

UNIB.E

UNIVERSIDAD IBEROAMERICANA DEL ECUADOR

FACULTAD DE COMUNICACIÓN Y TICS

CARRERA: INGENIERIA EN SOFTWARE

MÓDULO WEB PARA LA GESTIÓN INTERNA DE ACCESO A LOS APLICATIVOS DE UNA UNIVERSIDAD PÚBLICA DEL ECUADOR UBICADA EN EL CANTÓN RUMIÑAHUI, MEDIANTE LAS HERRAMIENTAS DE DESARROLLO ANGULAR Y SPRING BOOT.

Trabajo de Integración Curricular para la obtención del Título de Ingeniero en
Software

Autores:

Willian Manolo Conya Gavilanez

Karen Vanessa Tipan Tibanta

Tutor:

MSc. Juan Pabón.

Quito, Ecuador

Marzo, 2024

DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

1. Nosotros, **Willian Manolo Conya Gavilanez** y **Karen Vanessa Tipan Tibanta**, declaramos en forma libre y voluntaria que los criterios emitidos en el presente Trabajo de Integración Curricular, titulado: “**Módulo web para la gestión interna de acceso a los aplicativos de una Universidad pública del Ecuador ubicada en el cantón Rumiñahui, mediante las herramientas de desarrollo Angular y Spring Boot**”, previo a la obtención del título profesional de **Ingeniero en Software**, así como también los contenidos, ideas, análisis, conclusiones y propuestas son de exclusiva responsabilidad de nosotros, como autores.
2. Declaramos, igualmente, tener pleno conocimiento de la obligación que tiene la Universidad Iberoamericana del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT, en formato digital una copia del referido Trabajo de Integración Curricular para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública, respetando los derechos de autor.
3. Autorizamos, finalmente, a la Universidad Iberoamericana del Ecuador a difundir a través del sitio web de la Biblioteca de la UNIB.E (Repositorio Digital Institucional), el referido Trabajo de Integración Curricular, respetando las políticas de propiedad intelectual de la Universidad Iberoamericana del Ecuador.

Quito, DM., a los 23 días del mes de febrero de 202



Willian Conya

1728227487



Karen Tipan

1722686712

AUTORIZACIÓN DE PRESENTACIÓN FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR POR PARTE DEL TUTOR

PhD. Alicia Elizundia

Decana de la Facultad de Comunicación y Tics

Presente. -

Yo, **MSc JUAN FRANCISCO PABÓN**, Tutor del Trabajo de Integración Curricular realizado por los estudiantes **WILLIAN MANOLO CONYA GAVILANEZ** y **KAREN VANESSA TIPAN TIBANTA** de la carrera de **INGENIERÍA EN SOFTWARE** informo haber revisado el presente documento titulado **MÓDULO WEB PARA LA GESTIÓN INTERNA DE ACCESO A LOS APLICATIVOS DE UNA UNIVERSIDAD PÚBLICA DEL ECUADOR UBICADA EN EL CANTÓN RUMIÑAHUI, MEDIANTE LAS HERRAMIENTAS DE DESARROLLO ANGULAR Y SPRING BOOT**, el mismo que se encuentra elaborado conforme a lo establecido en el Reglamento de Titulación y el Manual de Estilo de la Universidad Iberoamericana del Ecuador, UNIB.E de Quito, por lo tanto, autorizo la entrega del Trabajo de Integración Curricular a la Unidad de Titulación para la presentación final ante el tribunal evaluador.

JUAN
FRANCI
SCO
PABON
ALAJO
Atentamente,

Firmado digitalmente
por JUAN FRANCISCO
PABON ALAJO
DN: cn=JUAN
FRANCISCO PABON
ALAJO c=EC
o=SECURITY DATA
S.A. 2 ou=ENTIDAD DE
CERTIFICACION DE
INFORMACION
Motivo: Soy el autor de
este documento
Ubicación:
Fecha: 2024-02-23
17:23:25-05

Juan Pabón

Tutor

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Comunicación y Tecnologías

Carrera: Ingeniería de Software

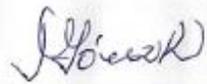
Modalidad: Semipresencial

Nivel: 3er nivel de Grado

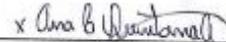
En el Distrito Metropolitano de Quito a los diecinueve días del mes de marzo del 2024 (19-03-2024) a las once horas con treinta minutos (11:30), ante el Tribunal de Presentación Oral, se presentó el señor: **CONYA GAVILANEZ WILLIAN MANOLO**, titular de la cédula de ciudadanía No. **1728227487** a rendir la evaluación oral del Trabajo de Integración Curricular: "**Módulo web para la gestión interna de acceso de usuarios a los aplicativos de una universidad pública del Ecuador ubicada en el cantón Rumiñahui, mediante las herramientas de desarrollo angular y spring boot.**", previo a la obtención del Título de Ingeniero de Software. Luego de la exposición, el referido estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	9.5 /10
Evaluación Oral del Trabajo de Integración Curricular	10 /10
Calificación Final del Trabajo de Integración Curricular	9.8 /10

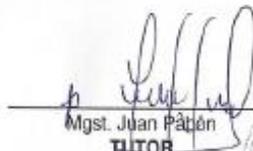
Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los diecinueve días del mes de marzo del 2024 (19-03-2024).



Ph.D. Jesús Gómez
VICERRECTOR



Ph.D. Luisa Taboada
DIRECTOR ACADEMICO



Mgst. Juan Patiño
TUTOR



Mgst. Byron Moreno
LECTOR

ACTA DE APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Facultad: Comunicación y Tecnologías

Carrera: Ingeniería de Software

Modalidad: Semipresencial

Nivel: 3er nivel de Grado

En el Distrito Metropolitano de Quito a los diecinueve días del mes de marzo del 2024 (19-03-2024) a las once horas con treinta minutos (11:30), ante el Tribunal de Presentación Oral, se presentó la señorita: **TIPAN TIBANTA KAREN VANESSA**, titular de la cédula de ciudadanía No. **1722686712** a rendir la evaluación oral del Trabajo de Integración Curricular: "**Módulo web para la gestión interna de acceso de usuarios a los aplicativos de una universidad pública del Ecuador ubicada en el cantón Rumiñahui, mediante las herramientas de desarrollo angular y spring boot.**", previo a la obtención del Título de Ingeniero de Software. Luego de la exposición, la referida estudiante obtiene las calificaciones que a continuación se detallan:

	Calificación
Lectura del Trabajo de Integración Curricular	9.5 /10
Evaluación Oral del Trabajo de Integración Curricular	10 /10
Calificación Final del Trabajo de Integración Curricular	9.8 /10

Para constancia de lo actuado, los miembros del Tribunal de Presentación Oral del Trabajo de Integración Curricular, firman el presente documento en unidad de acto, a los diecinueve días del mes de marzo del 2024 (19-03-2024).

PhD. Jesús Gómez
VICERRECTOR



PhD. Luisa Taborda
DIRECTOR ACADÉMICO

Mgst. Juan Pabón
TUTOR



Mgst. Byron Moreno
LECTOR

ÍNDICE DE CONTENIDO

DECLARACIÓN DE AUTORÍA Y AUTORIZACIÓN PARA LA DIFUSIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR	II
AUTORIZACIÓN DE PRESENTACIÓN FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR POR PARTE DEL TUTOR	III
RESUMEN	XI
ABSTRACT	XII
CAPÍTULO I	3
EL PROBLEMA	3
Planteamiento del problema	4
Objetivos de la Investigación	6
Objetivo General:	6
Objetivos Específicos:	6
Justificación e Impacto de la Investigación	6
Alcance del Proyecto	8
CAPITULO II	9
MARCO TEÓRICO	9
Antecedentes de la investigación	9
Bases Teóricas	12
Control de acceso	12
Seguridad informática	13
Desarrollo web	13
Gestión de usuarios	14
Servidor web	14
Servidor de aplicaciones	16
Arquitectura cliente – servidor	16
API	18
Backend	19
Frontend	20
Metodología	22
Fundamentación legal	24
CAPÍTULO III	1

MARCO METODOLÓGICO	1
Naturaleza de la investigación	1
Población y muestra	2
Población	2
Técnicas e instrumentos de recolección de datos	3
Técnica de recolección de datos	3
Técnicas de análisis de los datos	3
Operacionalización de la variable	4
Instrumento y recolección de datos:	6
CAPÍTULO IV	7
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS	7
Tabulación y análisis de resultados	7
Desarrollo del producto	13
Planeación	13
Diseño	23
Codificación	30
Pruebas	40
CAPÍTULO V	50
CONCLUSIONES Y RECOMENDACIONES	50
Conclusiones	50
Recomendaciones	52
REFERENCIAS BIBLIOGRÁFICAS	54
ANEXOS	59

ÍNDICE DE FIGURAS

Figura 1 Proceso actual de asignación de permisos	5
Figura 2 Arquitectura cliente – servidor. Tomado del autor Andrés Schiaffarino (2019)	18
Figura 3 Funcionamiento de una API. Tomado de Finerio Connect (2024).....	19
Figura 4 Fases de la metodología XP	24
Figura 5 Resultados obtenidos de la primera pregunta aplicada en la encuesta establecida. Autoría propia.....	7
Figura 6 Resultados obtenidos de la segunda pregunta aplicada en la encuesta. Autoría propia.....	8
Figura 7 Resultados obtenidos de la tercera pregunta aplicada en la encuesta establecida.	9
Figura 8 Resultados obtenidos de la cuarta pregunta aplicada en la encuesta establecida.	10
Figura 9 Resultados obtenidos de la quinta pregunta aplicada en la encuesta establecida.	10
Figura 10 Resultados obtenidos de la sexta pregunta aplicada en la encuesta establecida.	11
Figura 11 Resultados obtenidos de la séptima pregunta aplicada en la encuesta establecida.	12
Figura 12 Esquema del modelo de clases sobre del módulo Gestión de Usuarios.	30
Figura 13 Esquema del modelo lógico sobre del módulo Gestión de Usuarios.....	31
Figura 14 Configuración de seguridad web	38
Figura 15 Verificación de acceso a un recurso.....	39
Figura 16 Validación de acceso a un recurso.....	39
Figura 17 Resultados de las pruebas aplicadas al software del Módulo web.....	65
Figura 18 Resultados de la aplicación de correcciones.....	66

INDICE DE TABLAS

Tabla 1 Operacionalización de la variable	5
Tabla 2 Plantilla para la elaboración de una historia de usuario.....	13
Tabla 3 Historia de usuario: Iniciar sesión en el sistema	15
Tabla 4 Historia de usuario: Cambio de contraseña	15
Tabla 5 Historia de usuario: Iniciar sesión en el sistema	16
Tabla 6 Historia de usuario: Gestión de perfiles	16
Tabla 7 Historia de usuario: Gestión de opciones	17
Tabla 8 Historia de usuario: Gestión de opciones al perfil.....	18
Tabla 9 Historia de usuario: Asignación de perfil a un usuario	19
Tabla 10 Historia de usuario: Gestión de control de usuarios.....	20
Tabla 11 Iteración 1 - Establecimiento de la base	21
Tabla 12 Iteración 2 - Gestión de usuarios y permisos.....	21
Tabla 13 Iteración 3 - Integración con aplicativos Universitarios	22
Tabla 14 Iteración 4 - Mejoras y optimizaciones.....	22
Tabla 15 Plantilla para la elaboración de las Tarjeta CRC.....	24
Tabla 16 Tarjeta CRC: Iniciar sesión en el sistema	25
Tabla 17 Tarjeta CRC: Cambio de contraseña	25
Tabla 18 Tarjeta CRC: Gestión de Sistemas	26
Tabla 19 Tarjeta CRC: Gestión de perfiles	26
Tabla 20 Tarjeta CRC: Gestión de opciones	27
Tabla 21 Tarjeta CRC: Gestión de asignación de opciones al perfil.....	27
Tabla 22 Tarjeta CRC: Asignación de perfil a un usuario	28

Tabla 23 Tarjeta CRC: Gestión de control de usuarios.....	29
Tabla 24 Diccionario de datos: tabla OPCIÓN.....	32
Tabla 25 Diccionario de datos: tabla OPCPERFIL	33
Tabla 26 Diccionario de datos: tabla PERFIL	34
Tabla 27 Diccionario de datos: tabla SISTEMA	35
Tabla 28 Diccionario de datos: tabla USUARIO	36
Tabla 29 Diccionario de datos: tabla USUPERFIL.....	37
Tabla 30 Ejemplo de evaluación de prueba de aceptación.....	40
Tabla 31 Prueba de aceptación relacionada a la historia de usuario 1.....	42
Tabla 32 Prueba de aceptación relacionada a la historia de usuario 2.....	43
Tabla 33 Prueba de aceptación relacionada a la historia de usuario 3.....	44
Tabla 34 Prueba de aceptación relacionada a la historia de usuario 4.....	45
Tabla 35 Prueba de aceptación relacionada a la historia de usuario 5.....	46
Tabla 36 Prueba de aceptación relacionada a la historia de usuario 6.....	47
Tabla 37 Prueba de aceptación relacionada a la historia de usuario 7.....	48
Tabla 38 Prueba de aceptación relacionada a la historia de usuario 8.....	49

Willian Conya y Karen Tipan. **MÓDULO WEB PARA LA GESTIÓN INTERNA DE ACCESO A LOS APLICATIVOS DE UNA UNIVERSIDAD PÚBLICA DEL ECUADOR UBICADA EN EL CANTÓN RUMIÑAHUI, MEDIANTE LAS HERRAMIENTAS DE DESARROLLO ANGULAR Y SPRING BOOT.** Carrera Ingeniería de Software. Universidad Iberoamericana del Ecuador. Quito Ecuador. 2024. (105) pp.

RESUMEN

El propósito fundamental de esta investigación es el desarrollo de un módulo web centralizado destinado a la gestión de permisos de acceso a los aplicativos internos de una entidad universitaria para docentes, personal administrativo y estudiantes. En consonancia con la creciente presencia de la tecnología en todos los ámbitos, resulta imperativo que los procesos dentro de una institución educativa estén automatizados. En este contexto, la implementación de un módulo centralizado adquiere especial relevancia. El presente proyecto surgió como una respuesta innovadora para simplificar la asignación de permisos, salvaguardar la confidencialidad de los datos y optimizar los flujos de trabajo en el ámbito académico. Es esencial destacar que, en un entorno donde la tecnología y el internet son protagonistas, la mejora en la gestión de accesos se convierte en un componente fundamental para impulsar la eficiencia en la manipulación de información crítica en una universidad.

La propuesta, buscó no solo atender las necesidades actuales de asignación de permisos, sino también sentar las bases para un entorno académico más ágil y adaptativo. La importancia de este módulo centralizado radicó en su capacidad para actuar como una herramienta integral, facilitando la gestión de accesos de manera eficaz y promoviendo la adopción de prácticas modernas en la administración de información en el ámbito universitario. Se basa en el enfoque cuantitativo, paradigma positivista, la técnica empleada fue la entrevista y metodología de desarrollo XP.

Palabras Clave: Módulo web, accesos, Gestión, herramientas Angular y Spring Boot, Confidencialidad.

Willian Conya and Karen Tipan. **WEB MODULE FOR THE INTERNAL MANAGEMENT OF ACCESS TO APPLICATIONS OF A PUBLIC UNIVERSITY IN ECUADOR LOCATED IN THE CANTON RUMIÑAHUI, THROUGH THE DEVELOPMENT TOOLS ANGULAR AND SPRING BOOT.** Software Engineering Major. Ibero-American University of Ecuador. Quito Ecuador. 2024 (105) pp.

ABSTRACT

The fundamental purpose of this research is the development of a centralized web module aimed at managing permissions for teachers, administrative staff and students to the internal applications of a university entity. In line with the growing presence of technology in all areas, it is imperative that processes within an educational institution are automated. In this context, the implementation of a centralized module becomes especially relevant. It emerged as an innovative response to simplify permission assignment, safeguard data confidentiality, and optimize workflows in academia. It is essential to highlight that, in an environment where technology and the Internet are protagonists, improving access management becomes a fundamental component to boost efficiency in the manipulation of critical information in a university.

The proposal sought not only to address the current needs for assigning permits, but also to lay the foundations for a more agile and adaptive academic environment. The importance of this centralized module lay in its ability to act as a comprehensive tool, facilitating access management effectively and promoting the adoption of modern practices in information management in the university environment. It is based on the quantitative approach, positivist paradigm, the technique used was the interview and XP development methodology.

Keywords: Web Module, Access, management, Angular and Spring Boot tools, Confidentiality.

INTRODUCCIÓN

La presente investigación se enfoca en el desarrollo de un módulo web especializado que permita gestionar de manera eficiente y segura los permisos de acceso a los aplicativos internos de una universidad. La metodología de investigación empleada se fundamentó en el paradigma positivista y enfoque cuantitativo. Con respecto a la técnica utilizada para la recolección de datos se utilizó una encuesta conformada por siete preguntas cerradas, aplicada a seis personas pertenecientes a la Unidad de Tecnologías de la Información y Comunicación de la Universidad, cuya función es dar soporte al usuario final.

En cuanto al desarrollo y planificación del módulo se empleó la metodología ágil Extreme Programming; con respecto al desarrollo del front-end y back-end se utilizaron tecnologías avanzadas como Angular que facilita la creación de páginas dinámicas y SpringBoot por su facilidad de levantar API rest y microservicios. Como gestor de base de datos se utilizó Oracle Database y para la codificación del módulo web se emplearon los lenguajes Java y Typescript, para el front-end y back-end respectivamente. Por otra parte, para la verificación de funcionalidades se realizaron pruebas unitarias.

Esta investigación resultó en el desarrollo y despliegue de un producto de software. Con esto se facilita la labor del personal de soporte de la Unidad de Tecnologías de la Información y Comunicación UTIC's de la Universidad agilizando los procesos y asegurando que cada usuario tenga acceso eficiente a los aplicativos internos según sus roles y responsabilidades.

En el primer capítulo, se presenta el planteamiento del problema, el cual sumerge al lector en la comprensión de la forma actual en que el personal encargado de soporte de la Unidad de Tecnologías de la Información y Comunicación UTIC's de una Universidad del Ecuador realiza los procesos de asignación de permisos, además se detallan los objetivos, justificación y alcance de la presente investigación.

En el segundo capítulo se abordan los antecedentes de la investigación, donde se revisan documentos pertinentes al problema planteado en este estudio. Además, se

exponen las bases teóricas, las cuales ofrecen un entendimiento de las metodologías, tecnologías y lenguajes de programación empleados en el proyecto. Por último, se presentan los fundamentos legales, donde se especifican las leyes y regulaciones que serán consideradas en el desarrollo del sistema web.

En el tercer capítulo se detalla la metodología utilizada, incluyendo el tipo, nivel y diseño de la investigación. Se describe la población y muestra utilizada, así como la técnica de recolección de datos y el instrumento empleado.

El cuarto capítulo se verifica la validez, confiabilidad y utilidad de los datos obtenidos mediante la técnica empleada para el desarrollo del presente trabajo de investigación, además se presenta la propuesta del software, abordando la planificación del proyecto, su análisis y diseño. Se detallan las tecnologías empleadas en el proceso de desarrollo, concluyendo con las pruebas del sistema web.

Por último, en el quinto capítulo se redactan las conclusiones y recomendaciones que surgieron a lo largo de la investigación y durante el desarrollo del producto de software. Estas conclusiones y recomendaciones servirán como referencia para futuros proyectos que aborden temáticas similares.

CAPÍTULO I

EL PROBLEMA

El internet se ha convertido en una herramienta vital en la vida del ser humano facilitando enormemente el acceso a la información en cualquier lugar y hora. Además, ha desempeñado un papel fundamental en la evolución, simplificando la creación de aplicaciones web, impulsando significativos avances que han transformado la forma en que las personas y las empresas gestionan procesos.

“En esta era digital en la que vivimos, las aplicaciones web se han convertido en una parte esencial de nuestra vida diaria. Ya sea que estemos comprando productos en línea, leyendo noticias, comunicándonos con amigos o simplemente buscando información, las aplicaciones web están en todas partes y desempeñan un papel fundamental en nuestra experiencia en línea (Ridge, 2023).” En efecto, la omnipresencia de las aplicaciones web ha transformado radicalmente la forma en que interactuamos con el mundo digital.

Cabe recalcar que antes de la llegada del internet, las aplicaciones monolíticas desempeñaron un importante papel en la automatización de procesos en entidades y organizaciones durante un periodo considerable hasta el apareamiento de microservicios. “Mientras que una app de microservicios está constituida por diversos módulos y componentes que se comunican entre sí (pero sin por ello perder su grado de independencia), las aplicaciones monolíticas destacan por agrupar todas las funciones en un solo gran código (Correa, 2021).” Por otra parte, el depender del hardware local conllevó a bajas en rendimiento y escalabilidad ya que la capacidad de almacenamiento estaba limitada por la potencia del computador en donde estaba instalada la aplicación. Así, mientras que las aplicaciones monolíticas cumplieron un papel crucial en el pasado, las tecnologías modernas han superado estas limitaciones y han brindado soluciones más flexibles y adaptativas para las demandas actuales de conectividad y rendimiento.

Su impacto no solo se limita a la eficiencia en tareas específicas, sino que también moldea la manera en que experimentamos y participamos en la era digital, evidenciando su papel central en la evolución constante de nuestra interacción con la tecnología.

Planteamiento del problema

La gestión adecuada del acceso de los usuarios a los sistemas informáticos se ha vuelto fundamental para garantizar la seguridad y protección de los recursos digitales de una organización. La gestión de acceso se refiere al proceso mediante el cual, se controla y administra la autorización y autenticación de los usuarios para acceder a los sistemas, aplicaciones y datos de una entidad.

Según Samaniego y Ponce (2021), la seguridad es una condición que permite tener libertad ante el peligro, su principal objetivo es la protección contra los adversarios, por ejemplo, en la seguridad de un estado se debe proteger su soberanía, sus activos y su gente para que estos no sean atacados. En una organización, alcanzar un nivel de seguridad adecuado requiere de la implementación de un sistema de varias capas estratégicamente relacionadas con elementos en común, por lo tanto, es deber de la organización asegurarse de contar con estrategias debidamente planificadas y organizadas.

Actualmente, cuando un usuario ingresa como parte de la Universidad en el ámbito académico, es decir, como docente, estudiante o directivo, éste debe dirigirse a la Unidad de Tecnologías de la Información y Comunicación para que el personal encargado de soporte les asigne acceso a las aplicaciones correspondientes de acuerdo a su rol. Seguidamente, quien recibe la solicitud debe acercarse donde el desarrollador de software para que éste, mediante código conceda el acceso solicitado y dar una respuesta favorable al usuario. En muchas ocasiones el desarrollador no atiende esos requerimientos de forma inmediata por varias causas internas, para lo cual el tiempo empleado para esta acción ha sido de máximo de 2 días, volviendo esta gestión muy deficiente, siendo por ello necesaria una optimización en tiempos de respuesta. Para mejor entendimiento, ver figura 1.

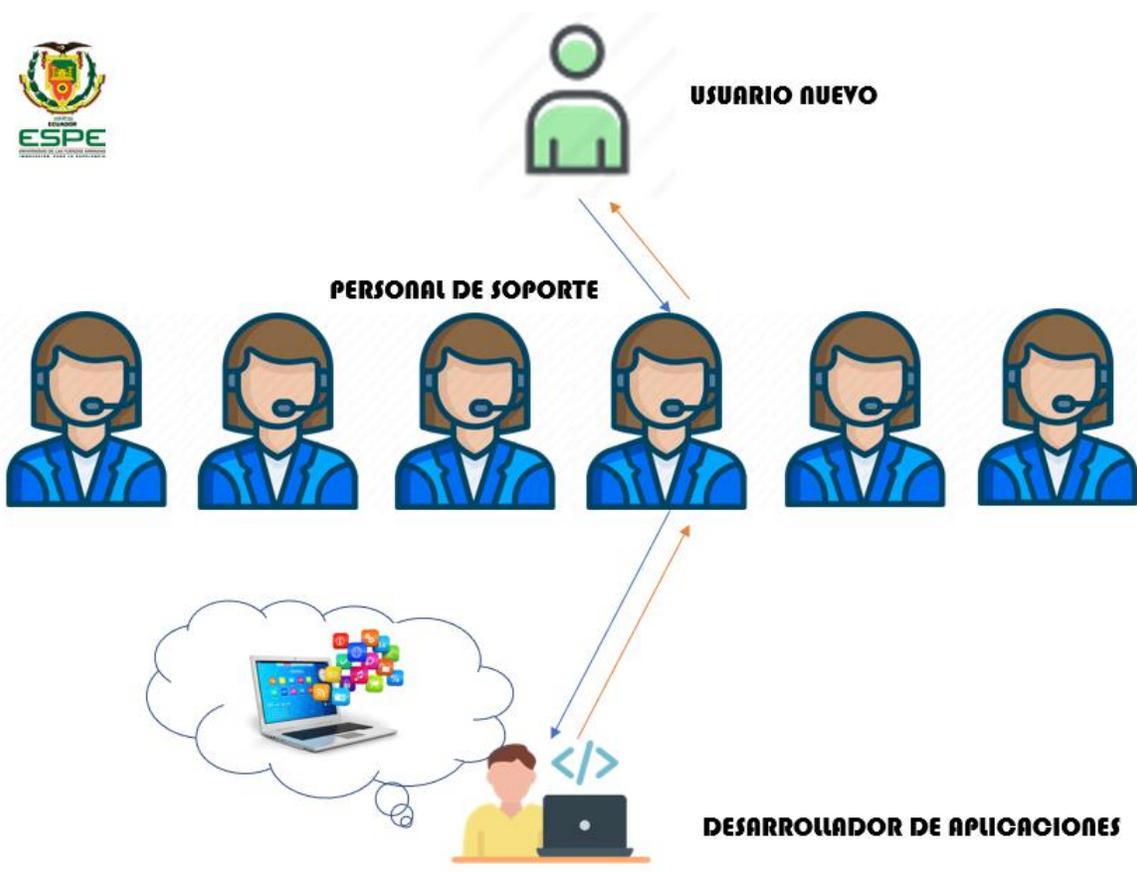


Figura 1 *Proceso actual de asignación de permisos*

La figura1 expone el problema al ser un único usuario quien está solicitando este acceso. ¿Pero qué ocurre cada semestre cuando ingresan masivamente nuevos estudiantes, se hacen contrataciones de nuevo personal docente y directivos? Es aquí donde radica el gran problema ya que la Universidad admite en cada periodo a cuatro mil nuevos estudiantes, y entre doscientos docentes por contrato. Esta avalancha de nuevos usuarios sobrecarga aún más los procesos de asignación de accesos, aumentando la presión sobre el personal de soporte y el desarrollador de software.

Por lo expuesto anteriormente se necesita crear un módulo web que facilite la gestión de permisos a los usuarios para el acceso a las diferentes aplicaciones internas logrando así una optimización en tiempos de respuesta.

Es así que se genera la siguiente interrogante de investigación: ¿Cómo diseñar y desarrollar un módulo web eficiente que automatice la gestión de acceso a los aplicativos

internos de una Universidad pública del Ecuador, asegurando una asignación de permisos ágil y eficaz?

Objetivos de la Investigación

Objetivo General:

Desarrollar un módulo eficiente de gestión de accesos para los sistemas informáticos internos de una Universidad pública del Ecuador, mediante el uso de tecnologías avanzadas de desarrollo como Angular y Spring Boot.

Objetivos Específicos:

1. Analizar los procesos actuales que se llevan a cabo en la Unidad de Tecnologías de la Información y Comunicación para la gestión de acceso a los aplicativos internos.
2. Diseñar un módulo web en colaboración estrecha con los usuarios finales, entregando funcionalidades de manera temprana y continua.
3. Desarrollar una interfaz de usuario intuitiva y amigable que facilite la asignación y revocación de permisos de acceso a las diferentes aplicaciones para los usuarios autorizados.

Justificación e Impacto de la Investigación

El presente trabajo de grado surge de la necesidad de desarrollar un módulo web empleando Tecnologías de Información y Comunicación (TIC's) para la gestión de asignación y revocación de permisos de acceso de usuario a los aplicativos internos de la Universidad de una forma más ágil y efectiva, logrando una mejor interacción entre los usuarios y el sistema.

En la actualidad, las Entidades Educativas han experimentado un crecimiento exponencial en la adopción de tecnologías digitales para mejorar sus procesos académicos y administrativos. Sin embargo, esta rápida expansión ha generado un

desafío significativo relacionado con la gestión de acceso a los diferentes aplicativos internos. La falta de un sistema centralizado y seguro puede llevar a problemas como ineficiencias en la administración de usuarios y accesos, y dificultades para el seguimiento y análisis del uso de las plataformas digitales. Por tanto, al no existir un módulo centralizado de gestión de usuarios en la Universidad, este proyecto se propone solventar este problema mediante un módulo web que aborde estas problemáticas y proporcione una solución eficiente y confiable para gestionar el acceso a los aplicativos internos, evitando que los procesos se vuelvan monótonos y afecten la productividad y efectividad de los mismos.

La relevancia científica y social de este proyecto radica en su potencial para contribuir al avance de la gestión tecnológica en el área de UTIC's de la Universidad. Al implementar un módulo web que centralice y simplifique el acceso a los diferentes aplicativos, se espera mejorar la experiencia de usuarios y volver eficientes los procesos actuales.

La importancia de este estudio radica en su enfoque práctico y aplicado. La investigación busca desarrollar una solución tangible y funcional, basada en las necesidades reales de la Universidad. El módulo web resultante no solo resolverá los problemas de gestión de acceso, sino que también permitirá a la institución ahorrar tiempo y recursos, aumentando su eficiencia operativa y mejorando la calidad del servicio que brinda a sus usuarios.

Los aportes teóricos y prácticos de esta investigación son significativos. Desde un punto de vista teórico, se exploran conceptos de gestión de acceso, seguridad informática y desarrollo web, generando conocimiento en el área de tecnologías aplicadas a la educación. Desde una perspectiva práctica, el módulo web desarrollado sirve como modelo y referente para otras instituciones educativas que enfrenten desafíos similares en la gestión de sus plataformas digitales, fomentando la adopción de mejores prácticas en el sector.

Los principales beneficiarios con los resultados de esta investigación serán la propia Universidad y su comunidad educativa en conjunto. En la Unidad de Tecnologías de la Información y Comunicación UTIC's, el personal encargado de dar soporte a los usuarios se beneficiarán al contar con una herramienta práctica para gestionar los accesos, lo que repercutirá en una mayor eficiencia en procesos y una reducción de tiempo.

Alcance del Proyecto

El alcance del proyecto implica el desarrollo de un Módulo web para la gestión interna de acceso de usuarios a los aplicativos existentes de una Universidad pública del Ecuador ubicada en el cantón Rumiñahui mediante las herramientas de desarrollo Angular y Spring Boot.

El área geográfica donde se suscribe el proyecto es en el área de la Unidad de Tecnologías de la Información y Comunicaciones de una Universidad pública del Ecuador ubicada en el cantón Rumiñahui.

La investigación propuesta se desarrollará en un período de 12 meses a partir de la aprobación del proyecto.

El módulo estará dirigido a toda la comunidad estudiantil, docente y administrativa de la Entidad Educativa en cuestión.

El módulo web se desarrollará exclusivamente para su uso en entornos web, sin incluir compatibilidad o funcionalidades específicas para entornos móviles o aplicaciones nativas. De igual manera tiene previsto mantener sin modificación los aplicativos internos.

El alcance del proyecto se limita a la creación del módulo de gestión de acceso, sin contemplar nuevos aplicativos ni modificaciones sustanciales a los sistemas ya establecidos.

La infraestructura se mantendrá sin modificaciones: se utilizarán los mismos servidores y red existentes. Se trabajará dentro de la infraestructura tecnológica vigente en la Institución universitaria.

En cuanto a las Políticas de Seguridad, se mantendrán las ya establecidas por la universidad, en tal sentido, se ajustará el módulo web a las políticas de seguridad existentes.

La capacitación prevista para el uso del módulo web, se limitará al personal encargado de la administración y uso del mismo. Se excluye a los usuarios finales.

Estas limitaciones tienen como objetivo definir el alcance específico del proyecto y garantizar que los objetivos establecidos se alcancen sin exceder los recursos y el tiempo asignados para su implementación.

CAPITULO II

MARCO TEÓRICO

El Marco teórico, según Salomao (2023), es definido como:

Un conjunto de conceptos, definiciones y proposiciones interrelacionados que explican o predicen fenómenos o relaciones entre ellos. Es una estructura o marco de ideas que se utiliza para guiar el proceso de investigación y ayuda a organizar y definir los conceptos clave que se estudian. Puede considerarse una hoja de ruta para la investigación, ya que proporciona una forma de guiar el proceso de investigación y ayuda a los investigadores a interpretar sus hallazgos.

Se puede deducir que es fundamental para establecer los fundamentos teóricos y conceptuales de un estudio, proporcionando la base necesaria para el desarrollo e interpretación de la investigación.

En este capítulo se presentan los antecedentes de la investigación y se exploran las bases teóricas y conceptuales relacionadas con el control de acceso, autenticación y autorización. Además, se analizan las bases legales y normativas que regulan la seguridad de la información. La comprensión

adquirida en este capítulo orienta el desarrollo del módulo y las estrategias de protección de recursos digitales, garantizando la seguridad informática en el ámbito educativo y en otras instituciones.

Antecedentes de la investigación

Para sustentar el presente trabajo, es necesario investigar trabajos de otros autores relacionados con el tema en cuestión. Es por ello que revisando los repositorios virtuales de las universidades del país se puede constatar que existen temas similares al que se está planteando, los cuales se detallan a continuación:

En primer lugar se presenta la tesis de Camacho (2015), con su **tema**: “Desarrollo e implementación de una plataforma web para el sistema de gestión de la información de proyectos de fiscalización realizados por la empresa TECNIE, accesible local y remotamente.”, elaborado en la Escuela Politécnica Nacional cuyo **objetivo general** se dirigió a “Desarrollar una plataforma web para el sistema de gestión de la información de

proyectos de fiscalización realizados por la empresa TECNIE, accesible local y remotamente.”

Esta tesis se centra en el tema de gestión, cuyo resultado permite acceder y trabajar remotamente desde cualquier lugar siempre y cuando exista una conexión a internet, en las ocasiones que sea necesario y autorizado por la empresa, lo cual implica una buena gestión en procesos informáticos ya que requiere una planificación sólida, comunicación efectiva, uso adecuado de recursos, capacitación, seguimiento y mejora continua, lo que en conjunto permitirá la ejecución exitosa de proyectos informáticos de manera eficiente, llevando a cabo el desarrollo de la plataforma web que solvente esta necesidad. Con ello se puede concluir que este trabajo destaca la importancia de adoptar soluciones tecnológicas avanzadas para optimizar los procesos empresariales y garantizar la ejecución exitosa de proyectos de manera eficiente.

A continuación, el trabajo de tesis de Mendoza (2017) denominado “Implementación de sistema web para la gestión y control de los procesos de la unidad de titulación de la carrera de Ingeniería en Sistemas de la Universidad Salesiana, sede Guayaquil”, elaborada en la Universidad Politécnica Salesiana cuyo **objetivo general** buscaba “Diseñar e implementar un sistema de control escolar en un ambiente web, utilizando software libre que a la vez sirva como base para las tres instituciones que conforman la Casa Salesiana “Cristóbal Colon”.”

Esta tesis trata sobre cómo llevar a cabo un control en procesos, es decir automatizar el sistema Académico para las Unidades Educativas que conforman la casa Salesiana con la finalidad de agilizar el proceso académico. Este enfoque demuestra una comprensión integral de la necesidad de optimizar los procesos educativos mediante soluciones tecnológicas innovadoras, lo que sin duda contribuirá significativamente a la eficiencia y efectividad de la gestión académica en la institución

Otro trabajo de Bazán (2022) titulado “Desarrollo de aplicación web para gestión de turnos en la escuela básica particular Monseñor Roberto María del Pozo”, elaborada en la Universidad Politécnica Salesiana sede Guayaquil cuyo **objetivo general** se dirigió a

“Desarrollar un aplicativo web para administración de turnos para la institución EEBP MONSEÑOR ROBERTO MARIA DEL POZO”.

Este trabajo está enfocado en el desarrollo de un software web para automatizar el proceso de atención a padres de familia, estudiantes y público en general de una manera óptima y satisfactoria, ya que existían inconvenientes de coordinación tanto de fechas y hora ocasionando malestar entre los usuarios; además de almacenar información en archivos Excel volviendo este proceso aún más deficiente y tiene varios puntos de comparación con la problemática del problema en cuestión de este proyecto. Este enfoque destaca la importancia de utilizar la tecnología para abordar los desafíos en la gestión de turnos y mejorar la experiencia de los usuarios en la institución educativa.

Finalmente, se presenta el trabajo de tesis de Aterhortua y Giraldo (2021) denominado “Desarrollo de una aplicación Web para la gestión de solicitudes, requerimientos e incidentes en la empresa Estructura IST, aplicando las buenas prácticas de ITIL” pertenecientes a la Institución Universitaria del Tecnológico de Antioquia de la ciudad de Medellín, Colombia, el objetivo general buscaba “Desarrollar una aplicación Web para la gestión de solicitudes, requerimientos e incidentes internos en la empresa Estructura IST, aplicando las buenas prácticas de ITIL v4.” Este trabajo busca mejorar el proceso de gestión de solicitudes en la empresa, permitiendo un mayor control y sistematización de las peticiones. La implementación de esta aplicación proporcionará una solución integral para optimizar la gestión de solicitudes, contribuyendo así a la eficiencia operativa y al cumplimiento de los estándares de calidad en el servicio.

Los trabajos de tesis y proyectos de grado analizados demuestran la importancia y el impacto significativo que tienen las aplicaciones web en diversos ámbitos, desde la gestión educativa hasta la optimización de procesos empresariales. Estos proyectos resaltan algunos aspectos fundamentales que conllevan una adecuada gestión y control sobre los procesos para garantizar un funcionamiento eficiente, seguro y confiable. Entre estos aspectos se destaca la gestión de usuarios, cuyo fin es administrar de manera adecuada los permisos y accesos de los usuarios a un sistema, asegurando que solo se tenga acceso a la información y funciones que les corresponden. Esto proporciona una

experiencia satisfactoria a los usuarios y garantiza que el sistema cumpla con los objetivos y requerimientos establecidos.

En conjunto, estos proyectos subrayan la relevancia de las aplicaciones web como herramientas clave para mejorar la eficiencia, la gestión y la experiencia del usuario en una variedad de contextos, desde el ámbito empresarial hasta el educativo. La tecnología web continúa siendo un área de investigación y desarrollo vital para abordar los desafíos actuales y futuros en diferentes campos. La gestión adecuada de usuarios es solo uno de los muchos aspectos que destacan cómo las aplicaciones web pueden mejorar la eficiencia y la calidad de los procesos en diversas organizaciones, y cómo siguen siendo una prioridad en la innovación tecnológica y el avance de la sociedad.

Bases Teóricas

Control de acceso

Para comprender mejor este concepto Fernández (2020) menciona que, el método garantiza que los usuarios sean auténticos en su autoevaluación.

La situación es similar a no tener más remedio que mostrar su identificación en un lugar designado.

El control de acceso es crucial para garantizar que todos los usuarios tengan el acceso necesario a los datos y recursos del sistema. ¿Podrías explicar qué implica el control de acceso? Más importante aún: en un conjunto de restricciones basadas en los datos y/o materiales a los que necesita acceder.'... Se basa en procedimientos de autenticación y autorización.

Con base en las definiciones dadas por ambos autores, se puede concluir que el control de acceso se revela como un método fundamental para garantizar la autenticidad de los usuarios y regular su acceso a datos y recursos del sistema. Este proceso, basado en autenticación y autorización, se asemeja al acto de mostrar un documento de identidad para confirmar la identidad en un espacio físico. En el ámbito digital, las directivas de control de acceso desempeñan un papel crucial, determinando quién puede acceder a determinados datos, aplicaciones y recursos, y bajo qué condiciones. Al igual que las

medidas de seguridad física, estas directivas protegen los espacios digitales, asegurando la integridad y confidencialidad de la información.

Seguridad informática

“Se entiende por seguridad informática al conjunto de medidas implantadas para eludir cualquier tipo de amenaza cibernética (...)” (Ceupe, 2020).

Por otra parte, acerca de la seguridad informática, Grupo Atico (2024) refiere que:

La protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados. Una buena Ciberseguridad no solo se debe basar en la prevención de ataques, sino también detección y corrección de los mismos, reduciendo los riesgos de exposición de la información, brindando confianza a los usuarios. (pág. 1)

Por lo antes mencionado se puede decir que, la seguridad informática se define como las medidas para prevenir amenazas cibernéticas. Implica la protección de información personal, empresarial o gubernamental en dispositivos diarios y redes. Además de la prevención de ataques, la ciberseguridad también se enfoca en la detección y corrección, reduciendo los riesgos y generando confianza en los usuarios. En resumen, abarca la defensa contra amenazas digitales y la preservación de la integridad y confidencialidad de la información.

Desarrollo web

Por desarrollo web entendemos aquellas disciplinas, técnicas y herramientas tecnológicas que permiten la creación de sitios o aplicaciones web que funcionan en un ambiente web y que se acceden a ellas a través de un navegador. Las tendencias en desarrollo web, frameworks y lenguajes de programación son muy cambiantes y existen muchas alternativas para cada propósito, por tal razón, los desarrolladores web deben actualizarse constantemente en herramientas robustas y modernas para desarrollar productos aceptables y funcionales en la web. (Zelaya,2020, pag.1)

El desarrollo web es el proceso de creación y mantenimiento de sitios web, aplicaciones web u otros elementos relacionados con la presencia online. Implica programar, diseñar y crear la estructura, apariencia y funcionalidad de recursos web para satisfacer necesidades específicas.

Gestión de usuarios

Blanton (2023) menciona que la gestión de usuarios Describe la capacidad de los administradores para gestionar el acceso de los usuarios a diversos recursos de TI, como sistemas, dispositivos, aplicaciones, sistemas de almacenamiento, redes, servicios SaaS y más.

La gestión de usuarios es una parte central de cualquier solución, especialmente las herramientas de servicio de directorio. Controlar y gestionar el acceso de los usuarios a los recursos de TI es fundamental para la seguridad de cualquier organización. La gestión de usuarios permite a los administradores controlar el acceso, la incorporación y la baja de los usuarios en todos los recursos de TI. Luego, un directorio de servicios identifica, autoriza y verifica el acceso de los usuarios a los recursos de tecnología de la información según las instrucciones del administrador de TI.

En pocas palabras, la gestión de usuarios implica monitorear y controlar la autorización del usuario a diversos recursos de tecnología de la información, como sistemas, dispositivos y aplicaciones.

Servidor web

Según Betania (2023), en términos sencillos define que:

Un servidor web es un ordenador que almacena, procesa y entrega archivos de sitios web a los usuarios desde un navegador.

Los servidores web están formados por hardware y software que utilizan el Protocolo de Transferencia de Hipertexto (HTTP) para responder a las peticiones de los usuarios de la web realizadas a través de la World Wide Web.

A través de este proceso, los servidores web cargan y entregan la página solicitada al navegador del usuario, como Google Chrome, por ejemplo.

Los servidores web también utilizan el Protocolo Simple de Transferencia de Correo (SMTP) y el Protocolo de Transferencia de Archivos (FTP) para procesar archivos para el correo electrónico o el almacenamiento.

Por otro lado, según la editorial Etecé menciona que:

En informática, un servidor web o Servidor HTTP es una pieza de software de comunicaciones que intermedia entre el servidor en el que están alojados los datos solicitados y el computador del cliente, permitiendo conexiones bidireccionales o unidireccionales, síncronas o asíncronas, con cualquier aplicación del cliente, incluso con los navegadores que traducen un código traducible (renderizable) a una página web determinada. O sea, se trata de programas que median entre el usuario de Internet y el servidor en donde está la información que solicita.

Los servidores web son programas de uso cotidiano en Internet, que emplean para comunicarse diversos protocolos de datos, siendo el más común y de alguna manera estándar el HTTP (HyperText Transfer Protocol). Sin embargo, es posible también usar el término para referirse al computador en el que están guardados los archivos que componen un sitio web, junto al software necesario para cumplir con la conexión de datos web.

Con base a las definiciones proporcionadas, se puede concluir que un servidor web es una entidad que combina hardware y software, utilizando el Protocolo de Transferencia de Hipertexto (HTTP) para responder a las solicitudes de los usuarios a través de la World Wide Web. Este servidor almacena, procesa y entrega archivos de sitios web a los navegadores de los usuarios, facilitando la carga y presentación de las páginas solicitadas.

Adicionalmente, se destaca que un servidor web, según la perspectiva informática, actúa como una pieza de software que media entre el servidor de datos y el computador del cliente. Facilita conexiones bidireccionales o unidireccionales, síncronas o asíncronas, con diversas aplicaciones del cliente, incluyendo navegadores web. Los servidores web utilizan protocolos como HTTP, SMTP y FTP para procesar archivos y brindar servicios como correo electrónico y almacenamiento.

En resumen, los servidores web son elementos esenciales en la infraestructura de Internet, permitiendo la comunicación eficiente entre los usuarios y los servidores que

almacenan la información solicitada. Además, su papel va más allá de la simple entrega de archivos, abarcando diversas funciones y protocolos para satisfacer las necesidades de la red.

Servidor de aplicaciones

Para comprender qué son los servidores de aplicaciones, se menciona que “los servidores de aplicaciones gestionan la lógica empresarial para generar contenido dinámico mediante la conexión con sistemas, servicios y bases de datos empresariales (...)” (Amazon, 2023). Asimismo, se potencian las funcionalidades de los servidores web al permitir la generación de contenido dinámico, la ejecución de la lógica de las aplicaciones y la integración con una variedad de recursos. Ofrecen un entorno de ejecución donde es posible ejecutar el código de la aplicación y establecer interacciones con otros elementos de software, tales como sistemas de mensajería y bases de datos.

Aportando con la definición de este concepto, se menciona que:

Los servidores de aplicaciones son programas de servidor en una red distribuida que proporciona el entorno de ejecución para un programa de aplicación. Más específicamente, el servidor de aplicaciones es el componente de tiempo de ejecución principal en todas las configuraciones y donde una aplicación se ejecuta realmente. El servidor de aplicaciones colabora con el servidor web para ofrecer una respuesta dinámica y personalizada a una solicitud de cliente. (IBM Documentation, 2023)

Con esto se define que, los servidores de aplicaciones desempeñan un papel fundamental al gestionar la lógica empresarial, ampliar las capacidades de los servidores web y proporcionar el entorno de ejecución esencial para la ejecución de programas de aplicación. Su colaboración con los servidores web contribuye a la entrega de respuestas dinámicas y personalizadas en entornos distribuidos.

Arquitectura cliente – servidor

Para comprender sobre este concepto Blancarte (2021) expone que se debe tener en cuenta que en una arquitectura cliente-servidor, el proveedor es el servidor que ofrece

un conjunto de servicios o recursos requeridos por el cliente. Los clientes se conectan al servidor para acceder a los recursos necesarios para su funcionamiento. En este contexto, el cliente actúa como una capa para visualizar los datos, mientras que el servidor ejecuta las acciones para modificar el estado. De esta manera, es el servidor el responsable de realizar las tareas más demandantes en el proceso.

En otras palabras, se define que:

La arquitectura cliente-servidor es un modelo de diseño de software que divide las funcionalidades de una aplicación en dos partes principales: el cliente y el servidor. En este modelo, el cliente es la interfaz de usuario que permite a los usuarios interactuar con la aplicación, mientras que el servidor es el encargado de procesar las solicitudes del cliente y enviar las respuestas correspondientes.

En un sistema cliente-servidor típico, el cliente y el servidor se comunican a través de una red, como Internet. El cliente envía solicitudes al servidor, que las procesa y envía las respuestas de vuelta al cliente. Esta comunicación se basa en el protocolo de comunicación que se utilice, como HTTP para aplicaciones web. (Jiménez, 2023)

La arquitectura cliente-servidor, como se expone en las definiciones, presenta una clara división de responsabilidades entre el cliente y el servidor. Una adición valiosa a esta comprensión es reconocer que esta arquitectura facilita la distribución eficiente de tareas en una aplicación.

En este modelo, el servidor se encarga de realizar las operaciones complejas y procesar las solicitudes de los clientes. Por otro lado, el cliente actúa como la interfaz de usuario, permitiendo a los usuarios interactuar con la aplicación de manera intuitiva. Esta división facilita una distribución eficiente de tareas, ya que el servidor maneja el trabajo pesado, mientras que el cliente se centra en proporcionar una experiencia de usuario fluida.

Esta arquitectura, al facilitar la comunicación entre el cliente y el servidor a través de redes, como Internet, se ha convertido en un pilar para el diseño de sistemas distribuidos y aplicaciones escalables. La eficacia en la gestión de recursos y la respuesta a las solicitudes son aspectos fundamentales que contribuyen al éxito y rendimiento de sistemas basados en la arquitectura cliente-servidor.

Para una mejor ilustración, ver figura 1.

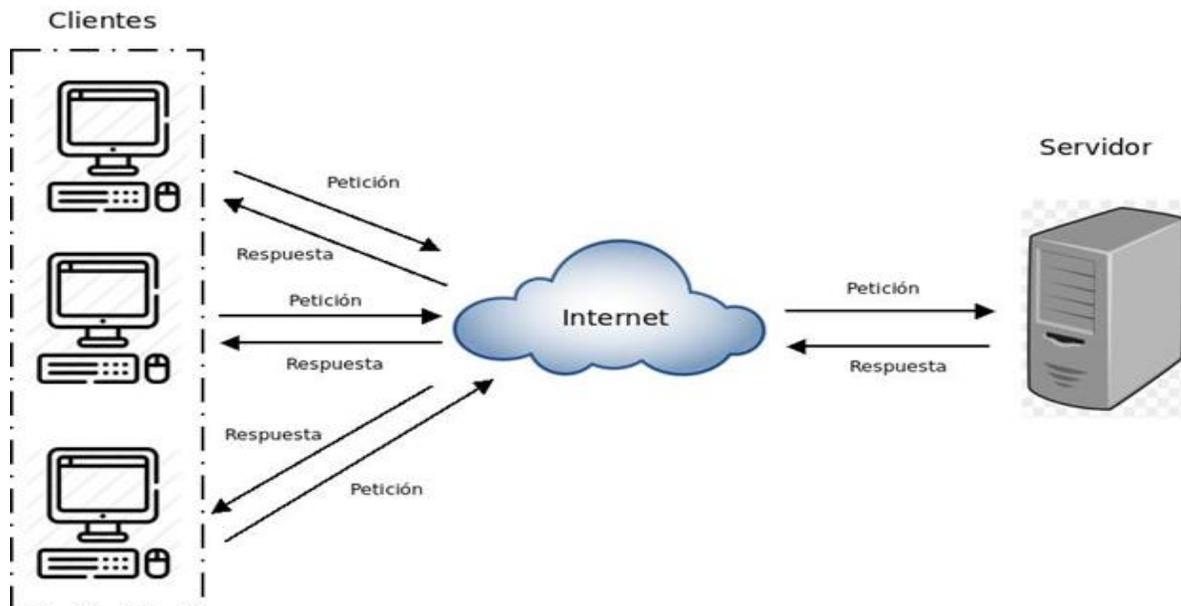


Figura 2 Arquitectura cliente – servidor. Tomado del autor Andrés Schiaffarino (2019)

API

Para una óptima comprensión sobre el término API, se menciona lo expresado por Cardozo (2021) quien expresa que la sigla "API", derivada de la expresión "Interfaz de Programación de Aplicaciones" o "Application Programming Interface" en inglés, hace referencia a una herramienta que actúa como puente entre diferentes sistemas, software y aplicaciones. Al utilizar una API, se brinda a los usuarios una experiencia más intuitiva y familiar, permitiéndoles interactuar con aplicaciones, software o incluso hojas de cálculo para acceder, modificar y guardar datos provenientes de diversos sistemas, sin necesidad de ingresarlos manualmente.

Por otra parte, Walker (2023) menciona que:

Interfaz de programación de aplicaciones (API) es una interfaz de software que permite que dos aplicaciones interactúen entre sí sin la intervención del usuario. API es una colección de funciones y procedimientos de software. En términos simples, API significa un código de software al que se puede acceder o ejecutar. API se define como un código que ayuda a dos softwares diferentes a comunicarse e intercambiar datos entre sí.

Para resumir el contexto de ambas definiciones, se expone que las API, o Interfaz de Programación de Aplicaciones, sirven como "traductores" que conectan sistemas, software y aplicaciones, ofreciendo una experiencia de usuario más accesible al permitir la interacción con datos de diferentes sistemas sin ingresar directamente a ellos. Su propósito fundamental es facilitar el intercambio eficiente de datos entre sistemas, automatizando procesos manuales y posibilitando la creación de nuevas funcionalidades. Funcionan como interfaces de software que permiten la interacción entre dos aplicaciones sin intervención del usuario, actuando en segundo plano para mejorar la conectividad digital y la eficiencia operativa.

Para una mejor ilustración del funcionamiento de una API, ver figura 2.



Figura 3 *Funcionamiento de una API. Tomado de Finerio Connect (2024)*

Backend

Según el sitio web Monster Digital Agency (2021) el backend se encarga de llevar a cabo tareas y operaciones que no están a la vista del usuario final, pero son esenciales para garantizar el correcto desempeño de la aplicación o página web.

En el contexto de un sitio web o aplicación, el usuario interactúa con una interfaz, conocida como frontend, que representa el "lado del usuario" y le facilita la navegación e interacción con el producto digital.

A continuación, se expone una definición sobre el término backend:

El backend es una parte trascendental dentro del desarrollo web y el desarrollo de aplicaciones, pues se encarga de todos los procesos necesarios para que la web se ejecute de forma correcta. El

backend ejecuta procesos y funciones que no son visibles para el usuario final, pero que tienen trascendental importancia en el buen funcionamiento de una app o web.

En una web o aplicación, el usuario interactúa con un interfaz (frontend), lo que entendemos como “el lado del usuario” y que hace que el usuario pueda navegar e interactuar con un producto digital. El backend, por su parte, es todo aquello que el usuario no ve, de hecho, se le denomina también “el lado del servidor” al estar alojado en la parte del servidor y únicamente ser accesible para los web masters o programadores de la web o aplicación. (Monster digital agency, 2021)

Se expone la definición de otro autor:

Backend, conocido como “el lado del servidor”, se refiere a la parte de una aplicación web o sitio web que no es visible para el usuario final, pero que es esencial para su funcionamiento.

En él se configuran todos los aspectos lógicos de una página web o aplicación; abarca la lógica, el almacenamiento de datos y las funciones de seguridad necesarias para que una aplicación funcione correctamente y sea fiable, de tal forma que todas las acciones solicitadas en la página web sean ejecutadas de manera correcta. (Arizbé, 2023)

Sobre la base de estas definiciones, se expone que el backend, esencial en el desarrollo web y de aplicaciones, se encarga de ejecutar procesos y funciones fundamentales para el correcto funcionamiento de una plataforma digital. Backend, también llamado “el lado del servidor”, opera en la sombra, alojándose en el servidor y siendo accesible solo para programadores. Esta parte invisible, según (2021), es vital para la ejecución adecuada de una aplicación web. Además, Arizbé (2023) destaca que el backend configura aspectos lógicos, almacenamiento de datos y funciones de seguridad, asegurando que todas las acciones solicitadas en la página web se ejecuten de manera correcta y fiable, contribuyendo así a la integridad y funcionalidad general del sistema.

Frontend

Arizbé (2023) expone que la parte visual y la interacción con el usuario son aspectos fundamentales del desarrollo web y de aplicaciones para garantizar una experiencia de usuario efectiva y atractiva. Una implementación cuidadosa del frontend resulta crucial para el éxito de un proyecto en línea. En los inicios de la creación de páginas web, estas eran bastante simples, pero con los avances tecnológicos actuales, se ha ampliado enormemente el potencial de diseño y funcionalidad en la web. Antes de la

popularización del término "frontend" en el ámbito del desarrollo web moderno, el enfoque principal se centraba en la estructura y el contenido básicos de los sitios web. Durante las etapas iniciales de la web, el trabajo se centraba principalmente en el lenguaje HTML, que se utilizaba para establecer la estructura básica de una página web mediante elementos como encabezados, párrafos, listas, enlaces y otros componentes de contenido.

Es la presentación visual y la interacción del usuario, lo que lo convierte en una parte crucial del desarrollo web y de aplicaciones para brindar experiencias de usuario efectivas y atractivas. Una implementación cuidadosa del frontend es fundamental para el éxito de un proyecto web. Cuando se comenzaron a crear páginas web, estas eran muy sencillas, sin embargo, en la actualidad el avance de la tecnología ha permitido que en una página web se pueda hacer cualquier cosa. Antes de que surgiera el término frontend en el contexto del desarrollo web moderno, la creación de sitios web estaba centrada en la estructura y el contenido básico. En las etapas iniciales de la web, se trabajaba principalmente con HTML, que se centraba en la estructura básica de una página web mediante elementos como encabezados, párrafos, listas, enlaces y otros componentes de contenido. (Arizbé, 2023)

Según el sitio web Kiwop (2023) menciona que:

El frontend, también conocido como el lado del cliente, es la parte de una página web que los usuarios ven y con la que interactúan directamente. Esto incluye el diseño visual, la estructura de la página, los estilos, el contenido y la interactividad. En pocas palabras, el frontend es lo que convierte una página web en una experiencia atractiva y funcional para los usuarios.

El front end developer implica traducir el diseño visual y las especificaciones de una página web en código HTML, CSS y JavaScript. Estos lenguajes de programación permiten crear la estructura de la página, aplicar estilos de diseño y añadir interactividad y funcionalidades a través de scripts.

Con estos conceptos se define que el frontend es una parte esencial en el desarrollo web, ya que representa la interfaz visual y la interacción directa con los usuarios. Su evolución, desde las páginas web simples hasta las actuales con amplias capacidades, destaca la importancia de una implementación cuidadosa para el éxito de un proyecto. Ser el "lado del cliente" implica que el frontend es responsable de la experiencia que los usuarios tienen al interactuar con una página web. La labor del frontend developer, al traducir el diseño en código y aplicar estilos e interactividad, es crucial para convertir una página web en una experiencia atractiva y funcional. El frontend no solo se trata de

estética, sino que es la puerta principal para ofrecer experiencias de usuario efectivas y satisfactorias en el mundo digital.

Metodología

Se evidencia la necesidad de investigar las metodologías disponibles y examinar las propuestas que delinear el proceso de desarrollo de sitios web más seguros y versátiles. En este sentido, se analizan las metodologías de desarrollo de software centradas en las aplicaciones web siendo esencial delimitar el contexto específico de estudio para un enfoque más preciso y efectivo.

La definición de metodología según MegaPractical (s-f) menciona lo siguiente:

Se puede definir la metodología de software como un enfoque, una manera de interpretar la realidad o la disciplina en cuestión, que en este caso particular correspondería a la Ingeniería de Software. De hecho, la metodología destinada al desarrollo de software se considera como una estructura utilizada para planificar y controlar el procedimiento de creación de un sistema de información especializada. (pág.2)

Por otra parte, según el sitio web Santander Universidades (2023) expone que:

las metodologías de desarrollo de software son un conjunto de técnicas y métodos organizativos que se aplican para diseñar soluciones de software informático. El objetivo de las distintas metodologías es el de intentar organizar los equipos de trabajo para que estos desarrollen las funciones de un programa de la mejor manera posible.

También menciona que a la hora de desarrollar productos o soluciones para un cliente o mercado específico se deben tener en cuenta factores como costo, planificación, dificultad, equipo de trabajo disponible, idiomas utilizados, etc.

Iniciar el desarrollo de productos sin una metodología clara dará como resultado un proceso aún más complejo, lo que provocará problemas, retrasos, errores y, en última instancia, un resultado final deficiente.

Entre las metodologías de desarrollo de software, podemos destacar dos grupos; las metodologías de desarrollo de software tradicionales y las metodologías de desarrollo ágiles. La presente investigación se enfocará en metodologías ágiles para el desarrollo del Módulo Web.

Metodologías de desarrollo ágiles

Para comprender que es una metodología de desarrollo ágil se debe tomar en cuenta que: “Se enfocan en la iteración y el trabajo en equipo para el desarrollo de software, así como en la entrega de software de alta calidad en un plazo de tiempo más corto, entre otros principios ágiles (...)” (Solera, 2022).

Cabe recalcar que las metodologías ágiles destacan por su capacidad para adaptarse a cambios, entregar valor continuamente, fomentar la colaboración activa y promover equipos autónomos, lo que la hace especialmente efectiva en entornos dinámicos y proyectos donde la incertidumbre y la evolución de los requisitos son comunes.

Según Raeburn (2022), expone que:

los marcos ágiles siguen un proceso iterativo, en el que se completa y revisa el marco al final de cada sprint, refinándolo para adaptarlo a los requisitos cambiantes y alcanzar la eficiencia máxima. Al igual que otros métodos ágiles, el diseño de la programación extrema permite a los desarrolladores responder a las solicitudes de los clientes, adaptarse y realizar cambios en tiempo real. Sin embargo, la programación extrema es mucho más disciplinada; realiza revisiones de código frecuentes y pruebas unitarias para realizar cambios rápidamente. Además, es muy creativa y colaborativa, ya que promueve el trabajo en equipo durante todas las etapas de desarrollo.

Por lo anteriormente expuesto, se considera que para el presente proyecto de titulación la metodología ágil Extreme Programming es la ideal y la que mejor se adapta en la elaboración del presente proyecto, para ello, a continuación, se detallan los pilares que fundamentan la elección.

La programación en pareja es una práctica clave en XP, y es perfecto ya que el equipo de este proyecto está conformado por dos integrantes permitiéndonos trabajar juntos en el mismo código. En un equipo de dos personas, esta práctica fomenta la revisión continua del código y el intercambio de conocimientos. Por otra parte, XP promueve la comunicación continua y la colaboración estrecha entre los miembros del equipo. En un equipo pequeño de dos personas, la comunicación directa y la colaboración son esenciales.

Esta metodología enfatiza la retroalimentación continua y la entrega frecuente de software funcional. XP permite ajustes y adaptaciones constantes, lo que es esencial para un desarrollo ágil y eficiente. Además, es conocida por su capacidad para adaptarse fácilmente a cambios en los requisitos. En equipos pequeños, donde la agilidad y la flexibilidad son especialmente valiosas, Extreme Programming permite una respuesta rápida a las necesidades cambiantes del proyecto o del cliente. A continuación, en la figura 3 se puede visualizar el ciclo de vida que comprende esta metodología, las cuales se profundizarán en el capítulo IV del presente proyecto.



Figura 4 Fases de la metodología XP

Fundamentación legal

Código de prácticas para la gestión de la seguridad de la información

Según Normas ISO (2017), la norma ISO/IEC 27002, también conocida como ISO 27002, es una norma internacional que forma parte de la serie ISO 27000 y establece el código de prácticas para la gestión de la seguridad de la información. Específicamente, ISO 27002 proporciona directrices detalladas para implementar controles de seguridad de la información dentro de una organización.

La norma ISO 27002 aborda un amplio espectro de temas relacionados con la seguridad de la información y proporciona recomendaciones para proteger los activos de información de una empresa, tanto físicos como electrónicos. Algunos de los aspectos clave que trata la norma incluyen: cita

1. Política de seguridad de la información: Define la estructura y el alcance de la política de seguridad de la información dentro de la organización, incluyendo roles y responsabilidades.
2. Gestión de activos: Aborda la identificación y clasificación de los activos de información, así como su protección, almacenamiento y disposición segura.
3. Control de acceso: Establece medidas para controlar el acceso a los recursos de información y sistemas, asegurando que solo las personas autorizadas tengan acceso a la información pertinente.
4. Seguridad física y del entorno: Proporciona pautas para proteger los recursos de información físicos, como salas de servidores y equipos, contra daños, robo o manipulación.
5. Gestión de incidentes de seguridad: Define procedimientos para la detección, registro y respuesta a incidentes de seguridad de la información, incluyendo la notificación de violaciones.
6. Cifrado y protección de datos: Aborda el uso de técnicas de cifrado y medidas de protección para asegurar la confidencialidad e integridad de los datos.
7. Seguridad en redes y comunicaciones: Establece medidas para proteger la seguridad de las redes y sistemas de comunicación, como cortafuegos, antivirus y detección de intrusiones.
8. Gestión de proveedores y terceros: Proporciona recomendaciones para asegurar que los proveedores y terceros que tienen acceso a la información de la organización cumplan con los requisitos de seguridad.
9. Concienciación y formación en seguridad: Establece pautas para promover la conciencia de seguridad entre el personal y proporcionar capacitación en seguridad de la información.

La norma ISO 27002 es una herramienta valiosa para ayudar a las organizaciones a establecer un marco sólido para la gestión de la seguridad de la información y mejorar la protección de sus activos más valiosos. Al seguir las directrices de esta norma, las organizaciones pueden reducir los riesgos de seguridad y proteger la confidencialidad, integridad y disponibilidad de la información que manejan.

CAPÍTULO III

En este capítulo se proporciona la estructura para la investigación, detallando la naturaleza de la misma, la población y muestra involucradas, las técnicas de recolección de datos, el análisis de los datos y la operacionalización de variables. En este contexto, se especifica el tipo de investigación aplicada, la población puede incluir usuarios y desarrolladores relevantes, las técnicas de recolección de datos pueden abarcar cuestionarios y pruebas de usabilidad, y el análisis de datos puede centrarse en evaluar el rendimiento del software o la satisfacción del usuario. La operacionalización de variables establece cómo se medirán conceptos como la eficiencia del software. Este marco metodológico guía la investigación, asegurando coherencia y rigurosidad, y proporciona una base para comprender la ejecución y contribución de la investigación al proyecto de software.

MARCO METODOLÓGICO

“El marco metodológico es la parte del escrito donde se argumentan los métodos, procedimientos, limitaciones para la recopilación de datos con relación a un tema o problema en específico (...)” (Rivas, 2022).

En este apartado del proyecto, se incluye el tipo de investigación, población, muestra, variables y los instrumentos o métodos utilizados, diseño y procedimiento.

Naturaleza de la investigación

La investigación propuesta se enmarca dentro del paradigma positivista, ya que busca obtener conocimiento objetivo y verificable sobre la gestión adecuada del acceso de usuarios a los sistemas informáticos y la seguridad de la información en una entidad educativa. Se basa en la recopilación de datos empíricos y la aplicación de métodos cuantitativos para analizar y validar los resultados obtenidos. El paradigma positivista permite establecer relaciones causales entre las variables y proporciona una visión objetiva y sistemática del problema de investigación.

El enfoque de la investigación es cuantitativo, lo que implica la recopilación y el análisis de datos numéricos para obtener conclusiones objetivas y generalizables sobre la gestión del acceso de usuarios y la seguridad de la información en el contexto educativo. Este enfoque proporciona una base sólida para evaluar la efectividad de las metodologías propuestas y desarrollar recomendaciones prácticas para mejorar la seguridad informática en las instituciones educativas.

El diseño de la investigación el diseño de la investigación se centrará en recopilar y analizar datos cuantitativos para proporcionar una evaluación rigurosa y basada en evidencia de la gestión del acceso de usuarios y la seguridad de la información en la entidad educativa. Esto permitirá identificar áreas de mejora y desarrollar recomendaciones prácticas para fortalecer la seguridad informática en el entorno educativo. Se recopilarán datos sobre diversos aspectos relacionados con la gestión del acceso y la seguridad informática, como la percepción de la eficacia de los controles de acceso, la frecuencia de incidentes de seguridad y la satisfacción con los procedimientos de seguridad existentes.

El módulo web se desarrollará utilizando las herramientas de desarrollo Angular y Spring Boot y se aplicará la metodología XP (Extreme Programming) para garantizar una entrega continua y eficiente del software. El enfoque de la investigación en su conjunto busca mejorar la gestión de acceso a los sistemas informáticos de la universidad y fortalecer la seguridad de la información para proteger los recursos digitales y garantizar el cumplimiento de requisitos normativos y legales.

Población y muestra

Población

Según el autor Arias (2006), la población es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Ésta queda delimitada por el problema y por los objetivos del estudio. Así mismo expresa el mismo autor, que: “si la población, por el número de unidades que la integran, resulta accesible en su totalidad, no será necesario extraer una muestra. En

consecuencia, se podrá investigar u obtener datos de toda la población objetivo” (Arias, 2012. pág. 83). Por lo tanto, la población de este proyecto está comprendida por seis personas que integran el personal de soporte de la Unidad de Tecnologías y Comunicaciones UTIC’s de la universidad donde se realiza la investigación.

Técnicas e instrumentos de recolección de datos

Técnica de recolección de datos

Para la recolección de datos de la presente investigación, la técnica empleada es la encuesta, la cual consta de un cuestionario de siete preguntas cerradas dirigidas al personal de soporte de la Unidad de TIC’S de la Universidad, mediante la herramienta de cuestionarios en línea Google Forms.

Dado que el tamaño de la población para lograr los objetivos es de 6 individuos, se enviará el cuestionario a esta cantidad exacta de usuarios, con lo cual, se obtendrán resultados confiables y válidos que reflejen los problemas que debería solventar el desarrollo del módulo en cuestión. Cada cuestionario contendrá preguntas diseñadas para recopilar información relevante que ayudarán a definir el diseño y funcionalidades del módulo web a desarrollar.

Técnicas de análisis de los datos

En el contexto del desarrollo del módulo web para la gestión de permisos a los aplicativos en una universidad, el análisis de datos es una fase crucial para entender las necesidades de los usuarios y garantizar el éxito del proyecto. Para realizar el análisis de datos se empleará la técnica de visualización de datos ya que utiliza gráficos para presentar los resultados de manera clara y comprensible.

Es importante recordar que el análisis de datos debe realizarse de manera ética y respetando la privacidad de los participantes. Los resultados del análisis de datos deben utilizarse para mejorar el módulo web y brindar una experiencia óptima a los usuarios de la universidad.

Operacionalización de la variable

La operacionalización de variables según Sampieri (2021) "es el proceso que describe las actividades u operaciones que se deben realizar para medir una variable" (p. 173). Es decir, se trata de convertir conceptos abstractos en variables medibles.

La operacionalización de variables es un proceso esencial en la investigación que implica definir claramente las variables teóricas en términos observables y medibles. Esto se logra traduciendo conceptos abstractos en acciones concretas que pueden ser manipuladas o medidas en un estudio. Esta práctica garantiza la claridad, precisión y reproducibilidad de los resultados, facilita la selección de instrumentos de medición adecuados, y proporciona una guía clara para el diseño del estudio, la recolección de datos y el análisis estadístico.

Tabla 1 Operacionalización de la variable

Variable	Concepto	Dimensiones	Indicador(e)
Procesos de gestión de permisos	Son las actividades y procedimientos llevados a cabo para administrar, controlar y regular los permisos de acceso a recursos, sistemas o información en un entorno específico.	Transparencia en los procesos de gestión	Grado de claridad en los procedimientos
		Complejidad en los procesos de gestión	Dificultad y complicación percibida en controlar los permisos
		Nivel de autonomía del usuario	Frecuencia con la que los usuarios piden intervención de un desarrollador de software
		Eficiencia del proceso	Asignación de manera oportuna, precisa
Satisfacción de los usuarios con los procesos actuales de asignación de permisos	Nivel de agrado y percepción de los usuarios con respecto a los procesos de asignación de permisos implementados por la Universidad.	Tiempo de respuesta	Tiempo promedio que tarda el desarrollador en responder a las solicitudes de asignación
		Actitud hacia la Innovación	Disposición de los usuarios hacia la adopción de nuevas tecnologías en el desarrollo de módulos
		Comunicación efectiva	Eficacia de la comunicación entre personal de desarrollo de software.

Instrumento y recolección de datos:

Para desarrollar el módulo propuesto de gestión de accesos de usuarios a los sistemas informáticos internos de una Universidad pública en Ecuador utilizando Angular y Spring Boot, se necesita realizar entrevistas con los usuarios quienes utilizarán el sistema para comprender sus necesidades, requisitos y expectativas en relación con el módulo de gestión de accesos. (Ver anexo 1)

CAPÍTULO IV

En el presente capítulo, se muestra el análisis de los datos obtenidos del cuestionario aplicado al personal que integra el grupo de soporte de la Unidad de Tecnologías de la Información y Comunicación de la universidad en cuestión, para la obtención de los requerimientos funcionales y no funcionales para el desarrollo del módulo web, de acuerdo con los lineamientos establecidos en el marco metodológico. Así como también, el desarrollo del módulo propuesto con cada una de las partes que establecen el ciclo de vida del software.

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

Resultados de la investigación

Tabulación y análisis de resultados

En este apartado se detallan minuciosamente los resultados obtenidos a través del cuestionario aplicado utilizando la herramienta de Google Forms. Se analiza detalladamente el porcentaje de respuestas, así como la relevancia e importancia atribuida al aplicativo por parte de los participantes.

1.-¿Son claros los procedimientos de gestión de permisos?
6 respuestas

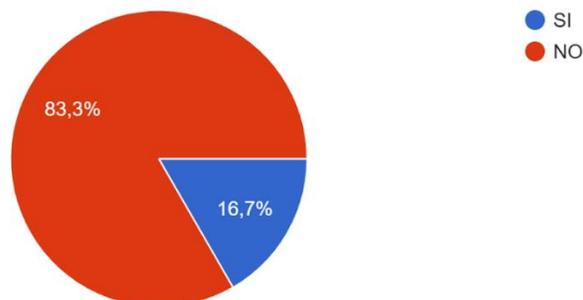


Figura 5 Resultados obtenidos de la primera pregunta aplicada en la encuesta establecida. Autoría propia

En la Figura 4, se visualiza que el 83,3% de las personas encuestadas consideran que el procedimiento de gestión de permisos no es claro. En tal sentido se requiere implementar acciones que faciliten a los usuarios la comprensión de estos procesos, entre las cuales se recomiendan las siguientes:

- Redactar los procedimientos de gestión de permisos en un lenguaje claro y conciso, evitando el uso de términos técnicos o jerga.
- Proporcionar instrucciones paso a paso para cada procedimiento.
- Utilizar ejemplos para ilustrar cómo aplicar los procedimientos en diferentes situaciones.
- Crear una base de conocimientos o un foro de preguntas y respuestas donde los usuarios puedan encontrar información y ayuda.
- Ofrecer formación a los usuarios sobre los procedimientos de gestión de permisos.

2.-¿Le resulta un proceso tedioso el cómo se maneja actualmente la gestión de permisos?
6 respuestas

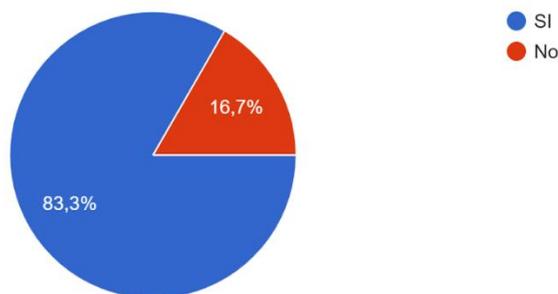


Figura 6 Resultados obtenidos de la segunda pregunta aplicada en la encuesta.
Autoría propia

En la Figura 5, el 83,3% de las personas encuestadas no están satisfechas con la claridad y simplicidad del proceso actual de gestión de permisos. En tal sentido se requiere implementar acciones que se simplifique el proceso actual de gestión de permisos entre las cuales recomendamos las siguientes:

- Un sistema centralizado puede simplificar la administración de permisos al proporcionar una única plataforma para gestionar todos los accesos.
- Permite una mejor visibilidad y control sobre los permisos de los usuarios.

3.- ¿Ha sido necesario que intervenga un desarrollador de aplicaciones en el proceso de asignación de permisos?

6 respuestas

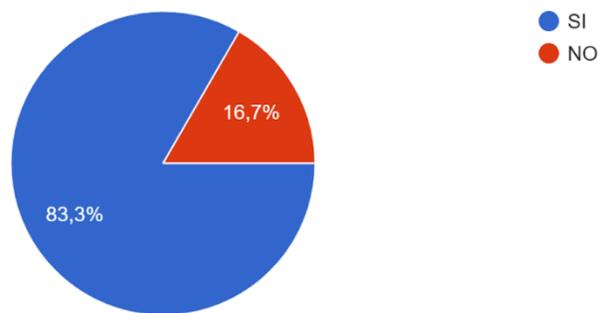


Figura 7 Resultados obtenidos de la tercera pregunta aplicada en la encuesta establecida.

El 83,3% de las personas encuestadas ha tenido que recurrir a un desarrollador de aplicaciones para que les ayude en el proceso de asignación de permisos. En tal sentido se requiere implementar acciones que reduzca la intervención de un desarrollador y que a su vez el proceso de asignación sea autónomo entre las posibles acciones recomendamos las siguientes:

- Desarrollar una herramienta de autoservicio que permita a los usuarios solicitar y gestionar sus propios permisos.
- Proporcionar ejemplos de casos de uso comunes.

4.- ¿Considera usted que el proceso actual de asignación de permisos necesita ser optimizado?
6 respuestas

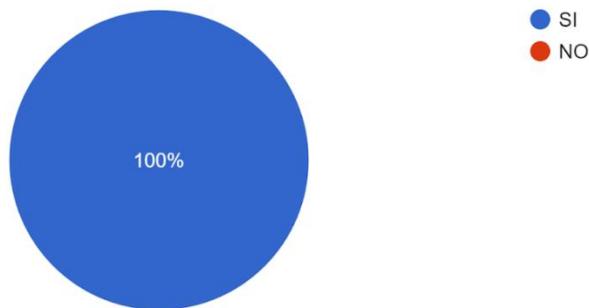


Figura 8 Resultados obtenidos de la cuarta pregunta aplicada en la encuesta establecida.

Todas las personas encuestadas consideran que el proceso actual de gestión de permisos es ineficiente. En tal sentido se requiere implementar acciones que optimicen la asignación de permisos entre las posibles acciones recomendamos las siguientes:

- Mejora la eficiencia y la transparencia del proceso.
- Realiza ajustes en el proceso de gestión de permisos según sea necesario.

5.-¿Ha experimentado problemas al solicitar la asignación de permisos al analista de aplicaciones para el acceso de los usuarios en los aplicativos?
6 respuestas

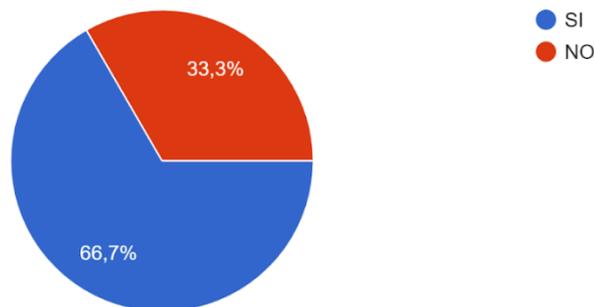


Figura 9 Resultados obtenidos de la quinta pregunta aplicada en la encuesta establecida.

El 66,7% de las personas encuestadas ha tenido dificultades para acceder a la información que necesita debido a los permisos de acceso. En tal sentido se requiere implementar acciones que reduzcan el número de incidencias al asignar permisos entre las posibles acciones recomendamos las siguientes:

- Mejorar la comunicación sobre los permisos de acceso: Informar a los usuarios sobre los permisos que tienen y cómo obtener acceso a la información que necesitan.
- Implementar un sistema de workflow para gestionar las solicitudes de acceso: Asegurar que las solicitudes de acceso se procesen de manera eficiente y oportuna.

6.- ¿Considera que se deberían emplear nuevas tecnologías en el desarrollo de los módulos de la Universidad?

6 respuestas

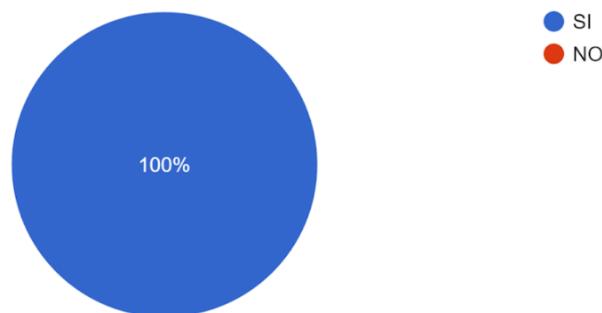


Figura 10 Resultados obtenidos de la sexta pregunta aplicada en la encuesta establecida.

Todas las personas encuestadas consideran que se deberían emplear nuevas tecnologías en el desarrollo de los módulos de la Universidad. Esto indica una clara necesidad y un fuerte interés por parte de la comunidad universitaria en la adopción de nuevas tecnologías para lograr esta implementación recomendamos las siguientes acciones:

- Implementar metodologías de desarrollo ágil para asegurar la flexibilidad y la adaptabilidad del proyecto.

- Involucrar a los usuarios finales en el proceso de desarrollo para obtener comentarios y garantizar que la aplicación cumpla con sus expectativas.

7.- ¿Cree que la colaboración entre UTICS y el analista de aplicaciones es eficiente?

6 respuestas

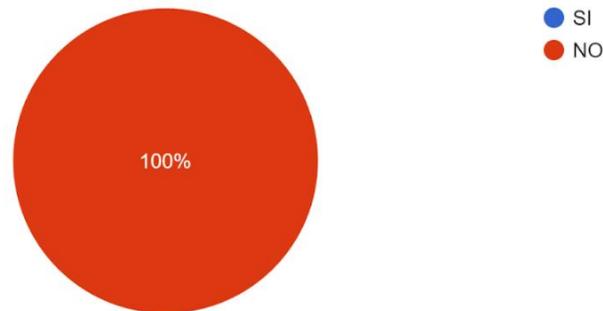


Figura 11 Resultados obtenidos de la séptima pregunta aplicada en la encuesta establecida.

Todas las personas encuestadas consideran que la colaboración entre Unidad de Tecnologías de la Información y Comunicaciones y el analista de aplicaciones es ineficiente. Es importante tomar medidas para mejorar la colaboración para lograr esta acción recomendamos las siguientes acciones:

- Documentar claramente los procesos y procedimientos para garantizar una comprensión compartida de las responsabilidades.
- herramientas y tecnologías que faciliten la colaboración, como plataformas de seguimiento de tickets.

Basándonos en los criterios previamente mencionados, y tras un exhaustivo análisis de los requisitos funcionales y no funcionales, se estableció la prioridad de cada uno de ellos. Esta priorización fue fundamental para la elaboración y diseño del presente trabajo de titulación.

Desarrollo del producto

En este apartado se muestra el proceso que se llevó a cabo para lograr el desarrollo del producto, basándonos para ello en las fases de la metodología elegida, Extreme Programming.

Planeación

Historias de usuario

Este ítem describe las funcionalidades específicas que se implementarán en el proyecto, desde la perspectiva del usuario. Cada historia de usuario representa un requisito o una característica del sistema que agrega valor para el cliente y los usuarios finales. Estas historias guían el desarrollo del proyecto y proporcionan un marco para la planificación de las iteraciones. A continuación, se muestra un ejemplo de la plantilla para la elaboración de una historia de usuario (*ver tabla 3*) con la respectiva descripción de los elementos que intervienen en ella y seguidamente se muestra un listado desarrollado de las mismas.

Tabla 2 *Plantilla para la elaboración de una historia de usuario*

Número:	Nombre de la historia:
Prioridad:	
Estimación de Tiempo:	
Descripción:	
Criterio de aceptación:	

Descripción de la plantilla para la generación de historias de usuario:

- En la casilla **Número** se proporciona el identificador para la historia de usuario.
- En la casilla **Nombre de la historia** se proporciona el título descriptivo que defina el objetivo principal de la historia de usuario.

- En la casilla **Prioridad** se proporciona la relevancia de la historia en comparación con otras, esto con el fin de priorizar la funcionalidad que se desea implementar. Estas relevancias pueden ser entre baja, media y alta.
- En la casilla **Estimación de tiempo** se realiza una estimación aproximada del tiempo que se necesita para completar en su totalidad la historia de usuario.
- En la casilla **Descripción** se indica la funcionalidad que se desea alcanzar con la historia de usuario.
- En la casilla **Criterio de aceptación** se proporciona los criterios mínimos que se deben alcanzar para poder cumplir con el objetivo de la historia de usuario.

Tabla 3 *Historia de usuario: Iniciar sesión en el sistema*

Número: 1	Nombre de la historia: Iniciar sesión en el sistema
------------------	--

Prioridad: Alta

Estimación de Tiempo: 1 semana

Descripción: Como usuario registrado deseo iniciar sesión por medio de mi usuario y contraseña para poder acceder a las funciones del módulo web.

Criterio de aceptación:

- La página para iniciar sesión debe contener ítems para el ingreso de usuario y contraseña.
- La página debe validar las credenciales del usuario ingresado.
- En caso de inicio exitoso de sesión se debe dirigir al usuario a la página principal del sistema.
- En caso de inicio de sesión fallido se debe mostrar el mensaje de error adecuado.

Tabla 4 *Historia de usuario: Cambio de contraseña*

Número: 2	Nombre de la historia: Cambio de Contraseña
------------------	--

Prioridad: *Baja*

Estimación de Tiempo: 4 días

Descripción: Como usuario del módulo web, quiero poder cambiar mi contraseña para mejorar la seguridad de la cuenta.

Criterio de aceptación:

- El enlace para ir a la página de cambio de contraseña debe estar en un lugar visible en la página principal.
- En la página de cambio de contraseña debe ingresar su contraseña actual.
- En la página de cambio de contraseña debe ingresar dos veces la nueva contraseña.
- Se debe validar que la nueva contraseña cumpla con los requisitos de seguridad establecidos por la normativa de la Universidad.

Tabla 5 *Historia de usuario: Iniciar sesión en el sistema*

Número: 3	Nombre de la historia: Gestión de Sistemas
------------------	---

Prioridad: Alta

Estimación de Tiempo: 1 semana

Descripción: Como administrador del módulo web, quiero poder gestionar los sistemas existentes, permitiendo la creación, edición, eliminación y actualización de sus detalles, incluyendo nombre, URL, estado y código de identificación, para mantener un registro actualizado y completo de los sistemas en el módulo web.

Criterio de aceptación:

- La página debe permitir ingresar registros en donde se ingresará los sistemas a los que posteriormente se le asignará tipos de perfiles de acceso.
- La página debe permitir ver los registros existentes.
- La página debe permitir editar los registros existentes.
- La página debe permitir activar o desactivar los registros existentes.

Tabla 6 *Historia de usuario: Gestión de perfiles*

Número: 4	Nombre de la historia: Gestión de perfiles
------------------	---

Prioridad: Alta

Estimación de Tiempo: 1 semana

Descripción: Como administrador del módulo web, quiero poder gestionar los perfiles de acceso asignándole el sistema al que pertenecerá este perfil, permitiendo la creación, edición, eliminación

Criterio de aceptación:

- La página debe permitir ingresar registros en donde se ingresará los nombres de los perfiles para su identificación al asignarle ese perfil a un usuario.
- La página deber permitir que al crear un perfil pueda seleccionar el sistema al que pertenecerá este.
- La página debe permitir ver los registros existentes.
- La página debe permitir editar los registros existentes.
- La página debe permitir activar o desactivar los registros existentes.

Tabla 7 *Historia de usuario: Gestión de opciones*

Número: 5	Nombre de la historia: Gestión de opciones
------------------	---

Prioridad: Alta

Estimación de Tiempo: 2 semanas

Descripción: Como administrador del módulo web, quiero gestionar las opciones que el usuario observe, en el cual ingrese los campos nombre, URL de destino, icono y posición en el menú, permitiendo la creación, edición, eliminación para personalizar la experiencia del usuario y la navegación dentro del sistema.

Criterio de aceptación:

- La página permitiría registrar los nombres de las opciones, el sistema al que pertenecen, la URL al que dirigirá la opción, el icono que visualiza el usuario para identificar la opción y el orden en que se desplegará esta opción.
- La página debe permitir ver los registros existentes.
- La página debe permitir editar los registros existentes.
- La página debe permitir activar o desactivar los registros existentes.

Tabla 8 *Historia de usuario: Gestión de opciones al perfil*

Número: 6	Nombre de la historia: Gestión asignación de opciones al perfil
------------------	--

Prioridad: Media

Estimación de Tiempo: 1 semana

Descripción: Como administrador del módulo, quiero asignar opciones a un perfil, y definir los permisos asociados a cada acción, como crear, modificar, eliminar e imprimir, para controlar y personalizar los accesos y acciones de los usuarios.

Criterio de aceptación:

- La página debe permitir desplegar y seleccionar todos los sistemas activos.
- La página debe permitir desplegar y seleccionar todos los perfiles activos asignados al sistema seleccionado previamente.
- La página debe permitir desplegar y seleccionar todas las opciones asignadas al sistema seleccionado y poder asignar estas opciones al perfil seleccionado.
- La página debe permitir asignar acciones como crear, editar, eliminar e imprimir que quiero que esa opción tenga para el perfil seleccionado.
- La página debe permitir editar los registros existentes.
- La página debe permitir activar o desactivar los registros existentes.

Tabla 9 *Historia de usuario: Asignación de perfil a un usuario*

Número: 7	Nombre de la historia: Asignación de perfil a un usuario
------------------	---

Prioridad: *Media*

Estimación de Tiempo: 2 semanas

Descripción: Como administrador del sistema, quiero poder asignar un perfil a un usuario específico, seleccionando primero el sistema al que pertenece el perfil, luego eligiendo el perfil deseado y finalmente ingresando el identificador único del usuario al que se le asignará el perfil, para controlar y gestionar los permisos de acceso de los usuarios dentro del sistema.

Criterio de aceptación:

- El usuario debe poder seleccionar el sistema al que pertenece el perfil que se asignará.
- Después de seleccionar el sistema, se deben mostrar todos los perfiles disponibles en ese sistema.
- El usuario debe poder seleccionar el perfil que desea asignar al usuario.
- Se debe proporcionar un campo para ingresar el identificador único del usuario al que se asignará el perfil.
- Después de ingresar el identificador del usuario y seleccionar el perfil, el usuario debe poder confirmar la asignación.
- Se deben realizar validaciones para garantizar que el usuario y el perfil seleccionados no existan previamente.

Tabla 10 *Historia de usuario: Gestión de control de usuarios*

Número: 8	Nombre de la historia: Gestión de control de usuarios
------------------	--

Prioridad: Media

Estimación de Tiempo: 2 semanas

Descripción: Como administrador del sistema, quiero poder ver y gestionar los perfiles asignados a un usuario específico, ingresando su identificador único, para visualizar los detalles de cada perfil, incluyendo el sistema al que pertenece, el nombre del perfil y su estado de activo o inactivo, y poder activar o desactivar perfiles según sea necesario.

Criterio de aceptación:

- El usuario debe poder ingresar el identificador único del usuario del cual desea ver y gestionar los perfiles asignados.
- Después de ingresar el identificador único del usuario, se deben mostrar todos los perfiles asignados a ese usuario.
- Para cada perfil asignado, se deben mostrar los siguientes detalles: el sistema al que pertenece, el nombre del perfil y su estado de activo o inactivo.
- El usuario debe poder activar o desactivar cada perfil directamente desde esta pantalla.
- Después de activar o desactivar un perfil, el usuario debe recibir una confirmación y los cambios deben reflejarse inmediatamente en la pantalla.

Plan de iteración

En esta sección detallamos como se organizará y ejecutará el proceso de desarrollo a través de ciclo cortos y repetitivos llamados iteraciones. En donde estableceremos los objetivos específicos que se abordarán en cada iteración, junto con las tareas necesarias para alcanzar esos objetivos. Este enfoque iterativo nos permite una entrega incremental del producto, facilita la adaptación a cambios y realizar ajustes según sea necesario, lo que contribuye a la mejora continua del proyecto.

A continuación, se muestra el plan de interacciones para el módulo web de gestión de acceso

Tabla 11 *Iteración 1 - Establecimiento de la base*

Proyecto: Módulo web de gestión de acceso

Iteración 1: Establecimiento de la Base

Duración: 1 semana

Objetivos:

- Configurar el entorno de desarrollo y la infraestructura del proyecto.
- Establecer la autenticación básica de usuarios.

Tareas:

- Configurar el repositorio de código y el entorno de pruebas.
 - Diseñar la arquitectura básica del sistema.
 - Implementar la autenticación de usuarios utilizando un sistema de inicio de sesión básico.
-

Tabla 12 *Iteración 2 - Gestión de usuarios y permisos*

Proyecto: Módulo web de gestión de acceso

Iteración 2: Gestión de Usuarios y Permisos

Duración: 3 semanas

Objetivos:

Integrar el módulo de gestión de acceso con los aplicativos universitarios existentes.

Tareas:

- Crear la interfaz de usuario para administrar usuarios y roles.
 - Implementar la lógica de asignación de permisos a usuarios y roles.
 - Desarrollar la funcionalidad de creación, edición y eliminación de usuarios.
-

Tabla 13 *Iteración 3 - Integración con aplicativos Universitarios*

Proyecto: Módulo web de gestión de acceso

Iteración 3: Integración con Aplicativos Universitarios

Duración: 4 semanas

Objetivos:

- Integrar el módulo de gestión de acceso con los aplicativos universitarios existentes.

Tareas:

- Investigar y establecer protocolos de integración con los aplicativos existentes.
 - Desarrollar la integración para permitir el acceso a los aplicativos utilizando las credenciales del módulo.
 - Realizar pruebas de integración y depuración.
-

Tabla 14 *Iteración 4 - Mejoras y optimizaciones*

Proyecto: Módulo web de gestión de acceso

Iteración 4: Mejoras y Optimizaciones

Duración: 2 semanas

Objetivos:

- Realizar mejoras en la interfaz de usuario y en la experiencia del usuario.
- Optimizar el rendimiento del sistema.

Tareas:

- Mejorar la usabilidad de la interfaz de usuario para una experiencia más intuitiva.
 - Optimizar consultas y procesos para mejorar la velocidad de respuesta.
 - Realizar pruebas de rendimiento y corrección de errores.
-

Diseño

Tarjetas Clase-Responsabilidad-Colaborador (CRC)

Según Pérez (2022), las tarjetas Clase-Responsabilidad-Colaborador es:

una actividad en grupo de modelado orientado a objetos en la cual el equipo puede manifestar y debatir ideas acerca del diseño de un sistema. Hace especial énfasis en la simplicidad, comunicación y límites de un sistema. Se suele utilizar en las primeras fases del desarrollo de una historia como paso previo a la implementación o escritura de un esquema UML (pág. 1)

En el marco de la metodología XP para el diseño de software orientado a objetos, se emplean las tarjetas CRC como una técnica de diseño y organización. Esta práctica implica la creación de una tarjeta CRC por cada historia de usuario, ya que cada una proporciona una funcionalidad directa al negocio.

A continuación, se muestra una plantilla de la Tarjeta CRC, seguidamente se detalla la descripción de cada elemento que la compone.

Tabla 15 *Plantilla para la elaboración de las Tarjeta CRC*

Nombre de la clase	
Responsabilidades:	Colaboradores:
Observaciones:	

Descripción de los elementos que conforman las Tarjetas CRC:

- En la casilla **Nombre de la clase** se proporciona la entidad u objeto dentro del sistema, que tiene responsabilidades específicas y colabora con otros objetos para alcanzar determinados comportamientos.
- En la casilla **Responsabilidades** se incluye las acciones que la clase debe ejecutar o los datos que se pueden guardar. Las responsabilidades pueden incluir operaciones que la clase debe realizar internamente o interacciones que debe tener con otros objetos.
- En la casilla **Colaboradores** se puede ingresar otras clases o componentes que pueden interactuar con la clase principal para que esta pueda cumplir con sus responsabilidades
- En la casilla **Observaciones** se puede ingresar comentarios adicionales o anotaciones significativas sobre la clase.

Seguidamente, se elaboran las tarjetas CRC por cada historia de usuario desarrollados anteriormente.

Tabla 16 Tarjeta CRC: Iniciar sesión en el sistema

IniciarSesion

Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Validar credenciales de usuario.• Iniciar sesión en el sistema.• Gestionar sesiones de usuario.	<ul style="list-style-type: none">• Base de datos de usuarios.• Interfaz de usuario (página de inicio de sesión).• Gestor de sesiones.

Observaciones:

Tabla 17 Tarjeta CRC: Cambio de contraseña

CambioContraseña

Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Validar la contraseña actual del usuario.• Validar y establecer la nueva contraseña del usuario.• Proporcionar retroalimentación al usuario sobre el éxito del cambio de contraseña.	<ul style="list-style-type: none">• Base de datos para verificar la contraseña actual y actualizar la nueva contraseña.• Interfaz de usuario para mostrar la página de cambio de contraseña y recibir las entradas del usuario.

Observaciones:

Tabla 18 Tarjeta CRC: Gestión de Sistemas

Sistema	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Almacenar información sobre el nombre del sistema, la URL, el estado y el código de identificación.• Proporcionar métodos para crear, leer, actualizar y eliminar sistemas.	<ul style="list-style-type: none">• Interfaz de usuario para la gestión de sistemas.• Base de datos para almacenar la información del sistema
Observaciones:	

Tabla 19 Tarjeta CRC: Gestión de perfiles

Perfil	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Mantener información sobre el nombre del perfil y su estado.• Asociar el perfil con un sistema.• Permitir la asignación de opciones y permisos al perfil.	<ul style="list-style-type: none">• Interfaz de usuario para la gestión de perfiles.• Clase de Opción para la asignación de opciones y permisos.
Observaciones:	

Tabla 20 *Tarjeta CRC: Gestión de opciones*

Opciones	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Almacenar información sobre el nombre de la opción, la URL de destino, el icono y el orden.• Asociar la opción con un sistema.• Permitir la asignación de opciones a perfiles de usuario.	<ul style="list-style-type: none">• Interfaz de usuario para la gestión de opciones.• Clase de Perfil para la asignación de opciones a perfiles.
Observaciones:	

Tabla 21 *Tarjeta CRC: Gestión de asignación de opciones al perfil*

Asignación Opciones Perfil	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Gestionar la asignación de opciones a un perfil de usuario.• Definir los permisos asociados a cada opción asignada, como crear, modificar, eliminar e imprimir.	<ul style="list-style-type: none">• Sistema: para obtener la lista de sistemas disponibles y sus opciones.• Perfil: para obtener la lista de perfiles disponibles y las opciones asignadas a un perfil específico.• Opción: para seleccionar las opciones disponibles y definir los permisos asociados.
Observaciones:	

Tabla 22 Tarjeta CRC: Asignación de perfil a un usuario

AsignaciónPerfilUsuario	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Seleccionar el sistema al que pertenece el perfil que se asignará.• Mostrar todos los perfiles disponibles en el sistema seleccionado.• Permitir la selección del perfil que se asignará al usuario.• Proporcionar un campo para ingresar el identificador único del usuario.• Confirmar la asignación del perfil al usuario.• Validar la selección del sistema, el perfil y el usuario.	<ul style="list-style-type: none">• Sistema: para obtener la lista de perfiles disponibles.• Perfil: para realizar la asignación al usuario seleccionado.• Usuario: para validar la existencia del usuario y realizar la asignación

Observaciones:

Tabla 23 *Tarjeta CRC: Gestión de control de usuarios*

GestionControlUsuarios	
Responsabilidades	Colaboradores
<ul style="list-style-type: none">• Mantener información sobre el identificador único del usuario y sus perfiles asignados.• Permitir la visualización y gestión de los perfiles asignados a un usuario.• Activar o desactivar perfiles asignados a un usuario.	<ul style="list-style-type: none">• Interfaz de usuario para el control de usuarios.• Clase de Perfil para la gestión de perfiles asignados.•
Observaciones:	

Codificación

Modelo de clases

Este modelo se enfoca en los aspectos concretos de implementación, como la definición de tablas y columnas en una base de datos relacional, la optimización de consultas y el diseño de índices. El modelo de clases se utiliza para guiar la implementación real del sistema y es fundamental para la construcción de la base de datos y la aplicación.

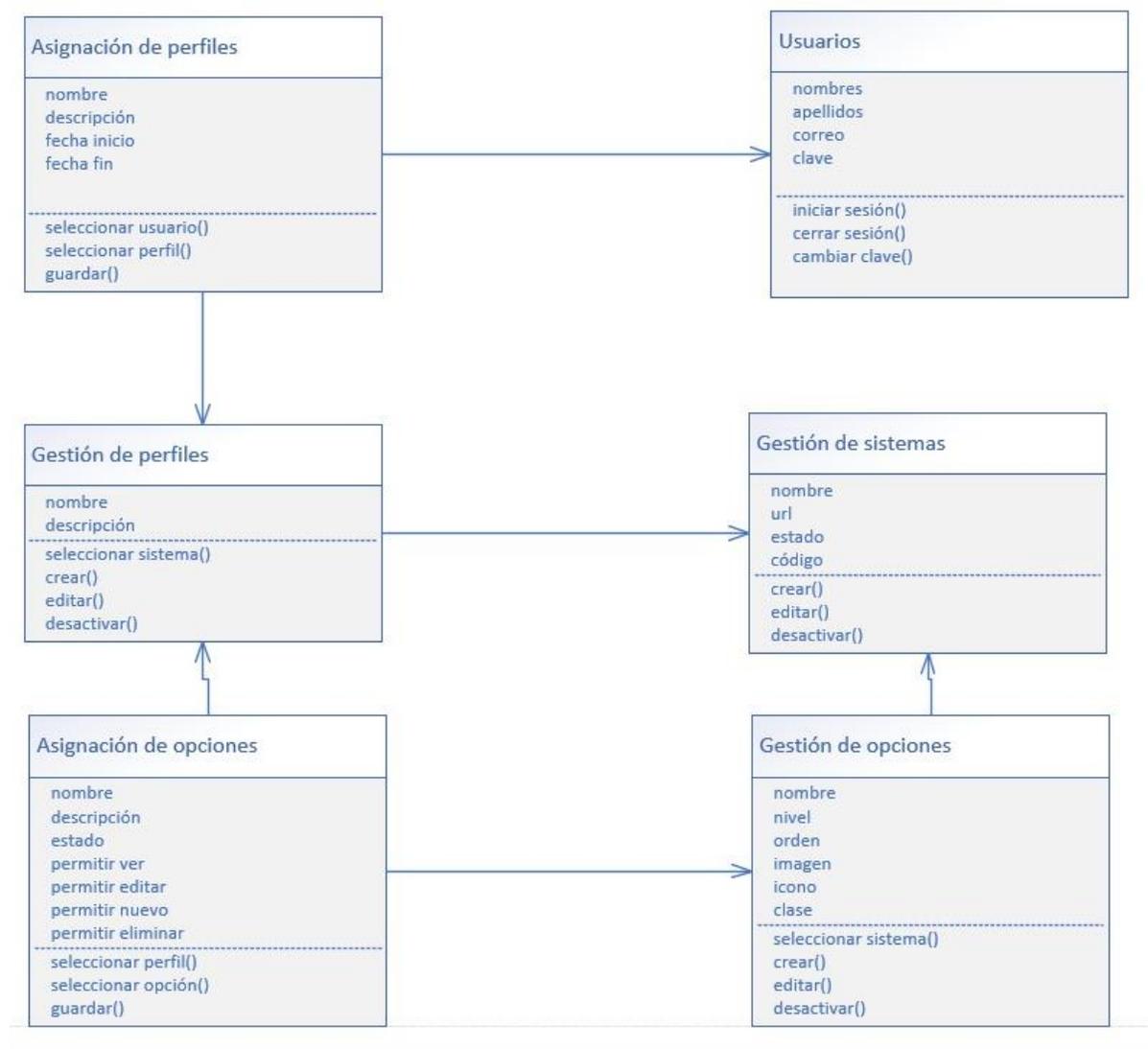


Figura 12 Esquema del modelo de clases sobre del módulo Gestión de Usuarios

Modelo de base de datos

En este modelo se traducen los conceptos del modelo conceptual en una estructura de datos más concreta, que generalmente se basa en un modelo de datos específico, como un modelo relacional. El modelo lógico define la organización de los datos, las relaciones entre las entidades y las restricciones de integridad de datos.

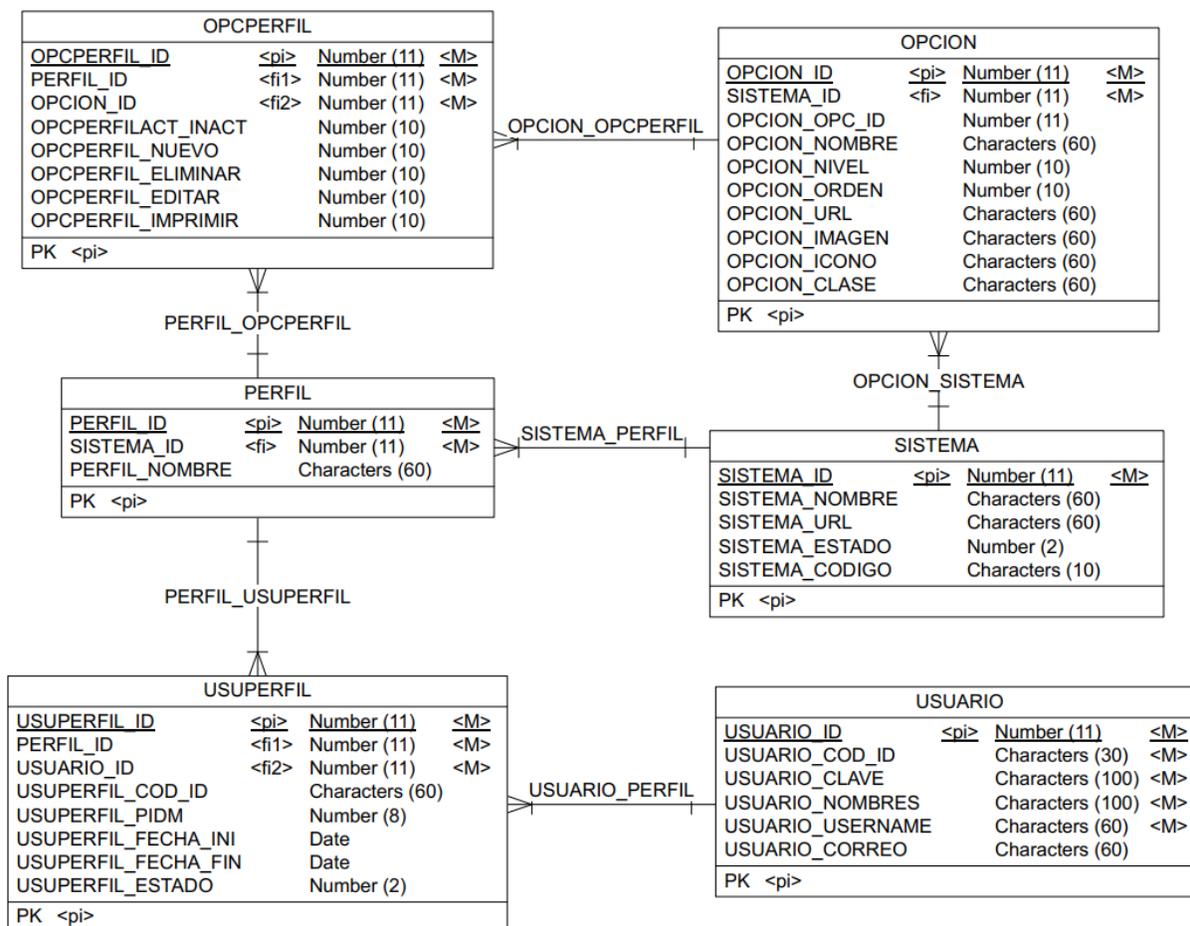


Figura 13 Esquema del modelo lógico sobre del módulo Gestión de Usuarios

Diccionario de datos

A continuación, se presenta el diccionario de datos de la aplicación en las tablas que intervienen en el Módulo Web de asignación de permisos.

Tabla 24 Diccionario de datos: tabla OPCIÓN

Nombre de la tabla: OPCION							
Descripción de la tabla: Guarda los datos de las opciones de acceso cada uno de los sistemas.							
Nombre	PK	Tipo De Dato	Longitud	Formato	FK	Requerido	Descripción
OPCION_ID	1	number	11	Entero		si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
SISTEMA_ID		number	11	Entero	SISTEMA	si	Código de la tabla sistema, indicará la opción del sistema al que pertenece
OPCION_OPC_ID		number	11	Entero		si	Código indicando la opción al que pertenece
OPCION_NOMBRE		varchar	60	cadena de caracteres		no	Nombre de la Opción
OPCION_NIVEL		number	10	Entero		no	Nivel
OPCION_ORDEN		number	10	Entero		no	Orden
OPCION_URL		varchar	60	cadena de caracteres		no	URL de la página web que abrirá la opción
OPCION_IMAGEN		varchar	60	cadena de caracteres		no	Imagen del sistema
OPCION_ICONO		varchar	60	cadena de caracteres		no	Color de fondo de la clase
OPCION_CLASE		varchar	60	cadena de caracteres		no	Color de fondo de la clase

Tabla 25 Diccionario de datos: tabla OPCPERFIL

Nombre de la tabla: OPCPERFIL							
Descripción de la tabla: Guarda los datos de las opciones que serán asignados cada uno de los perfiles.							
Nombre	PK	Tipo De Dato	Longitud	Formato	FK	Requerido	Descripción
OPCPERFIL_ID	1	number	11	entero		Si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
PERFIL_ID		number	11	entero	PERFIL	Si	Código del perfil, indica la opción que perfil le pertenece.
OPCION_ID		number	11	entero	OPCION	Si	Código de opción, indica qué opción le pertenece.
OPCPERFILACT_INACT		number	10	entero		No	Campo determinado para habilitar o deshabilitar la visualización de la opción de acuerdo al perfil 1 habilitado 0 deshabilitado
OPCPERFIL_NUEVO		number	10	entero		No	Campo determinado para habilitar o deshabilitar la acción del botón de acuerdo al perfil 1 habilitado 0 deshabilitado
OPCPERFIL_ELIMINAR		number	10	entero		No	Campo determinado para habilitar o deshabilitar la acción del botón de acuerdo al perfil 1 habilitado 0 deshabilitado
OPCPERFIL_EDITAR		number	10	entero		No	Campo determinado para habilitar o deshabilitar la acción del botón de acuerdo al perfil 1 habilitado 0 deshabilitado

Tabla 26 *Diccionario de datos: tabla PERFIL*

Nombre de la tabla: PERFIL

Descripción de la tabla: Guarda los datos de los perfiles(roles) para luego ser asignados a los usuarios

Nombre	Pk	Tipo de dato	Longitud	Formato	Fk	Requerido	Descripción
PERFIL_ID	1	number	11	Entero		si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
SISTEMA_ID		number	11	Entero	SISTEMA	si	Código de la tabla sistema, indica al perfil que sistema le pertenece.
PERFIL_NOMBRE		number	11	Entero		no	Descripción del perfil del sistema.

Tabla 27 Diccionario de datos: tabla *SISTEMA*

Nombre de la tabla: SISTEMA

Descripción de la tabla: Tabla que guarda los datos de los sistemas existentes de la Universidad

Nombre	PK	Tipo De Dato	Longitud	Formato	FK	Requerido	Descripción
SISTEMA_ID	1	number	11	number		si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
SISTEMA_NOMBRE		varchar	60	cadena de caracteres		no	Descripción del sistema
SISTEMA_URL		varchar	60	cadena de caracteres		no	Url del sitio del sistema
SISTEMA_ESTADO		number	2	entero		no	Estados del sistema 1 habilitado 0 deshabilitado
SISTEMA_CODIGO		varchar	60	cadena de caracteres		no	Identificador del sistema

Tabla 28 Diccionario de datos: tabla USUARIO

Nombre de la tabla: USUARIO							
Descripción de la tabla: Tabla que guarda los datos de los usuarios que administran el sistema							
Nombre	PK	Tipo de dato	Longitud	Formato	FK	Requerido	Descripción
USUARIO_ID	1	number	11	entero		si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
USUARIO_COD_ID		varchar	30	cadena de caracteres		Si	Numero de id, sirve para validar el ingreso al sistema
USUARIO_CLAVE		varchar	100	cadena de caracteres		Si	Contraseña de usuario para el ingreso al sistema
USUARIO_NOMBRES		varchar	100	cadena de caracteres		si	Nombres y apellidos del usuario
USUARIO_USERNAME		varchar	60	cadena de caracteres		si	Usuario del sistema académico
USUARIO_CORREO		varchar	60	cadena de caracteres		no	Correo institucional

Tabla 29 *Diccionario de datos: tabla USUPERFIL*

Nombre de la tabla: USUPERFIL							
Descripción de la tabla: Tabla que guarda los datos del perfil y el usuario asignado							
Nombre	PK	Tipo de dato	Longitud	Formato	FK	Requerido	Descripción
USUPERFIL_ID	1	number	11	entero		si	Código secuencial de la tabla, este dato será generado automáticamente mediante la utilización de una secuencia.
PERFIL_ID		number	11	entero	PERFIL	si	Código del perfil, indica al usuario que perfil le pertenece
USUARIO_ID		number	11	entero	USUARIO		Código del usuario, indica al usuario que perfil le pertenece
USUPERFIL_COD_ID		varchar	60	cadena de caracteres		no	Código id de sistema académico para asignar a un usuario un perfil
USUPERFIL_PIDM		number	8	entero		no	Código PIDM secuencial del sistema académico para asignar a un usuario un perfil.
USUPERFIL_FECHA_INI		date		fecha		no	Fecha inicio vigencia del registro.
USUPERFIL_FECHA_FIN		date		fecha		no	Fecha finalización de vigencia del registro.
USUPERFIL_ESTADO		number	2	entero		no	Campo determinado para habilitar o deshabilitar el acceso del usuario a dicho perfil 1 habilitado 0 deshabilitado.

A continuación se muestran capturas de pantalla de fragmento de código relevante en el desarrollo del lado del la lógica del negocio.

```
no usages  Willian Manolo Conya Gavilanez +3 *
@EnableWebSecurity
@Configuration
class WebSecurityConfig extends WebSecurityConfigurerAdapter {

    Willian Manolo Conya Gavilanez +2 *
    protected void configure(HttpSecurity http) throws Exception {
        http.csrf().disable()
            .addFilterAfter((Filter) new JWTAuthorizationFilter(), UsernamePasswordAuthenticationFilter.class)
            .authorizeRequests()
                .antMatchers(HttpMethod.GET, ...antPatterns: "/adm/id/**").permitAll()
                .antMatchers(HttpMethod.OPTIONS, ...antPatterns: "/*").permitAll()
                .antMatchers(HttpMethod.POST, ...antPatterns: "/adm/login").permitAll()
                .antMatchers(...antPatterns: "/adm/segupob").permitAll()
                .antMatchers(...antPatterns: "/adm/segup/**").permitAll()
                .antMatchers(...antPatterns: "/adm/public/**").permitAll().anyRequest().authenticated()
                .antMatchers(HttpMethod.GET, ...antPatterns: "/v2/api-docs",
                    "/configuration/ui",
                    "/swagger-resources/**",
                    "/configuration/security",
                    "/swagger-ui/**",
                    "/webjars/**",
                    "/v3/**"
                ).permitAll()
            .anyRequest().authenticated();
    }
}
```

Figura 14 Configuración de seguridad web

El fragmento de código en la figura 14 define una configuración de seguridad web para una aplicación Spring Boot. El código utiliza la anotación `@EnableWebSecurity` para habilitar la seguridad web y la clase `WebSecurityConfigurerAdapter` para personalizar la configuración de seguridad.

El método `configure (HttpSecurity http)` define las reglas de autorización para las solicitudes HTTP. Las siguientes reglas se definen en el código:

Las solicitudes GET a las rutas `/adm/id/**` se permiten para todos los usuarios, independientemente de si están autenticados o no.

Las solicitudes OPTIONS a cualquier ruta se permiten para todos los usuarios.

Las solicitudes POST a la ruta `/adm/login` se permiten para todos los usuarios.

Las solicitudes a las rutas `/adm/segupob` y `/adm/segup/**` se permiten para todos los usuarios.

Las solicitudes a las rutas /adm/public/** se permiten para todos los usuarios. Cualquier otra solicitud requiere que el usuario esté autenticado.

```
private Claims validateToken(HttpServletRequest request) {
    String jwtToken = request.getHeader(HEADER).replace(PREFIX, replacement: "");
    return Jwts.parser().setSigningKey(SECRET.getBytes()).parseClaimsJws(jwtToken).getBody();
}
```

Figura 15 Verificación de acceso a un recurso

El fragmento de código en la figura 15 verifica si el usuario actual tiene los permisos necesarios para acceder a un recurso específico. El proceso comienza con la obtención del token de autenticación del usuario de la solicitud HTTP. Este token se valida y, si es válido, se extrae la información del usuario, como roles y permisos. Luego, se comparan estos datos con los roles y permisos necesarios para acceder al recurso. Si coinciden, se concede el acceso al usuario. De lo contrario, se le niega el acceso. En resumen, este código actúa como un guardián que protege los recursos de la aplicación al permitir solo el acceso de usuarios con las credenciales adecuadas.

```
private void setUpSpringAuthentication(Claims claims) {
    List<String> authorities = (List<String>) claims.get("authorities");

    UsernamePasswordAuthenticationToken auth = new UsernamePasswordAuthenticationToken(claims.getSubject(), credentials: null,
        authorities.stream().map(SimpleGrantedAuthority::new).collect(Collectors.toList()));
    SecurityContextHolder.getContext().setAuthentication(auth);
}
```

Figura 16 Validación de acceso a un recurso

El fragmento de código en la figura 16 valida si el usuario actual tiene los permisos necesarios para acceder a un recurso específico. La lógica del código es simple: primero, se extrae la información del usuario, como roles y permisos, del objeto "Claims". Luego, se comparan estos datos con los roles y permisos requeridos para acceder al recurso. Si coinciden, se concede el acceso al usuario. De lo contrario, se le deniega el acceso. En resumen, este código actúa como una puerta de seguridad que protege los recursos de la aplicación al permitir solo el acceso de usuarios con las credenciales adecuadas.

Pruebas

Pruebas de aceptación

En base a las historias usuario se han desarrollado las pruebas de aceptación. Una prueba de aceptación es una evaluación formal que se realiza para determinar si un sistema cumple con los criterios de aceptación especificado en la historia de usuario. Como se muestra en la tabla 26, podemos observar la plantilla empleada para la generación de pruebas de aceptación.

Tabla 30 *Ejemplo de evaluación de prueba de aceptación*

Número:	Historia de Usuario:
Nombre:	
Descripción:	
Condiciones de ejecución:	
Entrada:	
Resultado obtenido:	
Observación:	
Evaluación de la prueba:	

A continuación, se detalla cada uno de los campos que componen la plantilla para la generación de las pruebas de validación.

- **Número:** Es un identificador único asignado a cada prueba de aceptación. Se utiliza para organizar y hacer referencia a las pruebas de forma individual.
- **Historia de Usuario:** Se refiere al identificador o número de la historia de usuario asociada a la prueba de aceptación. Cada historia de usuario representa un requerimiento funcional específico del sistema que debe ser probado.
- **Nombre:** Es un breve título o nombre que describe el propósito o el objetivo de la prueba de aceptación.
- **Descripción:** Proporciona una explicación detallada de lo que se espera probar en la prueba de aceptación. Incluye información sobre el contexto, los requisitos y los criterios que se deben cumplir.

- **Condiciones de ejecución:** Son las condiciones o situaciones necesarias que deben estar presentes para ejecutar la prueba de aceptación de manera efectiva. Esto podría incluir el estado del sistema, la autenticación de usuario, etc.
- **Entrada:** Es la información o los datos que se introducen en el sistema como parte de la ejecución de la prueba de aceptación. Esto puede incluir acciones del usuario, datos de prueba, etc.
- **Resultado obtenido:** Es el resultado o la respuesta que se observa después de ejecutar la prueba de aceptación. Indica lo que realmente sucedió después de realizar las acciones especificadas en la entrada.
- **Observación:** Sirve para reconocer las observaciones y comentarios realizados durante la ejecución de la prueba. Estas observaciones pueden estar relacionadas con el funcionamiento del software, la experiencia del usuario, posibles errores o problemas encontrados, sugerencias de mejora, entre otros aspectos relevantes para la evaluación del producto.
- **Evaluación de la prueba:** Es una evaluación subjetiva o cualitativa del resultado de la prueba. Se utiliza para determinar si la prueba fue exitosa o no, y a menudo incluye comentarios adicionales sobre el desempeño del sistema o cualquier problema encontrado durante la ejecución de la prueba.

A continuación, se muestra el desarrollo de las pruebas de aceptación elaborada para una de las historias de usuario presentadas anteriormente.

Tabla 31 *Prueba de aceptación relacionada a la historia de usuario 1*

Número: 1	Historia de Usuario: Iniciar sesión en el sistema
------------------	--

Nombre: Historia de Usuario

Descripción: Verificar que el sistema permite a un usuario iniciar sesión correctamente utilizando credenciales válidas

Condiciones de ejecución: No estar previamente autenticado en el sistema.

Entrada: Nombre de usuario y contraseña válidos.

Resultado obtenido: El sistema autentica al usuario y lo redirige a la página principal del sistema.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 32 *Prueba de aceptación relacionada a la historia de usuario 2*

Número: 2	Historia de Usuario: Cambio de contraseña
------------------	--

Nombre: Acceder al Proceso de Cambio de Contraseña

Descripción: Verificar que el sistema proporciona un enlace o botón claramente visible en la configuración de la cuenta para iniciar el proceso de cambio de contraseña.

Condiciones de ejecución: Estar autenticado en el sistema y acceder a la configuración de la cuenta.

Entrada: Hacer clic en el enlace o botón para cambiar la contraseña.

Resultado obtenido: El sistema redirige al usuario a una página segura de cambio de contraseña en donde ingresa la nueva contraseña además de la confirmación de la contraseña y luego es dirigido a la página de inicio de sesión.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 33 Prueba de aceptación relacionada a la historia de usuario 3

Número: 3	Historia de Usuario: Gestión de sistemas
------------------	---

Nombre: Acceso a la Interfaz de Registro

Descripción: Verificar que existe una interfaz clara y accesible para registrar un nuevo sistema dentro del sistema existente.

Condiciones de ejecución: Estar autenticado como administrador del sistema.

Entrada: Acceder a la sección de registro de nuevos sistemas.

Resultado obtenido:

El sistema muestra una interfaz clara y accesible para registrar un nuevo sistema.

El sistema muestra campos para ingresar el nombre, URL, estado y código de identificación del nuevo sistema.

El sistema muestra un mensaje de confirmación y redirige al usuario a la lista de sistemas registrados.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 34 Prueba de aceptación relacionada a la historia de usuario 4

Número: 4	Historia de Usuario: Gestión de perfiles
------------------	---

Nombre: Creación y Edición de Perfiles

Descripción: Verificar que, durante la creación y edición de perfiles, el usuario puede asignar un nombre identificativo para el rol que representará el perfil.

Condiciones de ejecución: Estar en la interfaz de creación o edición de perfiles.

Entrada: Asignar un nombre identificativo al perfil.

Resultado obtenido:

El sistema muestra una interfaz clara y accesible para gestionar los perfiles de usuario
El sistema permite al usuario asignar un nombre identificativo al perfil
El sistema muestra un mensaje de confirmación y redirige al usuario a la lista actualizada de perfiles.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 35 *Prueba de aceptación relacionada a la historia de usuario 5*

Número: 5	Historia de Usuario: Gestión de opciones
------------------	---

Nombre: Creación y Edición de Opciones

Descripción: Verificar que, durante la creación y edición de opciones, el usuario puede especificar el nombre de la opción, la URL de destino, el icono y el orden en que se desplegará en el menú.

Condiciones de ejecución: Estar en la interfaz de creación o edición de opciones del menú.

Entrada: Especificar el nombre, la URL, el icono y el orden de la opción.

Resultado obtenido: El sistema muestra una interfaz clara y accesible para gestionar las opciones del menú principal.

El sistema permite al usuario reordenar las opciones del menú de forma intuitiva.

El sistema muestra un mensaje de confirmación y redirige al usuario a la vista actualizada del menú principal.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 36 Prueba de aceptación relacionada a la historia de usuario 6

Número: 6 **Historia de Usuario:** Gestión de asignación de opciones al perfil

Nombre: Asignación de Opciones al Perfil.

Descripción: Verificar que el sistema permite al administrador asignar opciones a un perfil de usuario seleccionado, definiendo los permisos asociados a cada opción y asegurando la integridad de los datos.

Condiciones de ejecución: Estar autenticado como administrador del sistema y acceder a la interfaz de asignación de opciones al perfil.

Entrada: Seleccionar un sistema, un perfil y las opciones que se desean asignar, así como definir los permisos asociados.

Resultado obtenido:

Seleccionar un sistema válido.

Seleccionar un perfil existente en el sistema seleccionado.

Las opciones seleccionadas son válidas y no están duplicadas.

Los permisos asociados a cada opción son válidos (crear, modificar, eliminar, imprimir).

Después de realizar la asignación de opciones, el sistema muestra un mensaje de confirmación y redirige al usuario a la vista del perfil actualizada.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 37 Prueba de aceptación relacionada a la historia de usuario 7

Número: 7	Historia de Usuario: Asignación de perfil a un usuario
------------------	---

Nombre: Asignación de Perfil a Usuario

Descripción: Verificar que el sistema permite al administrador asignar un perfil a un usuario específico, asegurando que los datos ingresados sean válidos y no existan conflictos de asignación.

Condiciones de ejecución: Estar autenticado como administrador del sistema y acceder a la interfaz de asignación de perfil a usuario.

Entrada: Seleccionar un sistema, un perfil, ingresar el identificador único del usuario al que se le asignará el perfil y confirmar la asignación.

Resultado obtenido: El sistema realiza las siguientes validaciones:

- Seleccionar un sistema válido.
- Seleccionar un perfil existente en el sistema seleccionado.
- Ingresar un identificador único de usuario válido.
- Verificar que el usuario no tenga ya asignado el perfil seleccionado.
- Después de confirmar la asignación, el sistema muestra un mensaje de confirmación y redirige al usuario a la vista del usuario actualizada.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Tabla 38 Prueba de aceptación relacionada a la historia de usuario 8

Número: 8	Historia de Usuario: Gestión de control de usuarios
------------------	--

Nombre: Visualización y Gestión de Perfiles Asignados a un Usuario

Descripción: Verificar que el sistema permite al administrador ver y gestionar los perfiles asignados a un usuario específico, asegurando que los datos ingresados sean válidos y que los cambios se reflejen inmediatamente en la pantalla.

Condiciones de ejecución: Estar autenticado como administrador del sistema y acceder a la interfaz de control de usuarios.

Entrada: Ingresar el identificador único del usuario del cual se desean ver y gestionar los perfiles asignados, activar o desactivar perfiles.

Resultado obtenido: El sistema realiza las siguientes validaciones:

- Verificar que el identificador único del usuario sea válido.
- Mostrar todos los perfiles asignados a ese usuario, incluyendo detalles como el sistema al que pertenece, el nombre del perfil y su estado de activo o inactivo.
- Permitir al usuario activar o desactivar cada perfil directamente desde la pantalla.
- Después de activar o desactivar un perfil, el sistema muestra un mensaje de confirmación y los cambios se reflejan inmediatamente en la pantalla.

Observación: Se llevó a cabo la prueba de validación sin incidencias destacables, cumpliendo satisfactoriamente el 100% de los criterios de aceptación definidos en la historia de usuario correspondiente.

Evaluación de la prueba: Prueba satisfactoria.

Finalmente, se muestra el link del producto desarrollado: users.espe.edu.ec

CAPÍTULO V

En este capítulo, se presenta un análisis integral de los hallazgos y resultados obtenidos a lo largo del desarrollo de la tesis. Se sintetizan las conclusiones más relevantes derivadas de la investigación y el proceso de implementación del módulo web para la gestión de accesos a los aplicativos internos de la Universidad. Además, se ofrecen recomendaciones fundamentales basadas en las conclusiones alcanzadas, con el propósito de orientar acciones futuras y mejorar la eficiencia, la seguridad y la experiencia del usuario en el sistema. Este capítulo proporciona una visión panorámica de los logros alcanzados, así como un camino a seguir para el desarrollo continuo y la optimización del proyecto en el futuro.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Con respecto al objetivo general del presente trabajo de investigación, el Módulo web fue diseñado y ejecutado de acuerdo con la propuesta del estudio planteada, cumpliendo con los plazos establecidos. Se logró la automatización completa de los procedimientos necesarios para la gestión de los accesos a los aplicativos internos de la Universidad.

Después de analizar los procesos actuales llevados a cabo en la Unidad de Tecnologías de la Información y Comunicación para la gestión de acceso a los aplicativos internos a través de la encuesta, en relación al primer objetivo específico de este proyecto, se pueden extraer varias conclusiones significativas. En primer lugar, queda claro que existe una percepción generalizada entre los encuestados de que los procedimientos de gestión de permisos no son claros y que el proceso actual resulta tedioso, sugiriendo con esto, la necesidad de mejorar la comunicación y la documentación de los procedimientos, así como de optimizar el proceso para hacerlo más eficiente y menos engorroso para los usuarios. Además, la encuesta reveló que en algunos casos es necesario que intervenga un desarrollador de aplicaciones en el proceso de asignación de permisos, lo que indica una posible complejidad adicional en el proceso actual que debe abordarse. Los

resultados mostraron opiniones unánimes del cien por ciento en cuanto a la eficiencia de la colaboración entre UTIC's y el analista de aplicaciones, lo que sugiere que podría ser necesario mejorar la colaboración entre estas áreas para garantizar la eficacia y la eficiencia en la gestión de permisos

Basándonos en el segundo objetivo específico, se concluye que el diseño del módulo web se realizó de acuerdo con las mejores prácticas y estándares de la industria de desarrollo de software. En cuanto a minimización de riesgos de seguridad, la aplicación de la metodología XP permitió identificar y abordar de manera proactiva los riesgos de seguridad durante todo el ciclo de vida del desarrollo del módulo web. Las prácticas de desarrollo continuo, las revisiones de código en pareja y la implicación activa del cliente ayudaron a identificar y mitigar posibles vulnerabilidades de seguridad de manera oportuna. Con respecto a la protección de la información, se implementaron medidas efectivas para proteger la información sensible durante el diseño y la implementación del módulo web. Esto incluyó la encriptación de contraseñas, la gestión adecuada de accesos y permisos, y la implementación de controles de seguridad robustos en todas las capas del sistema, asegurando así la integridad y confidencialidad de los datos. Por otra parte, el módulo web desarrollado contribuye directamente a mejorar la gestión de accesos a los aplicativos internos por parte de los usuarios de la universidad. Al proporcionar una plataforma centralizada y segura para la gestión de accesos, el módulo web facilita el control y la administración eficiente de los permisos de los usuarios, lo que optimiza los procesos internos y mejora la seguridad de la información.

Por último, con respecto a la Interfaz de usuario intuitiva y amigable, el desarrollo del módulo se centró en crear una interfaz de usuario que fuera fácil de usar y comprendida por los usuarios finales. La combinación de Angular, Angular Material y PrimeNG permitió diseñar una interfaz moderna y atractiva, con elementos visuales coherentes y una navegación intuitiva, lo que facilita la asignación y revocación de permisos de acceso, además, la interfaz facilita el proceso de asignación y revocación de permisos de acceso a las diferentes aplicaciones. Los usuarios autorizados pueden realizar estas acciones de manera rápida y sencilla, lo que agiliza los procesos de administración y contribuye a

una gestión más eficiente de los permisos. Sobre la optimización del flujo de trabajo, la implementación de la metodología XP permitió adaptar la interfaz de usuario a las necesidades reales de los usuarios mediante iteraciones cortas y entregas incrementales. Esto permitió una optimización continua del flujo de trabajo, asegurando que la interfaz satisficiera las expectativas de los usuarios y se ajustara a sus necesidades específicas. En relación a la mejora de la experiencia del usuario, los usuarios pueden realizar sus tareas de manera más eficiente y con menos fricción, lo que aumenta la satisfacción del usuario y mejora la productividad en general.

Recomendaciones

En cuanto al seguimiento de Políticas de Seguridad, se recomienda mantener un seguimiento constante de las políticas de seguridad establecidas por la universidad durante todo el desarrollo e implementación del módulo web. Esto garantizará la integridad y confidencialidad de los datos de acceso de los usuarios.

Con respecto a pruebas de usabilidad, sería beneficioso realizar pruebas exhaustivas de usabilidad con los usuarios finales antes de la implementación completa del módulo. Esto ayudará a identificar cualquier área de mejora en la interfaz de usuario y garantizará que sea intuitiva y fácil de usar para todos los usuarios.

En cuanto a la capacitación continua, a pesar de que la capacitación inicial se limita al personal encargado de la administración y uso del módulo, se sugiere ofrecer sesiones de capacitación adicionales de manera periódica para mantener actualizados a los usuarios y garantizar un uso óptimo del sistema.

Sobre el monitoreo de rendimiento del módulo, se recomienda establecer un sistema de monitoreo continuo del rendimiento del módulo una vez implementado. Esto permitirá identificar y abordar cualquier problema de rendimiento de manera oportuna, asegurando una experiencia fluida para los usuarios.

Por otra parte, en relación a la evaluación de impacto, después de la implementación del módulo, sería útil realizar una evaluación de impacto para medir su efectividad y eficiencia en la gestión de accesos a los aplicativos internos. Esto proporcionará información valiosa para futuras mejoras y optimizaciones.

También es importante establecer un plan de mantenimiento proactivo para el módulo web, que incluya actualizaciones regulares, parches de seguridad y correcciones de errores. Esto garantizará su funcionamiento óptimo a lo largo del tiempo.

Por último, se sugiere recopilar regularmente comentarios y sugerencias de los usuarios sobre el módulo web y utilizar esta retroalimentación para realizar mejoras continuas. Esto ayudará a asegurar que el módulo cumpla con las necesidades cambiantes de la comunidad universitaria.

Estas recomendaciones están diseñadas para ayudar a garantizar el éxito continuo del proyecto de desarrollo e implementación del módulo web para la gestión de accesos a los aplicativos internos de la universidad.

REFERENCIAS BIBLIOGRÁFICAS

- Ridge, B. V. (2023, August 20). *La Importancia de una Aplicación Web en la Era Digital*. MEDIUM Multimedia Agencia de Marketing Digital. <https://www.mediummultimedia.com/web/cual-es-la-importancia-de-una-aplicacion-web/>
- ¿Qué es Es Una Aplicación Monolítica Vs. Microservicios? (2021, July). Codster. <https://codster.io/blog/aplicacion-monolitica-vs-microservicios/>
- Salomao. (2023). Obtenido de <https://mindthegraph.com/blog/es/que-es-el-marco-teorico/#:~:text=Un%20marco%20te%C3%B3rico%20es%20un,conceptos%20clave%20que%20se%20estudian>
- Camacho. (2015). *Desarrollo de una plataforma web para el sistema de gestión de la información de proyectos de fiscalización realizados por la empresa Tecnie, accesible local y remotamente*. Epn.edu.ec. <https://doi.org/T-IE/4105/CD%206318>
- Enrique, J. (2017). *Implementación de sistema web para la gestión y ceontrol de los procesos de la unidad de titulación de la carrera de ingeniería en Sistemas de la universidad Salesiana, sede Guayaquil*. Ups.edu.ec. <https://dspace.ups.edu.ec/handle/123456789/14482>
- Aurelio. (2023). *Desarrollo de aplicación web para gestión de turnos en la escuela de educación básica particular Monseñor Roberto María Del Pozo*. Ups.edu.ec. <http://dspace.ups.edu.ec/handle/123456789/24734>
- Atehortua Gallo, J y Rendon Goez, M. (2021). *Desarrollo de una aplicación Web para la gestión de solicitudes, requerimientos e incidentes en la empresa Estructura IST, aplicando las buenas prácticas de ITIL v4. Tecnológico de Antioquia, Institución Universitaria*.

Fernández, L. (2020, August 18). Control de acceso: qué es y cómo ayuda a proteger nuestros datos. *RedesZone*; *RedesZone*.
<https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es>

Ceupe Magazine. (2020). Obtenido de Seguridad informática y análisis de datos:
<https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html>

Grupo Atico. (2024). Obtenido de Relación entre privacidad y ciberseguridad en la protección de datos: <https://protecciondatos-lopd.com/empresas/ciberseguridad-privacidad/#:~:text=Medidas%20como%20cifrado%20de%20bases%20de%20datos%2C%20acceso,de%20protecci%C3%B3n%20de%20datos%2C%20acuerdos%20de%20confidencialidad%2C%20etc.>

Reyes, Z., & Javier, C. (n.d.). NUEVAS TENDENCIAS EN DESARROLLO WEB.
<https://www.itcha.edu.sv/publicaciones/ITCHA/1167-2020-12-01/1167-ARTICULO---NUEVAS-TENDENCIAS-EN-DESARROLLO-WEB.pdf>

Blanton, S. (2023, February 17). ¿Qué es la gestión de usuarios? - *JumpCloud*.
JumpCloud Spanish. <https://jumpcloud.com/es/blog/what-is-user-management>

Betania V. (2022, February 9). ¿Qué es un servidor web y cómo funciona? *Tutoriales Hostinger*; *Tutoriales Hostinger*. <https://www.hostinger.es/tutoriales/que-es-un-servidor-web>

Editorial Etecé. (2013-2024). Servidor web. Obtenido de <https://concepto.de/servidor-web/>

Enciclopedia concepto. (2013-2024). Servidor web. Obtenido de <https://concepto.de/servidor-web/>

AWS. (2023). Amazon Web Services, Inc. Servidores web en comparación con servidores de aplicaciones: diferencia entre servidores tecnológico <https://aws.amazon.com/es/compare/the-difference-between-web-server-and-application-server/>

IBM Documentation. (2023, February 3). [ibm.com. https://www.ibm.com/docs/es/i/7.3?topic=serving-application-servers](https://www.ibm.com/docs/es/i/7.3?topic=serving-application-servers)

Blancarte, O. (2021). Arquitectura Cliente-Servidor. [Reactiveprogramming.io. https://reactiveprogramming.io/blog/es/estilos-arquitectonicos/cliente-servidor](https://reactiveprogramming.io/blog/es/estilos-arquitectonicos/cliente-servidor)

Jiménez, L. (2023, July 6). La arquitectura cliente-servidor: interacción entre sistemas. [Leojimzdev.com. https://leojimzdev.com/la-arquitectura-cliente-servidor-interaccion-entre-sistemas/](https://leojimzdev.com/la-arquitectura-cliente-servidor-interaccion-entre-sistemas/)

Cardozo, L. (2021, March 3). API: ¡Qué es API, ejemplos y su importancia! Zenvia; Zenvia Inc. <https://www.zenvia.com/es/blog/que-es-api/>

Walker, A. (12 de 2023). Obtenido de <https://www.guru99.com/es/what-is-api.html>

Monster Digital Agency. (2021, June 3). ¿Qué es el Backend? Descubre todo sobre este concepto. Epitech Spain. <https://www.epitech-it.es/backend/>

Arizbé. (2023). Obtenido de Backend: ¿Qué es y para qué sirve?: <https://www.gluo.mx/blog/backend-que-es-y-para-que-sirve>

Arizbé. (2023). Frontend: ¿Qué es y cuál es su importancia? Obtenido de <https://www.gluo.mx/blog/frontend-que-es-y-cual-es-su-importancia>

blog2. (Kiv October 23). *Frontend: La parte visual y funcional de una página web*. Kiwop.
<https://www.kiwop.com/blog/frontend>

(kiwop, 2023)

Arizbé. (2023). *Obtenido de Backend: ¿Qué es y para qué sirve?*:
<https://www.gluo.mx/blog/backend-que-es-y-para-que-sirve>

Arizbé. (2023). *Frontend: ¿Qué es y cuál es su importancia?* *Obtenido de*
<https://www.gluo.mx/blog/frontend-que-es-y-cual-es-su-importancia>

Ceupe Magazine. (2020). *Obtenido de Seguridad informática y análisis de datos:*
<https://www.ceupe.com/blog/seguridad-informatica-y-proteccion-de-datos.html>

Kiwop. (2023). *Frontend: la parte visual y funcional de una página web*. *Obtenido de*
<https://www.kiwop.com/blog/frontend>

Megapractical. (s.f.). *Metodologías de desarrollo de software*. *Obtenido de*
<https://cdn2.hubspot.net/hubfs/371274/Desarrollo%20de%20Software/metodologias%20de%20desarrollo%20de%20software.pdf>

Santander Universidades. (2023, December 15). *Metodologías de desarrollo software | Blog Santander Open Academy*. *Santanderopenacademy.com; Santander Universidades*. <https://www.santanderopenacademy.com/es/blog/metodologias-desarrollo-software.html>

Solera, S. (2022, April 27). *Las mejores metodologías para un correcto desarrollo de software*. *Occamagenciadigital.com*. <https://www.occamagenciadigital.com/blog/las-mejores-metodologias-para-un-correcto-desarrollo-de-software>

Raeburn, A. (2022, November 28). *¿Qué es la programación extrema (XP)? [2022]* • *Asana*. *Asana; Asana*. <https://asana.com/es/resources/extreme-programming-xp>

Marco metodológico: *¿Cómo redactar y cuál es su estructura?* (2022, September 9).
Normas APA. <https://normasapa.in/marco->

ANEXOS

Anexo 1. Cuestionario sobre la Gestión de Accesos para Usuarios en una Universidad

Cuestionario para el desarrollo de la aplicación web para gestionar la solicitud de tutorías académicas por los estudiantes en la Universidad Iberoamericana del Ecuador.

Objetivos del instrumento: Entender las necesidades y preferencias de los usuarios para el desarrollo exitoso del aplicativo web.

Instrucciones: Lea con detenimiento cada ítem presentado. En cada pregunta usted debe seleccionar, en el casillero correspondiente una opción, según considere pertinente.

Se agradece el compromiso y el tiempo que ha dedicado en responder todas las preguntas del cuestionario.

Dirigido a: Este cuestionario está dirigida a las personas que integran el grupo de soporte de la Unidad de Tecnologías de la Información y Comunicación UTIC's de la universidad en la cual está enfocado el desarrollo del presente módulo web.

Cuestionario

1.- ¿Son claros los procedimientos de gestión de permisos?

- a) Si
- b) No

2.- ¿Le resulta un proceso tedioso el cómo se maneja actualmente la gestión de permisos?

- a) Si
- b) No

3.- ¿Ha sido necesario que intervenga un desarrollador de aplicaciones en el proceso de asignación de permisos?

- a) Si
- b) No

4.- ¿Considera usted que el proceso actual de asignación de permisos necesita ser optimizado?

- a) Si
- b) No

5.- ¿Ha experimentado problemas al solicitar la asignación de permisos al analista de aplicaciones para el acceso de los usuarios en los aplicativos?

- a) Si
- b) No

6.- ¿Considera que se deberían emplear nuevas tecnologías en el desarrollo de los módulos de la Universidad?

- a) Si
- b) No

7.- ¿Cree que la colaboración entre UTICS y el analista de aplicaciones es eficiente?

- a) Si
- b) No

Anexo 2. Validaciones del instrumento

Validación de instrumento por MSc. Myriam Álvarez 1era Revisión

https://drive.google.com/file/d/1QUKgxnNnS3LUYto_ijYXjx9bqVAet6vp/view?usp=sharing

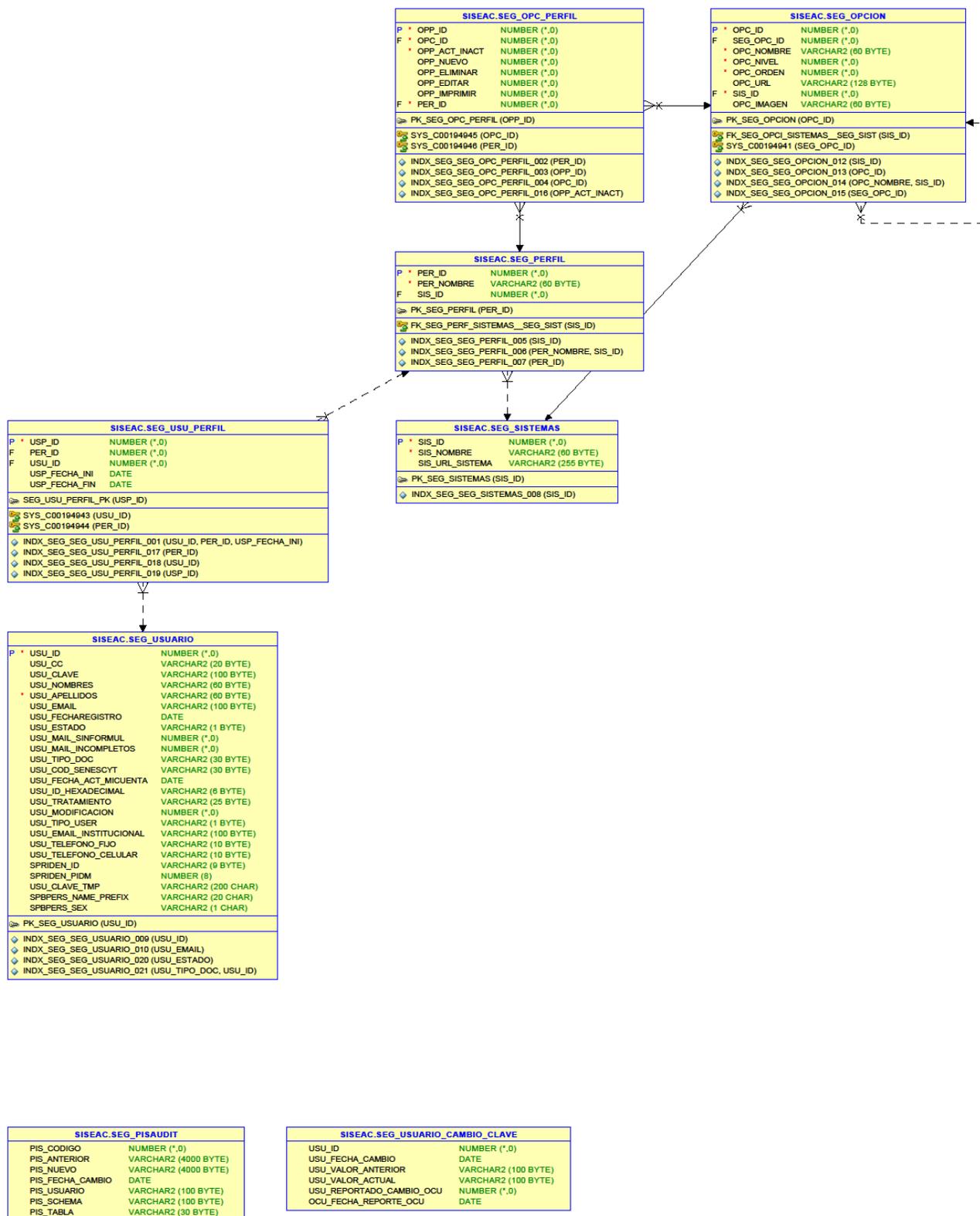
Validación de instrumento por MSc. Myriam Álvarez 2da Revisión

https://drive.google.com/file/d/1eM3lStvYPgfZT5U22NrLHC_pZhcgasuo/view?usp=sharing

Validación de instrumento por Msc. Harry Carpio

<https://drive.google.com/file/d/1LsKtRRgDN4GfpqMljpYNW1OHAOKSPxdG/view?usp=sharing>

Anexo 3. Tablas que conforman la base de datos del módulo de acceso



Anexo 4. Evaluación de la calidad del código

En esta sección se indicarán las pruebas implementadas para el módulo web gestión de usuarios.

Para las pruebas se utilizó una instancia de SonarQube. SonarQube, una herramienta de análisis estático de código abierto, desempeñó un papel integral en la evaluación de la calidad del código y la identificación de posibles problemas en el software.

En SonarQube, se asignan calificaciones basadas en las métricas y reglas analizadas para diferentes aspectos de la calidad del código, tales como seguridad, fiabilidad, seguridad y mantenibilidad. Estas calificaciones se representan con letras, como A, B, C, D y F, donde A indica una calidad excelente y F indica una calidad muy deficiente. A continuación, se explican el significado de cada una de las métricas que se aplicaran.

Fiabilidad

La fiabilidad en SonarQube mide la probabilidad de que un componente de software funcione sin fallos. Se calcula a partir de:

- **Densidad de defectos:** Número de defectos por cada 1.000 líneas de código (KLOC).
- **Complejidad ciclomática:** Medida de la complejidad de un programa, basada en el número de caminos independientes que pueden ejecutarse.

Objetivo: Un valor alto de fiabilidad indica que el software es menos propenso a fallar.

Seguridad

La seguridad en SonarQube mide la resistencia del software a ataques malintencionados. Se calcula a partir de:

- **Vulnerabilidades:** Número de vulnerabilidades conocidas que se encuentran en el código.
- **Puntos calientes de seguridad:** Líneas de código que son más propensas a ser explotadas por vulnerabilidades.
- **Huellas digitales de código OWASP:** Presencia de patrones de código que son conocidos por ser vulnerables a ataques.

Objetivo: Un valor alto de seguridad indica que el software es menos vulnerable a ataques.

Security Review

Realiza un análisis del código fuente de un software para identificar y corregir vulnerabilidades de seguridad. Este proceso se basa en una serie de reglas de seguridad predefinidas que se comparan con el código fuente.

Objetivo: Un valor alto de Security Review indica que el código es seguro lo que aumenta la confianza en su seguridad.

Mantenibilidad

La mantenibilidad en SonarQube mide la facilidad con la que el software puede ser modificado y actualizado. Se calcula a partir de:

- **Duplicación de código:** Porcentaje de código que se repite en diferentes partes del programa.
- **Complejidad del código:** Medida de la dificultad de entender y modificar el código.

Objetivo: Un valor alto de mantenibilidad indica que el software es más fácil de modificar y actualizar.

Para el uso de la herramienta SonarQube en el módulo web, se configuró en SonarQube que las pruebas se consideren aprobadas si todas las métricas obtienen una calificación de A; de lo contrario, la herramienta considerará las pruebas rechazadas. Con base en estas configuraciones, se escaneó el módulo web y se obtuvieron los siguientes resultados:

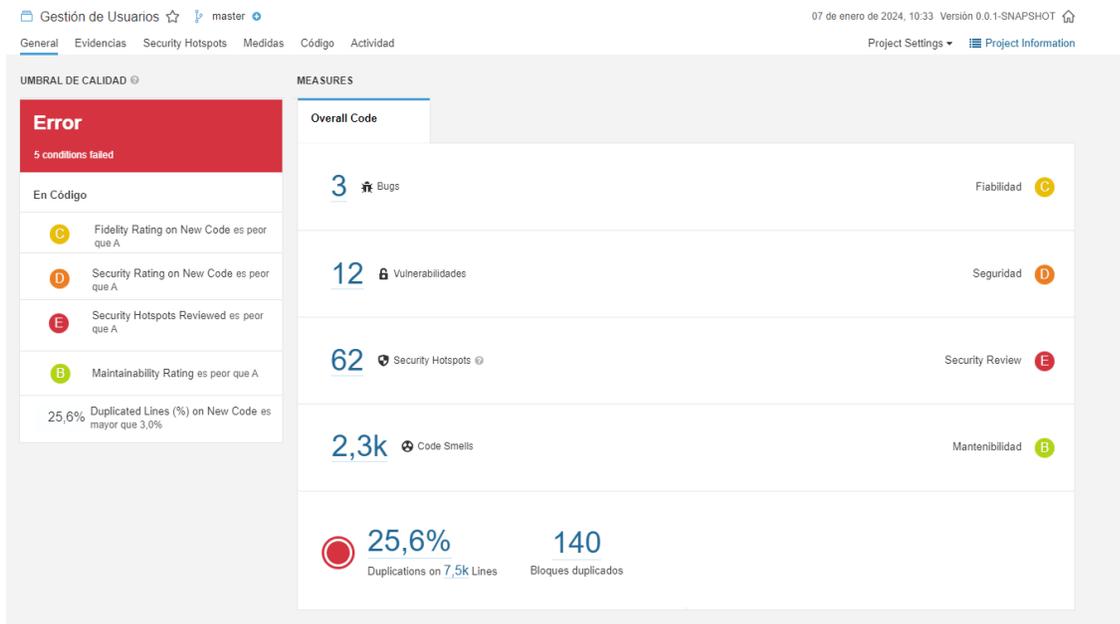


Figura 17 Resultados de las pruebas aplicadas al software del Módulo web

Como se puede apreciar en la figura 19, se obtuvieron las siguientes observaciones: 3 errores, 12 vulnerabilidades, 62 puntos críticos de seguridad y un 25.6% de duplicidad de código. Por lo tanto, se considera que las pruebas no fueron aprobadas debido a que no se cumplió con el umbral necesario, que en este caso sería obtener una calificación de A en todas las métricas.

Aplicación de correcciones:

Después de analizar y detectar los problemas en el módulo web durante el primer análisis, se procedió a aplicar las correcciones necesarias en diferentes iteraciones.

Posteriormente, se realizó un segundo análisis para verificar estas correcciones, obteniendo los siguientes resultados:

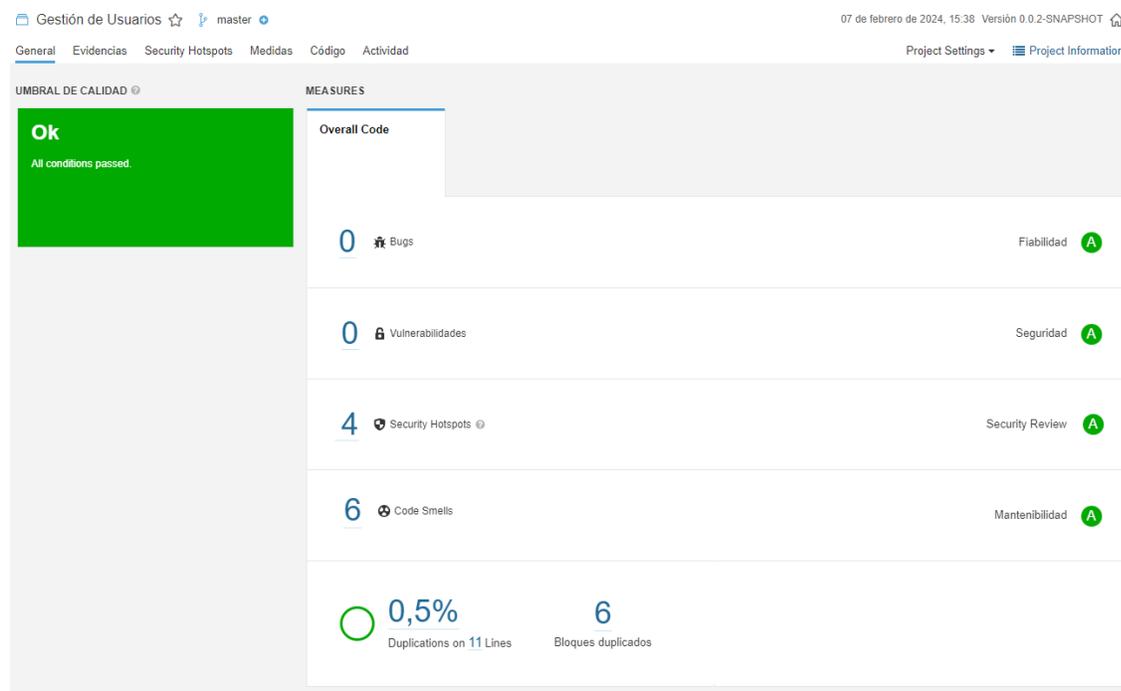


Figura 18 Resultados de la aplicación de correcciones

Como se puede apreciar en la figura 20, se obtuvieron las siguientes observaciones: 0 errores, 0 vulnerabilidades, 4 puntos críticos de seguridad y un 0.5% de duplicidad de código. Por lo tanto, se considera que las pruebas fueron aprobadas debido a que cumple con el umbral necesario, que en este caso sería obtener una calificación de A en todas las métricas.

En resumen, SonarQube ha cumplido con las métricas de calidad preestablecidas, con resultados sumamente satisfactorios en las pruebas realizadas.

Evidencia:

- Cumplimiento de métricas: SonarQube ha logrado alcanzar las metas de calidad fijadas previamente.
- Resultados de pruebas: Los casos de prueba arrojaron resultados altamente satisfactorios.

Impacto:

- Garantía de calidad: Se ha verificado que el producto cumple con los estándares de calidad esperados.
- Confianza en el producto: Los resultados de las pruebas brindan mayor seguridad en la confiabilidad del producto.

Recomendación:

Es recomendable continuar utilizando SonarQube para mantener y mejorar la calidad del producto