de gestión de claves centralizados.
    - Rotación periódica de claves de cifrado.
    - Restricción de acceso a claves a usuarios autorizados con autenticación multifactor (MFA).
    - Registro y auditoría de todas las operaciones con claves criptográficas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Previene accesos indebidos a claves de cifrado, garantizando la integridad y seguridad de los datos cifrados.

---

4. Cifrado de Copias de Seguridad

- **Identificador único:** SEG-004
- **Título:** Protección de Backups mediante Cifrado
- **Descripción:** Todas las copias de seguridad de la plataforma deben estar cifradas para evitar su acceso en caso de pérdida o robo.
- **Criterios de Aceptación:**
    - Cifrado automático de todas las copias de seguridad con **AES-256** o equivalente.
    - Almacenamiento de backups en ubicaciones seguras con acceso restringido.
    - Implementación de doble autenticación para la restauración de copias de seguridad.
    - Registro de auditoría de todas las operaciones de respaldo y recuperación.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Protege la confidencialidad de los datos médicos almacenados en copias de seguridad.

---

5. Monitorización y Prevención de Ataques a Canales Cifrados

- **Identificador único:** SEG-005
- **Título:** Detección y Protección Contra Ataques a Canales Cifrados
- **Descripción:** La plataforma debe contar con mecanismos de monitorización para detectar y prevenir ataques como **MITM (Man-in-the-Middle)** y vulnerabilidades en protocolos de cifrado.
- **Criterios de Aceptación:**
    - Implementación de herramientas de detección de ataques a tráfico cifrado (IDS/IPS).
    - Bloqueo de algoritmos de cifrado obsoletos (e.g., TLS 1.0, MD5, SHA-1).
    - Revisión periódica de configuraciones de seguridad en servidores y aplicaciones.
    - Notificación automática ante intentos de ataque detectados.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Refuerza la seguridad de las conexiones cifradas y previene ataques de interceptación de datos.

---

6. Verificación de Integridad de Datos Cifrados

- **Identificador único:** SEG-006
- **Título:** Validación de Integridad de Datos Protegidos
- **Descripción:** Los datos cifrados deben contar con mecanismos que aseguren su integridad y prevengan modificaciones no autorizadas.
- **Criterios de Aceptación:**
    - Implementación de funciones hash seguras (SHA-256 o superior) para verificar la integridad de datos cifrados.
    - Validación automática de datos tras procesos de cifrado y descifrado.
    - Registro de auditoría para detección de intentos de modificación no autorizados.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32

- **Justificación:** Garantiza que los datos almacenados no sean alterados sin autorización.

Requisitos de Autenticación Multifactor (MFA) para Usuarios Sensibles

1. Implementación Obligatoria de Autenticación Multifactor

- **Identificador único:** SEG-007
- **Título:** Requerimiento de MFA para Usuarios Sensibles
- **Descripción:** Todos los usuarios con acceso a información sensible (médicos, administradores y personal autorizado) deben utilizar **Autenticación Multifactor (MFA)** para acceder a la plataforma.
- **Criterios de Aceptación:**
    - Habilitación de MFA obligatoria para médicos, enfermeros y personal administrativo.
    - Uso de al menos **dos factores de autenticación**, combinando contraseña y un **segundo factor seguro** (TOTP, biometría, tarjeta criptográfica, SMS o autenticador móvil).
    - Bloqueo de acceso si no se supera la autenticación en dos factores.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001, RGPD Art. 32
- **Justificación:** Refuerza la seguridad de los accesos a datos críticos, evitando compromisos de credenciales.

---

2. Métodos de Autenticación Segura

- **Identificador único:** SEG-008
- **Título:** Métodos Aceptados para MFA
- **Descripción:** La plataforma debe soportar múltiples métodos de autenticación de segundo factor para que los usuarios elijan el más conveniente y seguro.
- **Criterios de Aceptación:**
    - Compatibilidad con aplicaciones de autenticación basadas en TOTP (Google Authenticator, Microsoft Authenticator).
    - Posibilidad de autenticación biométrica (huella dactilar, reconocimiento facial).

    - Opción de claves físicas (FIDO2, tarjetas criptográficas, YubiKey).
    - Desactivación del uso de SMS como único método de segundo factor por vulnerabilidad a ataques de SIM-swapping.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Permite mayor flexibilidad a los usuarios sin comprometer la seguridad.

---

3. Protección Contra Ataques de Fuerza Bruta y Phishing

- **Identificador único:** SEG-009
- **Título:** Prevención de Ataques de Acceso No Autorizado
- **Descripción:** Se deben aplicar controles para detectar y prevenir intentos de acceso fraudulentos o ataques de phishing.
- **Criterios de Aceptación:**
    - **Bloqueo de cuenta temporal** tras múltiples intentos fallidos de autenticación.
    - **Verificación de dispositivos confiables**, permitiendo solo accesos desde dispositivos previamente registrados.
    - **Protección contra phishing**, deshabilitando autenticaciones MFA en enlaces inseguros y promoviendo autenticadores de hardware.
    - **Registro de accesos y alertas en caso de detección de intentos de acceso sospechosos.**
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Minimiza riesgos de ataques dirigidos contra cuentas de usuarios con acceso privilegiado.

---

4. Configuración de Reglas de Acceso Basadas en Contexto

- **Identificador único:** SEG-010
- **Título:** Autenticación Adaptativa Según Riesgo

- **Descripción:** El sistema debe evaluar el contexto del intento de inicio de sesión y aplicar controles adicionales en caso de detectar anomalías.
- **Criterios de Aceptación:**
    - **Verificación de ubicación geográfica**, bloqueando accesos desde países no autorizados.
    - **Evaluación de dispositivo y navegador**, solicitando autenticación adicional en caso de uso de dispositivos desconocidos.
    - **Control de horarios de acceso**, restringiendo el inicio de sesión fuera de horarios laborales predefinidos.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Permite aplicar restricciones dinámicas para aumentar la seguridad sin afectar la usabilidad.

---

5. Administración Segura de Códigos de Recuperación

- **Identificador único:** SEG-011
- **Título:** Generación y Protección de Códigos de Recuperación de MFA
- **Descripción:** En caso de pérdida del segundo factor de autenticación, los usuarios deben contar con un método seguro de recuperación de acceso.
- **Criterios de Aceptación:**
    - Generación de **códigos de recuperación únicos y de un solo uso** para restablecer MFA.
    - Almacenamiento de códigos de recuperación solo en formato cifrado.
    - Implementación de un proceso seguro para solicitar la regeneración de códigos en caso de pérdida.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Evita accesos no autorizados y mantiene la disponibilidad del sistema en caso de pérdida del segundo factor.

---

6. Registro de Auditoría y Supervisión de Accesos con MFA

- **Identificador único:** SEG-012
- **Título:** Registro y Monitorización de Accesos con MFA
- **Descripción:** Todos los accesos autenticados con MFA deben ser registrados y monitoreados para detectar posibles actividades sospechosas.
- **Criterios de Aceptación:**
    - Registro en **logs de auditoría** de cada intento de autenticación, con detalles de usuario, IP, dispositivo y resultado del acceso.
    - **Alertas automáticas** en caso de múltiples intentos fallidos o cambios sospechosos en la configuración de MFA.
    - Generación de **informes periódicos** sobre accesos y fallos de autenticación para revisión por el equipo de seguridad.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Proporciona trazabilidad y detección temprana de intentos de acceso fraudulentos.

Requisitos de Registro de Auditoría y Trazabilidad de Accesos y Modificaciones

1. Registro de Accesos a la Plataforma

- **Identificador único:** SEG-013
- **Título:** Registro de Inicios de Sesión y Accesos a Datos
- **Descripción:** La plataforma debe registrar **todos los accesos de usuarios**, incluyendo médicos, personal administrativo y pacientes, con el fin de mantener una trazabilidad completa.
- **Criterios de Aceptación:**
    - Registro de **fecha, hora, usuario, IP de origen, dispositivo y resultado del acceso** (éxito/fallo).
    - Registro de accesos a **historias clínicas electrónicas y datos sensibles**.
    - Alertas de seguridad en caso de intentos de acceso fallidos reiterados o desde ubicaciones sospechosas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información

- **Fuente/Norma Aplicable:** ENS, ISO 27001, RGPD Art. 32
- **Justificación:** Permite identificar accesos indebidos y posibles intentos de intrusión en el sistema.

---

2. Registro de Modificaciones en los Datos

- **Identificador único:** SEG-014
- **Título:** Auditoría de Modificaciones en Datos de Pacientes
- **Descripción:** Todos los cambios en los datos de los pacientes, incluyendo ediciones y eliminaciones, deben quedar registrados en el sistema de auditoría.
- **Criterios de Aceptación:**
    - Registro detallado de **quién modificó qué datos y cuándo**.
    - Registro de la **versión anterior y posterior** de los datos modificados.
    - Implementación de una función de **reversión de cambios en caso de error o actividad sospechosa**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001, RGPD Art. 30
- **Justificación:** Asegura la integridad de los datos clínicos y permite rastrear actividades sospechosas o errores humanos.

---

3. Registro de Intentos de Acceso Fallidos y Bloqueos

- **Identificador único:** SEG-015
- **Título:** Registro de Intentos de Autenticación Fallidos
- **Descripción:** La plataforma debe registrar todos los intentos de acceso fallidos para detectar intentos de ataque y fraudes.
- **Criterios de Aceptación:**
    - Registro de intentos de inicio de sesión fallidos con detalle de **IP, usuario y motivo del fallo**.
    - Bloqueo automático de la cuenta tras un número definido de intentos fallidos.
    - Notificación al usuario y a los administradores en caso de intentos reiterados desde una misma IP o patrón sospechoso.

- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Reduce riesgos de ataques de fuerza bruta y phishing, protegiendo las credenciales de los usuarios.

---

4. Registro de Actividades de Usuarios con Privilegios

- **Identificador único:** SEG-016
- **Título:** Monitorización de Actividades de Administradores y Usuarios con Privilegios
- **Descripción:** Todas las acciones realizadas por usuarios con permisos administrativos deben ser registradas para garantizar el cumplimiento de seguridad.
- **Criterios de Aceptación:**
    - Registro de **acciones realizadas por administradores y personal técnico** (creación, eliminación o modificación de cuentas, ajustes de permisos, cambios en configuración).
    - Alertas automáticas ante **modificaciones críticas** realizadas por usuarios con privilegios.
    - Revisión periódica de los registros de actividad por parte del equipo de seguridad.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Evita abusos de privilegios y permite detectar actividades sospechosas dentro de la plataforma.

---

5. Almacenamiento Seguro y Protección de los Registros de Auditoría

- **Identificador único:** SEG-017
- **Título:** Protección y Conservación de Logs de Auditoría
- **Descripción:** Los registros de auditoría deben almacenarse de manera segura y ser protegidos contra modificaciones no autorizadas.
- **Criterios de Aceptación:**

    - **Cifrado de registros de auditoría** con AES-256.
    - Restricción del acceso a logs solo a personal autorizado.
    - **Retención de registros durante al menos 2 años**, según la normativa vigente.
    - Implementación de medidas contra manipulación y eliminación de logs sin autorización.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001, RGPD Art. 30
- **Justificación:** Garantiza la integridad y trazabilidad de los registros, evitando su manipulación o eliminación indebida.

---

6. Generación de Reportes de Seguridad y Análisis Periódico

- **Identificador único:** SEG-018
- **Título:** Supervisión y Reportes de Seguridad
- **Descripción:** Se deben generar informes periódicos sobre los accesos y modificaciones registradas en la plataforma para detectar anomalías y posibles amenazas.
- **Criterios de Aceptación:**
    - Generación de reportes **diarios/semanales/mensuales** de accesos y modificaciones.
    - Identificación de patrones anómalos en el uso del sistema.
    - Notificación automática al equipo de seguridad en caso de actividades sospechosas.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Facilita la detección temprana de incidentes de seguridad y permite tomar acciones correctivas.

Requisitos de Control de Acceso Basado en Roles (RBAC)

1. Implementación de Control de Acceso por Roles

- **Identificador único:** SEG-019
- **Título:** Asignación de Permisos Según Rol del Usuario
- **Descripción:** La plataforma debe aplicar un modelo **RBAC** que asigne permisos a los usuarios en función de su rol dentro del sistema.
- **Criterios de Aceptación:**
    - Definición de roles predeterminados (e.g., **médico, enfermero, administrativo, paciente**).
    - Restricción de acceso a datos sensibles solo a personal autorizado.
    - Validación de permisos antes de ejecutar cualquier acción dentro del sistema.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Minimiza el riesgo de acceso indebido a información crítica y refuerza la seguridad de los datos clínicos.

---

2. Principio de Mínimos Privilegios

- **Identificador único:** SEG-020
- **Título:** Aplicación del Principio de Privilegios Mínimos
- **Descripción:** Cada usuario solo debe tener acceso a los datos y funcionalidades estrictamente necesarias para el desempeño de sus funciones.
- **Criterios de Aceptación:**
    - Restricción del acceso a datos médicos solo a personal sanitario autorizado.
    - Limitación de permisos administrativos a los responsables del sistema.
    - Revisión periódica de permisos para evitar accesos innecesarios.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Reduce la superficie de ataque y previene accesos no autorizados a información confidencial.

---

3. Autorización y Validación de Permisos

- **Identificador único:** SEG-021
- **Título:** Verificación de Permisos Antes de Ejecutar Acciones
- **Descripción:** Antes de acceder a datos sensibles o realizar acciones críticas, la plataforma debe verificar los permisos del usuario.
- **Criterios de Aceptación:**
    - Implementación de controles de acceso antes de cada consulta o modificación de datos.
    - Bloqueo de intentos de acceso a funcionalidades restringidas.
    - Registro en auditoría de intentos fallidos de acceso a información protegida.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Evita accesos indebidos a información crítica y permite detectar intentos de abuso de privilegios.

---

4. Revisión Periódica de Permisos de Usuario

- **Identificador único:** SEG-022
- **Título:** Auditoría de Permisos y Roles de Usuarios
- **Descripción:** La plataforma debe realizar revisiones periódicas de los permisos otorgados a los usuarios para evitar accesos innecesarios.
- **Criterios de Aceptación:**
    - Implementación de un proceso de revisión de permisos cada **6 meses**.
    - Desactivación automática de cuentas inactivas por más de un tiempo definido (ejemplo: **90 días**).
    - Registro de auditoría de modificaciones en los permisos de usuario.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Reduce riesgos derivados de cuentas con permisos excesivos o que ya no son necesarias.

---

5. Control de Accesos a Datos Clínicos y Personales

- **Identificador único:** SEG-023
- **Título:** Restricción de Acceso a Datos Sensibles
- **Descripción:** La plataforma debe garantizar que solo los profesionales autorizados puedan acceder a los datos clínicos y personales de los pacientes.
- **Criterios de Aceptación:**
    - Restricción de acceso a historias clínicas únicamente a médicos y enfermeros.
    - Impedir que personal administrativo acceda a datos médicos sensibles.
    - Implementación de permisos diferenciados para acceso a datos personales y clínicos.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, RGPD Art. 32
- **Justificación:** Protege la privacidad del paciente y evita accesos indebidos a información médica.

---

6. Control de Permisos Temporales para Accesos Excepcionales

- **Identificador único:** SEG-024
- **Título:** Gestión de Permisos Temporales para Accesos Excepcionales
- **Descripción:** En casos justificados, la plataforma debe permitir accesos temporales a datos sensibles bajo supervisión.
- **Criterios de Aceptación:**
    - Implementación de solicitudes de acceso temporal con autorización previa.
    - Definición de un **tiempo máximo de acceso** antes de la revocación automática.
    - Registro detallado en auditoría de accesos temporales otorgados.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS

- **Justificación:** Permite gestionar situaciones excepcionales sin comprometer la seguridad de los datos.

---

7. Registro y Auditoría de Cambios en Permisos de Usuarios

- **Identificador único:** SEG-025
- **Título:** Auditoría de Modificaciones en Permisos de Usuario
- **Descripción:** Todas las modificaciones en los permisos de los usuarios deben ser registradas para garantizar trazabilidad y detectar posibles fraudes internos.
- **Criterios de Aceptación:**
    - Registro de cambios en permisos con detalle de **quién, cuándo y qué permisos fueron modificados**.
    - Alertas automáticas cuando se asignen permisos administrativos o acceso a datos sensibles.
    - Revisión periódica de cambios en permisos para detectar actividades sospechosas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Garantiza la transparencia en la gestión de accesos y previene posibles abusos de privilegios.

Requisitos de Protección contra Accesos No Autorizados y Amenazas Externas

1. Implementación de Firewalls y Filtrado de Tráfico

- **Identificador único:** SEG-026
- **Título:** Protección del Tráfico de Red con Firewalls y Filtrado
- **Descripción:** La plataforma debe contar con firewalls que controlen el tráfico entrante y saliente, bloqueando accesos no autorizados y ataques cibernéticos.
- **Criterios de Aceptación:**
    - Configuración de **firewalls de aplicación web (WAF)** para filtrar tráfico malicioso.
    - Filtrado de **IPs sospechosas o provenientes de regiones de alto riesgo**.

    - Monitorización del tráfico en tiempo real con alertas ante intentos de intrusión.
- **Prioridad:** Alta
- **Categoría:** Seguridad Perimetral
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Protege contra ataques de red y accesos no autorizados a la plataforma.

---

2. Implementación de Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)

- **Identificador único:** SEG-027
- **Título:** Monitoreo de Actividades Sospechosas con IDS/IPS
- **Descripción:** La plataforma debe integrar sistemas de detección y prevención de intrusiones para identificar y bloquear ataques en tiempo real.
- **Criterios de Aceptación:**
    - Implementación de un **IDS/IPS** para analizar tráfico sospechoso.
    - Generación de alertas ante intentos de acceso o patrones de ataque.
    - Bloqueo automático de direcciones IP que intenten explotar vulnerabilidades.
- **Prioridad:** Alta
- **Categoría:** Seguridad Perimetral
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Permite detectar y responder a intentos de ataque antes de que comprometan el sistema.

---

3. Protección contra Ataques de Fuerza Bruta

- **Identificador único:** SEG-028
- **Título:** Prevención de Ataques de Fuerza Bruta en Autenticación
- **Descripción:** La plataforma debe contar con medidas para bloquear intentos repetidos de acceso no autorizado mediante ataques de fuerza bruta.
- **Criterios de Aceptación:**
    - **Bloqueo temporal de cuentas** tras múltiples intentos fallidos de inicio de sesión.

    - Implementación de **captcha** tras intentos de acceso fallidos consecutivos.
    - Registro y monitoreo de intentos de autenticación fallidos.
- **Prioridad:** Alta
- **Categoría:** Seguridad de Accesos
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Evita que atacantes prueben combinaciones de credenciales para acceder a cuentas de usuario.

---

4. Protección contra Ataques de Denegación de Servicio (DDoS)

- **Identificador único:** SEG-029
- **Título:** Mitigación de Ataques DDoS
- **Descripción:** La plataforma debe contar con mecanismos para detectar y mitigar ataques de denegación de servicio (DDoS).
- **Criterios de Aceptación:**
    - Implementación de una **red de distribución de contenido (CDN)** para absorber tráfico malicioso.
    - Filtrado y bloqueo automático de tráfico anómalo en servidores.
    - Alertas en caso de detección de tráfico inusualmente elevado.
- **Prioridad:** Alta
- **Categoría:** Seguridad Perimetral
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Garantiza la disponibilidad del sistema ante ataques masivos que intenten interrumpir el servicio.

---

5. Protección contra Ataques de Ingeniería Social y Phishing

- **Identificador único:** SEG-030
- **Título:** Prevención de Ataques de Phishing e Ingeniería Social
- **Descripción:** La plataforma debe implementar medidas para prevenir fraudes basados en ingeniería social y ataques de phishing.
- **Criterios de Aceptación:**

    - Uso de **alertas en correos electrónicos sospechosos** que intenten suplantar la identidad de la plataforma.
    - Implementación de **políticas de seguridad para evitar compartir credenciales**.
    - **Capacitación periódica a los usuarios** sobre cómo identificar intentos de phishing.
- **Prioridad:** Media
- **Categoría:** Seguridad de Accesos
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Reduce el riesgo de que los usuarios sean engañados para revelar información sensible.

---

6. Control de Acceso a la Infraestructura y Monitorización de Sesiones

- **Identificador único:** SEG-031
- **Título:** Monitorización de Sesiones y Accesos a Infraestructura
- **Descripción:** Debe existir un sistema que controle los accesos a la infraestructura de la plataforma y detecte sesiones sospechosas.
- **Criterios de Aceptación:**
    - Implementación de **registro detallado de sesiones de usuario**.
    - Desconexión automática de sesiones inactivas por un período prolongado.
    - Restricción de acceso a la infraestructura solo a personal autorizado mediante VPN o redes seguras.
- **Prioridad:** Alta
- **Categoría:** Seguridad de Accesos
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Protege el acceso a la infraestructura del sistema y evita accesos indebidos.

---

7. Aplicación de Parcheo y Gestión de Vulnerabilidades

- **Identificador único:** SEG-032
- **Título:** Actualización y Corrección de Vulnerabilidades

- **Descripción:** La plataforma debe contar con un proceso de gestión de vulnerabilidades para detectar y corregir fallos de seguridad de manera proactiva.
- **Criterios de Aceptación:**
    - Implementación de **escaneos de vulnerabilidades periódicos**.
    - Aplicación de **actualizaciones y parches de seguridad** en sistemas y dependencias.
    - Notificación de vulnerabilidades críticas al equipo de seguridad y remediación en un tiempo máximo definido.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Reduce el riesgo de explotación de vulnerabilidades en la plataforma.

Requisitos de Seguridad Física y Lógica de los Centros de Datos

1. Control de Acceso Físico a los Centros de Datos

- **Identificador único:** SEG-033
- **Título:** Restricción de Acceso Físico a Personal Autorizado
- **Descripción:** El acceso a los centros de datos donde se almacena la plataforma debe estar limitado únicamente a personal autorizado.
- **Criterios de Aceptación:**
    - Implementación de **sistemas de control de acceso** (tarjetas RFID, biometría o códigos de seguridad).
    - Registro de accesos con **fecha, hora y persona autorizada**.
    - Implementación de zonas restringidas con acceso segmentado según roles.
- **Prioridad:** Alta
- **Categoría:** Seguridad Física
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Protege la infraestructura crítica de accesos no autorizados.

---

2. Protección Contra Incidentes Físicos (Incendios, Inundaciones, Cortes de Energía)

- **Identificador único:** SEG-034
- **Título:** Medidas de Protección ante Incidentes Físicos
- **Descripción:** Los centros de datos deben contar con medidas de seguridad para mitigar riesgos físicos como incendios, inundaciones o cortes eléctricos.
- **Criterios de Aceptación:**
    - Instalación de **sistemas de detección y extinción de incendios**.
    - Implementación de **sistemas de alimentación ininterrumpida (UPS)** y generadores eléctricos de respaldo.
    - Uso de **sensores de temperatura y humedad** para monitoreo en tiempo real.
- **Prioridad:** Alta
- **Categoría:** Seguridad Física
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Evita la interrupción del servicio por desastres físicos.

---

3. Monitoreo y Vigilancia de los Centros de Datos

- **Identificador único:** SEG-035
- **Título:** Sistemas de Videovigilancia y Detección de Intrusos
- **Descripción:** Se deben implementar sistemas de vigilancia para monitorear en tiempo real el acceso y las actividades dentro del centro de datos.
- **Criterios de Aceptación:**
    - Instalación de **cámaras de seguridad con grabación 24/7**.
    - Implementación de **sensores de movimiento y alarmas** en puntos de acceso.
    - Revisión periódica de registros de videovigilancia y alertas de seguridad.
- **Prioridad:** Media
- **Categoría:** Seguridad Física
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Permite detectar y prevenir accesos no autorizados o actividades sospechosas.

---

4. Segmentación de Redes y Protección Lógica

- **Identificador único:** SEG-036
- **Título:** Separación de Redes y Accesos Internos
- **Descripción:** Los sistemas críticos dentro del centro de datos deben estar segmentados para evitar accesos no autorizados entre ellos.
- **Criterios de Aceptación:**
    - Implementación de **segmentación de redes VLAN** para separar servicios críticos.
    - Restricción de accesos entre entornos de producción, pruebas y desarrollo.
    - Uso de **firewalls internos** para controlar el tráfico entre servidores.
- **Prioridad:** Alta
- **Categoría:** Seguridad Lógica
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Reduce el impacto de ataques internos y evita accesos indebidos a sistemas críticos.

---

5. Cifrado de Datos en los Servidores

- **Identificador único:** SEG-037
- **Título:** Cifrado de Información Sensible en Almacenamiento
- **Descripción:** Los datos almacenados en los servidores dentro del centro de datos deben estar cifrados para prevenir accesos no autorizados.
- **Criterios de Aceptación:**
    - Implementación de **cifrado AES-256** para bases de datos y archivos críticos.
    - Gestión segura de claves de cifrado mediante **Hardware Security Modules (HSM)**.
    - Restricción del acceso a claves de cifrado solo a personal autorizado.
- **Prioridad:** Alta
- **Categoría:** Seguridad Lógica
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Asegura la confidencialidad de los datos almacenados y minimiza riesgos en caso de accesos no autorizados.

---

6. Registro y Auditoría de Accesos a la Infraestructura

- **Identificador único:** SEG-038
- **Título:** Monitoreo de Accesos a la Infraestructura del Centro de Datos
- **Descripción:** Todos los accesos y modificaciones en la infraestructura del centro de datos deben ser registrados y auditados periódicamente.
- **Criterios de Aceptación:**
    - Registro de **accesos físicos y lógicos** a la infraestructura.
    - Implementación de **alertas en tiempo real** ante accesos no autorizados.
    - Auditoría periódica de registros para detectar posibles incidentes de seguridad.
- **Prioridad:** Alta
- **Categoría:** Seguridad Física y Lógica
- **Fuente/Norma Aplicable:** ISO 27001, ENS
- **Justificación:** Garantiza la trazabilidad y permite detectar actividades sospechosas.

---

7. Protección contra Ataques a la Infraestructura (Seguridad Perimetral)

- **Identificador único:** SEG-039
- **Título:** Seguridad Perimetral para la Infraestructura del Centro de Datos
- **Descripción:** Deben implementarse medidas de seguridad perimetral para evitar accesos físicos no autorizados al centro de datos.
- **Criterios de Aceptación:**
    - Instalación de **vallas de seguridad y acceso controlado** en instalaciones del centro de datos.
    - Implementación de **protocolos de seguridad para visitas** (autorización previa y registro).
    - Presencia de **seguridad física 24/7** en el centro de datos.
- **Prioridad:** Media
- **Categoría:** Seguridad Física
- **Fuente/Norma Aplicable:** ISO 27001, ENS

- **Justificación:** Protege la infraestructura contra accesos no autorizados y ataques físicos.

Requisitos de Cumplimiento con el RGPD y LOPDGDD en el Tratamiento de Datos de Salud

1. Legitimidad del Tratamiento de Datos de Salud

- **Identificador único:** LEG-001
- **Título:** Base Legal para el Tratamiento de Datos Médicos
- **Descripción:** El tratamiento de datos de salud solo podrá realizarse bajo una base legal válida, como el consentimiento explícito del paciente, la necesidad para la prestación de servicios sanitarios o el cumplimiento de una obligación legal.
- **Criterios de Aceptación:**
    - Justificación de la base legal utilizada en cada tratamiento de datos médicos.
    - Implementación de mecanismos de **obtención y registro de consentimiento** para tratamientos no obligatorios.
    - Cumplimiento con el **Artículo 9 del RGPD** sobre categorías especiales de datos.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 6 y 9; LOPDGDD
- **Justificación:** Asegura que el tratamiento de datos médicos se realice conforme a la legalidad, evitando sanciones.

---

2. Registro de Actividades de Tratamiento

- **Identificador único:** LEG-002
- **Título:** Documentación de Procesos de Tratamiento de Datos
- **Descripción:** Se debe llevar un **Registro de Actividades de Tratamiento (RAT)** donde se documenten todos los procesos relacionados con datos de salud, sus finalidades y medidas de seguridad aplicadas.
- **Criterios de Aceptación:**
    - Registro de **quién, cómo y por qué** se tratan los datos médicos.

    - Indicación de la base legal que justifica cada tratamiento.
    - Actualización periódica del registro según cambios en la normativa o el sistema.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 30; LOPDGDD
- **Justificación:** Asegura la trazabilidad y el cumplimiento normativo de los tratamientos de datos de salud.

---

3. Derechos de los Pacientes sobre sus Datos de Salud

- **Identificador único:** LEG-003
- **Título:** Garantía de los Derechos de los Pacientes sobre sus Datos
- **Descripción:** La plataforma debe permitir a los pacientes ejercer sus **derechos de acceso, rectificación, supresión, oposición y portabilidad** de sus datos personales y de salud.
- **Criterios de Aceptación:**
    - Implementación de una funcionalidad que permita a los pacientes **consultar y descargar su historia clínica** en formatos estructurados (ej. PDF, FHIR).
    - Mecanismo para que los usuarios soliciten la **rectificación o eliminación de datos** conforme a la normativa.
    - Procedimiento de verificación de identidad antes de procesar solicitudes.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 15-21; LOPDGDD
- **Justificación:** Garantiza el ejercicio de los derechos de los pacientes sobre su información personal.

---

4. Minimización y Limitación de Datos

- **Identificador único:** LEG-004
- **Título:** Limitación del Tratamiento de Datos Médicos al Mínimo Necesario

- **Descripción:** Solo se deben tratar los datos estrictamente necesarios para la finalidad establecida, evitando la recopilación y almacenamiento excesivo de información médica.
- **Criterios de Aceptación:**
    - Definición de **perfiles de acceso** con datos visibles según el rol del usuario.
    - Eliminación de datos innecesarios tras cumplir su finalidad.
    - Evaluación periódica de los datos almacenados para detectar información redundante.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 5(1)(c); LOPDGDD
- **Justificación:** Evita el almacenamiento masivo de información innecesaria, reduciendo riesgos de seguridad.

---

5. Seguridad en la Transferencia de Datos de Salud

- **Identificador único:** LEG-005
- **Título:** Protección de la Interoperabilidad y Transferencia de Datos Médicos
- **Descripción:** Toda transferencia de datos médicos debe realizarse utilizando mecanismos seguros y cumpliendo con las normativas de interoperabilidad sanitaria.
- **Criterios de Aceptación:**
    - Uso de **cifrado de extremo a extremo** en la transmisión de datos clínicos.
    - Implementación de protocolos **FHIR o HL7** para el intercambio seguro de información médica.
    - Registro de auditoría de todas las transferencias realizadas entre sistemas sanitarios.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 32; LOPDGDD
- **Justificación:** Protege la confidencialidad de la información médica y facilita su interoperabilidad con otros sistemas.

---

6. Evaluación de Impacto en la Protección de Datos de Salud (AIPD)

- **Identificador único:** LEG-006
- **Título:** Análisis de Impacto en Protección de Datos (AIPD)
- **Descripción:** Antes de iniciar cualquier tratamiento de datos médicos que implique alto riesgo para la privacidad, se debe realizar un **Análisis de Impacto en la Protección de Datos (AIPD)**.
- **Criterios de Aceptación:**
    - Evaluación de riesgos asociados al tratamiento de datos médicos.
    - Implementación de **medidas de mitigación de riesgos** antes del despliegue del sistema.
    - Revisión del AIPD cuando se introduzcan nuevas funcionalidades que afecten la privacidad.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 35; LOPDGDD
- **Justificación:** Permite identificar y reducir los riesgos de privacidad antes de la implementación del sistema.

---

7. Notificación de Brechas de Seguridad

- **Identificador único:** LEG-007
- **Título:** Procedimiento de Notificación de Incidentes de Seguridad
- **Descripción:** En caso de una brecha de seguridad que afecte datos médicos, la organización debe notificar a las autoridades y usuarios afectados dentro del plazo establecido por el RGPD.
- **Criterios de Aceptación:**
    - Implementación de un protocolo de **detección, contención y reporte de brechas de seguridad**.
    - Notificación a la Agencia Española de Protección de Datos (AEPD) dentro de las **72 horas posteriores a la detección del incidente**.
    - Comunicación a los pacientes afectados con información clara sobre el impacto de la brecha y medidas correctivas.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo

- **Fuente/Norma Aplicable:** RGPD, Art. 33-34; LOPDGDD
- **Justificación:** Cumple con la obligación de transparencia y permite mitigar el impacto de posibles incidentes de seguridad.

Requisitos de Adopción del Esquema Nacional de Seguridad (ENS) para Protección de Datos Sensibles

1. Clasificación y Categorización de la Información Sensible

- **Identificador único:** LEG-008
- **Título:** Identificación y Clasificación de los Datos Sensibles
- **Descripción:** La plataforma debe categorizar la información que gestiona según su **criticidad, confidencialidad, integridad y disponibilidad**, conforme a los niveles del ENS.
- **Criterios de Aceptación:**
    - Identificación de **datos de nivel ALTO** para la información de salud.
    - Documentación de la clasificación en una **política de seguridad de la información**.
    - Implementación de controles específicos según la criticidad de los datos.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** ENS, RD 311/2022
- **Justificación:** Asegura la aplicación de medidas de protección adecuadas a la sensibilidad de los datos.

---

2. Seguridad en la Gestión de Accesos y Privilegios

- **Identificador único:** LEG-009
- **Título:** Control de Accesos Según el Nivel de Seguridad del ENS
- **Descripción:** Los accesos a la plataforma deben gestionarse según el **principio de mínimo privilegio**, limitando la exposición de datos sensibles.
- **Criterios de Aceptación:**
    - Aplicación de **autenticación multifactor (MFA)** para usuarios con acceso a información crítica.

    - Implementación de **roles diferenciados** para personal sanitario, administrativo y pacientes.
    - Monitorización y auditoría de los accesos a datos sensibles.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Garantiza que solo usuarios autorizados puedan acceder a información de salud crítica.

---

3. Medidas de Seguridad en la Infraestructura Tecnológica

- **Identificador único:** LEG-010
- **Título:** Protección de la Infraestructura Conforme al ENS
- **Descripción:** La plataforma debe implementar medidas de **seguridad perimetral, monitorización y gestión de incidentes** para prevenir accesos no autorizados y ataques cibernéticos.
- **Criterios de Aceptación:**
    - Implementación de **firewalls perimetrales y sistemas de detección de intrusos (IDS/IPS)**.
    - Uso de **redes segmentadas** para separar los datos críticos del resto de la infraestructura.
    - Monitoreo en tiempo real con alertas ante accesos sospechosos o intentos de intrusión.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Reduce la superficie de ataque y fortalece la seguridad de la infraestructura donde se almacenan los datos médicos.

---

4. Registro y Auditoría de Incidentes de Seguridad

- **Identificador único:** LEG-011
- **Título:** Detección y Registro de Incidentes de Seguridad
- **Descripción:** Todo incidente de seguridad debe registrarse y gestionarse conforme a los protocolos del ENS, asegurando una respuesta rápida y eficaz.

- **Criterios de Aceptación:**
    - Registro de **todos los incidentes de seguridad** en un sistema de gestión de eventos.
    - Notificación de incidentes a la Agencia Española de Protección de Datos (AEPD) cuando corresponda.
    - Implementación de **protocolos de contención, respuesta y recuperación**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, RGPD, ISO 27001
- **Justificación:** Permite responder de manera eficiente a incidentes de seguridad y minimizar su impacto.

---

5. Resiliencia y Plan de Continuidad del Servicio

- **Identificador único:** LEG-012
- **Título:** Plan de Continuidad y Recuperación ante Desastres
- **Descripción:** La plataforma debe contar con un **Plan de Continuidad del Negocio (BCP)** y **Planes de Recuperación ante Desastres (DRP)** para garantizar la disponibilidad de los datos y servicios.
- **Criterios de Aceptación:**
    - Definición de **procedimientos para recuperación ante fallos** y ataques cibernéticos.
    - Implementación de **copias de seguridad cifradas y redundantes** en ubicaciones separadas.
    - Simulación de pruebas periódicas de recuperación de datos y continuidad operativa.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Asegura la disponibilidad y continuidad del servicio en caso de incidentes o ataques.

---

6. Aplicación del Principio de Seguridad por Defecto y Seguridad por Diseño

- **Identificador único:** LEG-013
- **Título:** Implementación de Seguridad desde el Diseño
- **Descripción:** La plataforma debe integrar medidas de seguridad desde la fase de diseño del sistema, siguiendo el principio de **Privacy by Design y Security by Default**.
- **Criterios de Aceptación:**
    - Incorporación de controles de seguridad desde la fase de desarrollo del software.
    - Aplicación de **políticas de cifrado, acceso restringido y anonimización de datos** desde el inicio.
    - Evaluaciones de seguridad continuas para la detección de vulnerabilidades en el código.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, RGPD, ISO 27001
- **Justificación:** Garantiza que la seguridad esté integrada en todas las fases del desarrollo del sistema.

---

7. Verificación y Auditoría del Cumplimiento del ENS

- **Identificador único:** LEG-014
- **Título:** Auditoría y Certificación del Cumplimiento del ENS
- **Descripción:** La plataforma debe someterse a auditorías periódicas para verificar su cumplimiento con el ENS y mejorar sus medidas de seguridad.
- **Criterios de Aceptación:**
    - Realización de **auditorías de seguridad anual** conforme a las directrices del ENS.
    - Corrección y mejora continua basada en los resultados de las auditorías.
    - Obtención de la certificación ENS si es requerida para su operación.
- **Prioridad:** Media
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Garantiza que la plataforma cumple con los estándares de seguridad exigidos por la normativa española.

Requisitos de Aplicación de la ISO/IEC 27001 para la Gestión de Seguridad de la Información

1. Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

- **Identificador único:** LEG-015
- **Título:** Adopción del SGSI según ISO 27001
- **Descripción:** La plataforma debe contar con un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en la norma ISO 27001 para garantizar la protección de los datos médicos.
- **Criterios de Aceptación:**
    - Definición de **políticas de seguridad de la información** alineadas con la ISO 27001.
    - Implementación de **controles de seguridad** para gestionar riesgos de la información.
    - Evaluación y mejora continua del SGSI a través de auditorías internas.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Garantiza la gestión integral de la seguridad de la información en la plataforma.

---

2. Evaluación y Gestión de Riesgos de Seguridad

- **Identificador único:** LEG-016
- **Título:** Análisis y Mitigación de Riesgos de Seguridad
- **Descripción:** La plataforma debe contar con un proceso de **identificación, evaluación y mitigación de riesgos** relacionados con la seguridad de los datos médicos.
- **Criterios de Aceptación:**
    - Realización de un **Análisis de Riesgos** conforme a la metodología ISO 27005.

    - Implementación de **medidas de mitigación** para los riesgos detectados.
    - Revisión periódica de los riesgos de seguridad y actualización de las estrategias de mitigación.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ISO/IEC 27005
- **Justificación:** Reduce la probabilidad de incidentes de seguridad y protege los datos de salud.

---

3. Cifrado y Protección de la Información Médica

- **Identificador único:** LEG-017
- **Título:** Cifrado de Datos Sensibles Según ISO 27001
- **Descripción:** Los datos almacenados y transmitidos deben ser protegidos mediante **mecanismos de cifrado robustos** para garantizar su confidencialidad.
- **Criterios de Aceptación:**
    - Implementación de **cifrado AES-256** para bases de datos y almacenamiento.
    - Uso de **TLS 1.2 o superior** en la transmisión de datos.
    - Protección de claves criptográficas mediante **Hardware Security Modules (HSM)**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ISO/IEC 27002
- **Justificación:** Protege la integridad y confidencialidad de los datos médicos almacenados y transmitidos.

---

4. Control de Accesos y Autenticación Segura

- **Identificador único:** LEG-018
- **Título:** Gestión Segura de Accesos y Privilegios
- **Descripción:** La plataforma debe aplicar controles estrictos para la **autenticación y gestión de accesos** a los datos de salud.
- **Criterios de Aceptación:**

    - Implementación de **autenticación multifactor (MFA)** para usuarios con acceso a información crítica.
    - Aplicación del **principio de mínimo privilegio**, limitando accesos innecesarios.
    - Auditoría y revisión periódica de los accesos de usuarios.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Previene accesos no autorizados y minimiza riesgos de filtraciones de datos.

---

5. Gestión de Incidentes de Seguridad

- **Identificador único:** LEG-019
- **Título:** Procedimientos de Respuesta ante Incidentes de Seguridad
- **Descripción:** La plataforma debe contar con un **plan de respuesta a incidentes de seguridad**, asegurando una actuación rápida y efectiva ante brechas de seguridad.
- **Criterios de Aceptación:**
    - Definición de **protocolos de detección, contención y mitigación de incidentes**.
    - Registro y análisis de incidentes en un **sistema de gestión de eventos de seguridad (SIEM)**.
    - Comunicación a la Agencia Española de Protección de Datos (AEPD) en caso de brechas de seguridad.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, RGPD
- **Justificación:** Permite detectar, responder y mitigar incidentes de seguridad de forma efectiva.

---

6. Auditorías Periódicas de Seguridad

- **Identificador único:** LEG-020
- **Título:** Evaluaciones de Seguridad según ISO 27001

- **Descripción:** Se deben realizar **auditorías periódicas** para evaluar la efectividad de las medidas de seguridad y detectar vulnerabilidades en la plataforma.
- **Criterios de Aceptación:**
    - Realización de **auditorías anuales de seguridad** conforme a la ISO 27001.
    - Corrección de vulnerabilidades detectadas en las evaluaciones de seguridad.
    - Implementación de mejoras continuas en las políticas y procedimientos de seguridad.
- **Prioridad:** Media
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Garantiza la mejora continua del sistema de seguridad de la información.

---

7. Formación y Concienciación en Seguridad de la Información

- **Identificador único:** LEG-021
- **Título:** Capacitación en Seguridad para Usuarios y Personal Administrativo
- **Descripción:** Todo el personal con acceso a la plataforma debe recibir **formación en seguridad de la información** para prevenir errores humanos y ataques de ingeniería social.
- **Criterios de Aceptación:**
    - Desarrollo de programas de **formación en ciberseguridad** para empleados y usuarios.
    - Realización de **simulacros de ataques de phishing** para evaluar la concienciación.
    - Evaluaciones periódicas para medir la efectividad de la formación en seguridad.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Reduce el riesgo de ataques por errores humanos y mejora la cultura de seguridad en la organización.

Requisitos de Gestión de Incidentes de Seguridad y Notificación a Autoridades (RGPD, ENS)

1. Protocolo de Gestión de Incidentes de Seguridad

- **Identificador único:** LEG-022
- **Título:** Establecimiento de un Protocolo de Gestión de Incidentes
- **Descripción:** La plataforma debe contar con un procedimiento documentado para la **detección, análisis, contención y resolución** de incidentes de seguridad.
- **Criterios de Aceptación:**
    - Implementación de un **Plan de Respuesta a Incidentes** basado en el ENS e ISO 27035.
    - Definición de **niveles de criticidad** para incidentes de seguridad.
    - Registro y documentación de cada incidente en un **sistema de gestión de eventos de seguridad (SIEM)**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001, RGPD Art. 32
- **Justificación:** Permite una respuesta eficaz ante incidentes, minimizando el impacto en la seguridad de los datos.

---

2. Registro y Monitorización de Incidentes

- **Identificador único:** LEG-023
- **Título:** Registro y Supervisión de Incidentes de Seguridad
- **Descripción:** Todos los incidentes de seguridad deben registrarse en un **sistema centralizado de auditoría y monitorización**, asegurando la trazabilidad y análisis posterior.
- **Criterios de Aceptación:**
    - Implementación de un **sistema de registro automático** de eventos de seguridad.
    - Supervisión continua de logs de accesos, modificaciones y transferencias de datos.

    - Generación de **informes periódicos de incidentes** para análisis forense.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, RGPD Art. 30
- **Justificación:** Garantiza la trazabilidad de los incidentes y facilita su análisis y resolución.

---

3. Notificación de Brechas de Seguridad a Autoridades

- **Identificador único:** LEG-024
- **Título:** Procedimiento de Notificación de Incidentes a la AEPD
- **Descripción:** En caso de una **brecha de seguridad que afecte datos personales**, la organización debe notificar a la Agencia Española de Protección de Datos (AEPD) dentro del plazo legal establecido.
- **Criterios de Aceptación:**
    - **Notificación obligatoria a la AEPD** en un plazo máximo de **72 horas** tras la detección del incidente.
    - Registro detallado del incidente, incluyendo naturaleza, alcance y medidas correctivas aplicadas.
    - Comunicación a los **usuarios afectados** cuando el incidente implique un **alto riesgo para sus derechos y libertades**.
- **Prioridad:** Alta
- **Categoría:** Cumplimiento Normativo
- **Fuente/Norma Aplicable:** RGPD, Art. 33 y 34; ENS
- **Justificación:** Cumple con la obligación de transparencia y permite mitigar el impacto de las brechas de seguridad.

---

4. Respuesta Rápida y Contención de Incidentes

- **Identificador único:** LEG-025
- **Título:** Estrategias de Contención y Respuesta Inmediata
- **Descripción:** La plataforma debe contar con mecanismos para **detener la propagación de incidentes y reducir su impacto** en los datos y servicios.
- **Criterios de Aceptación:**

    - Implementación de **protocolos de contención** que incluyan aislamiento de sistemas comprometidos.
    - Aplicación de **actualizaciones y parches de seguridad** para mitigar vulnerabilidades explotadas.
    - Notificación inmediata al equipo de respuesta a incidentes (CSIRT/CERT).
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Reduce el daño potencial de un incidente y permite una recuperación más rápida del servicio.

---

5. Comunicación y Concienciación sobre Seguridad

- **Identificador único:** LEG-026
- **Título:** Formación y Simulacros de Respuesta a Incidentes
- **Descripción:** Se deben realizar **capacitaciones periódicas y simulacros** para garantizar que el personal esté preparado para actuar ante un incidente de seguridad.
- **Criterios de Aceptación:**
    - Ejecución de **simulacros de ataques cibernéticos** al menos una vez al año.
    - Capacitación en **detección de amenazas y respuesta rápida** para empleados y administradores del sistema.
    - Evaluación y mejora del plan de respuesta basado en los resultados de los simulacros.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Mejora la capacidad de reacción y respuesta ante incidentes de seguridad.

---

6. Recuperación y Restauración de la Información

- **Identificador único:** LEG-027
- **Título:** Plan de Recuperación ante Incidentes de Seguridad

- **Descripción:** La plataforma debe contar con un **Plan de Recuperación de la Información** para garantizar la restauración rápida y segura de los datos afectados por un incidente.
- **Criterios de Aceptación:**
    - Implementación de **copias de seguridad automáticas y cifradas** en ubicaciones seguras.
    - Procedimiento documentado para la **restauración de datos en caso de pérdida o corrupción**.
    - Evaluación periódica del tiempo de recuperación (RTO) y punto de recuperación (RPO).
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Asegura la continuidad del servicio y minimiza la pérdida de datos en caso de un incidente.

---

7. Auditoría y Mejora Continua del Proceso de Gestión de Incidentes

- **Identificador único:** LEG-028
- **Título:** Evaluación y Optimización de la Respuesta a Incidentes
- **Descripción:** Se deben realizar revisiones periódicas de los procedimientos de gestión de incidentes para **mejorar continuamente** la capacidad de detección, respuesta y recuperación.
- **Criterios de Aceptación:**
    - Análisis post-incidente para identificar **causas raíz y medidas de prevención**.
    - Revisión y actualización periódica del **protocolo de gestión de incidentes**.
    - Implementación de **mejoras en seguridad** según las lecciones aprendidas de incidentes previos.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO 27001
- **Justificación:** Permite una respuesta más eficiente a futuros incidentes y reduce la probabilidad de que se repitan.

Requisitos de Copias de Seguridad y Recuperación ante Fallos (ISO 27001)

1. Implementación de un Sistema de Copias de Seguridad Automatizado

- **Identificador único:** CONT-001
- **Título:** Automatización del Respaldo de Datos
- **Descripción:** La plataforma debe contar con un sistema de copias de seguridad automáticas que garantice la **disponibilidad de la información médica y administrativa** en caso de fallos del sistema o incidentes de seguridad.
- **Criterios de Aceptación:**
    - Generación de copias de seguridad de forma **diaria, semanal y mensual**.
    - Realización de **copias incrementales** para optimizar el almacenamiento.
    - Almacenamiento de **copias cifradas** en ubicaciones seguras.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Garantiza la disponibilidad de los datos en caso de pérdida o corrupción.

---

2. Almacenamiento de Copias de Seguridad en Ubicaciones Seguras

- **Identificador único:** CONT-002
- **Título:** Almacenamiento Seguro de los Backups
- **Descripción:** Las copias de seguridad deben almacenarse en ubicaciones seguras para evitar accesos no autorizados o pérdidas de datos debido a desastres físicos.
- **Criterios de Aceptación:**
    - Uso de **almacenamiento en la nube con cifrado de extremo a extremo**.
    - Implementación de **ubicaciones redundantes** (on-premise + cloud).
    - Protección contra acceso no autorizado mediante **controles de acceso estrictos**.
- **Prioridad:** Alta

- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Protege la integridad y confidencialidad de los datos respaldados.

---

3. Recuperación Rápida de Datos ante Fallos del Sistema

- **Identificador único:** CONT-003
- **Título:** Procedimiento de Restauración de Copias de Seguridad
- **Descripción:** La plataforma debe contar con un procedimiento documentado para **recuperar los datos de forma rápida y eficiente** en caso de fallo o incidente.
- **Criterios de Aceptación:**
    - Establecimiento de un **Tiempo Máximo de Recuperación (RTO) ≤ 2 horas**.
    - Validación de la integridad de los datos después de la restauración.
    - Documentación de pruebas periódicas de restauración de datos.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Permite minimizar el impacto de un fallo y restaurar rápidamente la operatividad del sistema.

---

4. Cifrado de las Copias de Seguridad

- **Identificador único:** CONT-004
- **Título:** Protección Criptográfica de Backups
- **Descripción:** Todas las copias de seguridad deben estar **cifradas** para evitar accesos no autorizados en caso de pérdida o robo.
- **Criterios de Aceptación:**
    - Implementación de **cifrado AES-256** para las copias de seguridad.
    - Gestión de claves criptográficas a través de **Hardware Security Modules (HSM)**.
    - Restricción de acceso a las claves de cifrado solo a personal autorizado.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información

- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Garantiza la confidencialidad de los datos almacenados en copias de seguridad.

---

5. Pruebas Periódicas de Recuperación de Datos

- **Identificador único:** CONT-005
- **Título:** Validación de la Restauración de Backups
- **Descripción:** Se deben realizar pruebas periódicas de recuperación de datos para verificar que las copias de seguridad sean funcionales y estén disponibles en caso de necesidad.
- **Criterios de Aceptación:**
    - Ejecución de **simulacros de recuperación de datos** cada 6 meses.
    - Validación de la **integridad y consistencia** de los datos restaurados.
    - Registro de auditoría de cada prueba realizada.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Asegura que los backups sean útiles y efectivos en situaciones reales de recuperación.

---

6. Protección contra Ransomware y Manipulación de Backups

- **Identificador único:** CONT-006
- **Título:** Seguridad Adicional contra Ransomware y Manipulación
- **Descripción:** La plataforma debe garantizar que las copias de seguridad no puedan ser alteradas o eliminadas por **ataques de ransomware o accesos no autorizados**.
- **Criterios de Aceptación:**
    - Implementación de **backups inmutables** (Write Once, Read Many - WORM).
    - Restricción de modificaciones en las copias de seguridad mediante **controles de acceso estrictos**.
    - Supervisión y alertas en tiempo real ante intentos de alteración de backups.

- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Protege los backups contra ataques cibernéticos que buscan cifrar o eliminar datos críticos.

---

7. Registro y Auditoría de las Copias de Seguridad

- **Identificador único:** CONT-007
- **Título:** Registro y Auditoría del Proceso de Respaldo
- **Descripción:** Se debe llevar un **registro detallado** de cada copia de seguridad realizada, incluyendo información sobre su ubicación, fecha y estado de integridad.
- **Criterios de Aceptación:**
    - Registro automático de cada backup en un **sistema de gestión de auditoría**.
    - Alertas en caso de fallos en el proceso de copia de seguridad.
    - Accesibilidad a los registros solo para administradores autorizados.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Asegura la trazabilidad y supervisión del proceso de respaldo de datos.

Requisitos de Planes de Continuidad del Negocio en Caso de Incidentes de Ciberseguridad (ENS)

1. Implementación de un Plan de Continuidad del Negocio (PCN)

- **Identificador único:** CONT-008
- **Título:** Desarrollo e Implementación del Plan de Continuidad del Negocio
- **Descripción:** La plataforma debe contar con un **Plan de Continuidad del Negocio (PCN)** documentado, asegurando la operación en caso de incidentes de ciberseguridad.
- **Criterios de Aceptación:**

    - Definición de roles y responsabilidades en la gestión de la continuidad del negocio.
    - Identificación de procesos críticos y **tiempos máximos de recuperación (RTO y RPO)**.
    - Procedimientos para la activación y desactivación del PCN.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 22301
- **Justificación:** Asegura que la plataforma pueda seguir operando en caso de incidente grave.

---

2. Análisis de Impacto en el Negocio (BIA)

- **Identificador único:** CONT-009
- **Título:** Evaluación del Impacto de los Incidentes en la Plataforma
- **Descripción:** Se debe realizar un **Análisis de Impacto en el Negocio (BIA, Business Impact Analysis)** para identificar los efectos de un incidente de ciberseguridad en la plataforma.
- **Criterios de Aceptación:**
    - Identificación de **servicios críticos** y su nivel de dependencia tecnológica.
    - Evaluación del impacto financiero, legal y reputacional de la interrupción de cada servicio.
    - Definición de **umbrales de tolerancia a interrupciones**.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 22301
- **Justificación:** Permite priorizar la recuperación de servicios críticos para minimizar el impacto del incidente.

---

3. Procedimientos de Respuesta ante Incidentes de Ciberseguridad

- **Identificador único:** CONT-010
- **Título:** Plan de Respuesta ante Incidentes Críticos

- **Descripción:** Se deben definir **procedimientos de respuesta ante incidentes cibernéticos** para asegurar una reacción rápida y efectiva.
- **Criterios de Aceptación:**
    - Creación de un equipo de respuesta ante incidentes de ciberseguridad (CSIRT).
    - Implementación de **protocolos de comunicación interna y externa** durante una crisis.
    - Definición de escenarios de respuesta para ataques como **ransomware, denegación de servicio (DDoS) y accesos no autorizados**.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27035
- **Justificación:** Garantiza una respuesta organizada para minimizar el impacto de incidentes cibernéticos.

---

4. Pruebas y Simulacros del Plan de Continuidad

- **Identificador único:** CONT-011
- **Título:** Validación del PCN mediante Pruebas Regulares
- **Descripción:** Se deben realizar **pruebas y simulacros periódicos** para verificar la efectividad del Plan de Continuidad del Negocio.
- **Criterios de Aceptación:**
    - Ejecución de **simulacros anuales de recuperación ante incidentes**.
    - Evaluación de tiempos de respuesta y efectividad de los procedimientos.
    - Implementación de mejoras basadas en los resultados de las pruebas.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 22301
- **Justificación:** Garantiza que el plan de continuidad sea funcional y actualizado.

---

5. Comunicación y Coordinación con Autoridades y Proveedores

- **Identificador único:** CONT-012
- **Título:** Coordinación con Entidades Externas en Caso de Incidente

- **Descripción:** La plataforma debe contar con un **plan de comunicación** para incidentes de ciberseguridad que involucre a **autoridades reguladoras, socios tecnológicos y clientes**.
- **Criterios de Aceptación:**
    - Establecimiento de **canales de comunicación** con la Agencia Española de Protección de Datos (AEPD) y organismos de ciberseguridad (INCIBE, CCN-CERT).
    - Definición de **procedimientos para informar a los usuarios** en caso de interrupción del servicio.
    - Coordinación con **proveedores de servicios cloud y seguridad** para garantizar la continuidad operativa.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Facilita una respuesta coordinada ante incidentes de ciberseguridad.

---

6. Protección de Infraestructura y Redundancia de Servicios

- **Identificador único:** CONT-013
- **Título:** Implementación de Infraestructura Resiliente
- **Descripción:** La plataforma debe contar con una **arquitectura de alta disponibilidad**, garantizando redundancia en los servicios clave.
- **Criterios de Aceptación:**
    - Implementación de **infraestructura distribuida** para evitar puntos únicos de fallo.
    - Uso de **servidores replicados y balanceadores de carga** para mejorar la disponibilidad.
    - Redundancia en las conexiones a internet y centros de datos alternativos.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Minimiza el impacto de fallos en la infraestructura y garantiza la continuidad del servicio.

---

7. Revisión y Actualización del Plan de Continuidad

- **Identificador único:** CONT-014
- **Título:** Mantenimiento y Revisión Periódica del PCN
- **Descripción:** Se debe realizar una **revisión y actualización periódica** del Plan de Continuidad del Negocio, asegurando su alineación con la evolución del sistema y las amenazas emergentes.
- **Criterios de Aceptación:**
    - Evaluación y mejora del PCN cada **12 meses** o tras un incidente relevante.
    - Incorporación de **nuevas amenazas y vulnerabilidades** identificadas en el entorno digital.
    - Asegurar la **compatibilidad del PCN con los cambios en la plataforma y su infraestructura**.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 22301
- **Justificación:** Permite mantener el plan actualizado y adaptado a los riesgos actuales.

Requisitos de Alta Disponibilidad y Redundancia de los Datos (ISO 27001)

1. Infraestructura de Alta Disponibilidad

- **Identificador único:** CONT-015
- **Título:** Implementación de Alta Disponibilidad en la Plataforma
- **Descripción:** La plataforma debe diseñarse con una arquitectura que garantice **operatividad continua**, minimizando el tiempo de inactividad.
- **Criterios de Aceptación:**
    - Uso de **balanceadores de carga** para distribuir el tráfico entre múltiples servidores.
    - Implementación de **servidores en clúster** para asegurar redundancia en caso de fallos.
    - Configuración de **monitoreo en tiempo real** para detectar fallos y reaccionar automáticamente.
- **Prioridad:** Alta

- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Garantiza la disponibilidad de la plataforma y reduce la probabilidad de interrupciones.

---

2. Redundancia de Almacenamiento de Datos

- **Identificador único:** CONT-016
- **Título:** Replicación de Datos en Múltiples Ubicaciones
- **Descripción:** Los datos críticos deben ser replicados en tiempo real en múltiples ubicaciones para evitar pérdidas en caso de fallo de un servidor.
- **Criterios de Aceptación:**
    - Implementación de **replicación de bases de datos** en servidores primarios y secundarios.
    - Uso de **almacenamiento distribuido** en la nube con redundancia geográfica.
    - Verificación periódica de la consistencia de los datos replicados.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Protege la integridad de los datos y permite su recuperación en caso de incidentes.

---

3. Recuperación Automática ante Fallos

- **Identificador único:** CONT-017
- **Título:** Mecanismos de Recuperación Automática
- **Descripción:** La plataforma debe contar con mecanismos automáticos para **detectar y mitigar fallos** sin intervención manual.
- **Criterios de Aceptación:**
    - Implementación de **failover automático** para cambiar a servidores de respaldo en caso de fallo.
    - Configuración de **rearranque automático** de servicios en caso de caída inesperada.

    - Uso de herramientas de **autodiagnóstico y reparación automática** de fallos menores.
- **Prioridad:** Alta
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Permite la recuperación instantánea del servicio ante fallos de hardware o software.

---

4. Balanceo de Carga y Distribución del Tráfico

- **Identificador único:** CONT-018
- **Título:** Optimización del Tráfico y Recursos del Sistema
- **Descripción:** Se debe garantizar que la carga de tráfico se distribuya equitativamente entre los servidores para evitar sobrecargas.
- **Criterios de Aceptación:**
    - Implementación de un **balanceador de carga** para distribuir peticiones entre servidores.
    - Configuración de **escalado automático** para aumentar recursos en caso de tráfico elevado.
    - Monitoreo continuo del rendimiento para detectar posibles cuellos de botella.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Optimiza el rendimiento y asegura que la plataforma pueda manejar picos de demanda sin interrupciones.

---

5. Copias de Seguridad con Alta Disponibilidad

- **Identificador único:** CONT-019
- **Título:** Backups con Replicación y Disponibilidad Continua
- **Descripción:** Las copias de seguridad deben estar disponibles en múltiples ubicaciones y poder restaurarse sin afectar el servicio.
- **Criterios de Aceptación:**

    - Implementación de **backups automáticos y replicados en centros de datos distintos**.
    - Restauración de copias sin afectar la disponibilidad del sistema.
    - Auditoría periódica para validar la integridad de las copias almacenadas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Permite recuperar datos de forma rápida y segura en caso de incidentes o ataques.

---

6. Monitoreo Proactivo y Alertas de Disponibilidad

- **Identificador único:** CONT-020
- **Título:** Supervisión en Tiempo Real de la Disponibilidad del Servicio
- **Descripción:** Se debe monitorear continuamente la disponibilidad y rendimiento de la plataforma para detectar fallos de manera temprana.
- **Criterios de Aceptación:**
    - Uso de **herramientas de monitoreo en tiempo real** para la infraestructura.
    - Generación de **alertas automáticas** en caso de caídas o problemas de rendimiento.
    - Implementación de un **dashboard centralizado** para visualizar el estado de los sistemas.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Permite actuar rápidamente ante problemas y evitar interrupciones prolongadas.

---

7. Auditoría y Pruebas de Disponibilidad

- **Identificador único:** CONT-021
- **Título:** Validación Periódica de la Alta Disponibilidad

- **Descripción:** Se deben realizar pruebas periódicas para verificar la efectividad de las medidas de alta disponibilidad y redundancia.
- **Criterios de Aceptación:**
    - Ejecución de **pruebas de conmutación por error (failover testing)** cada 6 meses.
    - Evaluación de **tiempos de recuperación (RTO y RPO)** tras incidentes simulados.
    - Implementación de mejoras basadas en los resultados de las auditorías.
- **Prioridad:** Media
- **Categoría:** Continuidad del Negocio
- **Fuente/Norma Aplicable:** ISO/IEC 27001
- **Justificación:** Garantiza que la plataforma pueda recuperarse rápidamente y mantener la operatividad ante incidentes.

Requisitos de Compatibilidad con Estándares de Intercambio de Información Médica (FHIR, HL7)

1. Adopción del Estándar FHIR para la Interoperabilidad

- **Identificador único:** INT-001
- **Título:** Implementación de FHIR para el Intercambio de Datos Médicos
- **Descripción:** La plataforma debe utilizar el estándar **FHIR (Fast Healthcare Interoperability Resources)** para garantizar la interoperabilidad con otros sistemas sanitarios y facilitar el acceso estructurado a la información médica.
- **Criterios de Aceptación:**
    - Implementación de una **API RESTful basada en FHIR** para la interoperabilidad.
    - Soporte para **perfiles FHIR específicos** aplicables a historiales clínicos electrónicos.
    - Compatibilidad con **JSON y XML** para la representación de datos médicos.
- **Prioridad:** Alta
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO/HL7 27931
- **Justificación:** Facilita el intercambio estructurado de información médica con sistemas de terceros.

---

2. Compatibilidad con HL7 v2 y HL7 v3

- **Identificador único:** INT-002
- **Título:** Soporte para Protocolos HL7 v2 y HL7 v3
- **Descripción:** La plataforma debe ser compatible con los estándares **HL7 v2** y **HL7 v3** para garantizar la integración con sistemas hospitalarios que utilicen versiones anteriores de este estándar.
- **Criterios de Aceptación:**
    - Implementación de adaptadores para convertir datos entre **FHIR y HL7 v2/v3**.
    - Soporte para **mensajería HL7** mediante interfaces MLLP (Minimal Lower Layer Protocol).
    - Validación de la correcta conversión de mensajes entre versiones de HL7.
- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 v2, HL7 v3
- **Justificación:** Asegura la compatibilidad con sistemas heredados y mejora la integración con infraestructura hospitalaria existente.

---

3. Integración con Bases de Datos de Pacientes Basadas en FHIR

- **Identificador único:** INT-003
- **Título:** Estructuración de Historias Clínicas en FHIR
- **Descripción:** La plataforma debe almacenar las historias clínicas electrónicas en un formato compatible con **FHIR**, permitiendo consultas y actualizaciones basadas en este estándar.
- **Criterios de Aceptación:**
    - Implementación de **repositorios FHIR** para la gestión de historiales médicos.
    - Soporte para **módulos FHIR como Patient, Observation, Condition y MedicationRequest**.
    - Capacidad de interoperabilidad con **sistemas externos que usen bases de datos FHIR**.
- **Prioridad:** Alta

- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR R4
- **Justificación:** Garantiza la estandarización del almacenamiento de datos médicos y facilita su intercambio.

---

4. Soporte para Terminologías y Vocabularios Clínicos Estándar

- **Identificador único:** INT-004
- **Título:** Uso de Terminologías Médicas Normalizadas
- **Descripción:** La plataforma debe ser compatible con estándares de terminología médica para garantizar la precisión en el intercambio de datos clínicos.
- **Criterios de Aceptación:**
    - Compatibilidad con **SNOMED CT** para la codificación de diagnósticos y procedimientos médicos.
    - Soporte para **LOINC (Logical Observation Identifiers Names and Codes)** en pruebas de laboratorio.
    - Implementación de **ICD-10 y CPT** para clasificación de enfermedades y procedimientos.
- **Prioridad:** Alta
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** SNOMED CT, LOINC, ICD-10
- **Justificación:** Asegura la precisión en el intercambio de datos clínicos y mejora la interoperabilidad con otros sistemas de salud.

---

5. Seguridad en el Intercambio de Datos Médicos

- **Identificador único:** INT-005
- **Título:** Protección de la Información Médica en la Interoperabilidad
- **Descripción:** La plataforma debe garantizar la **seguridad y privacidad** de los datos médicos intercambiados con otros sistemas sanitarios.
- **Criterios de Aceptación:**
    - Implementación de **cifrado TLS 1.2 o superior** en la transmisión de datos.
    - Uso de **OAuth 2.0 y OpenID Connect** para autenticación segura de APIs.
    - Registro de auditoría de todas las transacciones de intercambio de datos.

- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO 27001, ENS, HL7 FHIR
- **Justificación:** Protege la confidencialidad de la información médica durante la interoperabilidad.

---

6. Implementación de APIs para Acceso a Datos en Tiempo Real

- **Identificador único:** INT-006
- **Título:** Interfaz de Programación de Aplicaciones (API) para Acceso a Datos
- **Descripción:** La plataforma debe ofrecer una **API basada en FHIR** que permita a sistemas externos acceder en tiempo real a datos clínicos de los pacientes.
- **Criterios de Aceptación:**
    - Implementación de endpoints FHIR para **consultar, modificar y eliminar registros médicos**.
    - Soporte para autenticación segura mediante **OAuth 2.0**.
    - Documentación de la API en **Swagger/OpenAPI** para facilitar la integración.
- **Prioridad:** Alta
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO 27001
- **Justificación:** Facilita el acceso seguro y en tiempo real a los datos médicos de los pacientes.

---

7. Auditoría y Validación de la Interoperabilidad

- **Identificador único:** INT-007
- **Título:** Evaluación Periódica de la Compatibilidad con FHIR y HL7
- **Descripción:** Se deben realizar auditorías y pruebas periódicas para garantizar la correcta interoperabilidad de la plataforma con otros sistemas sanitarios.
- **Criterios de Aceptación:**
    - Ejecución de **pruebas de compatibilidad** con FHIR y HL7 cada 6 meses.
    - Validación de la integridad y precisión de los datos intercambiados.
    - Registro de incidentes de interoperabilidad y aplicación de mejoras.

- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO 27001
- **Justificación:** Asegura la correcta integración de la plataforma con otros sistemas de salud.

Requisitos de Integración Segura con Bases de Datos Hospitalarias y Sistemas Externos

1. Seguridad en la Conexión con Bases de Datos Hospitalarias

- **Identificador único:** INT-008
- **Título:** Protección de la Conexión con Sistemas Externos
- **Descripción:** La plataforma debe garantizar una conexión segura con las bases de datos hospitalarias, protegiendo la información médica intercambiada.
- **Criterios de Aceptación:**
    - Implementación de **cifrado TLS 1.2 o superior** para la comunicación con bases de datos externas.
    - Uso de **VPNs o redes privadas seguras** para el intercambio de datos sensibles.
    - Autenticación mediante **certificados digitales** o claves API seguras.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS, HL7 FHIR
- **Justificación:** Protege la confidencialidad y seguridad de los datos médicos en la comunicación con bases de datos externas.

---

2. Integración con Sistemas de Historia Clínica Electrónica

- **Identificador único:** INT-009
- **Título:** Conectividad con Sistemas de Historia Clínica Electrónica
- **Descripción:** La plataforma debe permitir la integración con sistemas de **Historia Clínica Electrónica (HCE)** utilizados en hospitales y clínicas.
- **Criterios de Aceptación:**
    - Soporte para integración mediante **HL7 FHIR** y **HL7 v2/v3**.

    - Sincronización de datos en tiempo real para actualizaciones automáticas de historias clínicas.
    - Garantía de consistencia e integridad de datos entre sistemas conectados.
- **Prioridad:** Alta
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO/HL7 27931
- **Justificación:** Facilita el acceso a datos clínicos en diferentes entornos médicos, mejorando la continuidad asistencial.

---

3. Control de Accesos y Permisos en la Integración

- **Identificador único:** INT-010
- **Título:** Gestión de Accesos a Bases de Datos Externas
- **Descripción:** Se debe garantizar que solo **usuarios y sistemas autorizados** puedan acceder a las bases de datos hospitalarias integradas.
- **Criterios de Aceptación:**
    - Implementación de **control de acceso basado en roles (RBAC)** para definir permisos de acceso.
    - Uso de **OAuth 2.0 y OpenID Connect** para autenticación segura de sistemas externos.
    - Registro de auditoría de todos los accesos y modificaciones realizadas en bases de datos externas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Protege el acceso a la información médica y minimiza riesgos de accesos indebidos.

---

4. Validación de Datos en la Interoperabilidad

- **Identificador único:** INT-011
- **Título:** Verificación de la Integridad y Calidad de los Datos
- **Descripción:** La plataforma debe validar la **precisión, consistencia y calidad** de los datos intercambiados con bases de datos hospitalarias.

- **Criterios de Aceptación:**
    - Implementación de **validaciones automáticas** en la recepción y envío de datos.
    - Registro de **errores y discrepancias** en la interoperabilidad con sistemas externos.
    - Corrección automática o manual de datos inconsistentes detectados en la sincronización.
- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO 27001
- **Justificación:** Asegura que la información intercambiada sea precisa y confiable.

---

5. Integración con Sistemas de Facturación Electrónica

- **Identificador único:** INT-012
- **Título:** Conectividad con Plataformas de Facturación Electrónica
- **Descripción:** La plataforma debe permitir la integración con sistemas de **facturación electrónica** para gestionar pagos y transacciones asociadas a servicios médicos.
- **Criterios de Aceptación:**
    - Compatibilidad con estándares de facturación electrónica nacionales e internacionales (ej. **Facturae, XML UBL**).
    - Enlace entre datos de pacientes y facturación sin comprometer la confidencialidad médica.
    - Validación de transacciones en tiempo real y generación de reportes financieros.
- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Facilita la automatización de procesos administrativos en clínicas y hospitales.

---

6. Seguridad en la Transferencia de Datos Sensibles

- **Identificador único:** INT-013

- **Título:** Protección de Información Médica en la Interoperabilidad
- **Descripción:** Todos los datos sensibles transferidos a bases de datos externas deben estar protegidos mediante **medidas de seguridad avanzadas**.
- **Criterios de Aceptación:**
    - Uso de **cifrado de extremo a extremo** en la transmisión de datos médicos.
    - Implementación de **protocolos de integridad y no repudio** para verificar la autenticidad de la información intercambiada.
    - Aplicación de medidas de **anonimización y pseudonimización** cuando sea necesario.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS, RGPD
- **Justificación:** Protege la confidencialidad y privacidad de los datos médicos en su transferencia.

---

7. Auditoría y Monitorización de la Integración

- **Identificador único:** INT-014
- **Título:** Supervisión de la Interoperabilidad con Sistemas Externos
- **Descripción:** Se deben realizar auditorías periódicas y supervisión en tiempo real de la integración con bases de datos hospitalarias y otros sistemas externos.
- **Criterios de Aceptación:**
    - Monitoreo en tiempo real del estado de conexión con sistemas externos.
    - Auditorías periódicas de seguridad y cumplimiento normativo.
    - Generación de reportes de actividad y alertas en caso de anomalías en la interoperabilidad.
- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Garantiza la correcta integración y cumplimiento de las normativas de seguridad y privacidad.

Requisitos de Exportación de Datos en Formatos Estándar

1. Compatibilidad con Formatos de Interoperabilidad Estándar

- **Identificador único:** INT-015
- **Título:** Soporte para Formatos de Intercambio de Datos
- **Descripción:** La plataforma debe permitir la **exportación de datos clínicos y administrativos** en formatos estándar, asegurando la interoperabilidad con otros sistemas de salud.
- **Criterios de Aceptación:**
    - Compatibilidad con **FHIR (JSON, XML)** para la exportación de datos médicos.
    - Soporte para **HL7 v2/v3** en la transferencia de información hospitalaria.
    - Posibilidad de exportar datos en **CSV y PDF** para informes administrativos y clínicos.
- **Prioridad:** Alta
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, ISO/HL7 27931
- **Justificación:** Facilita la integración con otros sistemas de información en salud.

---

2. Exportación de Historias Clínicas Electrónicas

- **Identificador único:** INT-016
- **Título:** Generación y Exportación de Registros Médicos
- **Descripción:** La plataforma debe permitir a los usuarios **exportar y descargar** historias clínicas electrónicas en un formato estructurado.
- **Criterios de Aceptación:**
    - Generación de **documentos CDA (Clinical Document Architecture)** para exportación estructurada.
    - Posibilidad de descargar el historial médico en **PDF y JSON** para pacientes y profesionales.
    - Inclusión de **códigos SNOMED CT, LOINC e ICD-10** en los datos exportados.
- **Prioridad:** Alta

- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 CDA, ISO 13606
- **Justificación:** Permite el acceso estructurado y reutilizable a la información médica.

---

3. Exportación Segura de Datos Sensibles

- **Identificador único:** INT-017
- **Título:** Protección en la Exportación de Datos Médicos
- **Descripción:** La plataforma debe aplicar **medidas de seguridad** en la exportación de datos médicos para garantizar su integridad y confidencialidad.
- **Criterios de Aceptación:**
    - Aplicación de **cifrado AES-256** en archivos exportados.
    - Firma digital en documentos exportados para garantizar autenticidad.
    - Restricción de exportación a **usuarios autorizados**, con registro de auditoría.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS, RGPD
- **Justificación:** Protege la información médica en los procesos de exportación.

---

4. Integración con Sistemas de Terceros para Importación/Exportación

- **Identificador único:** INT-018
- **Título:** Interoperabilidad con Otros Sistemas Médicos
- **Descripción:** La plataforma debe permitir la **exportación e importación** de datos en formatos estándar compatibles con otros sistemas de gestión clínica.
- **Criterios de Aceptación:**
    - Compatibilidad con **FHIR Bulk Data API** para grandes volúmenes de datos.
    - Exportación en **DICOM** para imágenes médicas y radiografías.
    - Capacidad de importar datos desde otros sistemas en formatos HL7 y FHIR.
- **Prioridad:** Media

- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** HL7 FHIR, DICOM, ISO 27001
- **Justificación:** Facilita la interoperabilidad con sistemas externos y la transferencia de datos clínicos.

---

5. Generación de Reportes Personalizados

- **Identificador único:** INT-019
- **Título:** Exportación de Informes Personalizados en Diferentes Formatos
- **Descripción:** La plataforma debe ofrecer la posibilidad de generar **reportes personalizados** con datos clínicos y administrativos en distintos formatos.
- **Criterios de Aceptación:**
    - Exportación en **Excel (XLSX), CSV y PDF** para análisis administrativo.
    - Configuración de **filtros y parámetros** para personalizar los reportes.
    - Inclusión de gráficos y visualizaciones en los informes exportados.
- **Prioridad:** Media
- **Categoría:** Interoperabilidad
- **Fuente/Norma Aplicable:** ISO 27001, HL7 CDA
- **Justificación:** Facilita el análisis de datos para gestión clínica y administrativa.

---

6. Registro y Auditoría de la Exportación de Datos

- **Identificador único:** INT-020
- **Título:** Seguimiento de Exportaciones de Información Clínica
- **Descripción:** Todas las exportaciones de datos deben registrarse en un **sistema de auditoría**, permitiendo el rastreo de información sensible.
- **Criterios de Aceptación:**
    - Registro automático de **quién, cuándo y qué datos** fueron exportados.
    - Alertas en caso de exportaciones masivas no autorizadas.
    - Restricción de exportación solo a usuarios con permisos específicos.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS, RGPD

- **Justificación:** Asegura la trazabilidad de la información exportada y previene fugas de datos.

Requisitos de Registro de Eventos y Monitoreo de Actividades Críticas (ENS, ISO 27001)

1. Registro Detallado de Eventos de Seguridad

- **Identificador único:** AUD-001
- **Título:** Registro de Actividades y Eventos Críticos
- **Descripción:** La plataforma debe mantener un registro detallado de todos los eventos de seguridad y actividades críticas realizadas por los usuarios y el sistema.
- **Criterios de Aceptación:**
    - Almacenamiento de eventos como **inicios de sesión, accesos a datos sensibles, modificaciones y eliminaciones de registros**.
    - Registro de **dirección IP, usuario, dispositivo y hora del evento**.
    - Protección contra **modificación o eliminación** de registros de auditoría.
- **Prioridad:** Alta
- **Categoría:** Auditoría y Monitorización
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Asegura la trazabilidad y permite la detección de posibles incidentes de seguridad.

---

2. Monitoreo en Tiempo Real de Accesos y Actividades Críticas

- **Identificador único:** AUD-002
- **Título:** Supervisión en Tiempo Real de Eventos Críticos
- **Descripción:** La plataforma debe contar con un **sistema de monitoreo en tiempo real** que analice accesos y actividades sospechosas.
- **Criterios de Aceptación:**
    - Implementación de herramientas SIEM (**Security Information and Event Management**) para monitoreo centralizado.
    - Generación de **alertas automáticas** en caso de accesos inusuales o intentos de intrusión.

    - Revisión continua de patrones de uso para identificar **anomalías y posibles amenazas**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite la detección temprana de ataques o accesos no autorizados.

---

3. Protección de los Registros de Auditoría

- **Identificador único:** AUD-003
- **Título:** Integridad y Protección de los Registros de Auditoría
- **Descripción:** Todos los registros de auditoría deben estar protegidos contra modificaciones o eliminaciones no autorizadas.
- **Criterios de Aceptación:**
    - Aplicación de **cifrado AES-256** para proteger los archivos de auditoría.
    - Restricción de acceso a registros solo a **usuarios con privilegios específicos**.
    - Configuración de **backups periódicos de los registros** en servidores seguros.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Garantiza la integridad y disponibilidad de los registros de eventos.

---

4. Detección de Actividades Sospechosas

- **Identificador único:** AUD-004
- **Título:** Identificación y Prevención de Comportamientos Anómalos
- **Descripción:** El sistema debe detectar patrones de **comportamiento anómalos** que puedan indicar ataques o accesos indebidos.
- **Criterios de Aceptación:**
    - Implementación de **sistemas de detección de intrusos (IDS/IPS)** para analizar tráfico sospechoso.

    - Configuración de **alertas en caso de múltiples intentos de acceso fallidos** o actividad inusual.
    - Aplicación de algoritmos de **inteligencia artificial para detección de anomalías**.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite prevenir ataques internos y externos de forma proactiva.

---

5. Notificación de Eventos Críticos a Administradores

- **Identificador único:** AUD-005
- **Título:** Alertas Automáticas ante Eventos de Riesgo
- **Descripción:** Los administradores del sistema deben ser notificados de **eventos críticos en tiempo real**, asegurando una respuesta rápida ante incidentes.
- **Criterios de Aceptación:**
    - Configuración de **alertas en tiempo real** vía correo electrónico o SMS ante eventos sospechosos.
    - Clasificación de alertas en **niveles de criticidad (bajo, medio, alto)**.
    - Implementación de **protocolos de respuesta inmediata** en caso de alerta de seguridad.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Facilita la gestión y respuesta rápida ante amenazas de seguridad.

---

6. Análisis Forense y Auditoría de Incidentes

- **Identificador único:** AUD-006
- **Título:** Investigación de Incidentes mediante Registros de Auditoría
- **Descripción:** La plataforma debe contar con un sistema de **análisis forense** que permita investigar incidentes de seguridad a partir de los registros de eventos.
- **Criterios de Aceptación:**

    - Implementación de herramientas de **auditoría y análisis forense** de eventos.
    - Conservación de registros de auditoría por un mínimo de **2 años**.
    - Capacidad de reconstrucción de incidentes mediante la revisión de logs históricos.
- **Prioridad:** Media
- **Categoría:** Auditoría y Monitorización
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite la investigación de incidentes y el cumplimiento normativo.

---

7. Reportes Periódicos de Seguridad y Cumplimiento

- **Identificador único:** AUD-007
- **Título:** Generación de Informes de Seguridad
- **Descripción:** La plataforma debe generar **informes periódicos** sobre la actividad del sistema y la seguridad de la información.
- **Criterios de Aceptación:**
    - Generación de **reportes mensuales y anuales** sobre accesos, modificaciones y eventos críticos.
    - Comparación de datos históricos para detectar **tendencias de amenazas**.
    - Presentación de reportes a **autoridades y organismos reguladores** cuando sea requerido.
- **Prioridad:** Media
- **Categoría:** Auditoría y Monitorización
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite la supervisión continua y el cumplimiento normativo.

Requisitos de Realización de Auditorías de Seguridad Periódicas (ENS, ISO 27001)

1. Implementación de un Plan de Auditoría de Seguridad

- **Identificador único:** AUD-008
- **Título:** Planificación de Auditorías de Seguridad

- **Descripción:** La plataforma debe contar con un **plan anual de auditorías de seguridad**, que garantice la revisión continua de los controles de seguridad implementados.
- **Criterios de Aceptación:**
    - Definición de un **calendario de auditorías internas y externas**.
    - Identificación de **áreas críticas** a evaluar en cada auditoría.
    - Registro y documentación de los resultados de las auditorías.
- **Prioridad:** Alta
- **Categoría:** Auditoría y Cumplimiento
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite la mejora continua de la seguridad de la plataforma.

---

2. Auditorías Internas de Seguridad

- **Identificador único:** AUD-009
- **Título:** Evaluación de Seguridad a Nivel Interno
- **Descripción:** La plataforma debe realizar **auditorías internas** periódicas para detectar vulnerabilidades y evaluar el cumplimiento de los procedimientos de seguridad.
- **Criterios de Aceptación:**
    - Realización de auditorías internas al menos **cada 6 meses**.
    - Evaluación del cumplimiento de **políticas y controles de seguridad**.
    - Corrección de debilidades identificadas mediante **acciones de mejora**.
- **Prioridad:** Alta
- **Categoría:** Auditoría y Cumplimiento
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite detectar y corregir vulnerabilidades antes de que sean explotadas.

---

3. Auditorías Externas de Cumplimiento Normativo

- **Identificador único:** AUD-010
- **Título:** Verificación de Seguridad por Entidades Externas

- **Descripción:** La plataforma debe ser evaluada regularmente por **auditores independientes** para verificar su cumplimiento con el ENS y la normativa vigente.
- **Criterios de Aceptación:**
    - Contratación de auditorías externas **cada 12 meses**.
    - Evaluación del cumplimiento con **ENS, ISO 27001 y RGPD**.
    - Aplicación de recomendaciones de los auditores para mejorar la seguridad.
- **Prioridad:** Alta
- **Categoría:** Auditoría y Cumplimiento
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Garantiza el cumplimiento normativo y la certificación de seguridad del sistema.

---

4. Evaluación de Controles de Seguridad

- **Identificador único:** AUD-011
- **Título:** Revisión Periódica de Controles de Seguridad
- **Descripción:** Se debe evaluar la **efectividad de los controles de seguridad** implementados en la plataforma para detectar posibles fallos o mejoras.
- **Criterios de Aceptación:**
    - Revisión de **cifrado de datos, autenticación y control de accesos**.
    - Evaluación de la **protección contra amenazas cibernéticas**.
    - Generación de informes sobre la efectividad de los controles de seguridad.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Garantiza la adecuación y efectividad de los mecanismos de seguridad implementados.

---

5. Auditoría de Registro de Accesos y Actividades

- **Identificador único:** AUD-012
- **Título:** Verificación de Registros de Auditoría

- **Descripción:** Se debe realizar una auditoría periódica sobre los **registros de accesos y actividades** en la plataforma, detectando posibles accesos no autorizados o malas prácticas.
- **Criterios de Aceptación:**
    - Análisis de **logs de acceso y eventos críticos** cada 3 meses.
    - Identificación de patrones de comportamiento sospechosos.
    - Generación de alertas y aplicación de medidas correctivas si se detectan anomalías.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Permite la detección temprana de amenazas internas y externas.

---

6. Auditoría de Configuración de Infraestructura

- **Identificador único:** AUD-013
- **Título:** Evaluación de la Configuración de Servidores y Red
- **Descripción:** Se deben realizar revisiones periódicas de la **configuración de servidores, bases de datos y redes**, asegurando su alineación con las mejores prácticas de seguridad.
- **Criterios de Aceptación:**
    - Verificación de **configuraciones de firewall, VPNs y segmentación de red**.
    - Análisis de **políticas de acceso a bases de datos**.
    - Corrección de configuraciones incorrectas o desactualizadas.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Evita vulnerabilidades derivadas de configuraciones inseguras o desactualizadas.

---

7. Informe de Resultados y Aplicación de Mejoras

- **Identificador único:** AUD-014

- **Título:** Implementación de Mejoras Basadas en Auditorías
- **Descripción:** Tras cada auditoría, se deben generar **informes detallados** con las conclusiones y acciones de mejora recomendadas.
- **Criterios de Aceptación:**
    - Generación de **informes detallados** con los hallazgos de cada auditoría.
    - Creación de un **plan de acción** para corregir vulnerabilidades detectadas.
    - Seguimiento y verificación de la implementación de mejoras recomendadas.
- **Prioridad:** Media
- **Categoría:** Auditoría y Cumplimiento
- **Fuente/Norma Aplicable:** ENS, ISO/IEC 27001
- **Justificación:** Facilita la mejora continua de la seguridad de la plataforma y su cumplimiento normativo.

Requisitos de Gestión de Vulnerabilidades y Aplicación de Parches de Seguridad (ISO 27001)

1. Implementación de un Proceso de Gestión de Vulnerabilidades

- **Identificador único:** AUD-015
- **Título:** Establecimiento de un Programa de Gestión de Vulnerabilidades
- **Descripción:** La plataforma debe contar con un **proceso formal para la detección, análisis y mitigación de vulnerabilidades** en los sistemas y aplicaciones.
- **Criterios de Aceptación:**
    - Implementación de un **proceso de gestión de vulnerabilidades** basado en ISO 27002.
    - Clasificación de vulnerabilidades según su **criticidad y nivel de impacto**.
    - Documentación y seguimiento de vulnerabilidades detectadas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Asegura que las vulnerabilidades sean detectadas y corregidas antes de que puedan ser explotadas.

---

2. Escaneos de Vulnerabilidades y Pruebas de Penetración

- **Identificador único:** AUD-016
- **Título:** Detección Proactiva de Vulnerabilidades
- **Descripción:** La plataforma debe ser sometida a **escaneos de vulnerabilidades y pruebas de penetración (pentesting)** para identificar debilidades de seguridad.
- **Criterios de Aceptación:**
    - Ejecución de **escaneos de vulnerabilidades automatizados** cada 3 meses.
    - Realización de **pruebas de penetración externas e internas** al menos una vez al año.
    - Documentación de hallazgos y corrección de vulnerabilidades críticas en un plazo máximo de 30 días.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, OWASP, NIST
- **Justificación:** Permite identificar y corregir debilidades antes de que sean explotadas por atacantes.

---

3. Aplicación de Parches de Seguridad en Sistemas y Software

- **Identificador único:** AUD-017
- **Título:** Política de Actualización y Parcheo de Seguridad
- **Descripción:** La plataforma debe garantizar que todos los sistemas, aplicaciones y dependencias sean **actualizados y parchados regularmente**.
- **Criterios de Aceptación:**
    - Aplicación de **actualizaciones críticas** en un plazo máximo de 7 días tras su publicación.
    - Uso de un **sistema automatizado de gestión de parches** para servidores y aplicaciones.
    - Validación de actualizaciones en un **entorno de pruebas** antes de su despliegue en producción.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información

- **Fuente/Norma Aplicable:** ISO/IEC 27001, NIST, OWASP
- **Justificación:** Reduce el riesgo de explotación de vulnerabilidades en software y sistemas operativos.

---

4. Monitoreo de Vulnerabilidades en Tiempo Real

- **Identificador único:** AUD-018
- **Título:** Supervisión de Amenazas y Alertas de Seguridad
- **Descripción:** La plataforma debe contar con un sistema de **detección en tiempo real de amenazas y vulnerabilidades** mediante herramientas de monitoreo de seguridad.
- **Criterios de Aceptación:**
    - Implementación de **sistemas de detección de intrusos (IDS/IPS)** para identificar ataques en curso.
    - Integración con **bases de datos de amenazas globales (CVEs, NIST, OWASP)** para alertas tempranas.
    - Configuración de **notificaciones automáticas** a los administradores ante vulnerabilidades críticas.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Permite actuar de forma inmediata ante nuevas amenazas o vulnerabilidades detectadas.

---

5. Segmentación y Protección de Sistemas Críticos

- **Identificador único:** AUD-019
- **Título:** Reducción del Impacto de Vulnerabilidades en Sistemas Críticos
- **Descripción:** La plataforma debe contar con medidas de **segmentación de red y control de accesos** para limitar el impacto de posibles vulnerabilidades.
- **Criterios de Aceptación:**
    - Implementación de **segmentación de red (VLANs) para separar entornos de producción y pruebas**.
    - Aplicación de **firewalls y listas de control de acceso (ACLs)** para restringir comunicaciones innecesarias.

    - Uso de **principios de seguridad Zero Trust** para limitar el acceso a sistemas críticos.
- **Prioridad:** Alta
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, NIST, ENS
- **Justificación:** Minimiza la propagación de ataques o vulnerabilidades dentro de la infraestructura.

---

6. Evaluación de Riesgos de Seguridad Asociados a Vulnerabilidades

- **Identificador único:** AUD-020
- **Título:** Análisis de Impacto y Priorización de Correcciones
- **Descripción:** Se debe realizar una **evaluación de impacto de las vulnerabilidades detectadas**, priorizando su corrección según el nivel de riesgo.
- **Criterios de Aceptación:**
    - Clasificación de vulnerabilidades en **críticas, altas, medias y bajas**.
    - Análisis de impacto en la seguridad y operatividad del sistema.
    - Aplicación de **medidas de mitigación** para vulnerabilidades que no puedan corregirse inmediatamente.
- **Prioridad:** Media
- **Categoría:** Seguridad de la Información
- **Fuente/Norma Aplicable:** ISO/IEC 27001, NIST
- **Justificación:** Permite priorizar esfuerzos de mitigación y reducir riesgos de seguridad en el sistema.

---

7. Registro y Auditoría de la Gestión de Vulnerabilidades

- **Identificador único:** AUD-021
- **Título:** Documentación y Seguimiento de Vulnerabilidades
- **Descripción:** Todos los procesos de **detección, evaluación y mitigación de vulnerabilidades** deben ser registrados y auditados periódicamente.
- **Criterios de Aceptación:**
    - Registro de vulnerabilidades detectadas, su nivel de riesgo y la fecha de corrección.

    - Generación de **informes de seguridad** periódicos sobre la gestión de vulnerabilidades.
    - Evaluación y mejora continua basada en auditorías de seguridad.
- **Prioridad:** Media
- **Categoría:** Auditoría y Cumplimiento
- **Fuente/Norma Aplicable:** ISO/IEC 27001, ENS
- **Justificación:** Garantiza la trazabilidad y la mejora continua en la seguridad de la plataforma.
