UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y DISEÑO DÍGITAL

INGENIERÍA DE SOFTWARE

ASIGNATURA:

INGENIERÍA DE REQUERIMIENTOS

TEMA:

GA-CASO PRÁCTICO

DOCENTE:

ING. GUERRERO ULLOA GLEISTON CICERON

INTEGRANTES:

ARCALLE GREFA DARWIN ORLANDO

LOMBEIDA ESCALERAS BRYAN HUMBERTO

MUÑOZ VERA MELANIE MICHELLE

PACA PILATAZA LUIS ALBERTO

NIVEL:

4TO SOFTWARE

PARALELO:

“B”

AÑO LECTIVO:

2025-2026

https://github.com/Luispaca2002/IngenieriaRequerimientos.git

1. Análisis del Contexto y Entorno

El sistema informático de control de enfermería está diseñado específicamente para su implementación en un centro médico universitario para brindar servicios de atención primaria a estudiantes, docentes y personal administrativo. Este tipo de centro constituye un elemento clave para el bienestar integral de la comunidad académica y para el fortalecimiento de los procesos educativos vinculados al área de la salud.

Desde el enfoque académico, el sistema también debe contemplar a estudiantes en formación del área de salud, quienes participan en procesos supervisados de atención clínica. Por tanto, se requiere una solución tecnológica que facilite el acceso controlado a la información y que apoye el aprendizaje mediante herramientas integradas, sin comprometer la confidencialidad de los datos.

La institución dispone de equipos de cómputo operativos en cada área, conexión a internet estable y una red interna segura. Esta base tecnológica es adecuada para implementar un sistema que permita el registro, consulta y análisis de información clínica en tiempo real, con acceso segmentado según los perfiles de usuario.

Cualquier implementación tecnológica en este entorno debe cumplir con los marcos legales establecidos para el manejo de datos personales sensibles. La Ley Orgánica de Protección de Datos Personales exige confidencialidad, consentimiento informado del paciente y medidas técnicas que aseguren la integridad y privacidad de la información. Así mismo, deben respetarse los protocolos clínicos institucionales y las políticas internas de acceso a datos.

2. Identificación de Stakeholders

En esta tabla se presenta la identificación de las partes interesadas (stakeholders) de un sistema informático para el control de enfermería en un centro médico universitario, teniendo en consideración sus necesidades y expectativas.

Tabla I: *Necesidades y expectativas del stakeholder.*

Stakeholder	**Necesidades**	**Expectativas**
Personal médico	Acceder fácilmente al historial médico de pacientes, registrar diagnósticos.	Disminuir los procesos manuales, para poder acceder a la información de manera rápida.
Personal administrativo	Gestionar citas, controlar inventario, generar reportes.	Más eficiencia para la organización, clasificación y

		acceso a los documentos, que permita optimizar el tiempo de búsqueda.
Pacientes	Mejorar el tiempo de atención, facilitar el proceso de registro de citas.	Facilidad en el proceso del registro de citas.
Enfermeras y personal de enfermería	Registrar signos vitales, administrar medicamentos, dar indicaciones médicas, generar reportes.	Interfaz intuitiva, menor carga administrativa, mejor comunicación con médicos y rapidez en el registro.
Estudiantes en formación	Acceso controlado a información clínica, aprendizaje supervisado.	Comprensión del entorno hospitalario real e integración de herramientas tecnológicas en su formación.
Administradores del centro médico	Obtener informes de gestión (eficiencia, ocupación, tiempos), control de calidad de atención, cumplimiento de protocolos.	Mayor eficiencia operativa, toma de decisiones basada en datos reales, reducción de costos y optimización de recursos.
Departamento de TI	Seguridad de datos, copia de seguridad, mantenimiento del sistema, soporte técnico, escalabilidad.	Integración con otros sistemas clínicos, arquitectura robusta, menor intervención manual, facilidad de monitoreo.
Autoridades académicas/institucionales	Alineación con objetivos académicos y sus herramientas de evaluación del desempeño estudiantil.	Formación moderna, evaluación precisa y fortalecimiento de la reputación institucional gracias al uso de tecnologías avanzadas.

3. Establecer los Objetivos del Sistema

Objetivo general

Implementar un sistema informático de control de enfermería que optimice la gestión de los servicios de salud en el centro médico universitario, facilitando el seguimiento de la atención al paciente, mejorando la eficiencia operativa del personal encargado del sistema.

Objetivos específicos

- Capacitar al personal en el uso adecuado del sistema para garantizar su correcto funcionamiento.
- Mejorar la gestión de turnos del personal de enfermería mediante un sistema automatizado que facilite la planificación de los horarios y asegure una atención médica oportuna.
- Automatizar el envío de una copia digital de la receta médica al correo electrónico institucional del paciente para mejorar la accesibilidad a su tratamiento.

4. Revisión de Sistemas Similares

Se analizaron varios sistemas de información en salud aplicados en hospitales y entornos clínicos, los cuales brindan aprendizajes valiosos para diseñar un sistema de control enfocado en enfermería.

Sistema de evaluación en un hospital geriátrico

Emplea un algoritmo basado en lógica difusa temporal para valorar la calidad del tratamiento de pacientes con úlceras por presión. Al integrarse con los historiales clínicos digitales (EMR), permite verificar el cumplimiento de protocolos clínicos por parte del personal, y reduce el tiempo requerido para las evaluaciones sin perder precisión [1].

MicroShare

Es una propuesta tecnológica que utiliza una arquitectura de microservicios para el intercambio de información médica, preservando la confidencialidad del paciente. En lugar de usar métodos tradicionales para ocultar la identidad de los pacientes, incorpora mecanismos como el control de acceso por roles (RBAC) y tokens de autenticación (JWT) [2].

Sistema EHR Australia

Resalta la relevancia de mantener la integridad de los datos clínicos, advirtiendo que errores del sistema, prácticas inadecuadas como la copia repetida de textos o problemas al identificar al paciente, pueden afectar negativamente la atención sanitaria. Se subraya la importancia de

establecer estándares claros que garanticen la integridad de la información en tres etapas fundamentales [3]:

- La captura inicial de los datos
- Su correcta asociación con los pacientes
- Protección durante su almacenamiento y transmisión.

Prácticas destacadas

- Uso de herramientas automatizadas para medir la calidad del cuidado basado en guías clínicas actualizadas.
- Aplicación de mecanismos de acceso controlado mediante asignación de roles y autenticación segura de usuarios.
- Se utilizan técnicas modernas, como reemplazar los datos personales por identificadores simulados, con el fin de mantener la privacidad de la información médica.

Desafíos encontrados

- Alto nivel de complejidad técnica al implementar sistemas que utilizan lógica difusa y análisis a largo plazo.
- Posibilidad de fallos humanos durante la entrada o modificación de información clínica.
- Obstáculos para integrar distintos sistemas existentes debido a la falta de compatibilidad entre plataformas tecnológicas.

5. Determinación de Restricciones Técnicas y Legales

Analizar las restricciones legales y éticas, como la privacidad de los datos personales y el cumplimiento de normativas sanitarias.

Las restricciones legales y éticas se derivan de normativas que garantizan la privacidad, confidencialidad y seguridad de los datos personales, así como el respeto a los derechos y la integridad de las personas.

Privacidad de los datos personales

Principios de Tratamiento: El tratamiento de datos personales debe cumplir con principios como legalidad, lealtad, transparencia, finalidad, pertinencia, proporcionalidad, confidencialidad, calidad, exactitud, conservación, seguridad, responsabilidad proactiva y aplicación favorable al titular, según el artículo 10 de la *Ley Orgánica de Protección de Datos Personales*[4]. En resumen, esto implica que el sistema garantice que los datos sean utilizados únicamente con fines específicos y protegidos de acceso no autorizado.

Consentimiento Explícito: Según el artículo 26 de la *Ley Orgánica de Protección de Datos Personales* [4]**,** donde dice que, está prohibido el tratamiento de datos personales sensibles, a menos que exista una justificación legal específica (como el consentimiento explícito del titular, una obligación legal, fines médicos, etc.).

Derecho del Titular: De acuerdo con los artículos 13 al 20 de la *Ley Orgánica de Protección de Datos Personales* [4], los usuarios cuentan con derechos como el acceso, la rectificación, la supresión, la oposición, la portabilidad de sus datos y el derecho a no ser sometidos a decisiones automatizadas. Es responsabilidad del sistema asegurar que estos derechos puedan ejercerse de manera gratuita y en un plazo razonable.

Seguridad de los Datos: Según el artículo 10, literal j, de la *Ley Orgánica de Protección de Datos Personales* **[**4], los responsables del tratamiento de datos personales deben aplicar medidas de seguridad adecuadas, tanto técnicas como organizativas, de acuerdo con el estado actual de la tecnología. Estas medidas deben proteger los datos frente a riesgos y vulnerabilidades, considerando la naturaleza de los datos y el contexto en el que se gestionan. Esto incluye la realización de auditorías y evaluaciones periódicas para verificar el cumplimiento.

Confidencialidad de la Información de Salud

Confidencialidad: Conforme a lo dispuesto en los artículos 2 y 7 del *Reglamento De Información Confidencial En Sistema Nacional De Salud*[5], los datos de salud (resultados de exámenes, historial clínico, etc.) son estrictamente confidenciales. Solo personal autorizado puede acceder a ellos, y deben protegerse con sistemas seguros, ya sean físicos o digitales.

Secreto Medico: Según el artículo 6 del *Reglamento De Información Confidencial En Sistema Nacional De Salud*[5], es la obligación que tienen los profesionales de la salud de mantener en confidencialidad toda la información que los pacientes les confían durante la atención médica. Además, esta obligación se extiende a todo el personal involucrado en la atención dentro del sistema de salud.

Respeto a los Derechos y Bienestar

Integridad y Derechos: Según el artículo 5 del *Reglamento de Bienestar Universitario*[6]**,** se debe promover un ambiente de respeto hacia la integridad física, psicológica y sexual de los estudiantes, libre de cualquier forma de violencia. Cualquier sistema que procese información relacionada contar con mecanismos de protección rigurosa.

Establecer las restricciones técnicas, como los recursos disponibles (hardware, software, redes), la escalabilidad y la interoperabilidad.

Las limitaciones técnicas hacen referencia a las condiciones y exigencias que deben tomarse en cuenta para el diseño y operación del sistema.

Recursos disponibles

Hardware y Software: En relación con las medidas de seguridad previamente mencionadas, el sistema debe contar con mecanismos como el cifrado de la información y controles de acceso robustos. Esto conlleva que tanto hardware como el software debe ser capaces de soportar dichas funcionalidades. Asimismo, es importante considerar que, según el artículo 15 del *Reglamento De Información Confidencial En Sistema Nacional De Salud*[5]**,** el acceso a archivos electrónicos estará limitado únicamente a personal autorizado, mediante el uso de claves personales asignadas por el responsable del área o establecimiento.

Redes: Las exigencias de confidencialidad y protección implican que las redes utilizadas deben contar con mecanismos de seguridad, como firewalls y redes privadas virtuales (VPN), con el fin de proteger el envío de información sensible.

Escalabilidad

En cuanto a la escalabilidad, esta se refiere a la capacidad del sistema para adaptarse de manera eficientemente al crecimiento del número de usuarios, al aumento en la cantidad de datos procesados o complejidad de las operaciones, sin comprometer el rendimiento.

Según lo establecido en la norma ISO/IEC 25010:2011, los sistemas deben estar preparados para tolerar un incremento en la cantidad de usuarios sin afectar su funcionamiento [7].

Interoperabilidad

La interoperabilidad es la capacidad del sistema para integrarse y comunicarse eficazmente con otros sistemas o componentes, permitiendo un intercambio de información de manera fluida y coherente y sin perdidas.

Según el artículo 17 de la *Ley Orgánica de Protección de Datos Personales* **[**4]**,** se reconoce el derecho del titular a recibir y transferir sus datos personales en un formato compatible y estructurado que garantice la interoperabilidad entre sistemas. Esto asegura que los datos puedan transferirse fácilmente entre responsables sin obstáculos técnicos, facilitando un acceso rápido, económico y seguro.

Referencias

[1] E. Shalom, A. Goldstein, R. Wais, M. Slivanova, N. M. Cohen, and Y. Shahar, "Implementation and Evaluation of a System for Assessment of The Quality of Long-Term Management of Patients at a Geriatric Hospital".

[2] Yilong Yang, Quan Zu, Peng Liu, Defang Ouyang, and Xiaoshan Li, "MicroShare: Privacy-Preserved Medical Resource Sharing through MicroService Architecture", Accessed: Jun. 14, 2025. [Online]. Available: https://arxiv.org/pdf/1806.02134

[3] P. Vimalachandran, H. Wang, Y. Zhang, B. Heyward, and F. Whittaker, "Ensuring Data Integrity in Electronic Health Records: A Quality Health Care Implication".

[4] Ley, "LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES," Ecuador, May 2021. Accessed: Jun. 14, 2025. [Online]. Available: www.lexis.com.ec

[5] "REGLAMENTO DE INFORMACION CONFIDENCIAL EN SISTEMA NACIONAL DE SALUD," Jan. 2015, Accessed: Jun. 14, 2025. [Online]. Available: https://www.salud.gob.ec/wp-content/uploads/2022/09/A.M.-5216-Reglamento-de-informacion-confidencial-en-SNS.pdf

[6] "UTEQ REGLAMENTO DE LA UNIDAD DE BIENESTAR UNIVERSITARIO," Feb. 2023, Accessed: Jun. 14, 2025. [Online]. Available: https://www.uteq.edu.ec/assets/docs/ubu/docx-uteq-8-0001.pdf

[7] "ISO IEC 25010 2011 Systems and Software Quality Requirements and Evaluation SQuaRE Quality Model.pdf," https://es.slideshare.net/slideshow/iso-iec-25010-2011-systems-and-software-quality-requirements-and-evaluation-square-quality-modelpdf/256282123.