UNRC
Universidad Nacional Rosario Castellanos

CIBERSEGURIDAD EN SALUD DIGITAL

Andrea Yeretzi Ixtolinque Olvera
Lizeth Arteaga Vasquez
Yetlanetzi Fabiola Acosta Alonso
Yolanda Ivonne Cruz Martínez

Docente:
Oscar Mauricio Hernández Careaga

Fecha: Mayo 2026

ÍNDICE

SECCIÓN 1: Alcance

La sección Alcance de la norma ISO 27001 establece:

1.1 Finalidad del SGSI

La finalidad de implementar el SGSI en el proyecto EUS es establecer un marco de gestión que garantice la seguridad de los activos de información críticos, específicamente los datos clínicos y personales de los pacientes (incluyendo CURP, antecedentes patológicos y registros de salud). El objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de los expedientes digitales, cumpliendo con los estándares internacionales de seguridad y la normativa legal vigente en materia de salud.

1.2 Aplicabilidad

Este SGSI es de aplicación obligatoria para todo el personal, procesos y activos tecnológicos que integran el ecosistema EUS, incluyendo:

- Activos Tecnológicos: Infraestructura de nube (Supabase), base de datos de pacientes, servicios de autenticación, código fuente del Dashboard y el Expediente Médico.
- Procesos: Desarrollo de software, gestión de altas de pacientes, administración de accesos por roles (Médicos/Instituciones) y registro de firmas electrónicas.
- Partes interesadas: Desarrolladores, administradores del sistema, personal médico autorizado y las instituciones de salud conectadas a la plataforma.

1.3 Declaración de Cumplimiento (Cláusulas)

El sistema EUS manifiesta su compromiso de cumplir con los requisitos establecidos en las siguientes cláusulas normativas de la norma ISO/IEC 27001:2022 para demostrar su conformidad:

- Cláusula 4: Contexto de la organización.
- Cláusula 5: Liderazgo.
- Cláusula 6: Planificación.
- Cláusula 7: Apoyo.
- Cláusula 8: Funcionamiento (Operación).
- Cláusula 9: Evaluación del desempeño.
- Cláusula 10: Mejora.

1.4 Límites del Alcance (Inclusiones y Exclusiones)

Para efectos de la certificación y auditoría, se definen los siguientes límites:

- Inclusiones: Todos los servicios digitales proporcionados a través de la plataforma EUS, el almacenamiento de datos en Supabase y los servicios de autenticación vinculados a la CURP.
- Exclusiones: Quedan fuera del alcance los procesos físicos de gestión de pacientes que ocurran fuera de la plataforma digital (ej. expedientes físicos almacenados en papel en centros de salud externos, la infraestructura de hardware personal del médico o del paciente).

SECCIÓN 2: Referencias normativas

Para asegurar la correcta interpretación de los requisitos de este Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar el cumplimiento legal en el sector salud, se adoptan las siguientes referencias como base documental:

2.1 Referencia Obligatoria (ISO)

ISO/IEC 27000:2018 (Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario): Esta es la única norma de referencia explícita establecida por la norma ISO/IEC 27001. Se utiliza como el glosario oficial para interpretar cada término y requisito del SGSI del Proyecto EUS. Todo el personal técnico y administrativo con responsabilidades en el sistema deberá estar familiarizado con las definiciones aquí contenidas.

2.2 Referencias Legales y Normativas (Contexto EUS)

Para la operación del EUS, estas referencias son indispensables para demostrar la conformidad con las leyes de salud y protección de datos personales:

NOM-004-SSA3-2012, Del expediente clínico: Es la referencia normativa que dicta los criterios científicos, éticos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso y archivo del expediente clínico. Su cumplimiento asegura la validez legal de la información gestionada por el EUS.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP):

Dado que el EUS maneja datos sensibles de salud, esta ley es la referencia principal para garantizar el tratamiento legítimo, controlado e informado de los datos personales de los pacientes.

SECCIÓN 3: Términos y definiciones (ISO 27001:2022)

Para asegurar un entendimiento común y el cumplimiento normativo, se definen los siguientes términos clave, aplicados al contexto del Proyecto EUS:

3.1 Glosario de Términos

- **Controles de acceso:** Garantía de que el acceso físico y lógico a los activos está autorizado y restringido según los requisitos de seguridad.
- **Aplicación en EUS:** Implementación de autenticación (Login) y autorización basada en roles (RBAC) en Supabase para diferenciar médicos, instituciones y pacientes.
- **Activo de información:** Conjunto de información definido y gestionado como una sola unidad para ser protegido.
- **Aplicación en EUS:** Base de datos de expedientes (CURP, antecedentes médicos), código fuente del sistema y la infraestructura en la nube.
- **Riesgo:** Combinación de la probabilidad de que ocurra un suceso de seguridad y sus consecuencias.
- **Aplicación en EUS**: Probabilidad de acceso no autorizado a los registros médicos y el impacto en la privacidad del paciente y multas legales.
- **Evaluación de riesgos:** Proceso de identificación, análisis y evaluación de la necesidad de medidas adicionales.
- **Aplicación en EUS:** Análisis de vulnerabilidades en las peticiones de la API de Supabase y evaluación de la necesidad de cifrado adicional.
- **Tratamiento del riesgo**: Acciones para reducir los riesgos a un nivel aceptable.
- **Aplicación en EUS:** Implementación de políticas de Row Level Security (RLS) en la base de datos para prevenir fugas de datos entre médicos.
- **Alta dirección:** Grupo de personas con toma de decisiones al más alto nivel.
- **Aplicación en EUS:** Los responsables del proyecto encargados de los recursos, la visión estratégica y el cumplimiento legal ante las autoridades sanitarias.

3.2 Componentes Complementarios

Mejora Continua (CI)

Es el motor del SGSI. La norma exige que no seamos estáticos; el sistema debe evolucionar ante nuevas amenazas cibernéticas y cambios tecnológicos.

Nota de implementación: Como se ilustra en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), la mejora continua en EUS implica que cada vez que detectemos una brecha o implementemos una nueva función (como la firma electrónica), debemos re-evaluar los riesgos y ajustar nuestros controles de seguridad.

SECCIÓN 4: Contexto de la organización

El objetivo de esta sección es identificar las cuestiones internas y externas que son relevantes para el propósito de EUS y que afectan a su capacidad para lograr los resultados previstos de seguridad de la información.

4.1 Análisis del Contexto Interno

Para el desarrollo de EUS, hemos evaluado los siguientes factores críticos:Madurez: EUS es un proyecto en fase de desarrollo/lanzamiento (tipo startup).

Somos ágiles, lo que nos permite implementar controles de seguridad desde el código inicial (Security by Design), pero carecemos de una infraestructura histórica heredada.

- **Cultura organizativa:** Enfocada en la eficiencia digital y la innovación. La seguridad debe ser ágil y no friccionar el flujo de trabajo clínico.
- **Recursos y Madurez:** Contamos con un equipo técnico especializado en el desarrollo del sistema (Supabase/Frontend), pero con necesidades de capacitación continua en gestión de incidentes de ciberseguridad.
- **Formatos y Activos:** EUS es 100% digital. Los activos son datos de bases de datos (Supabase) y código fuente. No gestionamos papel, por lo que el enfoque es 100% ciberseguridad.
- **Complejidad y Sistemas:** Arquitectura basada en la nube. La complejidad radica en la correcta gestión de los permisos (RLS) en Supabase para asegurar que un médico no vea expedientes de otros hospitales.
- **Espacio físico:** Somos una organización remota/nube; el "perímetro" de seguridad es la identidad digital y la seguridad del código, no el edificio de oficinas.

4.2 Análisis del Contexto Externo

Los factores externos que impactan directamente nuestra estrategia de seguridad:

- **Competencia:** El mercado de Salud Digital es altamente competitivo e innovador. La seguridad es un diferenciador de valor para las instituciones que nos contratan.
- **Reguladores:** EUS opera bajo un entorno altamente regulado (ej. NOM-004-SSA3-2012). El incumplimiento normativo no solo es un riesgo técnico, sino legal y financiero severo.
- **Prevalencia de ataques:** El sector salud es actualmente el objetivo #1 para ataques de ransomware y robo de datos. Esto eleva la importancia de nuestra disponibilidad y cifrado de datos.
- **Consideraciones Ambientales:** Al depender de la nube (Supabase), nuestro riesgo ambiental es el de los proveedores de servicios cloud. Debemos asegurar que el proveedor cumpla con los estándares de disponibilidad (SLA).
- **Accionistas/Partes interesadas:** Los pacientes confían sus vidas y datos de salud en nosotros. Su preocupación principal es la privacidad y la confidencialidad.

4.3 Comprensión de las necesidades de las Partes Interesadas

Para cumplir con la norma, debemos identificar quiénes son y qué esperan de nosotros en términos de seguridad:

.

Partes Interesadas	**Necesidad / Expectativa**
Pacientes	Confidencialidad total de sus datos y disponibilidad de su historial.
Médicos	Sistema accesible, rápido y que garantice que su firma electrónica sea válida.
Instituciones de Salud	Cumplimiento legal, trazabilidad y protección de datos para evitar multas.
Autoridades Sanitarias	Integridad de expedientes clínicos y cumplimiento de normas vigentes.

4.4 Declaración del Alcance del SGSI

El alcance del Sistema de (SGSI) para el proyecto EUS se define de la siguiente manera:

Dimensión	Límite / Descripción
Ubicaciones Físicas	Infraestructura exclusiva remota (cloud). No incluye oficinas físicas de terceros ni centros de salud, excepto como puntos finales de acceso.
Redes y TEcnologías	Infraestructura en la nube (Supbase, Hosting), APIs, base de datos de pacientes (CURO), y los dispositivos de usuario final (navegadores web) utilizados por médicos e instituciones autorizados.
Personal (Interno / Externos)	**Incluidos:** Equipo de desarrollo EUS personal administrativo de EUS, **No incluidos:** Personal médico de instituciones externas (quienes son usuarios de la plataforma pero no gestionan la seguridad del SGSI).
Procesos y Servicios	**Incluidos:** Gestión de altas de pacientes, autenticación (login), consultas de historial clínico. firma electrónica de expedientes, auditoría de logs. **No incluidos:** Procesos internos de los hospitales (ej. facturación hospitalaria o gestión de personal de enfermería)
Interfaces Clave	Conexión con sistemas externos mediante APIs (cuando aplique) y el punto de entrada de la interfaz de usuario (Dashboard / Expediente).

4.5 Justificación del Alcance (Enfoque Pragmático)

Para priorizar la eficacia de nuestros recursos de seguridad, el alcance del presente SGSI se limita estrictamente a la gestión de la información clínica digitalizada dentro de la plataforma EUS. Esto permite concentrar los controles de seguridad en las capas de datos (Supabase) y la identidad del usuario, que son los activos críticos. Cualquier sistema o activo que no forme parte del ciclo de vida del EUS queda fuera de la responsabilidad de este SGSI.

4.6 Registro de Evidencia y Contexto (Consejo para Auditoría)

Para demostrar ante un auditor externo que el alcance fue definido mediante un análisis serio, mantenemos un archivo de evidencias que justifica nuestras decisiones:

- **Análisis de Contexto (Documento "Anexo 1 - Análisis Estratégico"):** Contiene el análisis de los problemas internos/externos (tipo DAFO/SWOT).
- Lista de partes interesadas (Pacientes, Médicos, Autoridades Sanitarias) y sus necesidades.
- **Actas de Reunión:** Registro de la revisión por la dirección (ej. reuniones con el CTO/dueño del proyecto) donde se acordó el alcance.
- **Matriz de Partes Interesadas:** Documento donde mapeamos qué espera cada parte (confidencialidad para el paciente, trazabilidad para el médico).

SECCIÓN 5: Liderazgo

El liderazgo es el pilar que sostiene todo el SGSI. La Alta Dirección no solo autoriza el presupuesto, sino que debe participar activamente en la cultura de seguridad del proyecto EUS.

5.1 Política de Seguridad de la Información (PSI)

Esta política es la declaración oficial de intenciones. Debe ser firmada por el director general o el equipo de alta dirección.

Política de Seguridad de la Información - Proyecto EUS

La dirección del Proyecto EUS reconoce que la información clínica de los pacientes y los datos de salud son nuestros activos más valiosos. Por ello, nos comprometemos a:

- **Proteger la confidencialidad, integridad y disponibilidad:** Garantizar que los expedientes electrónicos estén siempre disponibles para el personal médico autorizado y protegidos contra accesos no autorizados.
- **Cumplimiento Normativo:** Asegurar la adhesión estricta a la NOM-004-SSA3-2012 (Expediente Clínico) y a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- **Seguridad desde el Diseño:** Integrar controles técnicos (RLS en Supabase, cifrado) en cada nueva funcionalidad del sistema.
- **Mejora Continua:** Revisar y actualizar periódicamente este SGSI conforme a la evolución de las amenazas cibernéticas y las mejores prácticas internacionales (ISO 27001:2022).

- **Asignación de Recursos:** Proveer los recursos financieros, tecnológicos y humanos necesarios para mantener el sistema seguro.

Esta política es comunicada a todos los miembros del equipo y proveedores, siendo su cumplimiento un requisito indispensable para nuestra colaboración.

5.2 Funciones y Responsabilidades

Para que la seguridad no recaiga en una sola persona, hemos definido las siguientes responsabilidades claras:

- **Alta Dirección:** Establecer la estrategia, asignar presupuesto para auditorías/servidores y aprobar cambios críticos en la política.
- **Oficial de Seguridad (CISO / Responsable de SGSI):** Coordinar el cumplimiento, gestionar incidentes, liderar la capacitación del personal y reportar el desempeño del sistema ante la dirección.
- **Equipo de Desarrollo (EUS):** Implementar controles técnicos (ej. validación de entradas, seguridad en Supabase) y asegurar que el código no contenga vulnerabilidades.
- **Todo el personal (Médicos/Usuarios):** Responsables de mantener sus credenciales seguras y seguir las directrices de "Escritorio/Pantalla limpia" (no dejar sesiones abiertas).

5.3 Evidenciar Liderazgo ante el Auditor

Un auditor externo no sólo leerá documentos; entrevistará a la dirección. Deben estar preparados para demostrar que:

- **Participan activamente:** Conocen los riesgos principales del EUS (ej. el riesgo de una brecha en la base de datos).
- **Asignan Recursos:** Pueden explicar por qué decidieron invertir en [x] herramienta de seguridad o [x] capacitación.
- **Comunicación:** Saben cómo se comunican los objetivos de seguridad (ej. "en nuestra reunión mensual de equipo, revisamos si hubo intentos de acceso fallidos").

SECCIÓN 6: Panificación

6.1 Propósito y Objetivos

La evaluación de riesgos es el núcleo de nuestro SGSI eficaz. Dado que es imposible eliminar por completo la posibilidad de un incidente de seguridad, este proceso es esencial en EUS para:

- Aumentar la probabilidad de identificar todos los riesgos potenciales de manera sistemática.
- Asignar de manera inteligente nuestros recursos técnicos y financieros a las áreas más prioritarias.
- Tomar decisiones estratégicas de gestión que nos permitan alcanzar nuestros objetivos de seguridad y confidencialidad clínica.

6.2 Marco de Evaluación de Riesgos (Metodología)

Basándonos en las directrices de la norma ISO 27005, el proyecto EUS adopta el siguiente marco metodológico para garantizar la coherencia en la evaluación:

- **Identificación Sistemática:** Revisamos nuestros activos (ej. bases de datos, código, infraestructura de red) uno a uno, comprobando vulnerabilidades y registrando los controles actuales (ej. RLS en Supabase, Autenticación JWT).
- **Evaluación de Probabilidad:** Evaluamos la frecuencia con la que un riesgo podría materializarse (ej. Baja, Media, Alta).
- **Evaluación de Consecuencias:** Analizamos el impacto de cada riesgo sobre una base coherente (ej. impacto en la salud del paciente, impacto legal por multas, pérdida reputacional).
- **Clasificación del Riesgo:** Multiplicamos o cruzamos la Probabilidad por las Consecuencias para asignar una puntuación coherente.
- **Criterios de Acción:** Para cada nivel de riesgo, establecemos un plan de tratamiento documentado especificando la acción a emprender y su prioridad.

6.3 Registro de Riesgos y Activos

Para optimizar nuestros esfuerzos y cumplir con el Anexo A (5.9) de la norma, hemos unificado nuestro inventario de activos con la evaluación de riesgos.

A continuación, se presenta un extracto de nuestra matriz de riesgos, donde cada uno cuenta con un propietario asignado:

Activo de Información	Riesgo Identificado	Probabilidad	Consecuencia (Impacto)	Nivel de Riesgo	Propietario Asignado	Tratamiento / Acción
Base de Datos (Supabase)	Fuga de expedientes entre distintas instituciones.	Baja	Alta (Legal/Privacidad)	Medio-Alto	CTO / Líder de Desarrollo	Implementar estrictas políticas Row Level Security (RLS) por institucion_id.
Acceso a la Plataforma	Robo de credenciales de un médico por phishing.	Media	Alta	Alto	Oficial de Seguridad	Forzar Autenticación de Doble Factor (MFA) para médicos y educar al usuario.
Código Fuente (Frontend/API)	Alteración de la información de las recetas médicas.	Baja	Alta (Salud del paciente)	Alto	Equipo de Desarrollo	Generar un hash criptográfico en cada consulta firmada para garantizar su inmutabilidad.

6.4 Tratamiento del Riesgo

Para cada riesgo identificado en la evaluación, el proyecto EUS aplica criterios coherentes para determinar el plan de acción técnico o administrativo. Las opciones principales de tratamiento implementadas en nuestra arquitectura son:

- **Cambiar la probabilidad (Evitar vulnerabilidades):** Se implementan políticas de Row Level Security (RLS) en PostgreSQL para restringir los permisos. Esto evita proactivamente que un paciente pueda modificar su expediente, dejándolo exclusivamente en modo de lectura.
- **Cambiar las consecuencias (Mitigación de impacto):** Para mitigar el impacto de alteraciones no autorizadas en los diagnósticos, el sistema genera un hash criptográfico en la firma digital del médico. Esto garantiza la inmutabilidad del registro, ya que cualquier modificación invalidaría la firma.

- **Aceptar el riesgo:** Las decisiones informadas sobre la aceptación de riesgos operativos menores son documentadas y aprobadas por la Alta Dirección, considerando el costo-beneficio de los controles.

6.5 Declaración de Aplicabilidad (SoA - Statement of Applicability)

Como exige el Anexo A de la norma ISO 27001, EUS mantiene una Declaración de Aplicabilidad que justifica la implementación de los controles de seguridad. A continuación, se presenta un extracto representativo de nuestra matriz de controles:

La SoA del EUS contiene las 93 entradas de controles de seguridad enumeradas en el Anexo A de la norma. Cada control ha sido analizado individualmente para determinar su selección (con su respectiva justificación basada en nuestra evaluación de riesgos) o su exclusión formal.

6.5.1 Categorías de Controles (Aplicación al Contexto EUS)

Dado que EUS es una plataforma digital de salud alojada en la nube y gestionada de manera ágil, la aplicación de los controles del Anexo A se distribuye de la siguiente manera:

Controles Organizativos: Aplicables en su totalidad. Esta categoría rige la propiedad de los riesgos, la clasificación de la información (datos clínicos sensibles) y las políticas de seguridad de la información que la Alta Dirección ha establecido para cumplir con la NOM-004-SSA3-2012 y la LFPDPPP.

Controles de Personas: Aplicables. Se centran en garantizar que todo el personal técnico, desarrolladores y administradores del sistema EUS estén sujetos a acuerdos de confidencialidad estrictos y reciban concientización continua sobre ciberseguridad (por ejemplo, prevención de phishing).

Controles Tecnológicos: Inclusión Prioritaria. Constituyen el núcleo de nuestra defensa. Aquí se justifican controles como:

La implementación de Row Level Security (RLS) en nuestra base de datos (Supabase) para garantizar la segregación institucional.

El uso de funciones hash criptográficas para asegurar la inmutabilidad de la firma electrónica de los médicos.

Autenticación multifactor (MFA) y gestión estricta de accesos privilegiados.

Controles Físicos: Exclusión Parcial Justificada. Debido a que el ecosistema EUS opera bajo un modelo de infraestructura 100% en la nube (remoto) y no dispone de locales físicos propios para el almacenamiento de expedientes en papel o servidores locales, una gran parte de los controles de seguridad física (ej. perímetros de seguridad física, protección contra amenazas ambientales directas en oficinas) se excluyen de nuestra SoA. La responsabilidad sobre la seguridad física de los servidores recae en los Acuerdos de Nivel de Servicio (SLA) de nuestro proveedor de nube.

6.5.2 Documentación y Propiedad del Tratamiento

Los controles seleccionados no operan de forma aislada; forman parte integral de las pruebas del tratamiento del riesgo del EUS.

Toda la información referente a qué control mitiga qué riesgo se encuentra centralizada en nuestro Registro de Riesgos. La responsabilidad y propiedad de asegurar que estos controles se implementen, se auditen y se mantengan actualizados recae directamente en el Oficial de Seguridad y la Alta Dirección, garantizando así que las medidas de seguridad evolucionen a la par de las nuevas funcionalidades clínicas que se integren en la plataforma.

6.6 Objetivos de Seguridad de la Información y Planificación

Para asegurar el funcionamiento y la mejora de nuestro SGSI, la Alta Dirección ha establecido los siguientes objetivos medibles, alineados con la Política de Seguridad de la Información (PSI):

Objetivo 1: Inmutabilidad de los expedientes.

- Meta: Alcanzar el 100% de consultas médicas registradas con firma digital validada mediante hash criptográfico.
- Propietario: Equipo de Desarrollo EUS.
- Medición: Auditoría periódica de la tabla de registros en la base de datos.

Objetivo 2: Segregación de datos institucionales.

- Meta: Cero incidentes de acceso cruzado, garantizando mediante validación que una institución solo agregue y administre a los doctores de su competencia.
- Propietario: Oficial de Seguridad.
- Medición: Pruebas de penetración y revisión de políticas de inserción.

Objetivo 3: Acceso seguro de pacientes.

- Meta: 100% de los pacientes dados de alta deben configurar su acceso inicial mediante un enlace único seguro enviado a su correo.
- Propietario: Administrador del Sistema.
- Medición: Revisión de logs de creación de usuarios en Supabase Auth.

Guía y Selección de Controles (Basado en el Anexo A de ISO 27001:2022)

La norma ISO 27001:2022 sigue un enfoque basado en el riesgo, lo que requiere la identificación de amenazas y la posterior selección de controles adecuados del Anexo A para reducir, eliminar o gestionar dichos riesgos. En total, el Anexo A presenta 93 controles divididos en cuatro categorías principales, las cuales se aplican al ecosistema EUS de la siguiente manera:

SECCIÓN 7: Apoyo

La implantación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del proyecto EUS requiere de una estructura sólida de soporte. Esta sección determina los recursos, competencias, mecanismos de concienciación, canales de comunicación y el control de la información documentada necesarios para garantizar la resiliencia y eficacia del sistema.

7.1 Recursos

Para asegurar que el SGSI opere de manera eficaz y responda a un enfoque basado en riesgos, la organización determina y proporciona los recursos necesarios, clasificándolos en tres pilares fundamentales:

- **Infraestructura y Entorno (Capaces)**: Al ser una plataforma cloud-native, la infraestructura física principal (servidores de base de datos, almacenamiento de datos clínicos y hosting de la aplicación) se delega en proveedores de servicios en la nube controlados mediante Acuerdos de Nivel de Servicio (SLA). El entorno tecnológico del ecosistema EUS incluye el aprovisionamiento de bases de datos relacionales seguras, plataformas de despliegue automatizado y herramientas criptográficas avanzadas para la protección de datos de salud sensibles.
- **Talento Humano (Competentes):** Comprende al equipo de desarrollo de software, administradores de bases de datos, colaboradores de la plataforma de salud y el Oficial de Seguridad de la Información. Todos ellos cuentan con voz y representación en las reuniones periódicas de revisión por la dirección.
- **Conocimiento Organizacional**: Se reconoce el conocimiento técnico, las lecciones aprendidas sobre vulnerabilidades y el marco normativo de salud digital como un activo crítico de la organización.

7.2 Competencia

La eficacia de los controles tecnológicos (como el diseño de políticas de control de acceso a nivel de filas o Row Level Security) y organizativos depende estrictamente de las capacidades del personal. Para asegurar una base sólida de conocimientos, el proyecto EUS establece las siguientes directrices:

- **Definición de Requisitos**: Se establecen los perfiles de puesto técnicos y administrativos, especificando los conocimientos requeridos en desarrollo seguro, gestión de bases de datos en la nube, criptografía aplicada a datos de salud y cumplimiento normativo (por ejemplo, normativas nacionales de expediente clínico).
- **Determinación de Roles:** Se identifican con precisión las responsabilidades de cada miembro del equipo de desarrollo, asegurando que solo el personal con la competencia adecuada maneje la lógica de autenticación y los esquemas de bases de datos.
- **Evaluación y Verificación:** La competencia se evalúa mediante revisiones técnicas de código, certificaciones profesionales, evaluaciones internas de habilidades y registros de asistencia a cursos especializados.
- **Nota para Auditoría:** El proyecto mantiene una Matriz de Habilidades y Formación actualizada. Toda conformidad con los requisitos de competencia se demuestra documentalmente mediante certificados

académicos, constancias de capacitación técnica y evaluaciones de desempeño firmadas

7.3 Concienciación

Más allá de las competencias técnicas específicas, todo el personal involucrado en el ecosistema EUS (desarrolladores, editores, administradores y proveedores externos) debe comprender los fundamentos del SGSI para cimentar una cultura de seguridad corporativa. Todo el personal es concientizado formalmente sobre:

La existencia del SGSI y los objetivos estratégicos de proteger la integridad de los expedientes clínicos.

La Política de Seguridad de la Información y cómo los lineamientos de control de accesos y confidencialidad impactan directamente en sus actividades diarias.

Su contribución individual a la eficacia del sistema, reportando de inmediato debilidades de seguridad o accesos anómalos.

Las consecuencias administrativas, legales y contractuales que resulten del incumplimiento de las políticas y procedimientos del SGSI.

Estas acciones se integran de manera natural en los procesos existentes mediante inducciones al ingresar al proyecto, cláusulas de confidencialidad en los contratos de colaboración y sesiones informativas periódicas.

7.4 Comunicación

Para que los procesos del SGSI funcionen de manera fluida, las actividades de comunicación interna y externa se planifican de forma sistemática. El proyecto EUS define su plan general de comunicación mediante la siguiente matriz de control:

¿Qué se debe comunicar?	¿Cuándo comunicarlo?	¿A quién se debe incluir?	¿Cuál es el proceso / canal?
Actualizaciones de la Política de Seguridad.	Inmediatamente tras su aprobación o modificación anual.	Todo el personal, desarrolladores y colaboradores.	Correo electrónico institucional y repositorio documental.
Incidentes o vulnerabilidades críticas.	De forma inmediata tras su detección/confirmación.	Equipo técnico, Oficial de Seguridad y proveedores cloud si aplica.	Canales internos de comunicación técnica y sistemas de alerta automáticos.
Cambios en privilegios o accesos a la BD.	Al realizar altas, bajas o promociones de personal.	Administrador de Base de Datos y el usuario afectado.	Sistema de gestión de tickets o solicitudes formales firmadas.
Resultados de auditorías y revisiones.	Tras la conclusión de las auditorías del SGSI.	Alta Dirección, Oficial de Seguridad y coordinadores de área.	Reunión formal de revisión por la dirección y minutas documentadas.

7.5 Información Documentada

La información documentada que soporta el SGSI del proyecto EUS se gestiona para garantizar que sea exacta, comprensible y alineada con los requisitos legales de protección de datos de salud.

7.5.1 Procesos de Creación y Actualización

Cualquier documento nuevo o modificado (como este manual, políticas de control de accesos o registros de riesgo) debe ser revisado y aprobado por las personas designadas (Oficial de Seguridad o Alta Dirección) antes de su difusión general. Cada documento debe contar con una identificación clara (título, fecha, versión) y un formato que facilite su comprensión por parte de los usuarios finales.

7.5.2 Control de la Información Documentada

Para evitar modificaciones accidentales, corrupción de datos, eliminaciones no autorizadas o fugas de información hacia terceros, se aplican los siguientes controles:

- **Control de Acceso Riguroso**: Los documentos del SGSI y los manuales técnicos se almacenan en un sistema de gestión documental electrónico protegido con autenticación robusta. Se otorgan permisos de "Solo Lectura" para usuarios generales y permisos de "Edición" restringidos únicamente a los propietarios del documento.
- **Control de Cambios e Historial de Versiones:** Se mantiene un registro detallado (Ledger o Historial de Versiones) al inicio de cada documento normativo que detalla la fecha del cambio, el autor, los apartados modificados y la justificación de la actualización.
- **Almacenamiento y Respaldo**: Se ejecutan políticas automatizadas de copia de seguridad electrónica para evitar la pérdida de evidencia de auditoría y registros de cumplimiento.
- **Disposición Segura:** Cuando un documento pierde vigencia o la información sensible debe ser destruida, se aplican métodos de eliminación segura (borrado lógico permanente de archivos digitales o destrucción física de cualquier soporte material), o bien, se devuelve formalmente a su propietario si así lo estipulan los acuerdos legales.

SECCIÓN 8: Funcionamiento

La gestión de los riesgos para la seguridad de la información y la consecución de los objetivos del proyecto EUS requieren que nuestras estrategias teóricas se lleven a la práctica mediante la formalización de actividades operativas. En EUS, los procesos cotidianos deben diseñarse e implementarse considerando la seguridad desde su origen (Security by Design).

8.1 Planificación y Control Operacional

Para que el Sistema de Gestión de Seguridad de la Información (SGSI) opere de manera eficaz, es necesario formalizar las actividades de la plataforma en un conjunto de procesos claros. Algunos de estos procesos ya existen (como el desarrollo de código o el alta de médicos en el sistema) y simplemente se modifican para incluir controles de seguridad, mientras que otros se instauran específicamente para el SGSI (como las auditorías internas).

Para aplicar procesos eficaces dentro del ecosistema EUS, aplicamos las siguientes seis prácticas cruciales:

- **Formalización**: Los procesos seguros se crean adaptando las actividades habituales del ciclo de desarrollo de software y gestión hospitalaria de la plataforma.
- **Identificación Sistemática:** Cada proceso operativo (por ejemplo, la autenticación de usuarios o la consulta de expedientes) pasa por una identificación de los riesgos de ciberseguridad pertinentes.
- **Definición y Comunicación:** Se establece un conjunto claro de actividades para gestionar los riesgos cuando ocurre un evento crítico, como la incorporación de un nuevo desarrollador al proyecto o el alta de una nueva institución médica.
- **Asignación de Responsabilidades:** Se definen claramente las responsabilidades técnicas y administrativas para llevar a cabo dichas actividades.
- **Asignación de Recursos:** Se garantiza la disponibilidad de infraestructura en la nube (Supabase) y tiempo del equipo técnico para ejecutar las actividades operativas cuando sea necesario.
- **Evaluación Rutinaria**: Se evalúa periódicamente la coherencia con la que se siguen los procesos y su eficacia para mitigar los riesgos de fuga de datos o accesos no autorizados.
- **Nota Operativa (Propietarios de Proceso):** Para cada proceso clave del EUS, se designa a un "Propietario del Proceso" (por ejemplo, el Oficial de Seguridad o el Líder de Desarrollo), quien es el responsable directo de garantizar que los pasos 2 al 6 se cumplan de manera sistemática.

8.2 Evaluación de Riesgos en la Operación

Los métodos y técnicas de evaluación de riesgos definidos en la Sección 6 (Planificación) se aplican de manera continua a todos los procesos, activos tecnológicos (código fuente, API, bases de datos), información clínica y actividades dentro del alcance del SGSI.

Dado que las amenazas cibernéticas y la arquitectura de software no son estáticas, los resultados de nuestras evaluaciones de riesgo en EUS se revisan de forma frecuente: al menos una vez al año, o con mayor frecuencia si se detecta un riesgo significativo (como una vulnerabilidad crítica de Día Cero en las dependencias de nuestro código).

Además, las evaluaciones de riesgo se ejecutan obligatoriamente siempre que:

1. Se completan todas las acciones de Tratamiento de Riesgos estipuladas.
2. Se producen cambios sustanciales en la infraestructura tecnológica (migraciones de base de datos) o en los procesos operativos de la organización.
3. Se identifican nuevos vectores de ataque o riesgos cibernéticos emergentes.
4. La experiencia operativa, métricas del sistema o nueva información indican que la probabilidad o las consecuencias de un riesgo previamente identificado han cambiado.

8.3 Tratamiento de los Riesgos para la Seguridad de la Información

El plan de tratamiento de riesgos del EUS (como la implementación obligatoria de Row Level Security en Supabase o los hashes criptográficos en las firmas) no es simplemente una declaración documental de intenciones; es un mandato operativo que se ejecuta en el código y en la infraestructura.

Actualización del Plan: Cuando sea necesario introducir cambios derivados de nueva información sobre vulnerabilidades o modificaciones en los criterios de riesgo, el plan de tratamiento se actualiza y vuelve a ser autorizado por la Alta Dirección.

Evaluación del Impacto y Eficacia: Se evalúa de manera constante el impacto real de los controles implementados, registrando rigurosamente los resultados. En el EUS, esto se logra mediante:

- Revisiones periódicas por la dirección.
- Procesos de auditoría interna.

Evaluaciones técnicas exhaustivas, tales como pruebas de penetración (Pen Testing) en nuestra API y base de datos, revisiones de seguridad a nuestros proveedores (cloud hosting), y auditorías de código sin previo aviso.

SECCIÓN 9: Evaluación del rendimiento

Para garantizar que el Sistema de Gestión de la Seguridad de la Información (SGSI) del proyecto EUS protege de manera efectiva los expedientes clínicos y cumple con sus objetivos estratégicos, es imperativo evaluar su rendimiento de forma continua. Existen tres mecanismos principales mediante los cuales EUS evalúa la salud de su SGSI: la supervisión de la eficacia de los controles, la ejecución de auditorías internas y las reuniones de revisión por la dirección.

9.1 Seguimiento, medición, análisis y evaluación

El ecosistema EUS (basado en arquitecturas de nube y bases de datos como Supabase) genera un volumen masivo de datos transaccionales. Dado que no es práctico ni eficiente supervisar manualmente cada evento, la organización ha definido estratégicamente qué métricas y procesos deben monitorearse para generar información significativa y oportuna.

Para determinar nuestro enfoque de monitoreo, consideramos:

- **Procesos con amenazas frecuentes:** Intentos de inicio de sesión (autenticación) y peticiones a la API desde dispositivos no reconocidos.
- **Vulnerabilidades inherentes significativas**: El acceso a los datos sensibles de los pacientes (CURP, antecedentes médicos) mediante consultas a la base de datos.
- **Automatización**: Gran parte de nuestra supervisión se delega en herramientas automatizadas de logging en la nube que detectan anomalías en tiempo real.

Para cada proceso de supervisión dentro de la plataforma EUS, mantenemos una definición clara:

Cómo y cuándo se lleva a cabo: Por ejemplo, el monitoreo automatizado 24/7 de bloqueos de Row Level Security (RLS) o intentos fallidos de autenticación MFA.

Responsable: El Administrador del Sistema o el Oficial de Seguridad.

Comunicación y Escalada: Si los resultados identifican un rendimiento inaceptable (por ejemplo, una posible brecha de datos o un ataque de fuerza bruta), se activa inmediatamente el procedimiento de escalada, notificando a la Alta Dirección y al equipo técnico de guardia para la contención del incidente.

Nota de Cumplimiento: Se conservan registros (logs inmutables y reportes mensuales) de los resultados del monitoreo, los análisis de vulnerabilidades y cualquier actividad de escalado como evidencia para las auditorías.

9.2 Auditorías internas

El objetivo de las auditorías internas en el EUS es someter a prueba nuestros controles tecnológicos y administrativos para identificar debilidades estructurales y oportunidades de mejora antes de enfrentar una auditoría de certificación externa. Estas auditorías permiten a la Alta Dirección validar si el SGSI cumple

sistemáticamente con los requisitos de la norma ISO 27001 y las normativas de salud.

Las auditorías internas del EUS están diseñadas para comprobar:

La coherencia con la que los desarrolladores y médicos aplican los procesos, procedimientos y controles (ej. validación del uso correcto de firmas electrónicas).

Si los controles técnicos (cifrado, MFA, segregación de datos institucionales) están generando los resultados de protección previstos.

9.2.1 Requisitos y Planificación de la Auditoría

Para garantizar el valor de las auditorías, estas son ejecutadas por personal o consultores que son competentes, imparciales frente al área auditada y familiarizados tanto con la norma ISO 27001 como con arquitecturas en la nube.

El proyecto EUS mantiene un Plan de Auditoría Interna que asegura:

1. Que todos los procesos del SGSI se auditen dentro de un ciclo planificado (máximo tres años).
2. Que los procesos más críticos (como la gestión de identidades, la infraestructura de Supabase y la protección de datos clínicos) o aquellos con incidentes de seguridad previos se auditen con mayor frecuencia (enfoque basado en riesgos).

Toda no conformidad u oportunidad de mejora detectada durante la auditoría se registra formalmente. Las acciones correctivas requeridas son revisadas por los propietarios de los procesos técnicos y se aplican en los plazos acordados para rectificar cualquier debilidad significativa.

9.3 Revisión por la dirección

La revisión por la dirección es el punto de control formal donde la Alta Dirección del proyecto EUS evalúa la eficacia global del SGSI y asegura que este se mantenga alineado con la dirección estratégica de la plataforma y el cumplimiento normativo en salud digital.

Estas revisiones se llevan a cabo a intervalos planificados. No es obligatorio consolidar toda la revisión en una única y extensa reunión anual; en el modelo ágil del EUS, estas revisiones pueden integrarse en reuniones gerenciales periódicas, siempre que el programa general cubra como mínimo las áreas básicas requeridas

por la Cláusula 9.3 de la norma (estado de acciones previas, cambios en los riesgos, rendimiento de los controles, resultados de auditorías, etc.).

9.3.1 Información Documentada de la Revisión

Para demostrar el compromiso y el cumplimiento, EUS conserva información documentada de todas las revisiones por la dirección. Esta evidencia consiste generalmente en actas de reuniones o minutas que registran claramente:

- Las decisiones estratégicas tomadas respecto al SGSI (ej. aprobación de presupuesto para nuevas herramientas de seguridad).
- Las acciones preventivas o correctivas acordadas.
- Las responsabilidades asignadas y los plazos de ejecución.

SECCIÓN 10: Mejora

El objetivo clave de la implantación del SGSI en la plataforma del Expediente Único de Salud (EUS) es reducir de forma sistemática la probabilidad de ocurrencia de sucesos relacionados con la seguridad de la información, así como mitigar su impacto potencial en los datos clínicos de los usuarios. Reconociendo que ningún sistema de seguridad es infalible ni estático, un SGSI eficaz está diseñado para evolucionar con el tiempo, incrementando progresivamente la resistencia de la infraestructura tecnológica frente a amenazas y ataques cibernéticos.

10.1 No conformidad y acción correctiva

Uno de los principales motores de la mejora continua dentro del ecosistema EUS consiste en capitalizar el aprendizaje derivado de los incidentes de seguridad, las no conformidades detectadas en las auditorías internas, las desviaciones de rendimiento identificadas durante la supervisión automatizada, las quejas de las partes interesadas (médicos, pacientes o instituciones) y las directrices surgidas en las revisiones de la dirección.

Ante cualquier no conformidad o incidente de seguridad detectado, la organización mantendrá un registro estricto que documente de manera obligatoria los siguientes elementos:

Acciones de contención: Si el suceso generó consecuencias indeseables en la plataforma, se detallarán las medidas inmediatas adoptadas para contener y

mitigar el impacto (por ejemplo, el aislamiento temporal de un nodo de red o la revocación inmediata de un token de acceso).

Identificación de la causa raíz: Investigación profunda para determinar el origen real y subyacente que propició el fallo.

Acciones correctivas: Definición e implementación de medidas diseñadas específicamente para eliminar la causa raíz y evitar que el suceso vuelva a ocurrir.

Evaluación de la eficacia: Análisis posterior y verificación técnica para comprobar si las acciones correctivas adoptadas cerraron de forma definitiva la vulnerabilidad detectada.

Para asegurar que las acciones correctivas sean verdaderamente eficaces, el equipo técnico del EUS evitará soluciones superficiales, recurriendo a un análisis exhaustivo de la causa raíz de los problemas. Como herramienta preferente por su simplicidad y efectividad, se adopta el enfoque de los "Cinco Porqués", el cual consiste en partir del planteamiento del problema y cuestionar de manera sucesiva el origen de cada respuesta hasta identificar el fallo estructu

10.2.1 Ejemplo de Aplicación Práctica

Para ilustrar el funcionamiento de este mecanismo ante un escenario técnico crítico de la plataforma, se presenta el siguiente análisis:

Planteamiento del problema: Se detectó una consulta no autorizada a datos clínicos confidenciales dentro de la base de datos de la plataforma.

1. ¿Por qué ocurrió? Una modificación en el código de la aplicación deshabilitó temporalmente la política de seguridad a nivel de filas (Row Level Security o RLS) durante un despliegue.

2. ¿Por qué se deshabilitó? El desarrollador a cargo alteró la configuración técnica de la base de datos para realizar pruebas de integración rápidas y olvidó restaurar los privilegios restrictivos antes de subir los cambios al entorno de producción.

3. ¿Por qué se permitió subir el código a producción sin esta validación? El proyecto no pasó por una revisión de código automatizada o manual antes de integrarse al repositorio principal en GitHub.

4. ¿Por qué no se ejecutó la revisión obligatoria de código? El encargado de validar el flujo de despliegue seguro automatizado se encontraba ausente y la organización no había implementado un perfil de cobertura para suplir sus funciones técnicas.

5. ¿Por qué no existía una cobertura formal para esa función? El proceso de ausencia o baja de personal clave no estaba contemplado formalmente dentro del Procedimiento de Gestión de Cambios del proyecto, lo que impidió realizar una evaluación de riesgos orientada a la continuidad y seguridad de las operaciones.

Este desglose demuestra cómo un aparente descuido técnico en la base de datos tiene su verdadera causa raíz en una omisión de control administrativo dentro de la gestión de cambios, lugar donde se debe aplicar la acción correctiva definitiva.

10.3 Priorización y Evaluación del Riesgo en la Mejora

Considerando las limitaciones de tiempo y recursos técnicos de un equipo de desarrollo, el proyecto EUS aplicará un enfoque pragmático para gestionar las no conformidades. No todos los eventos requerirán un análisis exhaustivo de causa raíz.

Para optimizar los esfuerzos, el Oficial de Seguridad realizará una evaluación rápida de riesgo inmediatamente después de registrar el suceso. El análisis profundo de causa raíz y la formalización de acciones correctivas complejas se emprenderán de manera obligatoria y prioritaria únicamente para aquellos incidentes o no conformidades que presenten un nivel de riesgo medio, alto o crítico va va la confidencialidad de los expedientes médicos o la estabilidad de la API. Las incidencias de riesgo bajo se solventarán mediante correcciones directas y controladas en el flujo de mantenimiento habitual.