



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO

Instituto Tecnológico de Apizaco

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE APIZACO

ACCESO DIGITAL CARD-ITA: ANÁLISIS Y DISEÑO

TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

**PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

**PRESENTA:
STEPHANI NOYA HERNÁNDEZ**

**NOMBRE DEL ASESOR:
ING. MERCED PÉREZ MORENO**



APIZACO, TLAX., ENERO 2024



Apizaco, Tlaxcala, **09/agosto /2023**

OFICIO No: SC/OPV/167/23

ASUNTO: Liberación de proyecto
para titulación integral

MARTÍN ROJAS RAMÍREZ
JEFE DEL DEPTO. DE DIVISIÓN DE ESTUDIOS PROFESIONALES
P R E S E N T E.

POR ESTE MEDIO LE INFORMO QUE HA SIDO LIBERADO EL SIGUIENTE PROYECTO PARA LA TITULACIÓN INTEGRAL.

NOMBRE DEL EGRESADO:	STEPHANI NOYA HERNÁNDEZ
CARRERA:	INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
NO. DE CONTROL:	18370990
NOMBRE DEL PROYECTO:	ACCESO DIGITAL CARD- ITA: ANÁLISIS Y DISEÑO
PRODUCTO U OPCIÓN:	TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

AGRADEZCO DE ANTEMANO SU VALIOSO APOYO EN ESTA IMPORTANTE ACTIVIDAD PARA LA FORMACIÓN PROFESIONAL DE NUESTROS EGRESADOS.

ATENTAMENTE

*Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®*

ALAN AUGUSTO GALLEGOS CUELLAR
JEFE DEL DEPTO. DE SISTEMAS Y COMPUTACIÓN

c.c.p. División de Estudios Profesionales
c.c.p. Depto. de Servicios Escolares
c.c.p. Archivo
AAGC/mrol*



SECRETARÍA DE EDUCACIÓN PÚBLICA
NACIONAL
DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO
DEPARTAMENTO DE
SISTEMAS Y COMPUTACIÓN

MERCED PÉREZ MORENO
ASESOR INTERNO





EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO

Instituto Tecnológico de Apizaco
Subdirección de Planeación y Vinculación

Apizaco, Tlax., 10/enero/2024
No. OFICIO: DEP-CT/004/2024

ASUNTO: AUTORIZACIÓN DE IMPRESIÓN

STEPHANI NOYA HERNANDEZ
EGRESADA DE LA CARRERA DE
INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
CON NÚMERO DE CONTROL: 18370990
P R E S E N T E

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción **TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL** cuyo tema es: **"ACCESO DIGITAL CARD-ITA: ANÁLISIS Y DISEÑO"**, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga:

AUTORIZACIÓN DE IMPRESION

Debiendo entregar **3** empastados del mismo, apropiadamente encuadernados, a la brevedad, para presentar su acto de recepción profesional.

Sin otro particular por el momento, le envió un cordial saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®



MARTÍN ROJAS RAMÍREZ
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES

SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL
DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO
ESTUDIOS PROFESIONALES

c.p. archivo



INSTITUTO TECNOLÓGICO DE APIZACO



Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec, Municipio de Tzompantepec,
Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010 Ext. 304, e-mail:
dep_titulacion@apizaco.tecnm.mx



2024
Felipe Carrillo
PUERTO

Agradecimientos

Queridos seres queridos, compañeros de carrera y profesores.

Hoy, en este momento tan especial de mi vida, quiero expresar mi más profundo agradecimiento a cada uno de ustedes. Cada paso que he dado en este camino hacia la culminación de una etapa, ha estado lleno de desafíos, sacrificios y momentos inolvidables, y no podría haber llegado hasta aquí sin su apoyo incondicional.

En primer lugar, quiero dirigirme a mi amada familia. Mamá, Bertha Hernández González, tu valentía, esfuerzo y amor incansable han sido mi inspiración constante, gracias por ser mi ejemplo de fuerza y por sacrificar tanto para brindarnos un hogar lleno de amor y oportunidades.

Papá, Inocencio Noya Lugo, quiero agradecerte por tu apoyo y por brindarme las herramientas para enfrentar los desafíos de la vida.

Alejandro Noya, mi querido hermano, tu sonrisa y tu alegría contagiosa han sido mi motivación para superarme cada día. Los amo profundamente y estoy infinitamente agradecida por tenerlos en mi vida.

A mis compañeros de carrera, hoy celebramos juntos este logro, pero también quiero expresar mi gratitud por los momentos compartidos a lo largo de nuestros años de estudio. José Ángel Corona P., José Alfonso Lozano H. y Edgar García de la cadena Z. Han sido pilar fundamental en este arduo camino. Han estado allí en los momentos de estudio intenso, en las risas compartidas y en grandes desafíos. Agradezco su amistad, complicidad, compañía y apoyo constante, juntos hemos superado obstáculos y hemos celebrado los éxitos, y eso es algo que siempre atesoraré en mi corazón.

También quiero rendir homenaje a aquellos que, por diferentes razones, ya no están presentes en mi camino. Agradezco profundamente su influencia en mi formación como persona y profesional. Aunque el destino haya separado nuestros caminos, siempre llevaré en mi corazón los recuerdos compartidos. Envío un beso y un abrazo al cielo, con especial dedicación a mi querido Piolín, David...

Por último, quiero expresar mi gratitud a todos mis docentes y profesores. Han compartido su conocimiento, nutrido mi mente y han fomentado mi crecimiento académico. Agradezco su paciencia y dedicación para formar a profesionales comprometidos con la excelencia. A todos ustedes, mi familia, compañeros, amigos y profesores, les agradezco desde lo más profundo de mi corazón por su amor, apoyo y aliento a lo largo de este viaje. Han sido una fuente inagotable de inspiración y motivación, y gracias a su presencia y guía he logrado llegar a este importante hito en mi vida.

Con profundo agradecimiento.

Stephani Noya Hernández

Resumen

Las TIC'S están en constante cambio e impactando en todos los ámbitos de la sociedad, incluida la educación. La tecnología es una parte integral de la sociedad actual en constante avance. Como resultado, tenemos acceso a más conocimiento y la demanda de herramientas informáticas en la educación es cada vez más exigente. De esta forma, las TIC'S se han convertido en una herramienta de apoyo a las nuevas tecnologías en la educación.

La implementación de este proyecto implicará varios pasos clave, incluida la digitalización de los registros en papel existentes, el desarrollo de portales en línea y aplicaciones móviles para acceder al instituto y la implementación de medidas de seguridad para proteger los datos confidenciales. Además, el proyecto requerirá la colaboración entre la institución y de estudiantes inscritos en la misma, para garantizar la interoperabilidad de los registros digitales en diferentes sistemas y plataformas.

PALABRAS CLAVE: Credenciales de plástico, digitalización, Portal en línea, Aplicación móvil, Seguridad de datos, interoperabilidad, Eficiencia, Reducción de costo, Precisión de los datos, Integración de sistema, Almacenamiento digital.

Índice

Agradecimientos	I
Resumen	II
1. Introducción	1
2. Descripción de la empresa u organización y del puesto o área del trabajo el estudiante	2
3. Problemas a resolver, priorizándolos	5
4. Objetivos	5
5. Justificación	6
6. Descripción del proyecto	6
6.1 Alcances	7
6.2 Limitaciones	8
6.3 Delimitación	8
6.4 Antecedentes	8
7. Marco Teórico	10
7.1 Bases teóricas	10
7.1.1 Protocolo de investigación	10
7.1.3 Credenciales digitales	11
7.1.4 Transformación digital	11
7.1.5 Identidad digital	12
7.1.6 Gestión de identidades	12
7.1.7 Modelo de aceptación de tecnología (TAM)	13
7.1.8 Teoría de la identidad digital	13
7.1.9 Sistemas de información	14
7.1.10 Teoría del procesamiento	15
7.1.11 Seguridad de la información	15
7.1.12 Tecnología Blockchain	16
7.1.13 Diseño centrado en el ser humano	16
7.1.14 Ética digital	17
7.1.15 Aplicación móvil	17
7.1.16 Código QR	18
7.1.17 Usabilidad	18
7.1.18 Gestión de cambios	18

7.1.19 Adopción de tecnología.....	19
8. Desarrollo.....	20
8.1 Metodología.....	20
8.2 Ejecución de la metodología para el desarrollo del proyecto.....	22
8.2.1 Recopilación y análisis de requisitos.....	22
8.2.2 Diseño.....	23
8.2.3 Implementación.....	24
8.2.4 Prueba	25
8.2.5 Implementación y mantenimiento	26
8.3 Aplicar instrumento de evaluación.....	26
8.4 Desarrollo de las factibilidades del proyecto.....	28
8.5 Definición de requerimientos funcionales.....	28
8.6 Definición de requerimientos No funcionales	33
8.7 Diagrama de casos de uso	37
8.8 Depuración de casos de uso	41
8.9 Documentación de casos de uso	42
8.10 Pasos para crear un modelo de base de datos para el proyecto	47
8.10.1 Determinar el propósito de la base de datos	47
8.10.2 Identificar las entidades	48
9. Resultados.....	49
9.1 Presentación y discusión de los resultados	49
9.2 Modelamiento de base de datos.....	65
9.2.1 Defina los atributos	65
9.2.2 Definir las relaciones	66
9.2.3 Diseñe el esquema de la base de datos	67
9.2.4 Establezca las restricciones.....	68
9.3 Diagramas de secuencia	69
9.4 Diagramas de actividad	72
9.5 Selección de herramientas	73
9.6 Lista preliminar de clases	77
9.7 Diagrama de clases.....	79
9.8 Modelo Entidad Relación	81
9.9 Estructura y diseño del look and feel del sitio web	83

9.9.1 Login	84
9.9.2 Menú de navegación	85
9.9.3 Sección Inicio	87
9.9.4 Sección de Alumnos.....	89
9.9.5 Sección de Accesos	95
9.9.6 Perfil de Administrador	98
9.9.7 Paleta de colores	100
9.9.8 Tipografía	102
9.9.9 Tipografías a implementar.....	102
10. Estructura y diseño del Look and Feel de la app.....	103
10.1 Login	103
10.2 Credencial digital	104
10.3 Menú lateral	105
10.4 Perfil del alumno	106
10.5 Cerrar sesión	107
10.6 Paleta de colores	107
11. Diseño de los servicios a utilizar	109
11.1 Identifica las necesidades de los usuarios	109
11.2 Prioriza los servicios	110
11.3 Diseña la estructura y el flujo de la aplicación.....	110
12. Conclusiones	114
12.1 Recomendaciones	114
12.2 Experiencia profesional adquirida	115
13. Competencias desarrolladas	116
Fuentes de información	118

Índice de Figuras

Figura 1.- Foto del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco (2022)	2
Figura 2.- Localización del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco	3
Figura 3.- Modelo en cascada de cinco niveles, basado en las propuestas de Winston W. Royce. (IONOS, 2019)	20
Figura 4.- Diagrama casos de uso del acceso digital	40
Figura 5.- Casos de uso del administrador	41
Figura 6.- Casos de uso del estudiante	41
Figura 7.- Casos de uso completo	42
Figura 8.- Resultados pregunta 1.....	49
Figura 9.- Resultados pregunta 2.....	50
Figura 10.- Resultados pregunta 3.....	51
Figura 11.- Resultados pregunta 4.....	52
Figura 12.- Resultados pregunta 5.....	53
Figura 13.- Resultados pregunta 6.....	54
Figura 14.- Resultados pregunta 7.....	55
Figura 15.- Resultados pregunta 8.....	57
Figura 16.- Resultados pregunta 9.....	58
Figura 17.- Resultados pregunta 10.....	59
Figura 18.- Resultados pregunta 11.....	60
Figura 19.- Resultados pregunta 12.....	62
Figura 20.- Resultados pregunta 13.....	63
Figura 21.- Diagrama Entidad Relación del sistema	67
Figura 22.- Diagrama de secuencia de inicio de sesión Alumno a la aplicación.....	69
Figura 23.- Diagrama de secuencia de acceso	70
Figura 24.- Diagrama de secuencia de autorización de administrador	71
Figura 25.- Diagrama de clases del sistema	79
Figura 26.- Modelo Entidad Relación	81
Figura 27.- Panel Login del sitio web administrador	84
Figura 29.- Mensaje de error.....	84
Figura 28.- Mensaje de Login Exitoso	84
Figura 30.- Cifrado de contraseña	85
Figura 31.- Redireccionamiento de Login a pantalla de inicio del sitio web administrador	85
Figura 32.- Menú de navegación del sitio web administrador	86
Figura 33.- Sección inicio página web para administrador	87
Figura 34.- Graficas de resumen sección inicio	88
Figura 35.- Acceso rápido de sección Inicio	89
Figura 36.- Sección alumnos página web para administrador	89
Figura 37.- Lista de Alumnos de la sección alumnos del sitio web administrador	90
Figura 38.- Detalles de Alumno	90
Figura 39.- Agregar alumno de la sección Alumnos del sitio web administrador	92
Figura 40.- Mensaje de confirmación Agregar alumno	92
Figura 41.- Editar Información Alumno	92
Figura 42.- Actualizar Información Alumno	93

Figura 43.- Eliminar Alumno	93
Figura 44.- Mensaje de confirmación Eliminar alumno	94
Figura 45.- Búsqueda de Alumnos	94
Figura 46.- Sección Accesos.....	95
Figura 47.- Registro de accesos en tiempo real	96
Figura 48.- Filtro de Accesos por Día de la Semana	96
Figura 49.- Detalles de Acceso del Estudiante	97
Figura 50.- Resumen de Accesos	97
Figura 51.- Búsqueda Acceso.....	98
Figura 52.- Icono usuario Administrador	98
Figura 53.- Menú desplegable	98
Figura 54.- Perfil de Administrador	99
Figura 55.- Mensaje para agregar Administrador	99
Figura 56.- Agregar Administradores	99
Figura 57.- Mensaje de eliminar Administrador	100
Figura 58.- Eliminar Admin	100
Figura 59.- Actualizar Admin	100
Figura 60.- Editar Administrador	100
Figura 61.- Log Out Admin.....	100
Figura 62.- Paleta de colores Sitio Web	101
Figura 63.- Variación de colores	101
Figura 64.- Tipografía Arial	102
Figura 65.- Tipografía Helvetica.....	102
Figura 66.- Tipografía Open Sans.....	103
Figura 67.- Mensaje Login credenciales correctas.....	104
Figura 68.- Mensaje Login credenciales incorrectas	104
Figura 69.- Login App.....	104
Figura 70.- Credencial digital App.....	105
Figura 71.- Menú lateral de la App	106
Figura 72.- Sección Perfil de la App	106
Figura 73.- Log out App	107
Figura 74.- Paleta de colores App.....	108
Figura 75.- Variación de colores App.....	108
Figura 76.-Proceso de Login de la aplicación.....	111
Figura 77.- Diagrama para visualizar un estudiante	111
Figura 78.- Diagrama para Editar un estudiante.....	112
Figura 79.- Diagrama para Crear un nuevo estudiante.....	113
Figura 80.- Diagrama para Eliminar un estudiante	113

Índice de tablas

Tabla 1.- Requerimiento funcional RF0	29
Tabla 2.- Requerimiento funcional RF1	29

Tabla 3.- Requerimiento funcional RF2	29
Tabla 4.- Requerimiento funcional RF3	29
Tabla 5.- Requerimiento funcional RF4	30
Tabla 6.- Requerimiento funcional RF5	30
Tabla 7.- Requerimiento funcional RF6	30
Tabla 8.- Requerimiento funcional RF7	31
Tabla 9.- Requerimiento funcional RF8	31
Tabla 10.- Requerimiento funcional RF9	31
Tabla 11.- Requerimiento funcional RF10	32
Tabla 12.- Requerimiento funcional RF11	32
Tabla 13.- Requerimiento funcional RF12	32
Tabla 14.- Requerimiento funcional RF13	32
Tabla 15.- Requerimiento funcional RF14	33
Tabla 16.- Requerimiento No funcional RNF1	33
Tabla 17.- Requerimiento No funcional RNF2	34
Tabla 18.- Requerimiento No funcional RNF3	34
Tabla 19.- Requerimiento No funcional RNF4	34
Tabla 20.- Requerimiento No funcional RNF5	35
Tabla 21.- Requerimiento No funcional RNF6	35
Tabla 22.- Requerimiento No funcional RNF7	35
Tabla 23.- Requerimiento No funcional RNF8	36
Tabla 24.- Requerimiento No funcional RNF9	36
Tabla 25.- Requerimiento No funcional RNF10	36
Tabla 26.- Requerimiento No funcional RNF11	36
Tabla 27.- Requerimiento No funcional RNF12	37

Índice de anexos

ANEXO 1 ENCUESTA	119
ANEXO 2 GLOSARIO DE TÉRMINOS	119

1. Introducción

La digitalización de las credenciales escolares se refiere al proceso de convertir las credenciales educativas tradicionales de plástico, a formato digital. Esta transformación permite a los estudiantes identificarse como estudiantes, acceder a la institución y las áreas de servicios que esta ofrece, verificar sus credenciales académicas de manera fácil y segura mediante dispositivos digitales y plataformas en línea.

Para la institución educativa, la digitalización de las credenciales escolares puede agilizar los procesos administrativos y reducir los costos asociados con la producción de credenciales de plástico, almacenamiento y la gestión de registros en papel. También puede ayudar a aumentar la precisión y la seguridad de los datos, ya que los registros digitales se pueden cifrar y proteger contra el acceso no autorizado.

Las principales ventajas de digitalizar las credenciales escolares son la comodidad, la accesibilidad y la seguridad. Se puede acceder fácilmente a las credenciales digitales desde cualquier lugar, en cualquier momento, usando un dispositivo móvil. Esto elimina la necesidad de que los estudiantes lleven documentos físicos y les permite acceder a la institución educativa de forma más rápida, sencilla y segura.

Las credenciales escolares digitalizadas son más seguras que las que están en plástico, ya que pueden cifrarse y protegerse mediante firmas digitales y otras medidas de seguridad. Esto hace que sea mucho más difícil para los estafadores alterar o falsificar credenciales académicas, lo que reduce el riesgo de robo de identidad y otras formas de fraude.

En general, la digitalización de las credenciales escolares tiene el potencial de simplificar y acelerar el proceso de acceso, además de puede ayudar a modernizar y mejorar la eficiencia del sistema educativo, facilitando que los estudiantes accedan a las oportunidades educativas que necesitan para tener éxito en sus carreras.

2. Descripción de la empresa u organización y del puesto o área del trabajo el estudiante

Datos de la empresa

La historia de la sociedad tlaxcalteca, ha sido marcada e impulsada por el trabajo, el compromiso y la visión de hombres y mujeres que con determinación y ahínco han buscado el desarrollo del estado.

Sin duda, personalidades de gran trascendencia como Don Emilio Sánchez Piedras, entonces Gobernador Constitucional, comprometido con la juventud del estado, contando con el apoyo decisivo del Presidente de la República, el Lic. Luis Echeverría Álvarez, personaje visionario del futuro de la educación y de la juventud de esta región del país, gestiona y funda el Instituto Tecnológico Regional de Apizaco e inicia sus actividades el 1 de octubre del año de 1975.

El Tecnológico de Apizaco, desde hace más de cuatro décadas, se ha dedicado a propiciar alternativas reales y sustentables para la juventud de la región. Es una Institución que pertenece al Tecnológico Nacional de México, del cual formamos parte de 254 Tecnológicos distribuidos en los 32 estados del país.

El ITA ofrece en su formación educativa 9 Ingenierías, 3 Maestrías y un Doctorado, cuyas matrículas abarcan de manera integral una formación general básica que incluye el fortalecimiento científico y metodológico; todas las carreras cuentan con especialidades diseñadas para atender las necesidades de los sectores productivo y social. Los planes de estudio están basados en una estructura genérica, una especialidad y una residencia profesional.

Figura 1.- Foto del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco (2022)



En la Figura 1.- Foto del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco (2022), muestra lo siguiente: Foto vista aérea del Instituto Tecnológico de Apizaco del año 2022

Lugar donde se realizará el proyecto

Nombre: Tecnológico Nacional de México/Instituto Tecnológico de Apizaco

Dirección: Carretera Apizaco Tzompantepec, esquina con Av. Instituto Tecnológico S/N, Conurbado Apizaco – Tzompantepec

Teléfono: 2414172010 o 2414180321

Nombre del titular de la empresa: Sergio Octavio Rosales Aguayo

Sitio Web: <https://www.apizaco.tecnm.mx/>

Mapa de localización

Figura 2.- Localización del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco



En la Figura 2.- Muestra la Localización del Tecnológico Nacional de México/Instituto Tecnológico de Apizaco, muestra lo siguiente: Localización de la institución en vista de Google maps

Es una Institución de Servicios de Educación Superior Tecnológica comprometida en la formación de profesionales, que responde a los requerimientos de desarrollo Económico, Científico, Social y Cultural que demanda nuestro entorno, a través de la adecuada integración de nuestros recursos. Tecnológico Nacional de México/Instituto Tecnológico de Apizaco, desde más de cuatro décadas, se ha dedicado a propiciar alternativas reales y sustentables para la juventud de la región. Es una Institución que pertenece al Tecnológico Nacional de México, del cual formamos parte más de 261 Tecnológicos distribuidos en los 32 estados del país.

Misión:

Formar profesionistas que sean líderes visionarios, emprendedores, con capacidad de generar soluciones disruptivas, innovando en la ciencia y la tecnología, comprometidos con el desarrollo económico, responsabilidad social teniendo una visión sostenible y sustentable.

Visión:

Ser una Institución de educación superior tecnológica de vanguardia, formadora de ciudadanos del mundo, con conocimientos intercultural, respetando la diversidad social.

Valores:**Honestidad:**

Se demuestra día a día a través de la transparencia con la ejecución de las actividades laborales cotidianas.

Responsabilidad:

Es la actitud que caracteriza al personal en el cumplimiento de su tarea con eficacia y eficiencia en beneficio de la comunidad.

Lealtad:

Es la actitud que caracteriza al personal del Instituto Tecnológico de Apizaco, aplica sus conocimientos y habilidades en el logro de las metas institucionales, sin olvidar en ningún momento el lema:

“Pensar para servir, servir para triunfar ® ”

Área de trabajo del residente

El departamento de sistemas y computación

Resumen de las funciones del departamento:

Planear, coordinar, controlar y evaluar las actividades de docencia, investigación y vinculación en las áreas correspondientes a sistemas y computación que se imparten en el instituto tecnológico, de conformidad con las normas y lineamientos establecidos por la Secretaría de Educación Pública. Coordinar las actividades del departamento con las demás áreas de la Subdirección Académica. Elaborar el programa operativo anual y el anteproyecto de presupuesto del departamento y presentarlos a la Subdirección Académica para lo conducente.

3. Problemas a resolver, priorizándolos

El problema del uso de credenciales plásticas en el Instituto Tecnológico Nacional de México/ Instituto Tecnológico Apizaco, donde la División de Estudios Profesionales del Instituto Tecnológico Nacional de México/Instituto Tecnológico de Apizaco hay 3,877 estudiantes en el periodo enejun2023, donde necesitan portar una credencial de plástico, lo que lleva a un problema de vulnerabilidades de datos personales de los estudiantes, las credenciales de plástico se pueden extraviar, robar o clonar, lo que genera vulnerabilidades de seguridad en el sistema. Esto como resultante el acceso no autorizado a instalaciones y áreas de servicio. Así mismo el proceso de emisión y gestión de credenciales de plástico puede ser ineficiente, lo que genera largos tiempos de espera para los usuarios y cargas laborales para el personal del área correspondiente de emitir las credenciales, puede haber problemas con retrasos en la obtención de credenciales o errores en la información de las credenciales, todo esto nos lleva al Impacto ambiental, la producción de credenciales de plástico tienen un impacto negativo en el medio ambiente, contribuyendo a la generación de desechos y contaminación.

4. Objetivos

Objetivo general

El objetivo general es crear una aplicación para dispositivos móviles que sustituya la credencial de plástico y se genere una credencial digital mediante la utilización de un código QR esto para poder acceder al Instituto Tecnológico Nacional de México/Instituto Tecnológico de Apizaco.

Para llevar a cabo este objetivo se analizó que la mayoría de los usuarios utilizan un Smartphone, así es que se le facilita al usuario acceder de forma más rápida mediante la aplicación e ingresar a la institución ya que en ocasiones algunos alumnos llegan a olvidar su credencial, como tal la implementación de una aplicación móvil nos dará el rápido acceso al instituto del mismo modo podrá ser una forma de identificación para poder demostrar que son estudiantes del tecnológico.

Objetivos específicos

- Un mejor control de acceso y seguro para los datos personales de los estudiantes.
- Un control de acceso más seguro y eficaz para los datos personales de los estudiantes.
- Aumentar la seguridad de información personal de los alumnos.
- Brindar una alternativa al uso del plástico.

- Hacer una mejora con el uso de las Tics.

5. Justificación

Con el paso de los años, se ha ido implantando el uso de la tecnología en nuestra vida cotidiana hasta el punto de que ahora resulta complicado realizar algunas tareas o trabajos sin tecnología. Actualmente podemos decir que casi el 78% de todo lo que realizamos en el día está respaldado por la tecnología.

Los móviles han cobrado una gran importancia en nuestra vida y con ellos, han llegado las Apps móviles, que nos ayudan a tener cualquier servicio a la mano.

Para abordar estos problemas, el Instituto Tecnológico Nacional de México/Instituto Tecnológico de Apizaco podría considerar implementar un sistema más seguro y eficiente para emitir y administrar credenciales, como el uso de un sistema de credenciales digitales ya que la mayoría de los estudiantes cuentan con teléfonos móviles y acceso a Internet, estas herramientas se han convertido necesarias para las actividades diarias, debido a que las aplicaciones móviles (apps) son capaces de realizar funciones más específicas, por lo que se ha decidido hacer uso de las TICS. Disponibilidad de soporte técnico: La implementación de un nuevo sistema puede requerir un soporte técnico eficiente y oportuno. Los problemas técnicos o consultas de los usuarios relacionadas con las credenciales digitales deberán ser atendidos adecuadamente para garantizar un funcionamiento sin problemas.

El desarrollo de una aplicación móvil para el Instituto Tecnológico Nacional de México/Instituto tecnológico de Apizaco dará un valor agregado a los servicios que esta institución ofrece a sus alumnos, abriendo camino al desarrollo de nuevas soluciones que permitan acceder a la información en cualquier momento y desde cualquier lugar. La nueva tendencia de la tecnología es dar a los usuarios la posibilidad de tener todo lo que pueden llegar a necesitar en un dispositivo que brinde la capacidad de acceder a la información y a los servicios en cualquier momento.

El presente proyecto tiene como finalidad desarrollar una aplicación móvil, como medio viable que facilite el acceso de alumnos en caso de olvidar, extraviar o el desgaste de la credencial física. Brindando así un nuevo sistema de acceso a la institución.

6. Descripción del proyecto

El proyecto tiene como objetivo crear una aplicación móvil donde se encuentre en esta una credencial digital que permita a los estudiantes acceder al instituto por

medio de un código QR, el cual será escaneado en un lector de códigos QR en los accesos del instituto, eliminando la necesidad de credenciales de plástico.

El proyecto implica identificar la información requerida para crear las credenciales digitales, diseñar una plataforma segura con autenticación y encriptación, desarrollar una base de datos, probar la plataforma y brindar capacitación y soporte a los usuarios. Este proyecto tiene el potencial de mejorar la seguridad de datos personales, reducir la carga administrativa y mejorar la experiencia del usuario.

Aquí una breve descripción de cómo se ejecuta este proyecto:

Diseñar una plataforma digital: El siguiente paso sería diseñar una plataforma digital que pueda almacenar todos los datos de forma segura. La plataforma debe ser fácil de usar y debe ser accesible para estudiantes y administradores.

Integrar medidas de autenticación y seguridad: La plataforma debe incluir fuertes medidas de autenticación y seguridad para garantizar que solo las personas autorizadas puedan acceder a la información de las credenciales y al administrador. Esto incluye autenticación multifactor, protección con contraseña y encriptación.

Desarrollar una base de datos: Se debe desarrollar una base de datos para almacenar todas las credenciales digitalmente. Esta base de datos debe ser segura y debe poder manejar grandes volúmenes de datos.

Prueba y lanzamiento: La plataforma debe probarse exhaustivamente para asegurarse de que funciona según lo previsto. Una vez que se completan las pruebas, la plataforma se puede iniciar y poner a disposición de todos los estudiantes.

Brindar capacitación y soporte: Se debe brindar capacitación y soporte para garantizar que todos los usuarios puedan acceder a sus credenciales digitales. Esto podría incluir tutoriales en línea, soporte técnico y sesiones de capacitación.

6.1 Alcances

El presente documento contempla las líneas a seguir para desarrollar el proyecto de digitalización de credenciales escolares de los estudiantes universitarios haciendo uso de un tipo de tecnología contactless, como lo son los códigos QR (Quick Response Barcode) cuyo significado es Códigos de Respuesta Rápida, ya que actualmente, la universidad emite credenciales de plástico a estudiantes para acceder a las instalaciones del campus. Sin embargo, este sistema está desactualizado y presenta riesgos de seguridad. Para abordar estos problemas, el presente proyecto ha decidido digitalizar estas credenciales de plástico y reemplazarlas con un nuevo sistema, creando una plataforma digital que permita a

los estudiantes acceder a las instalaciones del campus a través de sus dispositivos móviles, el sistema debe ser seguro, confiable y fácil de usar, además de realizar la Integración de este sistema en el instituto.

6.2 Limitaciones

Si bien las credenciales digitales pueden ofrecer muchos beneficios para acceder a la universidad, también existen algunas limitaciones a considerar.

Problemas técnicos: Las credenciales digitales dependen de la tecnología, que puede ser propensa a fallas, mal funcionamiento o intentos de piratería. Si el sistema cae, o si hay problemas con las credenciales digitales, los estudiantes y el personal pueden no poder acceder a la universidad.

Costos: La implementación de sistemas de credenciales digitales puede ser costoso para las universidades, y puede haber costos continuos asociados con el mantenimiento y la actualización de los sistemas.

Preocupaciones de seguridad: Las credenciales digitales pueden estar sujetas a riesgos de seguridad, como el robo de identidad o el acceso no autorizado.

En general, las credenciales digitales pueden ofrecer muchos beneficios, pero es importante considerar cuidadosamente las posibles limitaciones y desafíos antes de implementarlos.

6.3 Delimitación

La integración de las tecnologías de la información y comunicaciones (TIC'S), está cada vez más presente en la vida diaria de las personas, y son muy importantes en la evolución de primeras tecnologías y que han ido en incremento en los últimos años, El proyecto buscará la sustitución de la credencial física de plástico, Se presenta una aplicación móvil diseñada únicamente para ejecutarse en dispositivos móviles Android, El proyecto está limitado solamente al uso de la aplicación, la aplicación será ejecutada únicamente en versiones Android 9 y posteriores, La aplicación está sujeta a funcionar únicamente con conexión a internet.

6.4 Antecedentes

El antecedente del proyecto de digitalización de credenciales de plástico para permitir el acceso a la universidad implica la necesidad de modernizar el proceso de verificación y otorgamiento de acceso a estudiantes.

Tradicionalmente, las universidades han emitido credenciales de plástico, como tarjetas de identificación o tarjetas de acceso, que las personas llevan físicamente para otorgar acceso a diversas instalaciones y áreas de servicios en el campus. Sin embargo, estas credenciales de plástico a menudo se pierden, son robadas, dañadas, lo que puede crear riesgos de seguridad, inconvenientes y gastos económicos por reposición para los estudiantes y la universidad, de igual manera los desechos de las credenciales de plástico contribuyen al cambio climático ya que La producción de plásticos contribuye en gran medida al cambio climático. Los residuos plásticos también ahogan nuestras vías fluviales, contaminan nuestros océanos, matan la vida silvestre y se infiltran en nuestra cadena alimentaria.

La digitalización de credenciales de plástico es una solución que aprovecha la tecnología para hacer que el proceso sea más seguro, eficiente y conveniente. Al reemplazar las credenciales de plástico con versiones digitales, las personas pueden acceder a las instalaciones y áreas de servicios del campus utilizando sus dispositivos móviles. Esto elimina la necesidad de tarjetas físicas y reduce el riesgo de extravió, robo, daño y contaminación del medio ambiente.

7. Marco Teórico

El marco teórico del proyecto de digitalización de credenciales de plástico para el acceso a la universidad involucrará varios conceptos y teorías clave.

7.1 Bases teóricas

Las bases teóricas del proyecto de digitalización de credenciales de plástico que permitir el acceso a la universidad, se pueden explicar a partir de los siguientes conceptos:

7.1.1 Protocolo de investigación

Un proyecto de digitalización de credenciales de plástico consiste en convertir credenciales físicas, como tarjetas de identificación, licencias de conducir y pasaportes, en formato digital. Aquí el protocolo de investigación para el proyecto:

Identifique a las partes interesadas del proyecto: identifique a todas las partes interesadas involucradas en el proyecto, incluido el patrocinador del proyecto, el equipo del proyecto, los usuarios finales y otras partes interesadas.

Definir el alcance y los objetivos del proyecto: defina claramente el alcance y los objetivos del proyecto, incluidas las credenciales que se digitalizarán, las tecnologías que se utilizarán y el cronograma del proyecto.

Realizar una evaluación de riesgos: Realice una evaluación de riesgos para identificar riesgos potenciales y desarrollar un plan de gestión de riesgos. Los riesgos pueden incluir violaciones de la seguridad de los datos, fallas del sistema o incumplimiento de los requisitos legales y reglamentarios.

Desarrollar los requisitos del proyecto: Desarrolle una lista detallada de los requisitos para el proyecto, incluido el hardware y el software necesarios, los requisitos de seguridad y privacidad de los datos y los requisitos de la interfaz de usuario.

Determinar las fuentes de datos: identifique las fuentes de los datos que se digitalizarán, incluidos los documentos físicos y las bases de datos.

Desarrollar un plan de administración de datos: Desarrolle un plan para administrar los datos a lo largo del proyecto, incluida la limpieza de datos, la migración de datos y el almacenamiento de datos.

Desarrollar un plan de prueba: Desarrolle un plan para probar las credenciales digitalizadas, incluidas las pruebas unitarias, las pruebas de integración y las pruebas del sistema.

Desarrollar un plan de capacitación: Desarrolle un plan para capacitar a los usuarios finales sobre cómo usar las credenciales digitalizadas, incluido cualquier nuevo software o hardware que sea necesario.

Desarrollar un plan de implementación: Desarrolle un plan para implementar las credenciales digitalizadas a los usuarios finales, incluidos los esfuerzos de comunicación o marketing necesarios.

Desarrollar un plan de mantenimiento y soporte: Desarrolle un plan para mantener y respaldar el sistema, incluidas las actualizaciones, actualizaciones o correcciones de errores necesarias.

Implementar el proyecto: Implementar el proyecto de acuerdo con el plan, monitorear el progreso y hacer los ajustes necesarios.

Evaluar el proyecto: Evaluar el éxito del proyecto e identificar áreas de mejora para futuros proyectos.

Seguir este protocolo de investigación ayudará a garantizar un proyecto exitoso de digitalización de credenciales de plástico.

7.1.3 Credenciales digitales

Las credenciales digitales se están volviendo cada vez más importantes para acceder a las universidades y otras instituciones educativas, ya que brindan una forma segura y portátil de representar la información de una persona.

El IMS Global Learning Consortium define las credenciales digitales como "representaciones electrónicas validadas, estandarizadas y portátiles de una calificación, logro, habilidad o interés".

Credenciales verificables: las Credenciales verificables son un tipo de credencial digital que permite a las personas probar su identidad, calificaciones y otros atributos de manera segura y preservando la privacidad. Estas credenciales se basan en estándares descentralizados e interoperables, como el modelo de datos de credenciales verificables W3C.

7.1.4 Transformación digital

La transformación digital se refiere a la integración de la tecnología digital en todos los aspectos de las operaciones de una organización, lo que genera cambios fundamentales en la forma en que la organización opera y entrega valor a sus partes interesadas. Una de las áreas donde la transformación digital está cobrando fuerza es en la creación de credenciales digitales para el acceso a la universidad.

La digitalización de las credenciales de plástico es parte de una tendencia más amplia hacia la transformación digital en muchas industrias, incluida la educación. El proyecto tiene como objetivo aprovechar la tecnología digital para mejorar la eficiencia y eficacia de los procesos de acceso a la universidad. Altbach, P. G. y De Wit, H. (2017).

Este artículo analiza cómo la transformación digital de la educación superior ha abierto nuevas oportunidades para la internacionalización y la creación de credenciales digitales. Gasevic, D., Jovanovic, J. y Pardo, A. (2017).

7.1.5 Identidad digital

La identidad digital se puede definir como la representación digital de un individuo o entidad que incluye sus características, atributos y comportamientos, que se utilizan para identificarlos en el mundo digital. Puede incluir datos personales como nombre, dirección de correo electrónico, cuentas de redes sociales, dirección IP e identificadores de dispositivos, entre otros. La digitalización de las credenciales de plástico para permitir el acceso a la universidad es un paso hacia la creación de una identidad digital para los estudiantes y el personal, que se puede utilizar para autenticar su identidad y otorgar acceso a los recursos.

De acuerdo con el Reglamento General de Protección de Datos de la Unión Europea (GDPR), la identidad digital es "cualquier información relacionada con una persona física identificada o identificable, una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física" (Artículo 4).

7.1.6 Gestión de identidades

La gestión de identidad se refiere al proceso de gestión y control de identidades digitales de personas, sistemas y dispositivos dentro de una organización o red. Abarca la creación, mantenimiento y terminación de identidades digitales, así como las políticas y procedimientos que rigen el acceso y uso de recursos digitales. Al digitalizar las credenciales de plástico, las universidades pueden implementar un sistema de gestión de identidad que puede controlar el acceso a los recursos y áreas de servicios del campus.

Según Gartner, "Identity and Access Management (IAM), en español como la Administración de identidad y acceso, es la disciplina de seguridad que permite a las personas adecuadas acceder a los recursos correctos en el momento correcto por las razones correctas." (Gartner, "Identity and Access Management (IAM)", July 2020)

La gestión de identidades se está volviendo cada vez más importante a medida que las organizaciones buscan gestionar el acceso a información y aplicaciones confidenciales, cumplir con las regulaciones y protegerse contra amenazas cibernéticas. Como afirma Forrester, "La identidad es la base de la confianza digital,

y las prácticas sólidas de administración de identidad son esenciales para una postura de seguridad sólida."(Forrester, "The Future of Identity And Access Management", May 2021)

La gestión eficaz de la identidad implica una combinación de soluciones tecnológicas, políticas y procedimientos. Esto puede incluir mecanismos de autenticación, autorización y control de acceso de usuarios, así como procesos de gobierno y administración de identidades. Como señaló el Instituto Nacional de Estándares y Tecnología (NIST), "la gestión de la identidad es un proceso complejo que implica equilibrar la seguridad y la facilidad de uso mientras se gestiona el acceso a los recursos y se protege la información confidencial." (NIST, "Identity and Access Management", October 2020)

7.1.7 Modelo de aceptación de tecnología (TAM)

El Modelo de Aceptación de Tecnología (TAM) es una teoría ampliamente utilizada en el campo de los sistemas de información que tiene como objetivo explicar y predecir la aceptación y el uso de la tecnología por parte de los usuarios. TAM fue propuesto por primera vez por Davis en 1989 y desde entonces ha sido objeto de varias mejoras y ampliaciones. En el contexto de este proyecto, el TAM se utilizaría para comprender los factores que influyen en la disposición de los estudiantes a adoptar credenciales digitales para acceder a la universidad.

El núcleo del modelo es la suposición de que la utilidad percibida (PU) y la facilidad de uso percibida (PEOU) son los dos determinantes principales de las actitudes e intenciones de los usuarios hacia el uso de una tecnología. PU se refiere al grado en que un usuario percibe que una tecnología mejorará su desempeño laboral o productividad, mientras que PEOU se refiere al grado en que un usuario percibe que una tecnología es fácil de usar y aprender.

Varios estudios han respaldado la validez y utilidad de TAM para explicar la aceptación y adopción de diversas tecnologías por parte de los usuarios. Por ejemplo, un estudio realizado por Venkatesh y Davis (2000) encontró que PU y PEOU predijeron significativamente las intenciones de los usuarios de adoptar una nueva aplicación de software. Además, un metanálisis de Venkatesh et al. (2003) sugirieron que TAM es un modelo sólido y confiable que se puede usar para explicar la adopción de tecnología en una amplia gama de contextos y entornos.

7.1.8 Teoría de la identidad digital

La Teoría de la Identidad Digital es un marco teórico que busca explicar cómo los individuos forman y expresan sus identidades en línea. Esta teoría se basa en la idea de que las tecnologías digitales han cambiado fundamentalmente la forma en que las personas interactúan entre sí y que esto ha dado lugar a nuevas formas de

formación y expresión de la identidad. El marco teórico se basaría en esta teoría para comprender cómo las credenciales digitalizadas pueden afectar el sentido de identidad de los estudiantes y cómo el nuevo sistema puede respaldar o mejorar sus prácticas de gestión de identidad.

Uno de los conceptos clave en la Teoría de la Identidad Digital es la idea de "rendimiento de la identidad". Según Turkle (1995), "El desempeño de la identidad se refiere a la forma en que los individuos construyen sus identidades a través de sus interacciones con los demás". En otras palabras, las personas usan plataformas en línea para construir y expresar sus identidades de maneras que están influenciadas por las expectativas y normas de las comunidades en línea en las que participan.

Otro aspecto importante de la Teoría de la Identidad Digital es la idea del "colapso del contexto". Este concepto se refiere a la forma en que las plataformas de comunicación en línea pueden colapsar los límites entre diferentes contextos sociales, dando lugar a nuevas formas de expresión de identidad e interacción social (boyd, 2014). Como explica boyd, "el colapso del contexto ocurre cuando las personas se ven obligadas a lidiar con múltiples audiencias en un solo contexto". Al reconocer el papel del desempeño de la identidad y el colapso del contexto, los investigadores pueden comprender mejor la naturaleza compleja y dinámica de la identidad digital en la sociedad contemporánea.

7.1.9 Sistemas de información

El proyecto implicaría el desarrollo de un sistema de información para gestionar las credenciales digitalizadas, se basaría como la gestión de bases de datos, la arquitectura de la información y el diseño de la experiencia del usuario para crear un sistema que sea fácil de usar y seguro.

Según Laudon y Laudon (2016), un sistema de información es "un conjunto de componentes interrelacionados que recopilan, procesan, almacenan y difunden datos e información y proporcionan un mecanismo de retroalimentación para cumplir un objetivo".

O'Brien y Marakas (2018) definen los sistemas de información como "un conjunto de componentes interrelacionados que recopilan, manipulan y difunden datos e información y proporcionan un mecanismo de retroalimentación para cumplir un objetivo".

Stair y Reynolds (2019) definen un sistema de información como "una combinación de personas, hardware, software, redes de comunicación y recursos de datos que recopilan, transforman y difunden información en una organización".

La implementación de un Sistema de Gestión de Aprendizaje (LMS) puede facilitar la creación y gestión de credenciales digitales. Un LMS permite el seguimiento de

información, que luego se pueden utilizar para generar credenciales digitales (Sun, Chen y Li, 2019).

7.1.10 Teoría del procesamiento

La Teoría del Procesamiento, también conocida como Teoría del Proceso Dual, describe cómo las personas procesan la información y toman decisiones. Esta teoría sugiere que las personas procesan la información de manera diferente en función de su conocimiento previo, experiencia y habilidades cognitivas. En el contexto de este proyecto, se basa en esta teoría para diseñar un sistema fácil de usar que tenga en cuenta las diversas capacidades cognitivas y perceptivas de los usuarios.

De acuerdo con la Teoría del Procesamiento, el sistema automático opera rápidamente y sin esfuerzo consciente, apoyándose en atajos mentales o heurísticas para tomar decisiones. Por otro lado, el sistema controlado opera de manera más lenta y deliberada, utilizando la lógica y el razonamiento para tomar decisiones (Kahneman, 2011).

Una de las contribuciones clave de la Teoría del Procesamiento es su explicación de la influencia de las heurísticas en la toma de decisiones. Las heurísticas son atajos mentales que las personas usan para simplificar la toma de decisiones, a menudo basadas en experiencias previas o normas culturales. Sin embargo, estas heurísticas pueden conducir a sesgos y errores en la toma de decisiones, particularmente cuando el contexto o entorno no es familiar o es complejo (Tversky & Kahneman, 1974).

7.1.11 Seguridad de la información

La seguridad de la información se refiere a la práctica de proteger la información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados.

Con la digitalización surge el riesgo de violaciones de la seguridad de la información. Es importante desarrollar un sistema que garantice la seguridad y privacidad de la información personal de los estudiantes.

Según ISO/IEC 27001, la seguridad de la información se define como "la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y la garantía de que la información permanecerá segura" (ISO/IEC 27001, 2013).

El Instituto Nacional de Estándares y Tecnología (NIST) define la seguridad de la información como "la protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de proporcionar confidencialidad, integridad y disponibilidad" (NIST, 2018).

Las credenciales digitales contienen información confidencial que debe protegerse del acceso no autorizado. La implementación de mecanismos de autenticación sólidos, como la autenticación multifactor, puede garantizar que solo los usuarios autorizados tengan acceso a las credenciales digitales (Rahman et al., 2019).

7.1.12 Tecnología Blockchain

La tecnología Blockchain es un libro de contabilidad digital descentralizado que permite a las partes registrar transacciones de manera segura y transparente. La tecnología se basa en una base de datos distribuida que almacena información en una red de computadoras, lo que elimina la necesidad de intermediarios como bancos o agencias gubernamentales. Cada bloque de la cadena contiene un hash criptográfico del bloque anterior, lo que crea una cadena de información irrompible. Esto garantiza la autenticidad de los datos y los hace a prueba de manipulaciones.

Según Investopedia, "Blockchain es un libro de contabilidad distribuido y descentralizado que registra la procedencia de un activo digital. Se utiliza para mantener un registro de las transacciones realizadas en una red y, por lo general, es administrado por una red entre pares que se adhiere a un protocolo para validar nuevos bloques. Una vez registrados, los datos en un bloque determinado no pueden modificarse retroactivamente sin alterar todos los bloques posteriores, lo que requiere el consenso de la mayoría de la red". (Investopedia, 2022)

El proceso de creación de credenciales digitales en la cadena de bloques implica la codificación de las credenciales en la cadena de bloques, la creación de una firma digital y la creación de un hash de los datos. Este proceso garantiza que los datos sean a prueba de manipulaciones y que cualquier persona con acceso a la cadena de bloques pueda verificarlos.

El uso de la tecnología blockchain puede mejorar la seguridad y la inmutabilidad de las credenciales digitales. Un sistema basado en blockchain puede garantizar que las credenciales digitales sean a prueba de manipulaciones, transparentes y seguras (Makridakis et al., 2018).

Con la creciente necesidad de soluciones de identidad digital, es probable que los sistemas de credenciales digitales basados en blockchain se vuelvan más frecuentes en el futuro esto para crear un sistema seguro y a prueba de manipulaciones.

7.1.13 Diseño centrado en el ser humano

El diseño centrado en el ser humano (HCD) es un enfoque para la resolución de problemas que se enfoca en comprender las necesidades, los deseos y las limitaciones de las personas que utilizarán el producto o sistema que se está diseñando. Cuando se trata de la creación de credenciales digitales, HCD se puede

utilizar para crear sistemas seguros, accesibles y fáciles de usar que satisfagan las necesidades de todas las partes interesadas involucradas. Este enfoque ha sido ampliamente citado y referenciado en varios campos, como el diseño, la ingeniería y los negocios, así como a través de normas como la ISO 9241-210. Organizaciones como Stanford d.school e IDEO han desarrollado juegos de herramientas para ayudar a aplicar los principios de HCD a varios desafíos, incluida la creación de credenciales digitales.

En el artículo de Harvard Business Review "Design Thinking Comes of Age", los autores argumentan que HCD es una herramienta fundamental para las empresas que buscan innovar y seguir siendo competitivas.

En resumen, HCD es una herramienta crucial para diseñar sistemas de credenciales digitales efectivos y fáciles de usar que satisfagan las necesidades y preferencias de los estudiantes.

7.1.14 Ética digital

La digitalización de credenciales plantea importantes cuestiones éticas relacionadas con la privacidad, la seguridad y la propiedad de los datos, el uso ético de datos y los derechos digitales para garantizar que el sistema se diseñe e implemente de manera ética y responsable.

"La ética digital es un campo emergente que busca desarrollar un marco para el uso ético de la tecnología digital, teniendo en cuenta los impactos sociales, económicos y ambientales de dicha tecnología". (Van den Hoven, 2015)

Las credenciales digitales deben almacenarse y transmitirse de forma segura para evitar el acceso no autorizado, la manipulación o el robo. El Instituto Nacional de Estándares y Tecnología (NIST) proporciona pautas para la gestión segura de la identidad digital, incluida la autenticación, la autorización y el cifrado.

La ética digital es un conjunto de principios y valores que guían el uso responsable y ético de la tecnología. En el contexto de este proyecto de credenciales digitales para el acceso a la universidad, la ética digital implica consideraciones como la privacidad, la seguridad, la precisión, la transparencia y la accesibilidad.

7.1.15 Aplicación móvil

Según Techopedia, una aplicación móvil es "un tipo de software diseñado para ejecutarse en un dispositivo móvil, como un teléfono inteligente o una tableta, que realiza una tarea específica o un conjunto de tareas para el usuario final" (Techopedia, n.d.).

El Instituto Nacional de Estándares y Tecnología (NIST) define una aplicación móvil como "una aplicación de software que se ejecuta en un dispositivo móvil y realiza ciertas tareas para el usuario" (NIST, 2011).

Crear una aplicación móvil de credenciales digitales para el acceso a la universidad implica diseñar y desarrollar una aplicación de software que permita a los estudiantes y profesores acceder a las diversas áreas de servicios a través de una plataforma digital segura.

7.1.16 Código QR

Un código QR (código de respuesta rápida) es un código de barras bidimensional que se puede escanear con un teléfono inteligente u otro dispositivo móvil. Los códigos QR pueden contener una variedad de información, incluidas las URL de sitios web, información de contacto o información de productos.

La Organización Internacional de Normalización (ISO) define un código QR como "una simbología bidimensional que consiste en una matriz de módulos nominalmente cuadrados dispuestos en un patrón de cuadrícula cuadrada" (ISO/IEC 18004:2015).

Los códigos QR se pueden utilizar como tecnología para crear credenciales digitales para el acceso a la universidad, lo que permite a los estudiantes y profesores acceder a las áreas de servicios a través de una plataforma digital segura.

7.1.17 Usabilidad

La usabilidad se puede definir como la facilidad con la que las personas pueden usar un producto o sistema para lograr sus objetivos de manera efectiva, eficiente y satisfactoria. La usabilidad es un aspecto crítico del diseño y desarrollo de productos, ya que afecta directamente la experiencia del usuario y la satisfacción general del usuario.

Al crear este proyecto de credenciales digitales para el acceso a la universidad, es importante considerar la usabilidad como un aspecto crítico del proceso de diseño y desarrollo, la usabilidad del sistema es fundamental para su éxito. El sistema debe diseñarse de manera que sea intuitivo, fácil de usar y eficiente.

7.1.18 Gestión de cambios

La introducción de un nuevo sistema puede ser perjudicial para los procesos y flujos de trabajo existentes. Es importante considerar cómo gestionar el cambio y garantizar que las partes interesadas estén adecuadamente preparadas y capacitadas.

La gestión del cambio es un enfoque estructurado para la transición de personas, equipos y organizaciones de un estado actual a un estado futuro deseado. Implica el proceso, las herramientas y las técnicas utilizadas para gestionar el lado humano del cambio, con el fin de lograr un resultado exitoso.

La gestión del cambio es un componente crítico a la hora de implementar el proyecto de credenciales digitales para el acceso a la universidad, ya que implica cambios en procesos, estructuras y sistemas.

7.1.19 Adopción de tecnología

El éxito del proyecto dependería de la adopción del nuevo sistema de credenciales digitales por parte de los estudiantes, profesores y personal. La adopción por parte del usuario y la gestión del cambio para comprender y abordar las posibles barreras a la adopción, es importante considerar factores que pueden influir en la adopción, como la facilidad de uso, la utilidad percibida y la compatibilidad percibida con los sistemas existentes.

La teoría de la difusión de la innovación, desarrollada por Rogers (2003), explica el proceso de adopción como un proceso social que implica la transferencia de información e innovación de los primeros adoptantes a los adoptantes posteriores. La teoría identifica cinco etapas en el proceso de adopción: conocimiento, interés, evaluación, prueba y adopción.

Al ofrecer credenciales digitales, la universidad puede posicionarse como líder en innovación educativa y atraer a más estudiantes. Además, las credenciales digitales pueden ayudar a las universidades a rastrear y administrar mejor los registros de los estudiantes.

En general, el marco teórico de este proyecto para digitalizar credenciales de plástico para acceder a una universidad se basa en una variedad de conceptos y teorías relacionadas con la adopción de tecnología, la gestión de identidades, el procesamiento de información, la tecnología blockchain y el diseño centrado en el ser humano para crear un entorno seguro y eficiente. Y un sistema fácil de usar para administrar las credenciales.

8. Desarrollo

8.1 Metodología

El modelo de cascada es un modelo clásico que se utiliza en el ciclo de vida de desarrollo de sistemas para crear un sistema con un enfoque lineal y secuencial. Se denomina cascada porque el modelo se desarrolla sistemáticamente de una fase a otra de forma descendente. GeeksforGeeks(2022).

La metodología en cascada, también conocida como modelo en cascada, es un enfoque secuencial lineal para la gestión de proyectos. Veamos cómo se puede aplicar a la creación de un proyecto de digitalización de credenciales plásticas de acceso a la universidad.

La Figura 3.- Modelo en cascada de cinco niveles, basado en las propuestas de Winston W. Royce. (IONOS, 2019), explica por qué el procedimiento lineal se denomina metodología en cascada.

Figura 3.- Modelo en cascada de cinco niveles, basado en las propuestas de Winston W. Royce. (IONOS, 2019)



En la Figura 3.- Modelo en cascada de cinco fases, explica lo siguiente:

Fases del desarrollo en cascada

- 1. Recopilación y análisis de requisitos:** en esta fase, el equipo del proyecto trabaja con las partes interesadas para identificar y documentar los requisitos del proyecto. El objetivo es definir el alcance del proyecto, identificar cualquier restricción o suposición y establecer una comprensión clara de los objetivos del proyecto. (Sommerville, 2015)

2. **Diseño:** En esta fase, el equipo del proyecto desarrolla un diseño detallado que cumple con los requisitos del proyecto. El diseño debe incluir arquitectura, modelos de datos, algoritmos e interfaces, entre otras cosas. El objetivo es crear un plan detallado que el equipo de desarrollo pueda usar para construir el producto. (Royce, 1970)
3. **Implementación:** en esta fase, el equipo de desarrollo construye el producto de acuerdo con las especificaciones de diseño. El enfoque está en escribir código y desarrollar los componentes necesarios del producto. La fase de implementación suele ser la parte que más tiempo consume del proceso de desarrollo. (Royce, 1970)
4. **Prueba:** en esta fase, el producto se prueba para garantizar que cumple con los requisitos del proyecto. Las pruebas pueden incluir pruebas unitarias, pruebas de integración, pruebas del sistema y pruebas de aceptación, entre otras cosas. El objetivo es identificar y corregir cualquier defecto en el producto antes de su lanzamiento. (Sommerville, 2015)
5. **Implementación y mantenimiento:** en esta fase, el producto se implementa a los usuarios finales. El objetivo es garantizar que el producto se entregue a los usuarios finales de manera oportuna y eficaz. Una vez que se implementa el producto, comienza la fase de mantenimiento, que implica soporte continuo y actualizaciones para garantizar que el producto permanezca efectivo y actualizado. (Sommerville, 2015)

Algunas de las características clave de la metodología de cascada son:

- **Secuencial y lineal:** la metodología Waterfall sigue un enfoque secuencial y lineal, donde cada fase del proceso de desarrollo se completa antes de pasar a la siguiente. El proceso fluye en una dirección, desde el análisis de requisitos, el diseño, la implementación, las pruebas y el despliegue. (Royce, 1970)
- **Basado en documentos:** la metodología Waterfall se basa en gran medida en la documentación para garantizar que los requisitos del proyecto estén bien definidos y que el progreso sea medible. Cada fase del proceso de desarrollo genera un conjunto de documentos que brindan una descripción detallada de los entregables, actividades e hitos. (Sommerville, 2015)
- **Enfatiza la planificación:** la metodología Waterfall enfatiza la planificación, con un enfoque en el análisis inicial, especificaciones detalladas y resultados bien definidos. La fase de planificación es fundamental para garantizar que el alcance, los plazos y los recursos del proyecto se entiendan y documenten bien. (Royce, 1970)
- **Flexibilidad limitada:** la metodología Waterfall ofrece una flexibilidad limitada para cambios en el alcance o los requisitos del proyecto una vez que ha comenzado el proceso de desarrollo. Cualquier cambio en los requisitos

o especificaciones requeriría que el proyecto vuelva a la fase anterior y rehaga el trabajo, lo que puede llevar mucho tiempo y ser costoso. (Sommerville, 2015)

- **Pruebas al final:** la metodología Waterfall realiza pruebas al final del proceso de desarrollo después de que el producto se haya desarrollado por completo. Esto puede generar problemas que se descubren más adelante en el proceso de desarrollo, lo que hace que sea más difícil y costoso solucionarlos. (Royce, 1970)
- **Predictivo:** la metodología Waterfall es un modelo predictivo que se basa en la planificación inicial y la documentación detallada para predecir el resultado del proyecto. Asume que los requisitos y especificaciones están bien definidos y entendidos, y que el proyecto avanza de acuerdo con el plan. (Sommerville, 2015)

En general, la metodología en cascada proporciona un enfoque estructurado y lógico para la gestión de proyectos, lo que permite un proceso paso a paso para la creación de un proyecto para digitalizar credenciales plásticas para el acceso a la universidad.

8.2 Ejecución de la metodología para el desarrollo del proyecto

8.2.1 Recopilación y análisis de requisitos

Definir el alcance del proyecto: Defina claramente el alcance, los objetivos y las limitaciones del proyecto, e identifique a las partes interesadas clave que se verán afectadas por el proyecto.

Utilizar un enfoque estructurado: Utilice un enfoque estructurado para la recopilación y el análisis de requisitos.

Establecer un plan de gestión de requisitos: Desarrolle un plan de gestión de requisitos que describa el proceso para recopilar, analizar, validar y priorizar requisitos, y defina roles y responsabilidades para el equipo del proyecto.

Realizar una evaluación de necesidades: Realice una evaluación de necesidades para comprender el proceso actual de emisión de credenciales de plástico, identifique los desafíos y limitaciones, y las oportunidades de mejora.

Identificar los requisitos funcionales y no funcionales: Identifique los requisitos funcionales del sistema, incluidas las características y capacidades requeridas para satisfacer las necesidades de las partes interesadas, y los requisitos no funcionales, incluida la seguridad, la confiabilidad y la facilidad de uso.

Usar plantillas estandarizadas: Use plantillas y herramientas estandarizadas para documentar los requisitos, como diagramas de casos de uso, historias de usuarios y matrices de seguimiento de requisitos, para garantizar la coherencia y la claridad.

Validar los requisitos: Valide los requisitos con las partes interesadas para garantizar que reflejen con precisión sus necesidades y expectativas.

Priorizar los requisitos: Priorice los requisitos en función de su importancia para las partes interesadas y los objetivos generales del proyecto.

Documentar todo: Documente todos los requisitos, decisiones y suposiciones realizadas durante el proceso de recopilación y análisis para garantizar la transparencia y la rendición de cuentas.

Revisar los requisitos: Revisar continuamente los requisitos a medida que avanza el proyecto y cambian las necesidades y expectativas de las partes interesadas para garantizar que los requisitos sigan siendo relevantes y actualizados.

8.2.2 Diseño

Defina la arquitectura del sistema: Defina la arquitectura del sistema, que incluye los componentes de hardware y software, sus interacciones y la infraestructura necesaria para respaldar el sistema.

Utilice un enfoque de diseño centrado en el usuario: Utilice un enfoque de diseño centrado en el usuario para garantizar que el sistema se diseñe teniendo en cuenta las necesidades, los objetivos y los comportamientos de los usuarios finales.

Cree especificaciones de diseño detalladas: Cree especificaciones de diseño detalladas que especifiquen cómo funcionará cada componente del sistema e interactuará con otros componentes.

Documente todas las decisiones de diseño: Documente todas las decisiones de diseño tomadas durante el proceso de diseño, incluidos los supuestos, las restricciones y las compensaciones, para garantizar la transparencia y la rendición de cuentas.

Priorice las características y la funcionalidad: Priorice las características y la funcionalidad en función de su importancia para las partes interesadas y los objetivos generales del proyecto.

Use patrones de diseño: Use patrones de diseño para estandarizar y simplificar el diseño de los componentes comunes del sistema y reducir el tiempo de desarrollo.

Diseño para la mantenibilidad: Diseñe el sistema para la mantenibilidad, para facilitar futuras actualizaciones y mejoras, y para reducir los costos de mantenimiento y soporte.

Diseño para la interoperabilidad: Diseñe el sistema para la interoperabilidad, para permitir la integración con otros sistemas y para garantizar que el sistema pueda comunicarse con las partes interesadas.

Realizar revisiones de diseño: Realice revisiones de diseño con las partes interesadas para garantizar que el diseño cumpla con sus necesidades y expectativas y para obtener comentarios sobre posibles mejoras.

Utilice la creación de prototipos y la simulación: Utilice la creación de prototipos y la simulación para validar el diseño, probar los componentes del sistema e identificar problemas o errores de diseño.

Garantice la seguridad y la privacidad: Diseñe el sistema teniendo en cuenta la seguridad y la privacidad para proteger los datos confidenciales, evitar el acceso no autorizado y cumplir con las normas de privacidad.

8.2.3 Implementación

Desarrollo de códigos QR: El sistema debe poder generar códigos QR únicos para cada estudiante, personal o miembro de la universidad. Este requisito es esencial ya que permite que el sistema genere identificadores únicos para cada individuo y permite un fácil acceso al sistema.

Desarrollo de la base de datos: El sistema debe mantener una base de datos de todos los estudiantes, el personal y los profesores, sus datos personales y sus códigos QR asociados.

Desarrollo de la aplicación móvil: El primer paso es desarrollar la aplicación móvil que se utilizará para escanear el código QR de la credencial plástica y autenticar el acceso del usuario a las instalaciones y servicios de la universidad. Esto implica escribir el código para la aplicación móvil, crear la interfaz de usuario y realizar pruebas para garantizar que la aplicación funcione según lo previsto.

Desarrollo del sitio web administrador: los administradores universitarios utilizan el sitio web para administrar los datos de acceso de los estudiantes y monitorear el uso de las credenciales digitales. Esto implica crear la interfaz de usuario y realizar pruebas para garantizar que el sitio funcione según lo previsto.

Integración de la aplicación móvil y el sitio web administrador: el siguiente paso es integrar la aplicación móvil y el sitio la web en un solo sistema. Esto implica

garantizar que la aplicación móvil y el sitio se comuniquen de manera efectiva y que los datos se transfieran de manera segura entre los dos.

Implementación de la base de datos: La base de datos almacena toda la información necesaria para autenticar a los usuarios y otorgar acceso a las instalaciones y áreas de servicio de la universidad. Esto implica configurar la infraestructura de la base de datos, crear el esquema de la base de datos e implementar medidas de seguridad para proteger los datos.

Implementación del sistema de códigos QR: El sistema de códigos QR consiste en generar códigos QR únicos para cada usuario y codificarlos con la información necesaria para autenticar su acceso a las instalaciones y áreas de servicio de la universidad. Esto implica implementar un sistema de generación de códigos QR, probar los códigos QR para garantizar que se puedan escanear e integrar el sistema de códigos QR con la aplicación móvil.

Implemente medidas de seguridad: Implemente medidas de seguridad, como encriptación, controles de acceso y detección de intrusos, para proteger el sistema del acceso no autorizado y garantizar la privacidad de los datos.

Capacite a los usuarios finales y administradores: Capacite a los usuarios finales y administradores sobre cómo usar el sistema y brinde soporte y mantenimiento continuos según sea necesario.

8.2.4 Prueba

Desarrollar casos de prueba: Desarrolle casos de prueba que cubran todos los requisitos y la funcionalidad del sistema, incluidos escenarios de prueba positivos y negativos.

Realice pruebas unitarias: Realice pruebas unitarias de los componentes individuales del sistema para garantizar que funcionen correctamente.

Realice pruebas de integración: Realice pruebas de integración para probar las interacciones entre los componentes del sistema y asegurarse de que funcionen juntos correctamente.

Realice pruebas del sistema: Realice pruebas del sistema para probar el sistema en su conjunto y asegurarse de que cumpla con los requisitos y funcione como se espera.

Realizar pruebas de aceptación: Realice pruebas de aceptación con los usuarios finales para garantizar que el sistema satisfaga sus necesidades y expectativas.

Realice pruebas de rendimiento: Realice pruebas de rendimiento para probar el rendimiento del sistema bajo cargas esperadas e inesperadas.

Realice pruebas de seguridad: Realice pruebas de seguridad para probar las medidas de seguridad del sistema e identificar posibles vulnerabilidades.

Realice pruebas de regresión: Realice pruebas de regresión para garantizar que los cambios o actualizaciones del sistema no afecten la funcionalidad existente.

Documente los resultados de las pruebas: Documente los resultados de cada prueba, incluidos los problemas o errores identificados, y realice un seguimiento hasta su resolución.

8.2.5 Implementación y mantenimiento

Implemente una metodología ágil: Implemente una metodología ágil para garantizar la flexibilidad y la adaptabilidad a lo largo del ciclo de vida del proyecto, lo que permite los cambios.

Realice revisiones periódicas de proyectos: Realice revisiones periódicas del proyecto para evaluar el progreso, identificar problemas y ajustar el plan del proyecto según sea necesario.

Implementar procesos de control de calidad: Implementar procesos de control de calidad para garantizar que los entregables cumplan con los estándares y requisitos de calidad del proyecto.

Establezca un plan de mantenimiento: Establezca un plan de mantenimiento para garantizar el mantenimiento, las actualizaciones y el soporte continuos del sistema.

Implemente procedimientos de respaldo y recuperación: Implemente procedimientos de respaldo y recuperación para garantizar que los datos y la funcionalidad del sistema se puedan recuperar en caso de una falla del sistema u otro problema.

Supervise el rendimiento del sistema: Supervise el rendimiento del sistema con regularidad para identificar problemas y oportunidades de mejora.

8.3 Aplicar instrumento de evaluación

En general, la aplicación de un instrumento de evaluación al inicio del proyecto para digitalizar credenciales de plástico ayuda a garantizar que el proyecto sea factible, esté alineado con las necesidades de las partes interesadas y tenga medidas claras para el éxito. También ayuda a establecer un plan de evaluación que se puede

utilizar para realizar un seguimiento del progreso y hacer los ajustes necesarios a lo largo del ciclo de vida del proyecto.

Para evaluar la viabilidad del proyecto: un instrumento de evaluación puede ayudar a evaluar la viabilidad del proyecto al examinar factores como la disponibilidad de recursos, los riesgos y desafíos potenciales, y la alineación con las metas y objetivos de la universidad.

Para identificar las necesidades de las partes interesadas: un instrumento de evaluación puede ayudar a identificar las necesidades y expectativas de los estudiantes, que pueden informar el diseño y la implementación del proyecto de digitalización.

Para establecer medidas de línea de base: Un instrumento de evaluación puede ayudar a establecer medidas de línea de base para el proyecto, que se pueden utilizar para seguir el progreso y evaluar los resultados y los impactos.

Para establecer métricas de desempeño: Un instrumento de evaluación puede ayudar a establecer métricas de desempeño que se pueden usar para medir la efectividad del proyecto en el cumplimiento de sus metas y objetivos.

Para desarrollar un plan de evaluación: Un instrumento de evaluación puede ayudar a desarrollar un plan para evaluar el proyecto, incluidos los métodos y herramientas que se utilizarán para recopilar y analizar datos, y el cronograma para realizar las evaluaciones.

Esta encuesta tuvo como objetivo investigar la viabilidad y factibilidades de implementar una aplicación móvil que incorpore una credencial digital con un código QR, tomando una muestra de 100 estudiantes, el objetivo es obtener una visión general de las opiniones y actitudes de los estudiantes sobre el nuevo sistema de acceso digital. La encuesta tuvo limitaciones de recursos de tiempo, presupuesto y personal para aplicar una encuesta más amplia, con el fin de conocer la opinión de los estudiantes. **(Anexo 1)**

El propósito de la aplicación es proporcionar un método más conveniente y seguro para acceder al instituto y sus áreas de servicios que esta ofrece. La encuesta recopiló datos sobre la familiaridad de los estudiantes con las credenciales digitales y los códigos QR y su disposición a usar la aplicación en el futuro. Los resultados de la encuesta informarán al desarrollo de la aplicación y orientar los esfuerzos futuros para mejorar el uso de las credenciales digitales en la educación.

8.4 Desarrollo de las factibilidades del proyecto

Antes de iniciar un proyecto de digitalización de credenciales mediante códigos QR, es fundamental realizar un estudio de factibilidad para determinar la viabilidad y potencial éxito del proyecto. A continuación, se detallan algunos pasos a seguir para poder desarrollar la factibilidad de este proyecto:

Definir los objetivos del proyecto: Antes de iniciar cualquier proyecto, es fundamental determinar los objetivos del proyecto. En este caso, el objetivo es digitalizar las credenciales de plástico mediante códigos QR.

Evaluar la viabilidad técnica: Determinar los requisitos técnicos del proyecto, incluidos los requisitos de hardware y software necesarios, las medidas de seguridad y los métodos para verificar la autenticidad de los códigos. Identifique los posibles desafíos y riesgos técnicos y evalúe la viabilidad de superarlos.

Desarrolle un plan de proyecto: Con base en la información recopilada durante el estudio de factibilidad, desarrolle un plan de proyecto detallado que incluya el cronograma, los hitos y los recursos necesarios para completar el proyecto.

Pruebe la viabilidad: Antes de invertir en el proyecto, realice un proyecto piloto para probar la viabilidad del sistema. Esto ayudará a identificar cualquier problema que deba abordarse antes de que se inicie el sistema.

Factibilidad de seguridad: El proyecto debe ser seguro, lo que significa que el sistema debe contar con fuertes medidas de seguridad para proteger la privacidad y confidencialidad de la información que se comparte. El sistema debe estar diseñado para evitar el acceso no autorizado, ataques y las filtraciones de datos.

FASE 2 Requerimientos

8.5 Definición de requerimientos funcionales

Los requisitos funcionales son un conjunto de especificaciones que definen las funciones o capacidades específicas que debe poseer un sistema o producto para satisfacer las necesidades de sus usuarios.

Requerimiento funcional	
Identificación del requerimiento	RF0
Nombre del requerimiento	Análisis de la información (estructura)
Descripción del requerimiento	El estudiante proporciona información importante como color, propósito, diseño correspondiente a su profesión.

Prioridad del requerimiento	Alta
------------------------------------	------

Tabla 1.- Requerimiento funcional RF0 muestra Análisis de la información

Requerimiento funcional	
Identificación del requerimiento	RF1
Nombre del requerimiento	Página web para administradores
Descripción del requerimiento	El software debe incluir una página web que permita a los administradores administrar el sistema lo que incluye agregar o eliminar cuentas de usuario, actualizar credenciales, generar informes y monitorear registros de acceso. La página web debe ser segura y fácil de usar.
Prioridad del requerimiento	Alta

Tabla 2.- Requerimiento funcional RF1 muestra Página web para administradores

Requerimiento funcional	
Identificación del requerimiento	RF2
Nombre del requerimiento	Herramientas administrativas
Descripción del requerimiento	La página web para administradores debe proporcionar herramientas para administrar las cuentas de los usuarios, generar registros de acceso y establecer políticas de acceso para las diferentes áreas de la universidad.
Prioridad del requerimiento	Alta

Tabla 3.- Requerimiento funcional RF2 muestra Herramientas administrativas

Requerimiento funcional	
Identificación del requerimiento	RF3
Nombre del requerimiento	Administración de usuarios
Descripción del requerimiento	El administrador debe poder administrar las cuentas de los usuarios, lo que incluye agregar, modificar, eliminar cuentas, cambiar su contraseña o ver sus registros de acceso. A través de la página web.
Prioridad del requerimiento	Alta

Tabla 4.- Requerimiento funcional RF3 muestra dministración de usuarios

Requerimiento funcional	
Identificación del requerimiento	RF4
Nombre del requerimiento	Almacenamiento de credenciales digitales
Descripción del requerimiento	El software debe permitir a los administradores almacenar las credenciales digitales de cada estudiante en una base de datos segura. Las credenciales digitales deben incluir información del estudiante, como nombre, foto, programa de estudio, fechas de inscripción y cualquier otra información relevante.
Prioridad del requerimiento	Alta

Tabla 5.- Requerimiento funcional RF4 muestra Almacenamiento de credenciales digitales

Requerimiento funcional	
Identificación del requerimiento	RF5
Nombre del requerimiento	Integración con los sistemas existentes
Descripción del requerimiento	El sistema debe poder integrarse con los sistemas universitarios existentes.
Prioridad del requerimiento	Alta

Tabla 6.- Requerimiento funcional RF5

Requerimiento funcional	
Identificación del requerimiento	RF6
Nombre del requerimiento	Generación de códigos QR
Descripción del requerimiento	El software debe permitir a los administradores generar códigos QR para la credencial digital de cada estudiante.
Prioridad del requerimiento	Alta

Tabla 7.- Requerimiento funcional RF6

Requerimiento funcional	
Identificación del requerimiento	RF7
Nombre del requerimiento	Digitalización de credenciales
Descripción del requerimiento	El software debe poder capturar la información relevante de las credenciales de plástico y convertirla a

	un formato digital que pueda almacenarse y escanear con un escáner y usarse para el acceso. Luego, el sistema debe almacenar las credenciales digitalizadas en una base de datos segura, luego, el sistema debe almacenar las credenciales digitalizadas en una base de datos segura.
Prioridad del requerimiento	Alta

Tabla 8.- Requerimiento funcional RF7

Requerimiento funcional	
Identificación del requerimiento	RF8
Nombre del requerimiento	Emisión de tarjetas
Descripción del requerimiento	El administrador debe poder emitir nuevas credenciales digitales a los usuarios según sea necesario a través de la página web.
Prioridad del requerimiento	Alta

Tabla 9.- Requerimiento funcional RF8

Requerimiento funcional	
Identificación del requerimiento	RF9
Nombre del requerimiento	Aplicación Móvil
Descripción del requerimiento	El software debe incluir una aplicación móvil que permita a los usuarios acceder a las instalaciones y áreas de servicios de la universidad utilizando su dispositivo móvil. La aplicación móvil debe estar disponible para dispositivos Android, y debe ser fácil de usar e intuitiva.
Prioridad del requerimiento	Alta

Tabla 10.- Requerimiento funcional RF9

Requerimiento funcional	
Identificación del requerimiento	RF10
Nombre del requerimiento	Escaneo de credenciales
Descripción del requerimiento	El sistema debe poder escanear y leer la información de las credenciales digitales para verificar y luego validar la

	identidad del usuario comparándola con una base de datos de credenciales válidas.
Prioridad del requerimiento	Alta

Tabla 11.- Requerimiento funcional RF10

Requerimiento funcional	
Identificación del requerimiento	RF11
Nombre del requerimiento	Control de acceso
Descripción del requerimiento	El sistema debe controlar y habilitar el acceso, permitiendo a los usuarios acceder únicamente a las áreas o servicios que están autorizados a utilizar y mostrar los mensajes de error apropiados si el usuario no está autorizado para acceder a un área en particular.
Prioridad del requerimiento	Alta

Tabla 12.- Requerimiento funcional RF11

Requerimiento funcional	
Identificación del requerimiento	RF12
Nombre del requerimiento	Autenticación de usuarios
Descripción del requerimiento	El sistema debe autenticar la identidad de los usuarios y verificar que está autorizado para acceder a las instalaciones o áreas de servicios de la universidad a través de la aplicación móvil o página web.
Prioridad del requerimiento	Alta

Tabla 13.- Requerimiento funcional RF12

Requerimiento funcional	
Identificación del requerimiento	RF13
Nombre del requerimiento	Validación de credenciales
Descripción del requerimiento	El software debe poder validar la autenticidad de la credencial digitalizada realizando una suma de verificación u otro procedimiento de validación para garantizar que los datos no hayan sido alterados.
Prioridad del requerimiento	Alta

Tabla 14.- Requerimiento funcional RF13

Requerimiento funcional	
Identificación del requerimiento	RF14
Nombre del requerimiento	Informes y análisis
Descripción del requerimiento	El software debe proporcionar informes detallados y herramientas de análisis para ayudar a los administradores a comprender el comportamiento de los usuarios y realizar un seguimiento de los patrones de uso en toda la universidad.
Prioridad del requerimiento	Alta

Tabla 15.- Requerimiento funcional RF14

8.6 Definición de requerimientos No funcionales

Los requisitos no funcionales son el rendimiento, la usabilidad, la seguridad y otras características que debe poseer el software para satisfacer las necesidades y expectativas de sus usuarios. Estos son algunos requisitos no funcionales para un proyecto de software que implica la digitalización de credenciales de plástico para acceder a una universidad.

Requerimiento No Funcional	
Identificación del requerimiento	RNF1
Nombre del requerimiento	Rendimiento
Descripción del requerimiento	La aplicación móvil y la página web deben cargarse rápidamente y responder a las entradas del usuario sin demoras significativas. El proceso de escaneo de credenciales debe ser rápido y preciso, y el software debe poder manejar una gran cantidad de solicitudes simultáneas sin ralentizarse.
Prioridad del requerimiento	Alta

Tabla 16.- Requerimiento No funcional RNF1

Requerimiento No Funcional	
Identificación del requerimiento	RNF2
Nombre del requerimiento	Seguridad y privacidad del sistema
Descripción del requerimiento	El sistema debe implementar las medidas de seguridad adecuadas para proteger los datos, la privacidad del

	usuario, incluido el cifrado de datos en tránsito y en reposo, la autenticación y autorización del usuario y los controles de acceso para evitar el acceso no autorizado.
Prioridad del requerimiento	Alta

Tabla 17.- Requerimiento No funcional RNF2

Requerimiento No Funcional	
Identificación del requerimiento	RNF3
Nombre del requerimiento	Escalabilidad
Descripción del requerimiento	El software debe estar diseñado para escalar horizontal y verticalmente, para adaptarse a un número creciente de usuarios y solicitudes. El sistema debe poder agregar nuevos servidores o recursos para manejar el tráfico y la carga adicionales.
Prioridad del requerimiento	Alta

Tabla 18.- Requerimiento No funcional RNF3

Requerimiento No Funcional	
Identificación del requerimiento	RNF4
Nombre del requerimiento	Confiabilidad
Descripción del requerimiento	El software debe ser confiable y estable, con un tiempo de inactividad o errores mínimos. El proceso de escaneo de credenciales debe ser preciso y consistente, y el software debe poder recuperarse rápidamente de las fallas.
Prioridad del requerimiento	Alta

Tabla 19.- Requerimiento No funcional RNF4

Requerimiento No Funcional	
Identificación del requerimiento	RNF5
Nombre del requerimiento	Usabilidad
Descripción del requerimiento	La aplicación móvil y la página web deben diseñarse para que sean fáciles de usar y navegar, con una interfaz limpia e intuitiva que sea accesible para

	usuarios con diferentes niveles de experiencia y conocimientos. El proceso de escaneo de credenciales debe ser sencillo y requerir una intervención mínima del usuario.
Prioridad del requerimiento	Alta

Tabla 20.- Requerimiento No funcional RNF5

Requerimiento No Funcional	
Identificación del requerimiento	RNF6
Nombre del requerimiento	Accesibilidad
Descripción del requerimiento	El software debe ser accesible para usuarios con discapacidades y cumplir con estándares de accesibilidad como WCAG 2.1. El proceso de escaneo de credenciales debe diseñarse para adaptarse a usuarios con diferentes capacidades y necesidades.
Prioridad del requerimiento	Alta

Tabla 21.- Requerimiento No funcional RNF6

Requerimiento No Funcional	
Identificación del requerimiento	RNF7
Nombre del requerimiento	Seguridad
Descripción del requerimiento	El software debe diseñarse teniendo en cuenta la seguridad e implementar las medidas adecuadas para proteger los datos y la privacidad del usuario, como el cifrado, la autenticación y los controles de acceso. El software también debe cumplir con los estándares de seguridad relevantes, como ISO 27001.
Prioridad del requerimiento	Alta

Tabla 22.- Requerimiento No funcional RNF7

Requerimiento No Funcional	
Identificación del requerimiento	RNF8
Nombre del requerimiento	Cumplimiento
Descripción del requerimiento	El software debe cumplir con las leyes y reglamentaciones pertinentes, como las leyes de protección de datos, y

	poder demostrar el cumplimiento mediante auditorías y otras medidas.
Prioridad del requerimiento	Alta

Tabla 23.- Requerimiento No funcional RNF8

Requerimiento No Funcional	
Identificación del requerimiento	RNF9
Nombre del requerimiento	Mantenibilidad
Descripción del requerimiento	El software debe diseñarse para que sea fácil de mantener y actualizar, con una documentación clara y un código bien organizado que sea fácil de entender y modificar. La base de datos de credenciales debe ser fácil de actualizar y administrar.
Prioridad del requerimiento	Alta

Tabla 24.- Requerimiento No funcional RNF9

Requerimiento No Funcional	
Identificación del requerimiento	RNF10
Nombre del requerimiento	Interoperabilidad
Descripción del requerimiento	El software debe poder funcionar sin problemas con otros sistemas y plataformas, y estar diseñado con estándares abiertos y API que permitan la integración con otras herramientas de software.
Prioridad del requerimiento	Alta

Tabla 25.- Requerimiento No funcional RNF10

Requerimiento No Funcional	
Identificación del requerimiento	RNF11
Nombre del requerimiento	Compatibilidad
Descripción del requerimiento	La aplicación móvil debe ser compatible con una amplia gama de dispositivos móviles, diversas versiones del sistema operativo Android, y la página web debe ser compatible con una variedad de navegadores web.
Prioridad del requerimiento	Alta

Tabla 26.- Requerimiento No funcional RNF11

Requerimiento No Funcional	
Identificación del requerimiento	RNF12
Nombre del requerimiento	Facilidad de uso
Descripción del requerimiento	El software debe diseñarse con una interfaz fácil de usar para garantizar la facilidad de uso y minimizar los errores del usuario. La aplicación móvil y la página web deben ser intuitivas y fáciles de navegar, con instrucciones y avisos claros.
Prioridad del requerimiento	Alta

Tabla 27.- Requerimiento No funcional RNF12

8.7 Diagrama de casos de uso

Los actores principales en este diagrama son el estudiante, el administrador y el escáner de credenciales. El Estudiante es el usuario principal del sistema, que necesita acceder a las instalaciones y áreas de servicios de la universidad utilizando su credencial digital. El administrador es responsable de administrar el sistema, lo que incluye agregar nuevas credenciales y monitorear los registros de acceso. El escáner de credenciales es el dispositivo que lee y verifica las credenciales digitalizadas. En la Figura 4.- Diagrama de casos de uso, muestra lo siguiente:

Panorama del administrador

Puede gestionar las credenciales digitales a través del sitio web. Esto podría incluir agregar o eliminar credenciales, así como administrar el acceso de los usuarios. Si el Administrador necesita eliminar una credencial digital, puede hacerlo a través del portal web. Si el Administrador necesita revocar una credencial digital (por ejemplo, si el estudiante ya no está matriculado en la universidad), puede hacerlo a través del portal web. Las credenciales digitales se almacenan en una base de datos segura para garantizar su integridad y autenticidad.

Los principales casos de uso en este diagrama incluyen de un administrador:

Acceso al sitio web administrador: El administrador puede realizar tareas como ver los perfiles de los estudiantes, crear, editar y eliminar cuentas de usuario. Estas tareas son accesibles a través de una página web de administrador.

Iniciar sesión: Implica que el sitio web verifique la identidad del administrador que intenta acceder al sitio. Esto es a través de su nombre de usuario y contraseña.

Administrar credenciales: Implica que el administrador acceda a una página web para administrar las credenciales digitales. Esto podría incluir agregar o eliminar credenciales, así como administrar el acceso de los usuarios.

Registrar Credenciales: El Administrador puede registrar las nuevas credenciales digitales y almacenar la información en la base de datos del sistema y asociándolas con la cuenta de un estudiante.

Verificar Credencial: Implica verificar la autenticidad de la credencial digital. Esto podría hacerse escaneando el código QR o comparando la información de la credencial con la base de datos.

Actualizar credenciales: El administrador puede modificar la información asociada con las credenciales de un estudiante.

Reportar Credenciales Extraviadas o Robadas: El administrador puede reportar una credencial de plástico extraviada o robada al sistema, lo que desactivará la credencial digital asociada y evitará el acceso no autorizado.

Verificar acceso: El administrador puede verificar el acceso de un estudiante a una instalación o servicio dentro del sitio web.

Ver registros de acceso: El administrador puede ver los registros de acceso de los estudiantes a las instalaciones y áreas de servicios, incluida la hora y la ubicación de cada de acceso.

Cerrar sesión: Permite al administrador cerrar la sesión del sitio web.

Panorama del estudiante

El alumno Abre la aplicación móvil e inicia sesión a través del número de control del estudiante y contraseña. Una vez que el estudiante ha sido autenticado, puede ver su credencial digital en su dispositivo. Si el estudiante necesita presentar su credencial digital a una figura de autoridad (por ejemplo, un profesor o vigilante), puede escanear el código QR en el lector de código QR para verificar su autenticidad. En la En la Figura 4.- Diagrama de casos de uso, muestra lo siguiente:

Los principales casos de uso en este diagrama incluyen de un estudiante:

Acceso a la App: El estudiante puede realizar tareas como ver su propio perfil, ver su credencial digital a través de una aplicación móvil para verificar sus credenciales.

Iniciar sesión: Implica que el sistema verifique la identidad del usuario que intenta acceder a la credencial digital. Esto es a través de su número de control y contraseña.

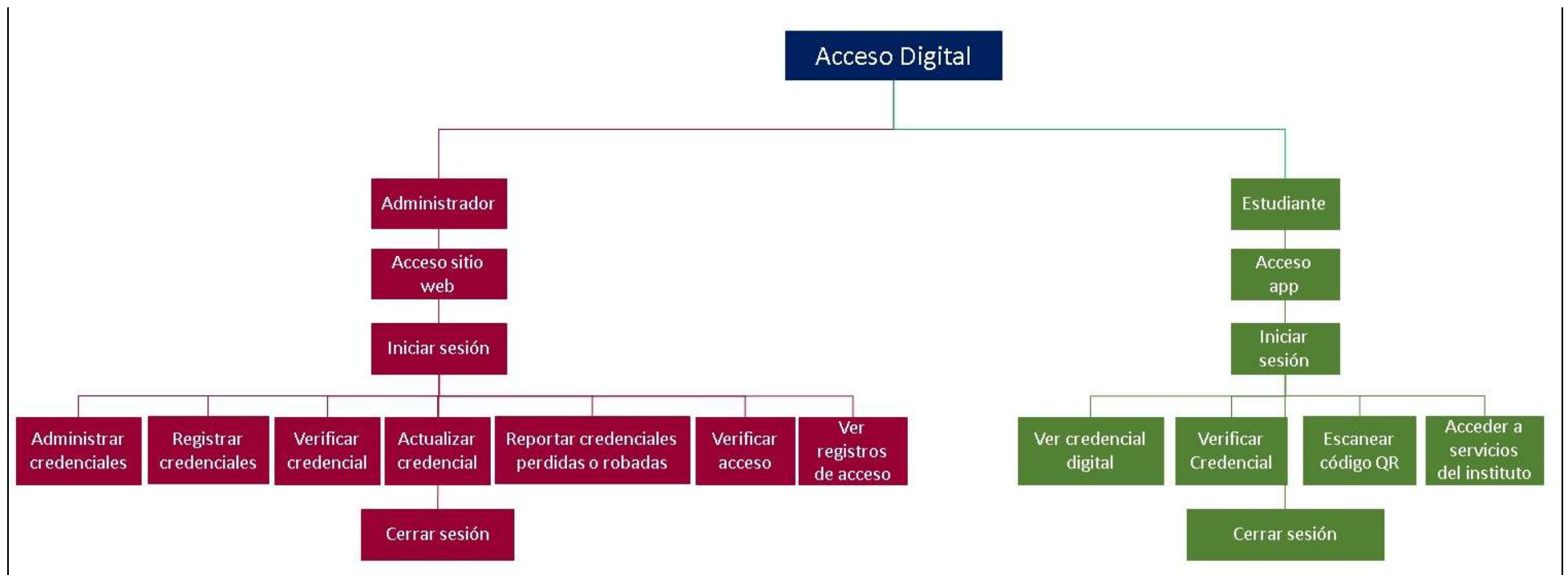
Verificar Credencial: Implica verificar la autenticidad de la credencial digital. Esto podría hacerse escaneando un código QR.

Escanear código QR: Le permite al estudiante usar su aplicación móvil para escanear el código QR de su credencial digital y acceder a la institución y a sus áreas de servicio.

Cerrar sesión: Permite al alumno cerrar la sesión de la aplicación.

Diagrama casos de uso

Figura 4.- Diagrama casos de uso del acceso digital

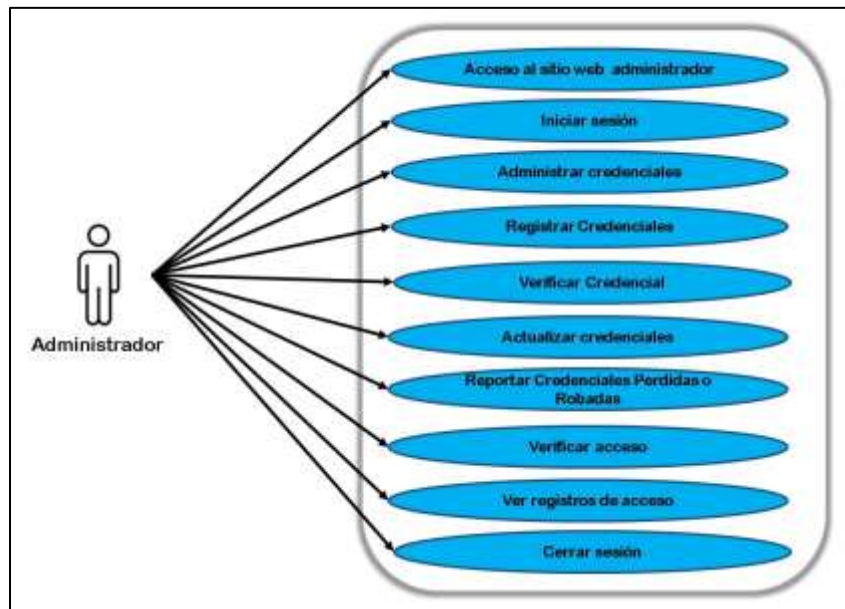


8.8 Depuración de casos de uso

Revisar el diagrama de casos de uso y sugerir algunas mejoras:

Casos de uso del administrador

Figura 5.- Casos de uso del administrador



Casos de uso del estudiante

Figura 66.- Casos de uso del estudiante

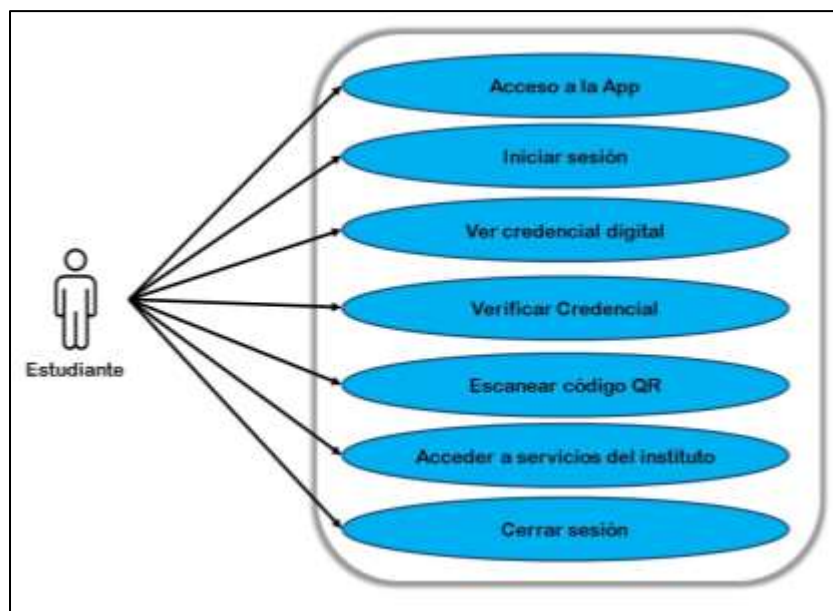
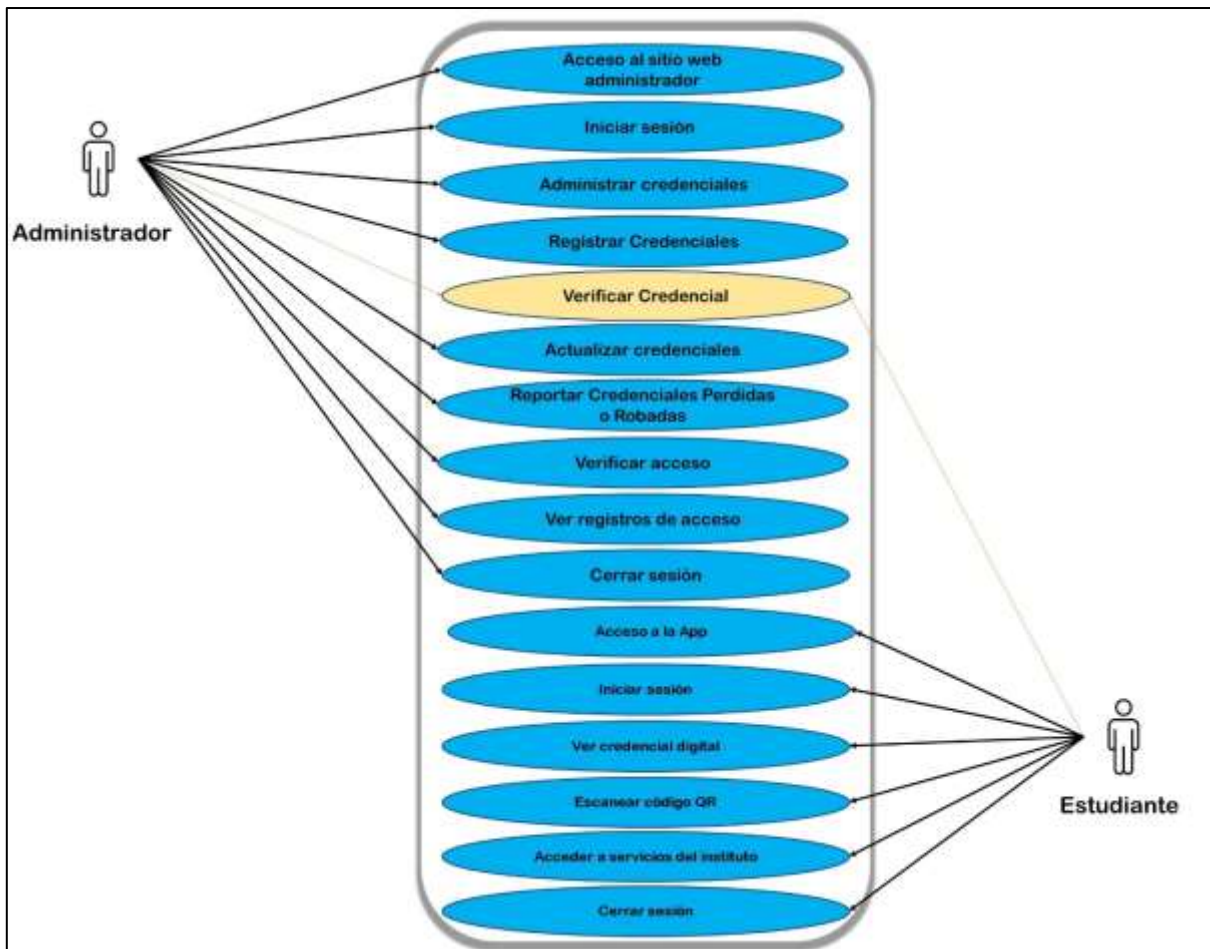


Figura 7.- Casos de uso completo



8.9 Documentación de casos de uso

Caso de Uso: Acceso Digital

La Figura 7.- Casos de uso completo, muestra lo siguiente:

Descripción: Este caso de uso consiste en acceder a la credencial digital a través de una aplicación móvil y administrarlas por medio de un sitio web para personas autorizadas.

Actores: Estudiante y Administrador.

Condición previa: El usuario ha descargado la aplicación móvil y tiene acceso a su credencial digital, El administrador tiene acceso al sitio web donde se administran las credenciales.

Condición posterior: se ha accedido con éxito.

Acceso al sitio web administrador

Descripción: Este caso de uso implica que el administrador puede realizar tareas como ver los perfiles de los estudiantes, crear y editar cuentas de usuario. Estas tareas son accesibles a través de una página web de administrador.

Actores: Administrador

Condición previa: El administrador tiene acceso al sitio web.

Condición posterior: El administrador ha entrado con éxito al sitio web.

Iniciar sesión

Descripción: Implica que el sitio web verifique la identidad del administrador que intenta acceder al sitio. Esto es a través de su nombre de usuario y contraseña.

Actores: Administrador

Condición previa: El administrador conoce sobre el sitio web.

Condición posterior: El administrador tiene permiso a todas las herramientas.

Administrar credenciales

En la Figura 5.- Casos de uso del administrador, muestra lo siguiente:

Descripción: Este caso de uso implica que el Administrador acceda a una página web para administrar las credenciales digitales. Esto podría incluir agregar o eliminar credenciales, así como administrar el acceso de los usuarios.

Actores: Administrador

Condición previa: El administrador tiene acceso al sitio web.

Condición posterior: El administrador ha gestionado con éxito las credenciales digitales.

Registrar Credenciales

Descripción: Este caso de uso consiste en crear una versión digital de la credencial de plástico. Esto podría implicar escanear la credencial y almacenar la información en una base de datos.

Actores: Administrador

Precondición: El Administrador tiene acceso a la información de las credenciales de los alumnos.

Condición posterior: Se ha creado y almacenado con éxito en la base de datos una versión digital de la credencial de plástico.

Verificar Credencial

Descripción: Este caso de uso consiste en verificar la autenticidad de la credencial digital. Esto podría hacerse escaneando un código QR o comparando la información de la credencial con una base de datos.

Actores: Estudiante, Administrador

Precondición: El estudiante o administrador tiene acceso a la credencial digital y está intentando verificar su autenticidad.

Condición posterior: La autenticidad de la credencial digital se ha verificado con éxito.

Actualizar credenciales

Descripción: Este caso de uso permite a los usuarios autorizados actualizar la información de la credencial digital. Esto podría incluir actualizar la información personal o agregar.

Actores: Administrador

Precondición: El usuario ha sido autenticado y tiene acceso a la modificación de información.

Condición posterior: La credencial digital se ha actualizado correctamente con la nueva información.

Reportar credenciales pérdidas o robadas

Descripción: Este caso de uso le permite al Administrador eliminar una credencial digital si es necesario (por ejemplo, si el estudiante ya no está inscrito en la universidad).

Actores: Administrador

Precondición: El Administrador tiene acceso a la página web y la credencial digital que desea eliminar.

Condición posterior: La credencial digital se ha eliminado con éxito de la base de datos y el estudiante ya no puede acceder a ella.

Verificar acceso

Descripción: El administrador puede ver en tiempo real el acceso de los estudiantes a las instalaciones y áreas de servicios, incluida la hora y la ubicación de cada de acceso.

Actores: Administrador

Precondición: El administrador está monitoreando el funcionamiento de acceso en tiempo real.

Condición posterior: El sistema funciona exitosamente.

Ver registros de acceso

Descripción: El administrador puede ver los registros de acceso de los estudiantes a las instalaciones y áreas de servicios, incluida la hora y la ubicación de cada de acceso.

Actores: Administrador

Precondición: El administrador está revisando la información de los estudiantes.

Condición posterior: El sistema guarda registro de los lugares donde accedió el estudiante.

Cerrar sesión

Descripción: El administrador puede cerrar sesión del sitio web de forma segura.

Actores: Administrador

Precondición: El administrador termino el monitoreo de acceso.

Condición posterior: El cierre de sesión es exitoso.

Acceso a la App

La Figura 6.- Casos de uso del estudiante, representa lo siguiente:

Descripción: El estudiante puede realizar tareas como ver su propio perfil, ver sus credenciales digitales a través de una aplicación móvil y escanear códigos QR para verificar sus credenciales.

Actores: Estudiante

Condición previa: El estudiante descargo la app.

Condición posterior: El administrador ha entrado con éxito al sitio web.

Iniciar sesión

Descripción: Implica que la App verifique la identidad del estudiante que intenta acceder al sitio. Esto es a través de su nombre de usuario y contraseña.

Actores: Administrador

Condición previa: El administrador conoce sobre el sitio web.

Condición posterior: El administrador tiene permiso a todas las herramientas.

Ver credencial

Descripción: Este caso de uso permite a los usuarios autorizados ver la credencial digital. Esto podría hacerse a través de la aplicación móvil.

Actores: Estudiante

Precondición: El usuario ha sido autenticado y tiene acceso a la credencial digital.

Condición posterior: El usuario ha visto correctamente la credencial digital.

Escanear código QR

Descripción: Este caso de uso le permite al estudiante usar su aplicación móvil para escanear el código QR en el lector.

Actores: Estudiante

Precondición: El estudiante tiene la aplicación móvil y acceso a su credencial digital.

Condición posterior: El estudiante ha escaneado con éxito el código QR y puede ver su credencial digital en su dispositivo.

Acceder a áreas de servicio del instituto

Descripción: Este caso de uso le permite al estudiante acceder al instituto y sus áreas de servicios como biblioteca, cafetería entre otros.

Actores: Estudiante

Precondición: El estudiante tiene que escanear su credencial digital.

Condición posterior: El estudiante accede con éxito al instituto y sus áreas de servicios.

Cerrar sesión

Descripción: El estudiante puede cerrar sesión de la aplicación de forma segura.

Actores: Estudiante

Precondición: El estudiante concluyo su horario académico.

Condición posterior: El cierre de sesión es exitoso.

8.10 Pasos para crear un modelo de base de datos para el proyecto

Determinar el propósito de la base de datos: Identificar el propósito de la base de datos, lo que implica determinar qué tipo de datos se almacenarán en la base de datos, cómo se utilizarán los datos y quién accederá a los datos.

Identificar las entidades: Comienza por identificar las entidades involucradas en el sistema. En este caso, las entidades son estudiantes, credenciales digitales, accesos y administrador.

Defina los atributos: Para cada entidad, defina los atributos que se almacenarán en la base de datos. Por ejemplo, para la entidad estudiante, los atributos pueden ser el nombre, el número de control, el correo electrónico y el número de teléfono.

Definir las relaciones: Determinar las relaciones entre las entidades. Por ejemplo, un estudiante tiene una credencial digital con un código QR único que se puede escanear con un lector de códigos en la entrada de la universidad. Asimismo, el personal universitario tendrá acceso a las credenciales digitales y registros de entrada/salida.

Diseñe el esquema de la base de datos: En función de las entidades y relaciones identificadas, diseñe el esquema de la base de datos. Por ejemplo, puede crear tablas.

Establezca las restricciones: defina las restricciones que deben aplicarse en la base de datos. Por ejemplo, el código QR para cada credencial digital debe ser único y un estudiante solo puede tener una credencial digital activa a la vez.

Seguir estos pasos puede ayudarlo a crear un modelo de base de datos eficiente y efectivo para el proyecto dado.

8.10.1 Determinar el propósito de la base de datos

El propósito de la base de datos es almacenar información relacionada con los datos de los estudiantes. Esto incluye el nombre del estudiante, número de control, estado

de inscripción y cualquier otra información relevante necesaria para verificar su identidad y acceso a la universidad. La base de datos también almacenara información sobre cada código QR, como cuándo y dónde se emitió, con fines de seguimiento y auditoría. El personal autorizado, como administradores, tendrían acceso seguro a la base de datos para verificar las credenciales de los estudiantes en los puntos de entrada.

8.10.2 Identificar las entidades

Las identidades de esta base de datos son 4 las cuales son

Estudiantes

La tabla Estudiantes contendría información sobre los estudiantes, como su nombre, correo electrónico y contraseña, así como también un ID de estudiante único y otra información relevante.

Administradores

De manera similar, la tabla Administradores almacenaría información sobre los administradores e incluiría un campo admin_id y otra información relevante.

Unión Admin_Estudiant

Al crear esta tabla de combinación, podemos establecer una relación de muchos a muchos entre las tablas de administradores y estudiantes, donde cada administrador puede administrar varios estudiantes y cada estudiante puede ser administrado por varios administradores. Esto nos permite modelar con mayor precisión la relación del mundo real entre administradores y estudiantes en nuestro sistema.

Registro de Acceso

La tabla de registro de acceso rastrearía cuándo y dónde los usuarios acceden a la universidad, incluido su ID de usuario, la marca de tiempo del acceso y la ubicación del acceso y otra información relevante.

Credencial Digital

La tabla de credenciales digitales almacenaría la información necesaria para generar y mostrar el código QR y otra información relevante.

9. Resultados

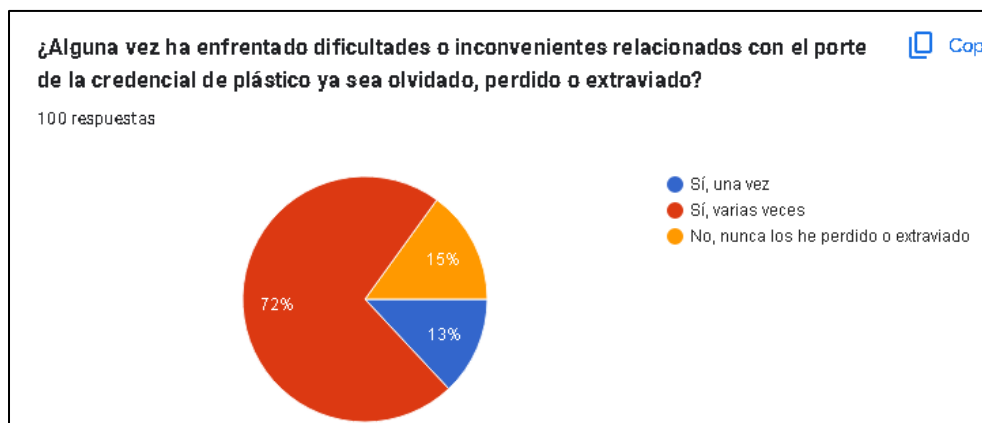
9.1 Presentación y discusión de los resultados

En esta etapa del proyecto, nos adentramos en la presentación y discusión de los resultados obtenidos a través de una encuesta realizada a 100 estudiantes. El objetivo de esta encuesta fue recopilar información relevante que nos permitiera comprender las opiniones, percepciones y necesidades de los estudiantes en relación con nuestro proyecto. El cuestionario constaba de 13 reactivos cuidadosamente diseñados para abordar diferentes aspectos relacionados con la implementación de nuestra aplicación móvil y la sustitución de las credenciales físicas por un sistema de identificación digital basado en códigos QR.

En esta sección, comparte los hallazgos principales de la encuesta y analizaremos en detalle los resultados obtenidos. Explorando las respuestas de los estudiantes, identificar patrones y tendencias, y extraer conclusiones significativas que ayudarán a evaluar la viabilidad y eficacia del proyecto. Además, abre espacio para la discusión de los resultados, donde se reflexiona sobre las implicaciones de estos hallazgos y las posibles acciones que se podrían tomar para mejorar y optimizar el sistema en función de los comentarios y sugerencias recibidos.

Pregunta 1

Figura 8.- Resultados pregunta 1



En la Figura 8.- Resultados pregunta 1, muestra lo siguiente:

Representación de los resultados:

Pregunta: *¿Alguna vez ha enfrentado dificultades o inconvenientes relacionados con el porte de la credencial de plástico ya sea olvidado, perdido o extraviado?*

Sí, una vez: **13%**

Sí, varias veces: **72%**

No, nunca los he perdido o extraviado: **15%**
TOTAL: **100%**

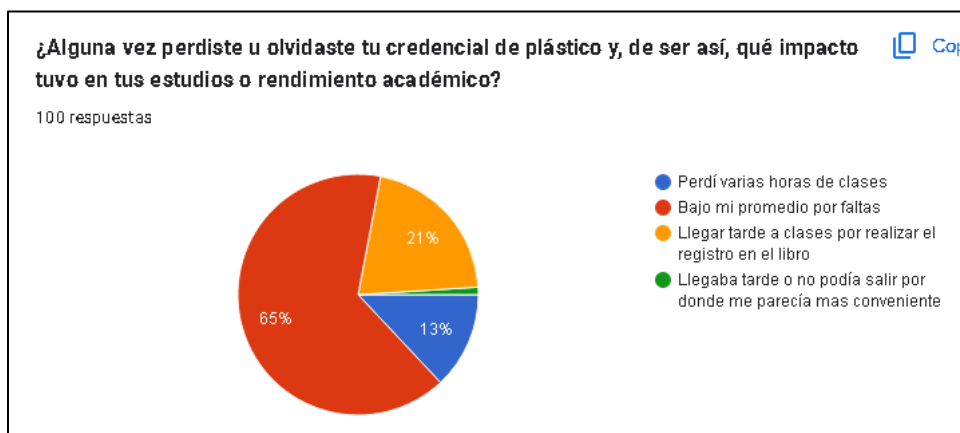
Discusión de los resultados:

Según los resultados de la encuesta, un porcentaje significativo de los estudiantes ha enfrentado dificultades o inconvenientes relacionados con el porte de la credencial de plástico. El 72% de los encuestados ha experimentado estas dificultades en varias ocasiones, mientras que el 13% de los participantes ha tenido esta experiencia en una sola ocasión. Por otro lado, el 15% de los estudiantes encuestados informa que nunca ha perdido o extraviado su credencial de plástico.

Estos resultados resaltan un problema común que muchos estudiantes han enfrentado con las credenciales físicas. Las dificultades relacionadas con el olvido, pérdida o extravío de las credenciales pueden causar inconvenientes significativos, como el acceso denegado a las instalaciones universitarias o la necesidad de solicitar reemplazos frecuentes.

Pregunta 2

Figura 9.- Resultados pregunta 2



En la Figura 9.- Resultados pregunta 2, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Alguna vez perdiste u olvidaste tú credencial de plástico y, de ser así, qué impacto tuvo en tus estudios o rendimiento académico?

Perdí varias horas de clases: **13%**

Bajó mi promedio por faltas: **65%**

Llegar tarde a clases por realizar el registro en el libro: **21%**

Llegaba tarde o no podía salir por donde me parecía más conveniente: **1%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados revelan que la pérdida u olvido de la credencial de plástico ha tenido un impacto significativo en el rendimiento académico de los estudiantes encuestados. El 65% de los participantes informa que su promedio se vio afectado por faltas debido a la pérdida u olvido de la credencial. Esta situación resalta la importancia de contar con una alternativa más eficiente y confiable para el acceso a las instalaciones universitarias.

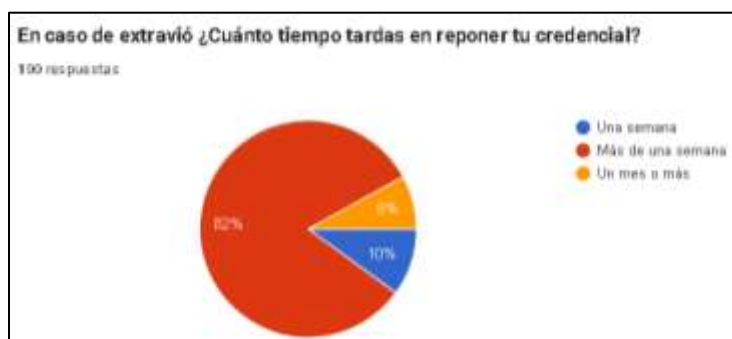
Además, el 21% de los estudiantes indica que llegar tarde a clases debido a la necesidad de realizar el registro manual en un libro ha sido un efecto negativo de la pérdida u olvido de la credencial. Esto implica que el proceso actual de registro manual puede retrasar el inicio de las clases y afectar la puntualidad de los estudiantes.

Por otro lado, el 13% de los encuestados menciona que ha perdido varias horas de clases como resultado de no tener su credencial. Este impacto directo en la asistencia a clases puede afectar negativamente el aprendizaje y la participación en actividades académicas.

Es importante destacar que solo el 1% de los estudiantes indicó que el impacto de la pérdida u olvido de la credencial fue la dificultad para llegar tarde o salir por donde les resultaba más conveniente. Aunque es un porcentaje bajo, esto resalta la incomodidad y restricciones que pueden surgir debido a la dependencia de la credencial física.

Resultado 3

Figura 10.- Resultados pregunta 3



En la Figura 10.- Resultados pregunta 3, muestra lo siguiente:

Representación de los resultados:

Pregunta: En caso de extravío, ¿Cuánto tiempo tardas en reponer tú credencial?

Una semana: **10%**

Más de una semana: **82%**

Un mes o más: **8%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados revelan que la reposición de una credencial extraviada lleva un tiempo considerable para la mayoría de los estudiantes encuestados. Un alto porcentaje, el 82%, menciona que tarda más de una semana en obtener una nueva credencial después de haberla extraviado. Esto indica que el proceso actual de reemplazo de las credenciales físicas implica una demora significativa y puede generar inconvenientes adicionales para los estudiantes.

Un porcentaje menor, el 10%, indica que tarda aproximadamente una semana en obtener una nueva credencial. Aunque este tiempo es más corto en comparación con el grupo anterior, sigue siendo un período considerable en el cual los estudiantes pueden enfrentar dificultades para acceder a las instalaciones universitarias.

Por último, el 8% de los participantes informa que tarda un mes o más en reponer su credencial extraviada. Este grupo representa a los estudiantes que enfrentan el mayor tiempo de espera para obtener una nueva credencial. Este retraso prolongado puede tener un impacto negativo en su capacidad para acceder a las instalaciones universitarias y participar en actividades académicas de manera oportuna.

Pregunta 4

Figura 11.- Resultados pregunta 4



En la Figura 11.- Resultados pregunta 4, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Cuál es el motivo por el que te tardas en reponer tú credencial?

Económico (Costo de reposición): **30%**

Falta de tiempo: **46%**
Desconocimiento del proceso: **18%**
Tiempo de entrega: **6%**
TOTAL: **100%**

Discusión de los resultados:

Los resultados muestran los diferentes motivos que contribuyen a la demora en la reposición de las credenciales por parte de los estudiantes encuestados. El factor más mencionado es la falta de tiempo, con un 46% de los participantes señalándolo como motivo para tardar en reponer su credencial. Esto indica que los estudiantes tienen dificultades para encontrar un momento adecuado en sus agendas ocupadas para ocuparse del proceso de reposición.

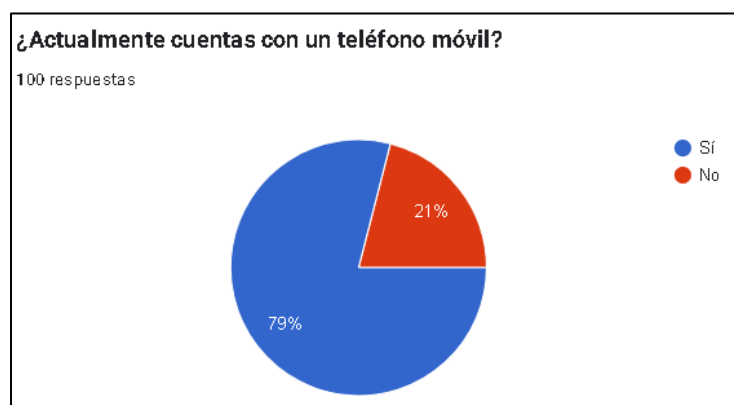
Otro motivo significativo es el factor económico, con el 30% de los estudiantes indicando que el costo de reposición es un factor que contribuye a la demora. Esto sugiere que algunos estudiantes pueden enfrentar restricciones financieras para cubrir los gastos asociados con la obtención de una nueva credencial.

El desconocimiento del proceso también se identifica como un motivo para la demora en la reposición, con el 18% de los estudiantes admitiendo que no están completamente familiarizados con el proceso necesario para obtener una nueva credencial. Esta falta de información puede dificultar el inicio del proceso y retrasar la obtención de la credencial de reemplazo.

Finalmente, el 6% de los participantes menciona el tiempo de entrega como un motivo para la demora en la reposición. Esto sugiere que algunos estudiantes experimentan retrasos en la entrega de las nuevas credenciales, lo cual puede ser un factor frustrante y que contribuye a la espera prolongada.

Pregunta 5

Figura 12.- Resultados pregunta 5



En la Figura 12.- Resultados pregunta 5, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Actualmente cuentas con un teléfono móvil?

Sí: **79%**

No: **21%**

TOTAL: **100%**

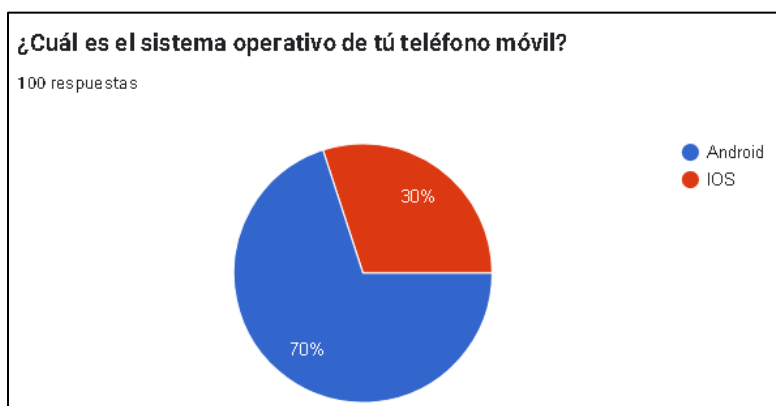
Discusión de los resultados:

Los resultados revelan que la gran mayoría de los estudiantes encuestados, con un 79%, cuentan actualmente con un teléfono móvil. Esto indica que la mayoría de los estudiantes tienen acceso a un dispositivo móvil, lo cual es un factor clave para la implementación exitosa de nuestra aplicación móvil. El hecho de que el 79% de los participantes tengan un teléfono móvil sugiere una amplia disponibilidad de dispositivos y un alto grado de familiaridad con el uso de tecnología móvil. Esto facilitaría la adopción de la aplicación móvil propuesta en nuestro proyecto, ya que la mayoría de los estudiantes ya poseen el hardware necesario para utilizarla.

Sin embargo, es importante tener en cuenta que el 21% de los estudiantes encuestados no cuenta con un teléfono móvil. Esto indica que un segmento de la población estudiantil puede no tener acceso a dispositivos móviles, lo cual debe considerarse al diseñar estrategias de implementación y brindar alternativas de acceso para aquellos estudiantes que no poseen un teléfono móvil.

Pregunta 6

Figura 13.- Resultados pregunta 6



En la Figura 13.- Resultados pregunta 6, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Cuál es el sistema operativo de tu teléfono móvil?

Android: **70%**

iOS: **30%**

TOTAL: 100%

Discusión de los resultados:

Los resultados muestran la distribución de los sistemas operativos utilizados por los estudiantes encuestados en sus teléfonos móviles. El 70% de los participantes indica que utilizan el sistema operativo Android, mientras que el 30% utiliza iOS.

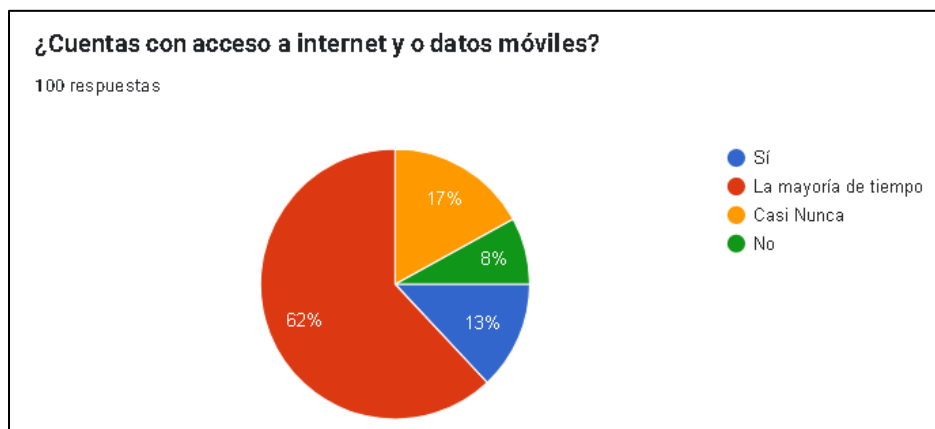
El hecho de que el sistema operativo Android sea el más comúnmente utilizado por los estudiantes encuestados refleja la prevalencia de dispositivos Android en el mercado. Esto sugiere que una gran mayoría de los estudiantes posee teléfonos móviles Android, lo cual es relevante para el desarrollo de la aplicación móvil. Al dirigirnos a la mayoría de los usuarios con dispositivos Android, podemos asegurarnos de que nuestra aplicación sea compatible con la plataforma más utilizada.

Sin embargo, es importante tener en cuenta que el 30% de los estudiantes utiliza dispositivos iOS, lo cual representa una parte significativa de la población encuestada. Esto indica que también debemos considerar la compatibilidad con el sistema operativo iOS al desarrollar nuestra aplicación móvil, para garantizar que los usuarios de dispositivos iOS puedan acceder a todas las funcionalidades de la aplicación.

En resumen, estos resultados resaltan la importancia de considerar la compatibilidad con los sistemas operativos Android y iOS al desarrollar la aplicación móvil para nuestro proyecto. Al abordar ambas plataformas, podemos asegurarnos de que la aplicación sea accesible para la mayoría de los estudiantes encuestados, independientemente del sistema operativo que utilicen en sus teléfonos móviles.

Pregunta 7

Figura 14.- Resultados pregunta 7



En la Figura 14.- Resultados pregunta 7, muestra lo siguiente:

Representación de los resultados:

Pregunta: *¿Cuentas con acceso a internet y/o datos móviles?*

Sí: **13%**

La mayoría de tiempo: **62%**

Casi nunca: **17%**

No: **8%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados revelan la disponibilidad y el nivel de acceso a internet y datos móviles por parte de los estudiantes encuestados. La mayoría de los participantes, con un 62%, afirman contar con acceso a internet y/o datos móviles la mayor parte del tiempo. Esto indica que la mayoría de los estudiantes tienen una conectividad estable y confiable, lo cual es fundamental para el funcionamiento adecuado de nuestra aplicación móvil.

Por otro lado, un porcentaje significativo, el 17%, menciona que cuentan con acceso a internet y/o datos móviles casi nunca. Esto puede deberse a limitaciones económicas o a la falta de disponibilidad de servicios de internet en ciertas áreas. Estos estudiantes pueden enfrentar dificultades adicionales para utilizar una aplicación móvil que requiera una conexión constante a internet.

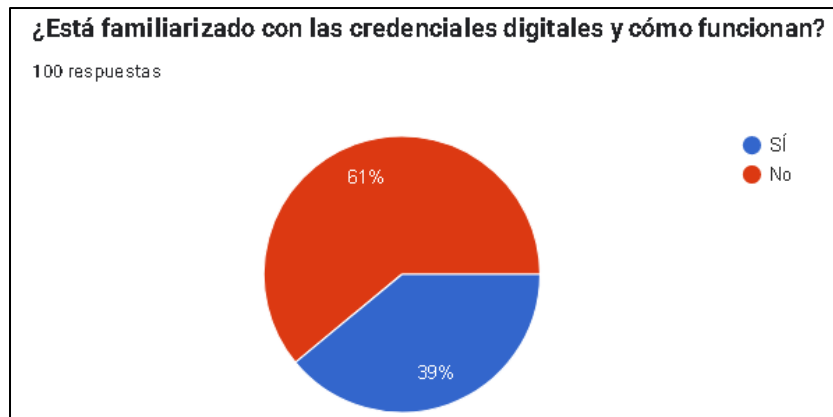
Un pequeño porcentaje, el 13%, indica que cuentan con acceso a internet y/o datos móviles, pero no de manera constante. Esto implica que estos estudiantes pueden experimentar intermitencias en su conectividad, lo que puede afectar la experiencia de uso de la aplicación móvil.

Además, el 8% de los participantes informa que no cuentan con acceso a internet y/o datos móviles en absoluto. Esto puede ser un factor limitante para su capacidad de utilizar una aplicación móvil que requiera conectividad en línea.

En general, estos resultados resaltan la importancia de tener en cuenta la disponibilidad y la calidad del acceso a internet y datos móviles al desarrollar nuestra aplicación móvil. Deberíamos diseñar la aplicación de manera que funcione de manera óptima tanto en situaciones de conectividad estable como en situaciones de conectividad limitada. También es importante proporcionar alternativas para aquellos estudiantes que tienen dificultades para acceder a internet o datos móviles de manera consistente.

Pregunta 8

Figura 15.- Resultados pregunta 8



En la Figura 15.- Resultados pregunta 8, muestra lo siguiente:

Representación de los resultados:

Pregunta: *¿Está familiarizado con las credenciales digitales y cómo funcionan?*

No: **61%**

Sí: **39%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados muestran que una mayoría de los estudiantes encuestados, con un 61%, no están familiarizados con las credenciales digitales y cómo funcionan. Esto indica que la mayoría de los estudiantes tienen poco conocimiento o comprensión de las credenciales digitales en el contexto de nuestro proyecto.

Por otro lado, un 39% de los participantes afirma estar familiarizado con las credenciales digitales y cómo funcionan. Esto sugiere que un segmento significativo de los estudiantes tiene algún nivel de conocimiento sobre las credenciales digitales y su utilización.

Estos resultados destacan la importancia de brindar una adecuada educación y capacitación sobre las credenciales digitales a aquellos estudiantes que no están familiarizados con ellas. Es esencial garantizar que los usuarios comprendan los beneficios y el funcionamiento de las credenciales digitales en comparación con las tradicionales credenciales físicas de plástico.

Pregunta 9

Figura 16.- Resultados pregunta 9



En la Figura 16.- Resultados pregunta 9, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Le resultaría conveniente tener su credencial de plástico de forma digital en una aplicación móvil para acceder al instituto y a sus servicios?

Sí, mucho más conveniente: **60%**

Sí, algo más conveniente: **14%**

No, aproximadamente el mismo nivel de conveniencia: **23%**

No, menos conveniente: **3%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados muestran una clara preferencia por tener la credencial de plástico de forma digital en una aplicación móvil para acceder al instituto y a sus servicios. El 60% de los participantes considera que sería mucho más conveniente, mientras que el 14% opina que sería algo más conveniente. Estos resultados reflejan una aceptación positiva de la idea de migrar hacia una credencial digital en lugar de la tradicional credencial física.

Sin embargo, también es importante tener en cuenta que el 23% de los encuestados considera que el nivel de conveniencia sería aproximadamente el mismo. Esto indica que un segmento considerable de los estudiantes no ve una diferencia significativa entre la credencial de plástico y la credencial digital en términos de conveniencia. Es fundamental comprender las razones detrás de esta percepción y abordarlas adecuadamente para asegurar una adopción amplia y exitosa de la credencial digital.

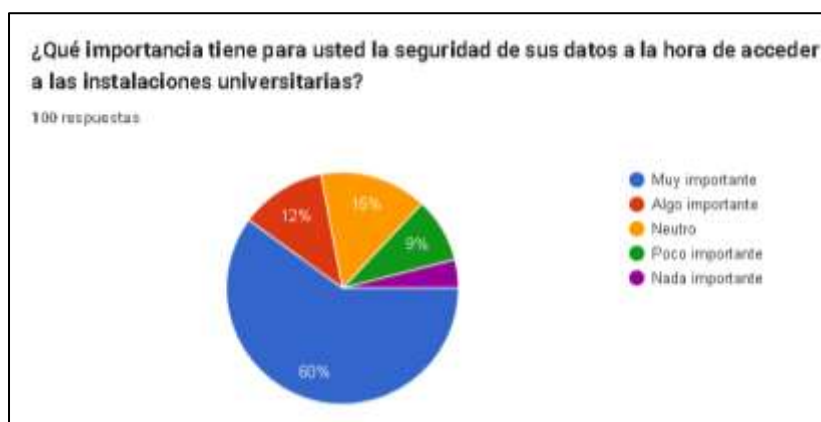
Es interesante observar que solo el 3% de los participantes considera que la credencial digital sería menos conveniente. Esto puede ser atribuido a factores como la falta de familiaridad o resistencia al cambio. Es importante brindar

información y demostrar los beneficios y la facilidad de uso de la credencial digital para superar estas preocupaciones y promover su adopción.

En general, estos resultados respaldan la idea de implementar una credencial digital en una aplicación móvil para acceder al instituto y a sus servicios. La mayoría de los estudiantes encuestados perciben que sería una opción mucho más conveniente o algo más conveniente en comparación con la credencial de plástico. Esto refuerza la importancia de continuar con el desarrollo de la aplicación móvil en nuestro proyecto y trabajar en su usabilidad y funcionalidad para satisfacer las necesidades y expectativas de los estudiantes.

Pregunta 10

Figura 17.- Resultados pregunta 10



En la Figura 17.- Resultados pregunta 10, muestra lo siguiente:

Representación de los resultados:

Pregunta: ¿Qué importancia tiene para usted la seguridad de sus datos a la hora de acceder a las instalaciones universitarias?

Muy importante: **60%**

Algo importante: **12%**

Neutro: **15%**

Poco importante: **9%**

Nada importante: **4%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados revelan que la seguridad de los datos es una preocupación significativa para la mayoría de los estudiantes encuestados. Un 60% considera que la seguridad de sus datos es muy importante al acceder a las instalaciones

universitarias. Esto indica que estos estudiantes valoran y priorizan la protección de su información personal y confidencial.

Además, un 12% opina que la seguridad de sus datos es algo importante, lo que sugiere que también consideran relevante la protección de sus datos, aunque no al mismo nivel de importancia que el grupo anterior.

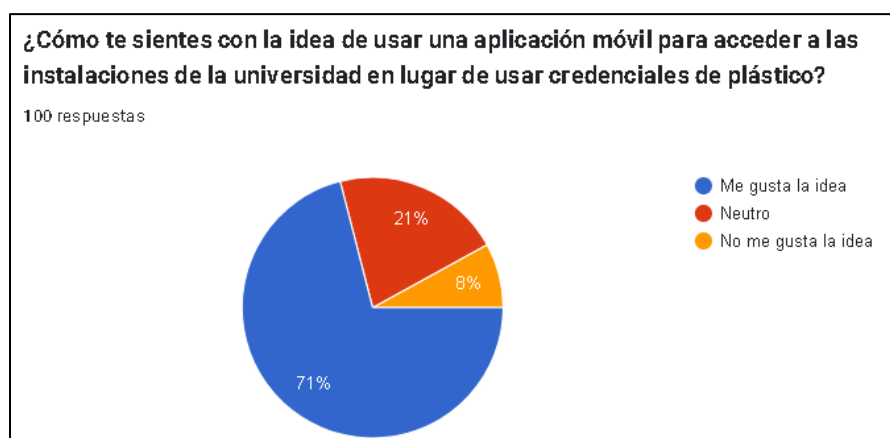
Un 15% de los participantes se muestra neutro en cuanto a la importancia de la seguridad de sus datos. Esto puede deberse a diversas razones, como falta de conciencia sobre los riesgos de seguridad o una percepción de que la protección de datos es responsabilidad exclusiva de la institución universitaria. Es importante abordar estas percepciones neutrales y proporcionar información adicional para fomentar una mayor conciencia sobre la importancia de la seguridad de los datos.

Por otro lado, un porcentaje menor de estudiantes (9%) considera que la seguridad de sus datos es poco importante, y un 4% opina que no es importante en absoluto. Estas respuestas pueden ser el resultado de una falta de comprensión sobre los riesgos de seguridad o una confianza excesiva en la protección de datos proporcionada por la institución. Es crucial educar a estos estudiantes sobre la importancia de la seguridad de los datos y los posibles impactos negativos de una brecha de seguridad.

En general, estos resultados subrayan la necesidad de implementar medidas sólidas de seguridad en nuestra aplicación móvil para garantizar la protección de los datos de los estudiantes. Es esencial diseñar y desarrollar el sistema de forma segura, utilizando técnicas de encriptación y autenticación adecuadas para salvaguardar la información personal y confidencial de los usuarios.

Pregunta 11

Figura 18.- Resultados pregunta 11



En la Figura 18.- Resultados pregunta 11, muestra lo siguiente:

Representación de los resultados:

Pregunta: *¿Cómo te sientes con la idea de usar una aplicación móvil para acceder a las instalaciones de la universidad en lugar de usar credenciales de plástico?*

Me gusta la idea: **71%**

Neutro: **21%**

No me gusta la idea: **8%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados muestran una receptividad general hacia la idea de utilizar una aplicación móvil en lugar de las credenciales de plástico para acceder a las instalaciones universitarias. La mayoría de los participantes (71%) indican que les gusta la idea, lo que sugiere que están abiertos y entusiasmados con la posibilidad de adoptar una solución digital para acceder a las instalaciones.

Un porcentaje considerable de estudiantes (21%) se muestra neutro en cuanto a la idea de utilizar una aplicación móvil. Esto puede deberse a una falta de familiaridad con las aplicaciones móviles o a una preferencia por las credenciales de plástico debido a su familiaridad y comodidad. Es importante abordar las preocupaciones y dudas de este grupo, proporcionando información adicional y demostrando los beneficios y la facilidad de uso de la aplicación móvil.

Por último, un 8% de los participantes expresa que no les gusta la idea de utilizar una aplicación móvil para acceder a las instalaciones. Esto puede ser debido a diversas razones, como preocupaciones sobre la seguridad de los datos, resistencia al cambio o preferencia por métodos tradicionales. Es fundamental abordar estas preocupaciones y brindar información adicional sobre los beneficios y las mejoras que ofrece la aplicación móvil en comparación con las credenciales de plástico.

En general, la mayoría de los estudiantes encuestados muestran una actitud positiva hacia la idea de utilizar una aplicación móvil para acceder a las instalaciones universitarias. Esto respalda la dirección de nuestro proyecto y la implementación de una solución digital para reemplazar las credenciales de plástico. Sin embargo, es importante considerar las preocupaciones y dudas de aquellos estudiantes que se muestran neutrales o no están de acuerdo, a fin de abordar sus inquietudes y garantizar una adopción exitosa de la aplicación móvil.

Pregunta 12

Figura 19.- Resultados pregunta 12



En la Figura 19.- Resultados pregunta 12, muestra lo siguiente:

Representación de los resultados:

Pregunta: *¿Estaría dispuesto a participar en un programa piloto para probar una aplicación móvil donde tenga tu credencial digital para poder acceder a la institución y los servicios que esta ofrece, y de ser así, qué factores influirían en su decisión de participar?*

Sí: **76%**

No: **24%**

TOTAL: **100%**

Discusión de los resultados:

Los resultados muestran que la mayoría de los participantes (76%) estaría dispuesto a participar en un programa piloto para probar una aplicación móvil con una credencial digital para acceder a la institución y sus servicios. Esto indica un alto nivel de interés y disposición por parte de los estudiantes para probar nuevas soluciones tecnológicas y participar activamente en la implementación de mejoras en el acceso a la institución.

Es alentador ver que un porcentaje significativo de estudiantes está dispuesto a participar en el programa piloto, ya que esto proporcionará información valiosa y retroalimentación directa para mejorar la aplicación móvil y garantizar su funcionalidad y usabilidad. La participación activa de los estudiantes en el proceso piloto ayudará a identificar posibles problemas, evaluar la efectividad de la aplicación y ajustarla según las necesidades y preferencias de los usuarios.

Sin embargo, un 24% de los participantes indica que no estaría dispuesto a participar en el programa piloto. Las razones detrás de esta respuesta pueden

variar, desde preocupaciones de privacidad y seguridad hasta una falta de interés o disponibilidad de tiempo para participar en actividades adicionales. Es importante abordar estas preocupaciones y considerar estrategias para incentivar la participación de este grupo, como brindar información adicional sobre las medidas de seguridad implementadas y los beneficios de ser parte del programa piloto.

En términos de factores que influirían en la decisión de participar, es importante considerar las preferencias individuales de los estudiantes. Algunos posibles factores que podrían influir en su decisión incluyen:

- Confianza en la seguridad de la aplicación y la protección de datos personales.
- Comodidad y facilidad de uso de la aplicación móvil.
- Conveniencia en términos de acceso y uso de la aplicación.
- Beneficios adicionales ofrecidos a través del programa piloto, como acceso anticipado a nuevas funciones o servicios.
- Incentivos o recompensas proporcionados a los participantes del programa piloto.

En resumen, la mayoría de los estudiantes encuestados se muestra dispuesta a participar en un programa piloto para probar una aplicación móvil con una credencial digital. Sin embargo, es importante abordar las preocupaciones y dudas de aquellos que no están dispuestos a participar y considerar los factores que influirían en la decisión de participar para garantizar una alta tasa de participación y retroalimentación efectiva.

Pregunta 13

Figura 20.- Resultados pregunta 13

¿Tiene algún otro comentario o sugerencia relacionada con la implementación de credenciales digitales basadas en dispositivos móviles para el acceso a la universidad?

Respuestas

No
ninguno
Bu
no
no
por el momento no
NO

En la Figura 20.- Resultados pregunta 13, muestra lo siguiente:

Aunque muchos participantes no ofrecieron comentarios adicionales o sugerencias específicas relacionadas con la implementación de credenciales digitales basadas en dispositivos móviles, es alentador notar que algunos expresaron su deseo de que esta solución se implemente. Esto sugiere un interés general y una receptividad positiva hacia la adopción de credenciales digitales en lugar de las tradicionales credenciales de plástico.

La falta de comentarios adicionales puede deberse a varios factores, como la simplicidad del cuestionario o la falta de conocimiento y experiencia previa de los participantes en relación con las credenciales digitales. Sin embargo, el hecho de que algunos participantes hayan mencionado que esperan que se implemente esta solución indica que existe un reconocimiento de los beneficios potenciales de las credenciales digitales en términos de conveniencia, seguridad y eficiencia.

En general, los resultados sugieren una actitud positiva hacia las credenciales digitales basadas en dispositivos móviles para el acceso a la universidad. Sin embargo, se debe continuar con el proceso de consulta y participación de los estudiantes para garantizar que las soluciones implementadas aborden adecuadamente sus necesidades y preocupaciones, y para fomentar una adopción exitosa de las credenciales digitales.

9.2 Modelamiento de base de datos

9.2.1 Defina los atributos

Estudiantes

- **Id_estudiante**
- Nombre
- Apellido Paterno
- Apellido Materno
- Edad
- Fecha de nacimiento
- Dirección
- Correo electrónico
- Número de control
- Contraseña
- Numero de celular
- Carrera
- Semestre
- Ciclo Escolar
- Estudiante Activo

Administradores

- **Id_administrador**
- Nombre
- Apellido Paterno
- Apellido Materno
- Edad
- Fecha de nacimiento
- Dirección
- Correo electrónico
- Contraseña
- Número de celular

Unión Admin_Estudiant

- **Id_administrador**
- **Id_estudiante**

Credencial Digital

- **Id_credencial**
- QR

- **Id_estudiante**

Registro de Acceso

- **Id_Acceso**
- Ubicación_de_acceso
- Fecha
- Hora
- **Id_credencial**

9.2.2 Definir las relaciones

Tabla de estudiantes: Esta tabla almacenaría información sobre cada estudiante, como su nombre, carrera e identificación. Cada estudiante tendría una identificación única, que sería la clave principal de la tabla.

Tabla de administradores: Esta tabla almacenaría información sobre cada administrador, como su nombre, ID y credenciales de inicio de sesión. Cada administrador puede administrar varios estudiantes y cada estudiante puede ser administrado por varios administradores. Para modelar esta relación de muchos a muchos, necesitaría crear una tabla de unión.

Tabla de credenciales digitales: Esta tabla almacenaría información sobre cada credencial digital, como su identificación única y la identificación del estudiante al que corresponde. Cada estudiante tendría una relación de uno a uno con una credencial digital, lo que significa que cada estudiante tendría solo una credencial digital y cada credencial digital correspondería a un solo estudiante. Para modelar esta relación, la tabla Credenciales digitales incluiría una clave foránea que haga referencia al ID del alumno en la tabla Alumnos.

Tabla de registros de acceso: esta tabla almacenaría información sobre cada vez que se escanea una credencial digital, como la fecha y la hora del escaneo y la identificación de la credencial digital que se escaneó. Cada registro de acceso correspondería a una credencial digital y cada credencial digital correspondería a un estudiante. Para modelar esta relación, la tabla de registros de acceso incluiría una clave externa que hace referencia al ID de la credencial digital en la tabla de credenciales digitales.

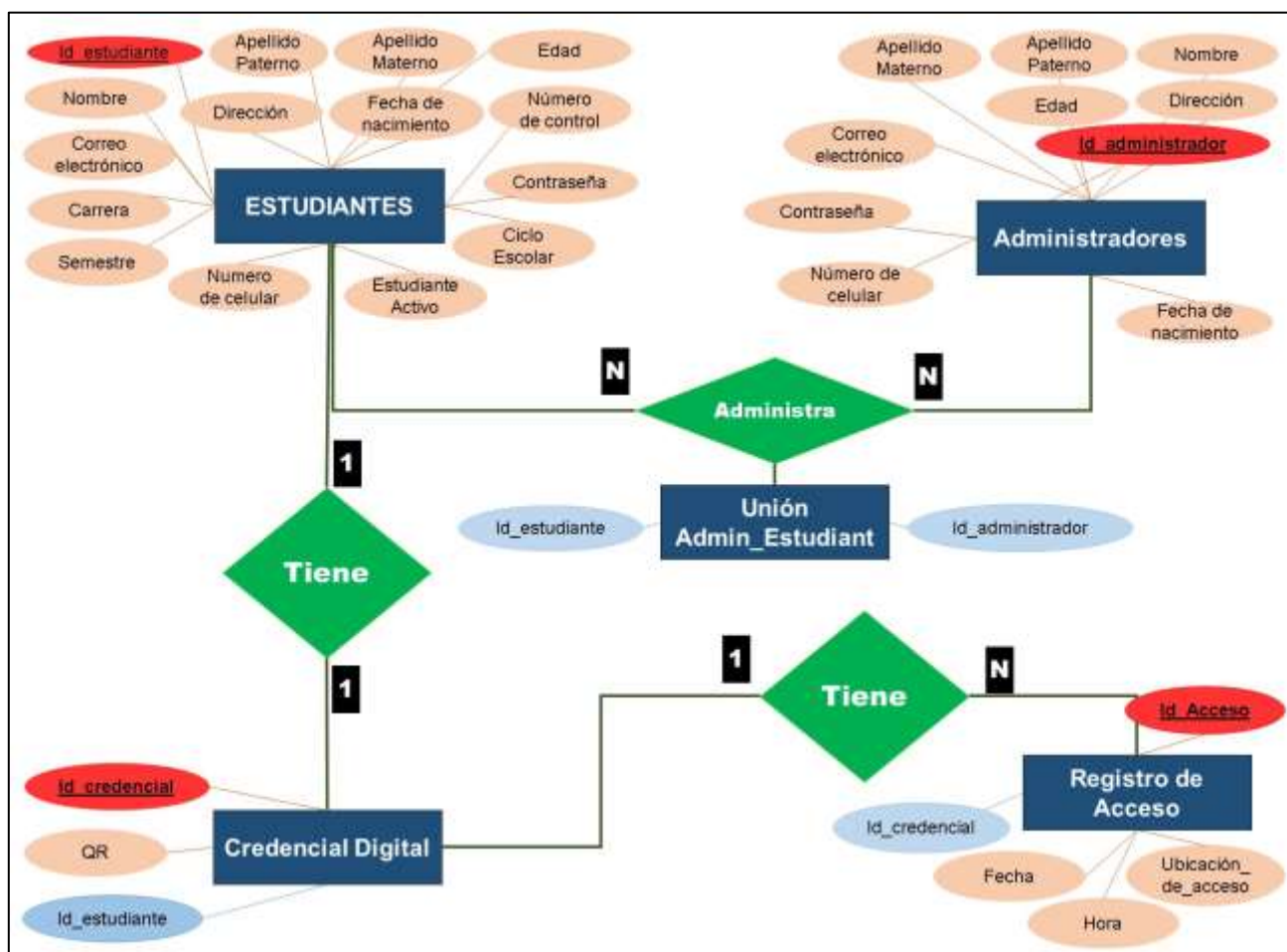
Tabla de unión Administradores Estudiantes: Esta tabla tendría dos claves foráneas, una que hace referencia al ID del administrador en la tabla Administradores y otra que hace referencia al ID del estudiante en la tabla Estudiantes. Esto le permitiría asociar varios administradores con varios estudiantes.

En general, el uso de una tabla de unión en la relación de muchos a muchos entre la tabla de administradores y la tabla de estudiantes le permitiría administrar de manera eficaz el acceso y los permisos de varios administradores a varios estudiantes.

9.2.3 Diseñe el esquema de la base de datos

Diagrama Entidad Relación

Figura 21.- Diagrama Entidad Relación del sistema



En la Figura 21.- Diagrama Entidad Relación, muestra lo siguiente:

La tabla Estudiantes contiene información sobre cada estudiante, incluida su identificación, nombre y carrera.

La tabla Credenciales digitales contiene información sobre cada credencial digital, incluida su identificación, la identificación del estudiante al que pertenece y la fecha en que se emitió y caduca.

La tabla de registros de acceso contiene información sobre cada registro de acceso, incluida su identificación, la identificación de la credencial digital que se utilizó para acceder a la universidad, la fecha y hora del acceso y la ubicación de la entrada donde se produjo el acceso.

La tabla Administradores contiene información sobre cada administrador, incluidos su ID, nombre, correo electrónico y contraseña.

Tenga en cuenta que

- Los rectángulos de color azul representan las entidades.
- Los óvalos indican los atributos de las entidades.
- Las claves principales se indican de color rojo.
- Las claves externas se indican de color azul.
- Los rombos verdes entre las entidades indican las relaciones entre ellas.
- Las relaciones de uno a muchos y muchos a muchos son indicadas por una nomenclatura de 1:N y las relaciones de muchos a muchos indicadas por una nomenclatura de N:N.

9.2.4 Establezca las restricciones

1. Cada alumno solo puede tener una credencial digital, y cada credencial digital solo puede corresponder a un alumno. Esta relación uno a uno asegura que cada estudiante solo pueda acceder a la universidad utilizando su propia credencial digital única, y que cada credencial digital corresponda a un solo estudiante.
2. Cada registro de acceso debe estar asociado a una credencial digital válida. Esto garantiza que los registros de acceso solo se registren cuando se escanee una credencial digital válida.
3. Cada registro de acceso debe estar asociado con una fecha y hora únicas. Esto garantiza que no se puedan crear múltiples registros de acceso para la misma credencial digital al mismo tiempo.
4. Cada registro de acceso debe estar asociado con una credencial digital válida que pertenezca a un estudiante válido. Esto asegura que solo los estudiantes que tengan credenciales digitales válidas puedan acceder a la universidad y que solo se creen registros de acceso para estudiantes válidos.

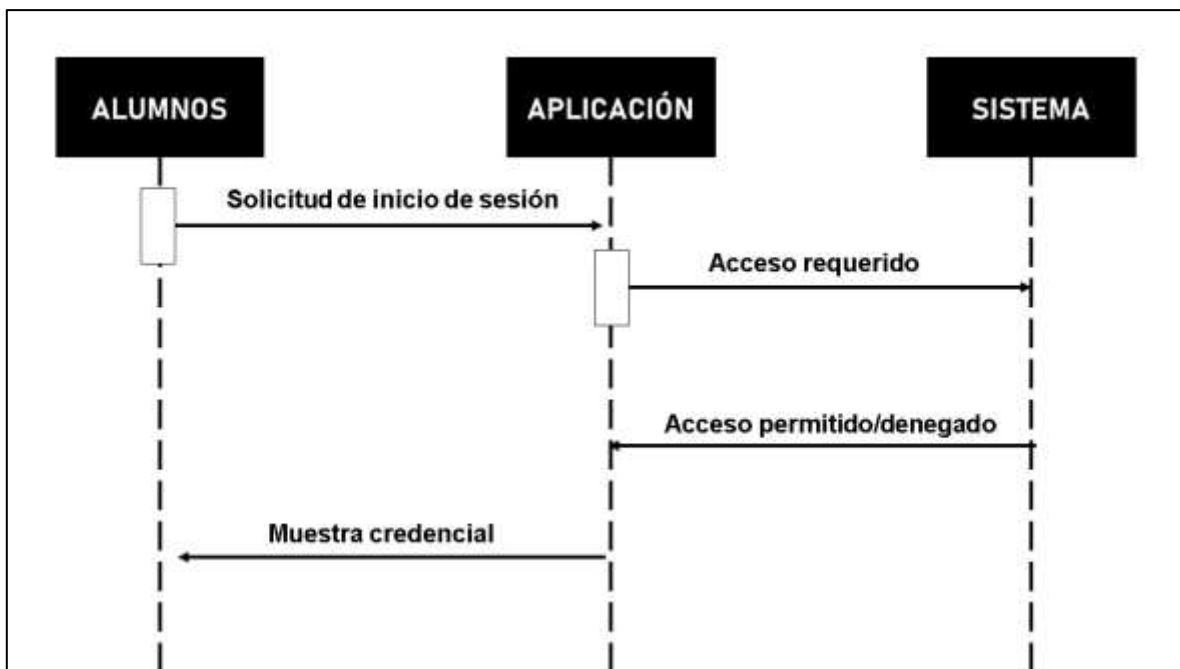
5. Cada administrador puede gestionar varios alumnos y cada alumno puede ser gestionado por varios administradores. Esta relación de muchos a muchos garantiza que varios administradores puedan administrar de manera efectiva a los estudiantes en el sistema y que cada estudiante pueda ser administrado por varios administradores.
6. Cada administrador debe tener credenciales de inicio de sesión válidas para acceder al sistema. Esto asegura que solo los administradores autorizados puedan acceder al sistema y administrar el estudiante y acceder a las tablas de registro.

Estas restricciones y reglas ayudan a garantizar la seguridad y la integridad del sistema y evitan cualquier acceso o modificación no autorizados a la base de datos.

9.3 Diagramas de secuencia

Diagrama de secuencia de inicio de sesión Alumno a la aplicación

Figura 22.- Diagrama de secuencia de inicio de sesión Alumno a la aplicación



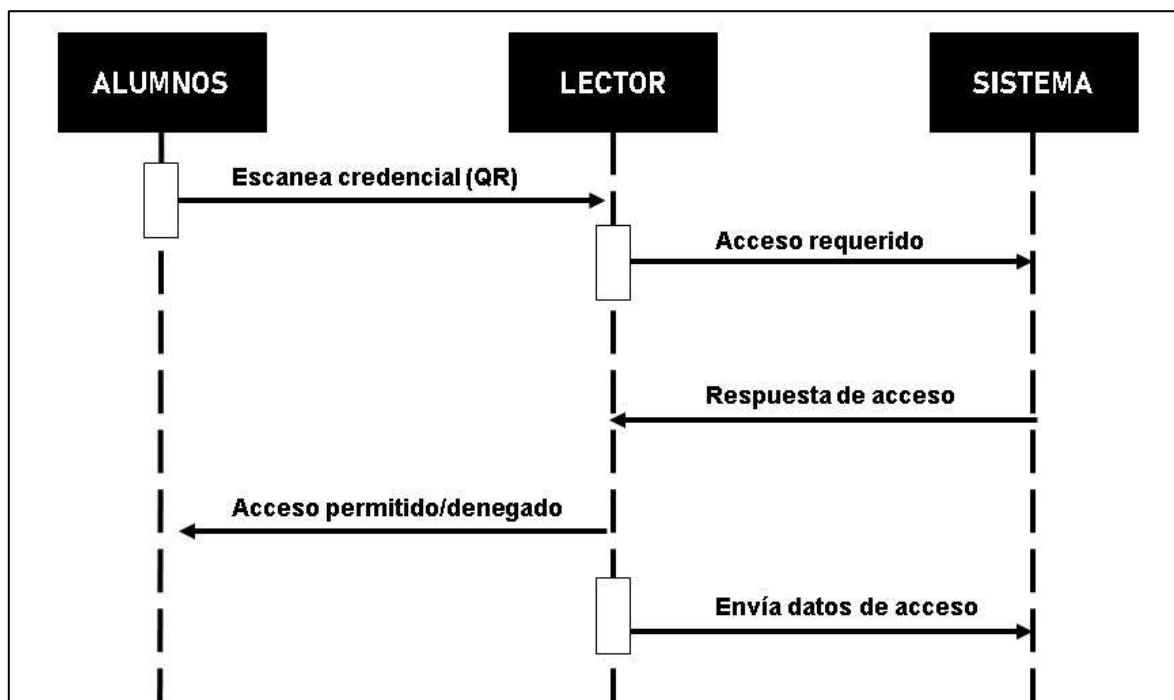
En la Figura 22.- Diagrama de secuencia de inicio de sesión alumnos a la aplicación, muestra lo siguiente:

En este diagrama de secuencia, el usuario inicia una solicitud de inicio de sesión ingresando sus credenciales (por ejemplo, número de control y contraseña) en la

aplicación móvil. La aplicación móvil envía la solicitud de acceso requerido, que verifica las credenciales y envía una respuesta que indica si el inicio de sesión fue permitido o denegado.

Diagrama de secuencia de acceso

Figura 23.- Diagrama de secuencia de acceso

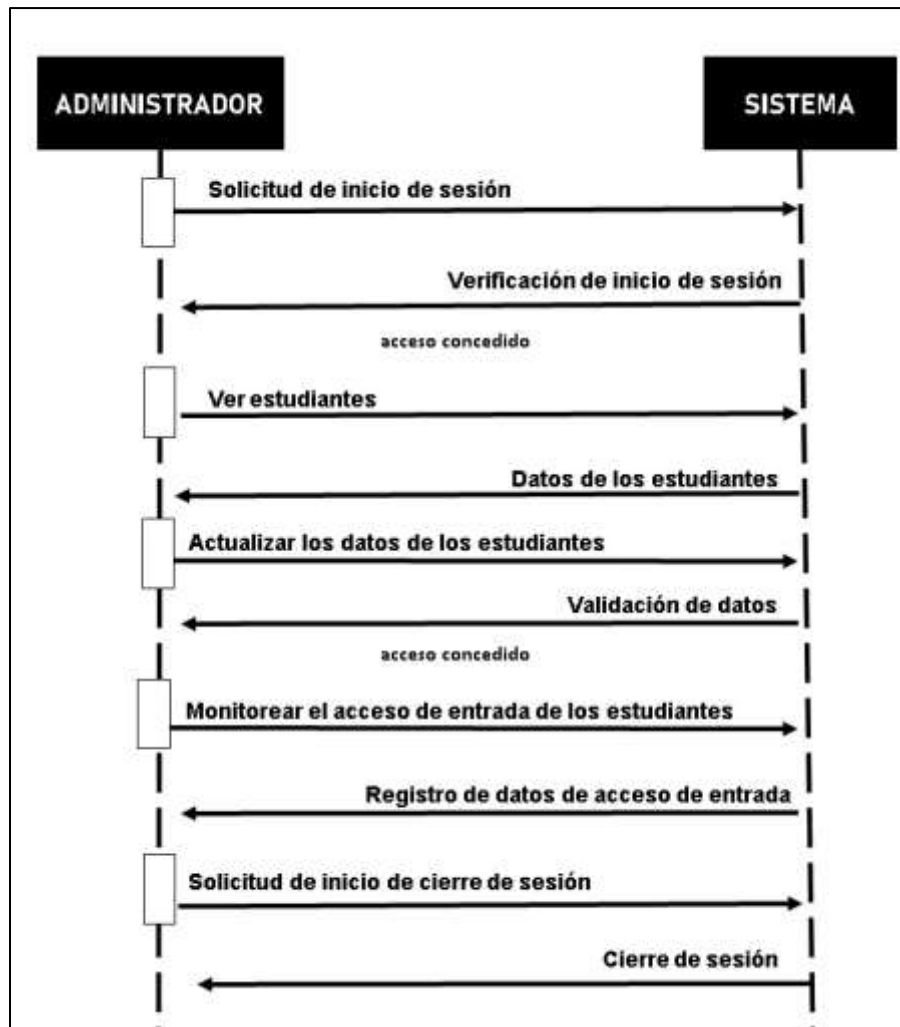


En la Figura 23.- Diagrama de secuencia de acceso, muestra lo siguiente:

En este diagrama de secuencia, el estudiante escanea su credencial digital (el código QR) al lector en la entrada del instituto. El lector escanea el código QR y envía una solicitud de acceso al sistema. El sistema verifica la credencial y devuelve una respuesta que indica si se debe otorgar o denegar el acceso. Luego, el lector permite o deniega el acceso según la respuesta del servidor. El lector envía los datos de acceso de entrada y salida del estudiante al sistema.

Diagrama de secuencia de autorización de administrador

Figura 24.- Diagrama de secuencia de autorización de administrador



En la Figura 24.- Diagrama de secuencia autorizado de ministrador, muestra lo siguiente:

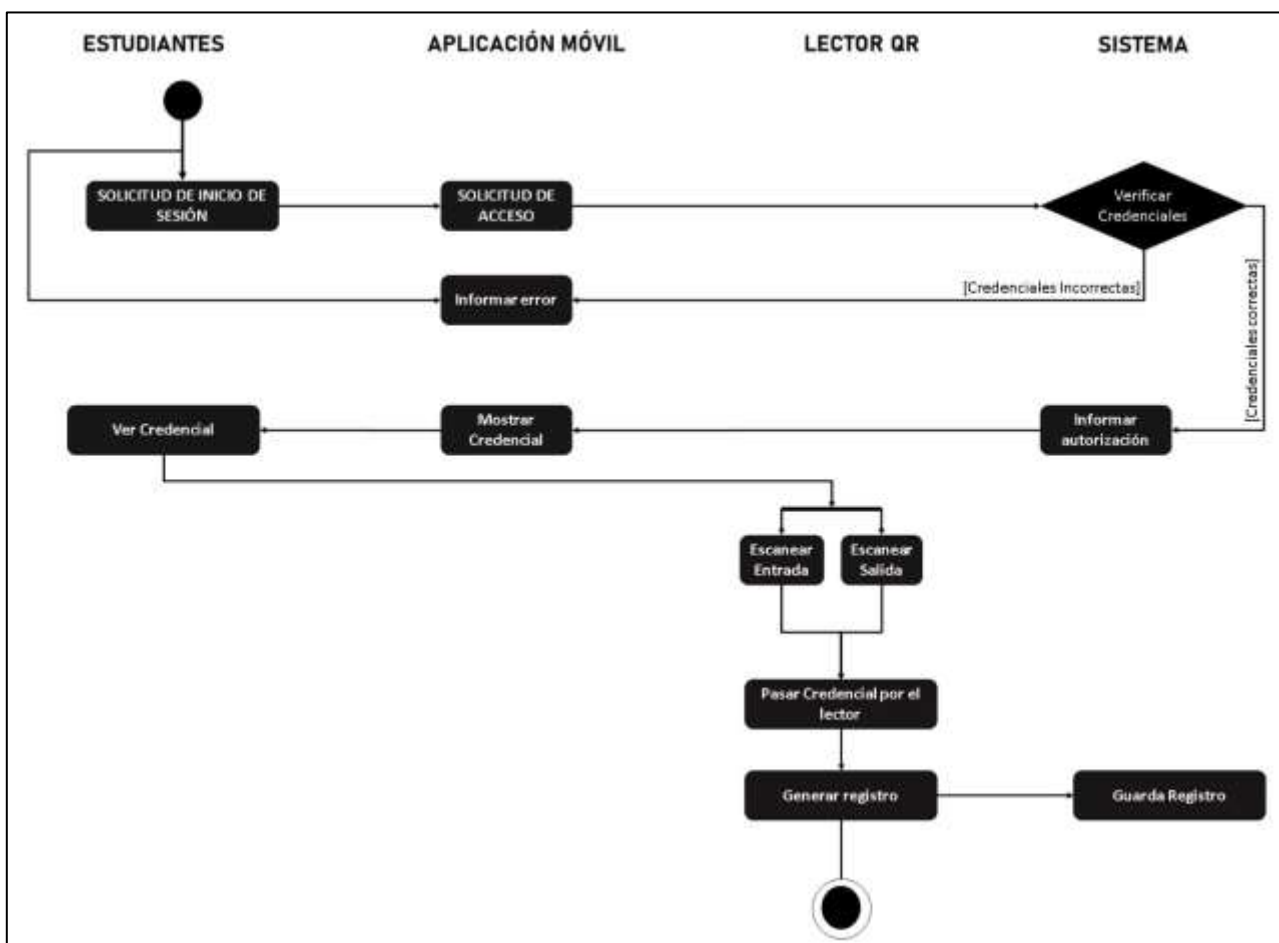
En el diagrama anterior, el administrador inicia la solicitud de inicio de sesión en el sistema proporcionando su nombre de usuario y contraseña. El sistema verifica las credenciales de inicio de sesión y otorga acceso al administrador si son válidas.

Una vez que haya iniciado sesión, el administrador puede ver los datos de los estudiantes y actualizarlos según sea necesario.

El administrador también puede monitorear el acceso de entrada y salida de los estudiantes a través del sistema. El sistema registra los datos de acceso de entrada y proporciona al administrador un registro de acceso.

Finalmente, el administrador inicia la solicitud de cierre de sesión y el sistema responde con una respuesta de cierre de sesión para finalizar la sesión.

9.4 Diagramas de actividad



En la Figura 25.- Diagrama de actividades del sistema, muestra lo siguiente:

El diagrama comienza con la actividad "Inicio de sesión del estudiante" en el lado izquierdo, que inicia el estudiante que ingresa sus credenciales (por ejemplo, número de control y contraseña) en la aplicación móvil. Luego, la aplicación envía una solicitud al sistema para verificar las credenciales, que se representa mediante la actividad "Verificar credenciales".

Si las credenciales son válidas, el sistema responde con un mensaje de "Inicio de sesión permitido" y el estudiante es redirigido a la actividad "Acceso", donde presenta su credencial digital (código QR) al lector en la entrada del instituto. Luego, el lector escanea el código QR y envía una solicitud al sistema para otorgar acceso. El sistema verifica la credencial y devuelve un mensaje de "Conceder acceso" o "Denegar acceso", dependiendo de si la credencial es válida o no.

Si se otorga el acceso, el estudiante puede ingresar al instituto y el sistema registra los datos de acceso, incluida la hora, la fecha y la ubicación de la entrada. Luego, el sistema actualiza el registro de acceso del estudiante, representado por la actividad "Actualizar registro de acceso".

En el lado derecho del diagrama, tenemos la actividad "Inicio de sesión del administrador", que es iniciada por el administrador que ingresa sus credenciales (nombre de usuario y contraseña) en el sistema. El sistema verifica las credenciales y, si son válidas, otorga acceso al administrador.

Una vez que haya iniciado sesión, el administrador tiene acceso a la "Base de datos de estudiantes", donde puede ver y modificar los datos de los estudiantes según sea necesario. Las actividades "Ver datos del alumno" y "Actualizar datos del alumno" representan estas acciones. Adicionalmente, el administrador puede monitorear la entrada y salida de cada estudiante a través del sistema, representado por la actividad "Monitor de Acceso". Esta actividad le permite al administrador ver el registro de acceso de cada estudiante y rastrear sus movimientos en todo el instituto.

Finalmente, el administrador puede cerrar sesión en el sistema, lo que está representado por la actividad "Cerrar sesión". Una vez que se inicia la solicitud de cierre de sesión, el sistema responde con un mensaje de "Respuesta de cierre de sesión" y la sesión finaliza.

En general, el diagrama de actividades proporciona una representación visual de las diferentes actividades que tienen lugar en el sistema, incluido el inicio de sesión, el control de acceso, la gestión de la base de datos de los estudiantes, la supervisión del registro de acceso y el cierre de sesión. También muestra las relaciones entre las diferentes actividades, así como los actores involucrados (estudiante y administrador) y el flujo de control del sistema.

9.5 Selección de herramientas

En el contexto de un proyecto, la sección de herramientas se refiere a la descripción de las herramientas, software, tecnologías u otros recursos utilizados durante el desarrollo del proyecto. Esta sección proporciona información detallada sobre las herramientas utilizadas para llevar a cabo diversas tareas y actividades relacionadas con el proyecto.

En la sección de herramientas, se enumeran y describen las herramientas específicas utilizadas en diferentes áreas del proyecto, como desarrollo de software, diseño, gestión de bases de datos, pruebas, análisis de datos, entre otros. Esto puede incluir lenguajes de programación, frameworks, bibliotecas, editores de código, herramientas de diseño gráfico, sistemas de gestión de bases de datos, software de pruebas, herramientas de seguimiento de proyectos, entre otros.

Además de proporcionar una lista de herramientas, es importante brindar detalles sobre cómo se utilizaron y qué funciones o ventajas específicas ofrecieron en el contexto del proyecto. Esto ayuda a los lectores a comprender mejor las decisiones tomadas y las metodologías utilizadas durante el desarrollo.

La sección de herramientas es importante porque permite a los lectores y a los miembros del equipo del proyecto conocer las tecnologías y recursos utilizados, lo que facilita la replicación o adaptación del proyecto en otros contextos. También proporciona transparencia y permite evaluar la idoneidad de las herramientas seleccionadas para el desarrollo del proyecto.

Herramientas de Diseño:

Adobe Illustrator: Adobe Illustrator para el diseño de las credenciales digitales y la creación de la paleta de colores. Esta herramienta proporciona una amplia gama de funciones y herramientas para la creación de ilustraciones vectoriales y diseño gráfico. Con Adobe Illustrator, pude diseñar las credenciales digitales de manera precisa, utilizando formas, colores, tipografías y otros elementos gráficos para lograr un diseño atractivo y profesional. Además, aproveché las capacidades de Adobe Illustrator para crear una paleta de colores coherente y armoniosa que reflejara la identidad visual del proyecto.

Estructura de Pantallas

Adobe Illustrator: Utilicé Adobe Illustrator para crear la estructura de pantallas de la aplicación móvil. Esta herramienta me permitió diseñar y organizar los elementos de interfaz de usuario de manera visual, lo que resultó en un flujo de navegación intuitivo y una experiencia de usuario coherente. Con Adobe Illustrator, pude diseñar y colocar los diferentes elementos de la interfaz de usuario, como botones, iconos, campos de entrada y etiquetas, de acuerdo con las mejores prácticas de diseño y usabilidad.

Además de Adobe Illustrator, también se seleccionó otras herramientas de diseño gráfico y prototipado, como Adobe XD, Adobe primiere pro, Adobe animated y Sketch, para crear prototipos interactivos y realizar pruebas de usabilidad con los usuarios. Estas herramientas permitieron simular la experiencia de uso de la aplicación antes de su implementación, lo que ayudó a identificar posibles mejoras y realizar ajustes en el diseño.

Herramienta de Prototipado:

Wondershare Mockitt (o Mockitt App): Wondershare Mockitt (o Mockitt App) como herramienta de prototipado para crear prototipos interactivos de la aplicación móvil. Esta herramienta ofrece una interfaz intuitiva y funcionalidades que facilitan la creación de prototipos de alta fidelidad. Con Wondershare Mockitt, pude diseñar y enlazar las diferentes pantallas de la aplicación para simular la experiencia de uso de forma interactiva.

El uso de Mockitt para crear los flujos de navegación de la aplicación, definir transiciones entre pantallas y agregar interacciones como toques, deslizamientos y animaciones. Esto me permitió presentar una representación visual y funcional de la aplicación a los interesados y obtener su retroalimentación temprana.

La elección de Wondershare Mockitt se basó en su facilidad de uso, su amplio conjunto de elementos y plantillas predefinidos, y su capacidad para generar prototipos interactivos que se asemejan a la experiencia de uso final de la aplicación.

Herramienta de Diseño para Base de Datos:

MySQL Workbench: MySQL Workbench como herramienta para el desarrollo de la estructura y elementos de la base de datos del proyecto. MySQL Workbench es una herramienta visual que proporciona una interfaz gráfica intuitiva para diseñar, modelar y administrar bases de datos MySQL.

Con MySQL Workbench, pude crear y definir la estructura de la base de datos para el proyecto de la aplicación móvil. Esto incluyó la creación de tablas, la definición de campos y tipos de datos, la especificación de claves primarias y secundarias, y el establecimiento de relaciones entre las tablas. Utilicé el lenguaje de modelado de bases de datos (como el Modelo Entidad-Relación) para representar visualmente la estructura de la base de datos y asegurarme de que cumpliera con los requisitos del proyecto.

Además, MySQL Workbench ofreció funcionalidades para generar scripts SQL a partir del diseño del modelo de base de datos, lo que facilitó la implementación y migración de la base de datos en el entorno de desarrollo.

La elección de MySQL Workbench se basó en su amplia adopción y popularidad como herramienta de administración de bases de datos MySQL, su interfaz visual intuitiva y su capacidad para agilizar el diseño y desarrollo de la estructura de la base de datos.

Herramientas para la Base de Datos:

Visual Studio Code: Visual Studio Code como mi entorno de desarrollo integrado (IDE) principal para el desarrollo del proyecto. Visual Studio Code proporciona un entorno de desarrollo liviano y altamente personalizable que me permitió trabajar con eficiencia en la creación y edición de los archivos relacionados con la base de datos. Con Visual Studio Code, pude escribir y depurar código SQL directamente en el editor, lo que facilitó la creación y modificación de la estructura de la base de datos.

XAMPP: XAMPP como un paquete de software que incluye Apache, MySQL, PHP y phpMyAdmin, lo que me permitió configurar y ejecutar un servidor web y una base de datos local en mi entorno de desarrollo. Con XAMPP, pude crear un entorno de desarrollo local completo que simula el entorno de producción en el que se ejecutaría la aplicación móvil. Esto me permitió desarrollar y probar la interacción entre la aplicación móvil y la base de datos de manera eficiente.

phpMyAdmin: phpMyAdmin como una interfaz web para administrar y manipular la base de datos MySQL. phpMyAdmin proporciona una interfaz gráfica intuitiva para realizar tareas relacionadas con la base de datos, como la creación de tablas, la inserción y actualización de datos, la ejecución de consultas SQL y la gestión de usuarios y privilegios. Con phpMyAdmin, pude interactuar con la base de datos de forma visual y realizar acciones administrativas sin tener que escribir consultas SQL manualmente.

La elección de estas herramientas, como Visual Studio Code, XAMPP y phpMyAdmin, se basó en su facilidad de uso, su amplia adopción en la comunidad de desarrollo y su capacidad para proporcionar un entorno de desarrollo y administración de la base de datos eficiente y efectivo.

Herramientas para el Desarrollo de la Aplicación:

Android Studio: Android Studio como mi entorno de desarrollo principal para la creación de la aplicación móvil. Android Studio es el IDE oficial para el desarrollo de aplicaciones Android y proporciona un conjunto completo de herramientas y recursos para diseñar, codificar, depurar y compilar aplicaciones móviles de manera eficiente. Con Android Studio, pude crear la interfaz de usuario de la aplicación, escribir el código fuente en el lenguaje de programación Java o Kotlin, y realizar pruebas y depuración en un emulador o dispositivo físico.

Visual Studio Code: Visual Studio Code como un IDE adicional para el desarrollo de la aplicación. Visual Studio Code es un editor de código ligero y altamente personalizable que proporciona soporte para múltiples lenguajes de programación, incluyendo Java y Kotlin. Con Visual Studio Code, pude editar y revisar el código fuente de la aplicación de manera eficiente, además de aprovechar las extensiones y complementos disponibles para mejorar la productividad durante el desarrollo.

Para la conexión con la base de datos y la generación de la credencial digital:

Conexión con la Base de Datos: Visual Studio Code para escribir el código que establece la conexión con la base de datos MySQL. Utilicé librerías y API adecuadas para realizar operaciones de lectura y escritura en la base de datos, como la

recuperación de información de los estudiantes y la actualización de los registros de acceso.

Generación de la Credencial Digital: Tanto Android Studio como Visual Studio Code para implementar la funcionalidad de generación de la credencial digital. Utilicé los datos obtenidos de la base de datos para construir la credencial digital y mostrarla en la aplicación móvil. Esto incluyó el diseño de la interfaz de la credencial y la programación de la lógica para mostrar la información correspondiente a cada estudiante.

La elección de estas herramientas, como Android Studio y Visual Studio Code, se basó en su popularidad en el desarrollo de aplicaciones móviles, su amplia gama de características y su comunidad activa de desarrolladores.

9.6 Lista preliminar de clases

Estudiante: una clase que representa a un estudiante que usa la aplicación móvil para acceder al instituto.

Administrador: una clase que representa a un administrador que administra la base de datos de estudiantes y el sistema de control de acceso.

Credencial digital: una clase que representa la credencial digital del estudiante, que contiene el código QR utilizado para el acceso.

Access Reader: una clase que representa el lector de códigos QR en la entrada del instituto, que escanea las credenciales digitales.

Sistema de control de acceso: una clase que representa el sistema principal que controla el acceso al instituto.

Registro de acceso: una clase que representa el registro de acceso de los estudiantes al instituto, incluidas las horas y ubicaciones de entrada y salida.

Credenciales de usuario: una clase que representa las credenciales de inicio de sesión para estudiantes y administradores.

Base de datos de estudiantes: una clase que representa la base de datos que contiene información del estudiante, incluido el nombre, el número de control y otros detalles relevantes.

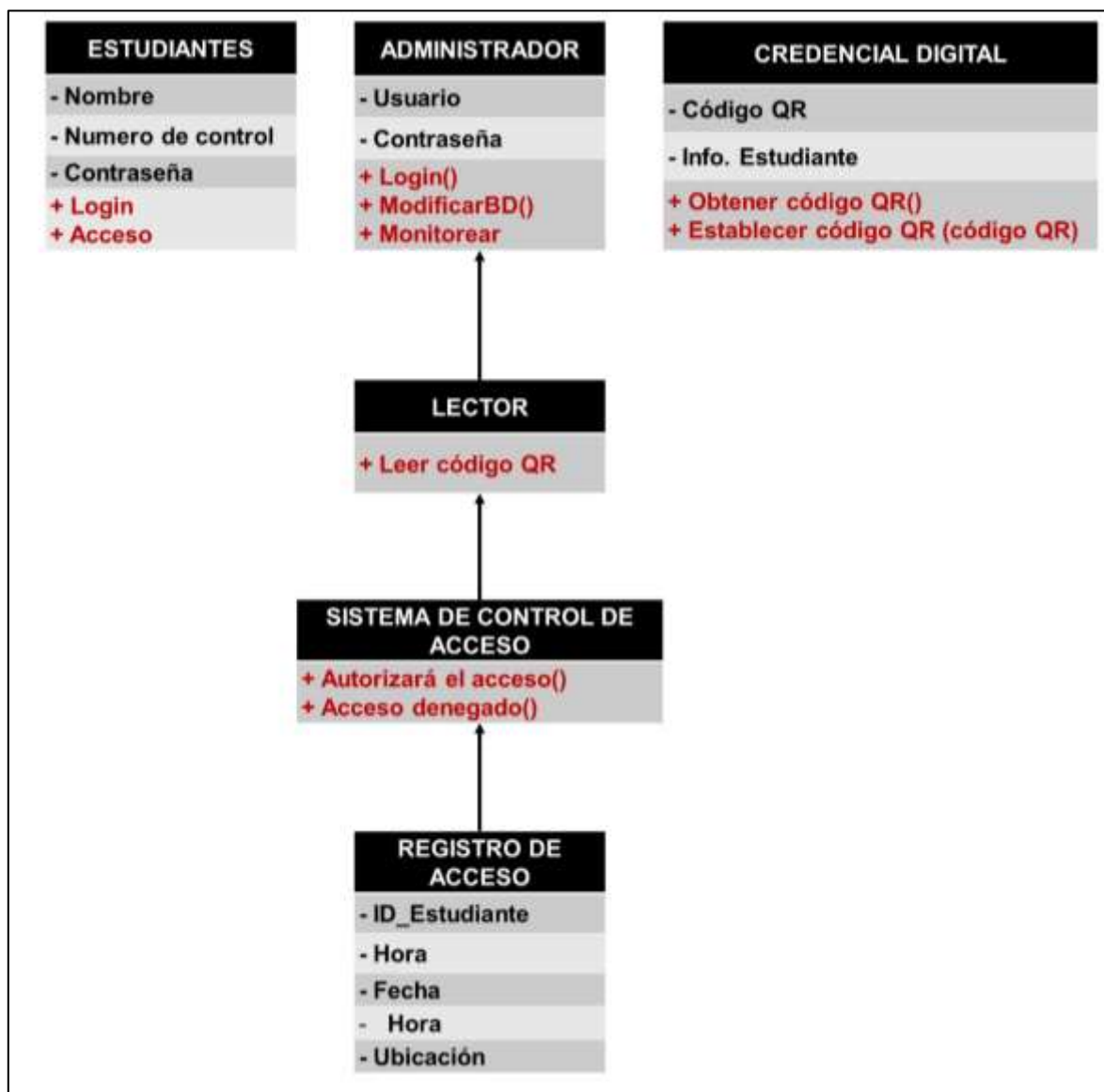
Estas clases pueden tener atributos y métodos asociados, según los requisitos específicos de este proyecto. Por ejemplo, la clase Estudiante podría tener atributos como nombre, número de control y contraseña, así como métodos para iniciar sesión y acceder al instituto. La clase Registro de acceso podría tener atributos

como ID de estudiante, fecha y hora de entrada, fecha y hora de salida y ubicación, así como métodos para actualizar el registro y recuperar datos de acceso.

Es importante identificar las clases y sus relaciones al principio del proceso de desarrollo para garantizar un sistema funcional y bien diseñado.

9.7 Diagrama de clases

Figura 25.- Diagrama de clases del sistema



En la Figura 26.- Diagrama de clases del sistema, muestra lo siguiente:

En este diagrama de clases, las clases están representadas por rectángulos con sus nombres, y las relaciones entre ellas están representadas por líneas. Las flechas indican la dirección de las relaciones.

La clase Estudiante representa a un estudiante que usa la aplicación móvil para acceder al instituto. Tiene atributos como nombre, número de control y contraseña, y métodos para iniciar sesión y acceder al instituto.

La clase Administrador representa a un administrador que administra la base de datos de estudiantes y el sistema de control de acceso. Tiene atributos como

nombre de usuario y contraseña, y métodos para iniciar sesión y modificar la base de datos y acceder al registro de acceso.

La clase DigitalCredential representa la credencial digital del alumno, que contiene el código QR utilizado para el acceso. Tiene un atributo qrCode, así como métodos para obtener y configurar el código QR.

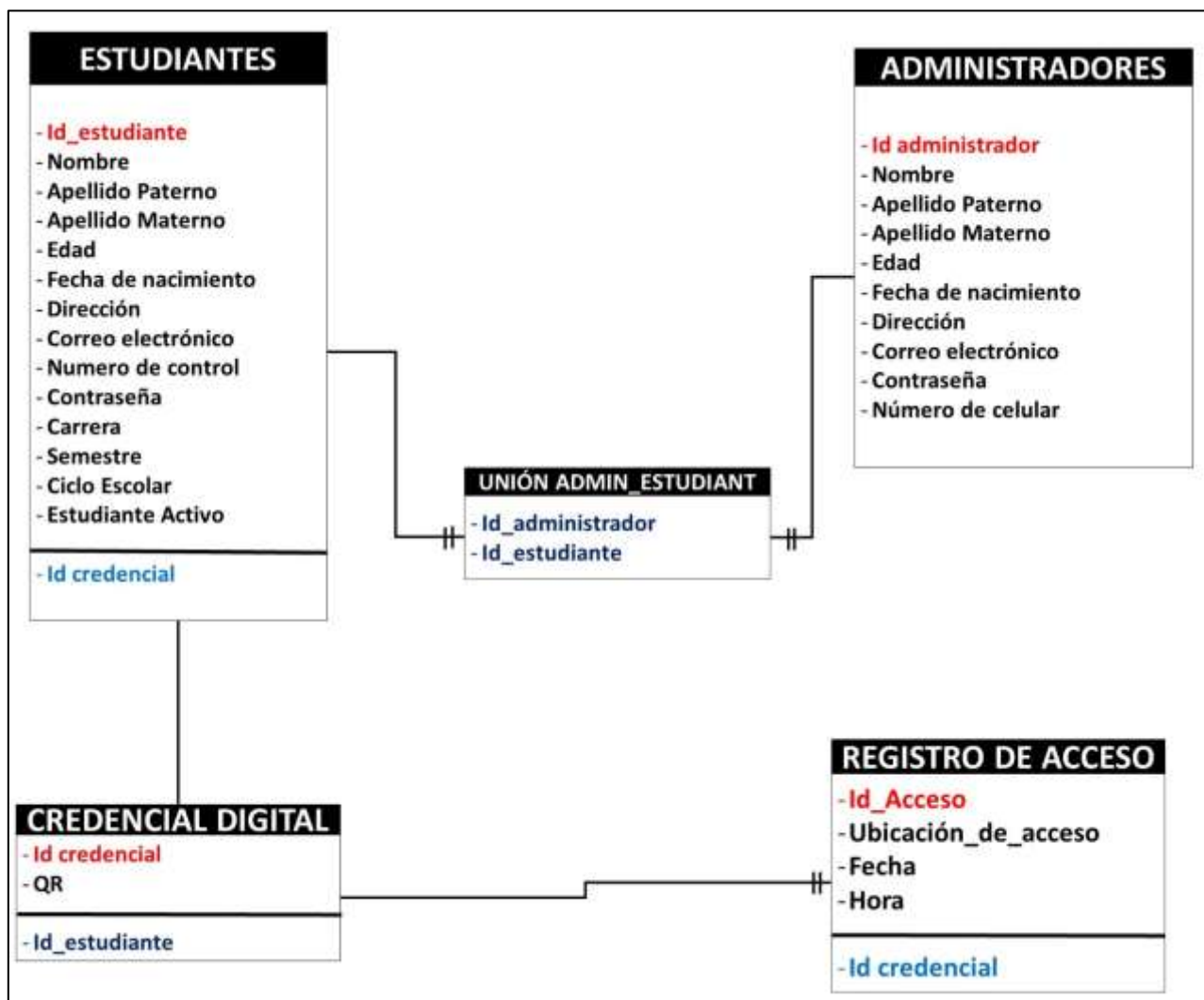
La clase AccessReader representa el lector de códigos QR en la entrada del instituto, que escanea las credenciales digitales. Tiene un método readQRCode().

La clase AccessControlSystem representa el sistema principal que controla el acceso al instituto. Tiene métodos para conceder y denegar el acceso.

La clase AccessLog representa el registro de acceso de las estudiantes al instituto, incluidas las horas y ubicaciones de entrada y salida. Tiene atributos como ID de estudiante, hora y fecha de entrada, hora y fecha de salida y ubicación, así como métodos para actualizar el registro y recuperar datos de acceso.

9.8 Modelo Entidad Relación

Figura 26.- Modelo Entidad Relación



En la Figura 26.- Modelo entidad relacion muestra lo siguiente:

El diagrama entidad-relación (ER) fue creado para representar la estructura de la base de datos utilizada en el proyecto de la aplicación móvil de credenciales digitales para el acceso a la universidad. Este diagrama es una herramienta visual poderosa que muestra las entidades principales, sus atributos y las relaciones entre ellas.

El diagrama consta de varias entidades clave que representan las principales entidades involucradas en el sistema:

Tabla de Estudiantes: Esta entidad representa a los estudiantes del instituto y contiene los siguientes atributos: ID, Nombre y Carrera. El atributo ID es la clave

primaria de esta entidad, lo que garantiza que cada estudiante tenga una identificación única.

Tabla de Administradores: Esta entidad representa a los administradores del sistema y contiene los atributos de ID, Nombre y Credenciales de inicio de sesión. El atributo ID es la clave primaria de esta entidad. Los administradores tienen la capacidad de gestionar varios estudiantes y, a su vez, cada estudiante puede ser gestionado por varios administradores. Para modelar esta relación de muchos a muchos, se utiliza una tabla de unión llamada "Administradores Estudiantes", que contiene las claves foráneas que hacen referencia a los ID de administrador y estudiante correspondientes.

Tabla de Credenciales Digitales: Esta entidad representa las credenciales digitales asociadas a cada estudiante. Contiene los atributos de ID y el ID del estudiante al que pertenece. El atributo ID es la clave primaria de esta entidad, y el ID del estudiante se establece como una clave foránea que referencia el ID del estudiante en la tabla de Estudiantes. Se establece una relación uno a uno entre la tabla de Estudiantes y la tabla de Credenciales Digitales, lo que significa que cada estudiante tiene una única credencial digital y cada credencial digital corresponde a un solo estudiante.

Tabla de Registros de Acceso: Esta entidad registra cada vez que se escanea una credencial digital. Contiene los atributos de ID, Fecha y Hora de escaneo, e ID de la Credencial Digital. El atributo ID es la clave primaria de esta entidad. Se establece una relación entre la tabla de Registros de Acceso y la tabla de Credenciales Digitales, donde el ID de la Credencial Digital se establece como una clave foránea que referencia el ID de la Credencial Digital correspondiente. Esta relación garantiza que cada registro de acceso esté asociado con una credencial digital válida.

Además de las entidades, se han establecido restricciones en el diagrama para asegurar la integridad y la consistencia de los datos:

Cada alumno solo puede tener una credencial digital, y cada credencial digital solo puede corresponder a un alumno. Esta restricción de relación uno a uno asegura que cada estudiante solo pueda acceder a la universidad utilizando su propia credencial digital única, y que cada credencial digital corresponda a un solo estudiante.

Cada registro de acceso debe estar asociado a una credencial digital válida. Esto garantiza que los registros de acceso solo se registren cuando se escanee una credencial digital válida.

Cada registro de acceso debe tener una fecha y hora únicas. Esto evita la creación de múltiples registros de acceso.

9.9 Estructura y diseño del look and feel del sitio web

El sitio web está dirigido exclusivamente a administradores y tiene como objetivo principal realizar operaciones de administración de alumnos y monitoreo de accesos, aquí hay consideraciones adicionales para la estructura y diseño del Look and Feel:

Login: Implementa un mecanismo de validación para verificar la autenticidad de las credenciales ingresadas. Esto puede incluir comprobar si el nombre de usuario y la contraseña coinciden con los registros almacenados en la base de datos.

Panel de administración intuitivo: Diseña un panel de administración claro y fácil de usar. Organiza las funciones relacionadas con la administración de alumnos y monitoreo de accesos en secciones lógicas y fáciles de navegar. Utiliza un diseño intuitivo que permita a los administradores realizar fácilmente las tareas necesarias.

Formularios y CRUD (Crear, Leer, Actualizar, Eliminar): Utiliza formularios claros y bien diseñados para permitir a los administradores agregar, editar y eliminar registros de alumnos. Diseña una interfaz atractiva y fácil de entender para las operaciones CRUD, asegurando que los campos requeridos estén claramente identificados y que haya validaciones de datos para evitar errores.

Visualización de datos: Proporciona una interfaz clara y concisa para mostrar la información de los alumnos y sus accesos. Utiliza tablas, gráficos u otros elementos visuales para presentar los datos de manera organizada y comprensible. Incluye opciones de filtrado y búsqueda para facilitar la exploración de la información.

Informes y estadísticas: Si es relevante para la administración, considera incluir informes y estadísticas que brinden una visión general de los accesos de los alumnos. Utiliza gráficos o tablas resumidas para mostrar tendencias, patrones o métricas importantes.

Seguridad: Dado que este sitio web está destinado a administradores, asegúrate de implementar medidas de seguridad adecuadas. Utiliza autenticación y autorización sólidas para garantizar que solo los administradores autorizados puedan acceder y realizar cambios en la base de datos.

Retroalimentación y mensajes de confirmación: Diseña mensajes claros y descriptivos para proporcionar retroalimentación a los administradores cuando realicen acciones en el sitio web. Utiliza mensajes de confirmación para asegurar que los administradores estén al tanto de las operaciones realizadas y evita cualquier confusión o errores inadvertidos.

Diseño responsivo: Al igual que mencioné anteriormente, asegúrate de que el diseño del sitio web sea responsivo para que los administradores puedan acceder y utilizar la plataforma desde diferentes dispositivos, como computadoras de escritorio, tabletas o teléfonos móviles.

9.9.1 Login

Diseña una página de inicio de sesión que sea fácil de usar y estéticamente agradable. Debe tener campos para que los administradores ingresen su nombre de usuario y contraseña.

Figura 27.- Panel Login del sitio web administrador



En la Figura 27.- Muestra la estructura del Panel Login del sitio web administrador, donde refiere lo siguiente:

Validación de credenciales: Implementar un mecanismo de validación para verificar la autenticidad de las credenciales ingresadas. Esto puede incluir comprobar si el usuario y la contraseña coinciden con los registros almacenados en la base de datos.

Mensajes de error: Si las credenciales ingresadas son incorrectas, muestra mensajes de error claro y descriptivo para informar a los administradores sobre el problema específico. Esto les ayudará a volver a intentarlo.

Figura 29.- Mensaje de error



Figura 28.- Mensaje de Login Exitoso



En las Figuras 28 y 29.- Diagrama de clases del sistema, muestra lo siguiente:

Seguridad: Implementa medidas de seguridad adecuadas, como el cifrado de contraseñas, para proteger la información confidencial de los administradores.

Figura 30.- Cifrado de contraseña

Contraseña	*****
-------------------	-------

En la Figura 30.- cifrado de contraseña, muestra lo siguiente:

Redireccionamiento: En la Figura 32.- Redireccionamiento de Login a pantalla de inicio del sitio web administrador, explica que después de que un administrador inicie sesión exitosamente, redirígelo a una página de inicio personalizada para administradores, donde puedan acceder a las diferentes funciones y herramientas disponibles.

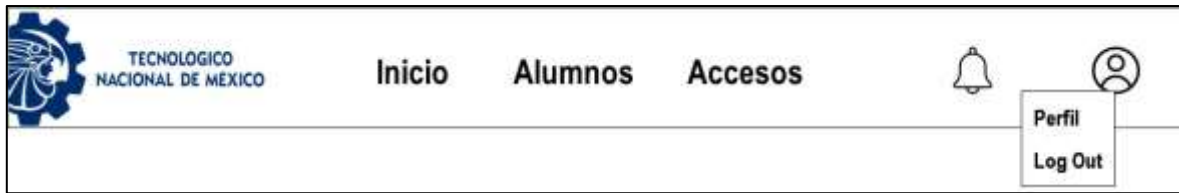
Figura 31.- Redireccionamiento de Login a pantalla de inicio del sitio web administrador



9.9.2 Menú de navegación

- El panel de administración debe tener un diseño limpio y organizado.
- En la parte superior de la página, puedes colocar una barra de navegación horizontal con las siguientes secciones:
- "Inicio": Esta sección puede mostrar un resumen de estadísticas clave, como el número total de alumnos y el número de accesos recientes.
- "Alumnos": Aquí los administradores podrán ver una lista de todos los alumnos registrados y realizar operaciones CRUD (crear, leer, actualizar y eliminar) para gestionarlos.
- "Accesos": En esta sección, los administradores podrán monitorear los accesos de cada alumno y ver registros detallados de cada escaneo de credencial.
- Además de la barra de navegación, puedes incluir un panel lateral desplegable que contenga enlaces rápidos a las secciones principales y proporcionar una navegación más rápida.

Figura 32.- Menú de navegación del sitio web administrador



En la Figura 32.- Menú de navegación del sitio web administrador, donde muestra lo siguiente:

Descripción detallada de cada elemento del menú del sitio web:

Inicio:

En la sección de inicio, se puede mostrar un resumen ejecutivo de la actividad reciente del sistema. Esto puede incluir estadísticas clave, como el número total de alumnos registrados, el número de accesos recientes.

Alumnos:

La sección de alumnos es donde los administradores pueden administrar y mantener la lista de alumnos registrados. Aquí se podrá ver una lista de todos los alumnos, con detalles básicos como el nombre, la carrera y el estado de la credencial digital. Donde incluye un formulario con botones para agregar un nuevo alumno, editar la información existente o eliminar alumnos si es necesario.

Al hacer clic en un alumno específico, puedes mostrar una página detallada con información adicional, como el número de identificación, los accesos recientes y cualquier otra información relevante.

Accesos:

La sección de accesos permite a los administradores monitorear los accesos de cada alumno. Puede mostrar una lista de los últimos accesos registrados, incluyendo detalles como la fecha y hora del acceso, el alumno asociado y cualquier información adicional relevante. Proporciona opciones de filtrado y búsqueda para que los administradores puedan encontrar rápidamente los registros específicos que deseen revisar. Si es necesario, puedes agregar gráficos o estadísticas para visualizar la actividad de acceso de manera más clara.

Perfil de usuario:

El icono de usuario en el menú de navegación es una excelente opción para acceder al perfil del administrador actual. Al hacer clic en el icono de usuario, puedes mostrar un menú desplegable con opciones como "Perfil" y "Cerrar sesión".

La opción "Perfil" puede dirigir al administrador a una página donde pueden ver y editar su información personal, como nombre, correo electrónico, foto de perfil, etc. La opción "Cerrar sesión" permite al administrador salir del sistema de manera segura.

9.9.3 Sección Inicio

La sección de inicio es la página principal del sistema de administración para los usuarios con privilegios de administrador. Su objetivo principal es proporcionar un resumen ejecutivo y una visión general de la actividad reciente del sistema. Aquí hay algunas ideas sobre qué contenido y funcionalidades se pueden incluir en la sección de inicio.

Figura 33.- Sección inicio página web para administrador



En la Figura 33.- Sección inicio página web para administrador, muestra lo siguiente:

Resumen ejecutivo: Proporciona una visión general de los datos clave y las métricas relevantes para la administración del sistema. Mostrar información como el número total de alumnos registrados, el número de accesos recientes. Esto permite a los administradores tener una idea rápida del estado general del sistema.

Estadísticas y gráficos: Utiliza gráficos o visualizaciones para presentar datos importantes de manera visualmente atractiva. Puede mostrar gráficos de barras, gráficos circulares o líneas para representar el número de accesos diarios/semanales/mensuales, comparativos entre diferentes períodos de tiempo, etc. Esto ayudará a los administradores a identificar tendencias y patrones en la actividad de acceso.

Figura 34.- Graficas de resumen sección inicio



En la Figura 34.- Graficas de resumen sección inicio, muestra lo siguiente:

Accesos rápidos: Proporciona enlaces o botones de acceso rápido a las funciones o secciones más utilizadas del sistema. Esto permite a los administradores acceder directamente a las áreas de interés sin tener que navegar por múltiples pantallas.

Figura 35.- Acceso rápido de sección Inicio



9.9.4 Sección de Alumnos

Figura 36.- Sección alumnos página web para administrador



En la Figura 36.- Sección alumnos página web para administrador, muestra lo siguiente:

Lista de Alumnos: Muestra una lista de todos los alumnos registrados en el sistema. Puedes presentarlos en una tabla con columnas que incluyan información relevante como nombre, carrera, ID, y otras características que sean pertinentes. Además, puedes incluir opciones para ordenar y filtrar la lista, lo que facilitará la búsqueda de alumnos específicos.

Figura 37.- Lista de Alumnos de la sección alumnos del sitio web administrador



En la Figura 37.- Lista de alumnos de la sección alumnos del sitio web administrador, muestra lo siguiente:

Detalles de Alumno: Al hacer clic en un alumno de la lista, se abrirá una página o un panel donde se mostrarán todos los detalles relacionados con ese alumno en particular. Aquí puedes mostrar información adicional como información escolar, información personal, y la posibilidad de activar o desactivar la credencial por seguridad en caso de robo o extravió.

Figura 38.- Detalles de Alumno

En la Figura 38.- Detalles del alumno, muestra lo siguiente:

Agregar/Editar Alumno: Proporciona la opción de crear nuevos registros de alumnos en el sistema o editar la información existente. Esto implicaría un formulario donde los administradores puedan ingresar o modificar datos como el nombre, carrera, número de control, y otra información relacionada con el alumno. Asegúrate

de incluir validaciones de datos para garantizar la integridad y consistencia de la información.

Figura 39.- Agregar alumno de la sección Alumnos del sitio web administrador

The screenshot shows the 'Agregar alumno' form in the 'Alumnos' section of the website administrator. The form is titled 'Agregar alumno' and includes a search bar on the left. The form fields are organized into two main sections: 'Información Escolar' and 'Información personal'. The 'Información Escolar' section includes fields for 'Nombre', 'Apellido Paterno', 'Apellido Materno', 'Número de control', 'Comando', 'Carrera', 'Semestre', 'Escuela', and 'Estudiante activo'. The 'Información personal' section includes fields for 'Edad', 'Fecha de nacimiento', 'Sexo', and 'Correo Electrónico'. There are also 'Activar' and 'Desactivar' buttons. The form is submitted by clicking the 'Guardar' button. The top navigation bar includes 'Inicio', 'Alumnos', and 'Accesos'.

Figura 40.- Mensaje de confirmación Agregar alumno

The screenshot shows a confirmation dialog box with the text '¿DESEA AGREGAR ESTE ALUMNO?'. There are two buttons: 'SI' (Yes) and 'NO' (No).

Figura 41.- Editar Información Alumno

The screenshot shows the 'Editar' form in the 'Alumnos' section of the website administrator. The form is titled 'Editar' and includes a search bar on the left. The form fields are organized into two main sections: 'Información Escolar' and 'Información personal'. The 'Información Escolar' section includes fields for 'Nombre', 'Apellido Paterno', 'Apellido Materno', 'Número de control', 'Comando', 'Carrera', 'Semestre', 'Escuela', and 'Estudiante activo'. The 'Información personal' section includes fields for 'Edad', 'Fecha de nacimiento', 'Sexo', and 'Correo Electrónico'. There are also 'Activar' and 'Desactivar' buttons. The form is submitted by clicking the 'Guardar' button. The top navigation bar includes 'Inicio', 'Alumnos', and 'Accesos'.

Figura 42.- Actualizar Información Alumno

The screenshot shows the 'Actualizar' (Update) form for a student record. The interface includes a top navigation bar with 'Inicio', 'Alumnos', and 'Accesos' tabs. A sidebar on the left contains a list of student icons. The main form area has a search bar and a list of action buttons: 'Editar', 'Actualizar' (highlighted with a mouse cursor), 'Cancelar', and 'Eliminar'. The form itself is divided into two main sections: 'Información Escolar' and 'Información personal'. The 'Información Escolar' section includes fields for 'Nombre', 'Apellido Paterno', 'Apellido Materno', 'Número de control', 'Contraseña', 'Centro', 'Semestre', 'Ciclo Escolar', and 'Estatus actual'. The 'Información personal' section includes fields for 'Edad', 'Fecha de nacimiento', 'Dirección', and 'Correo electrónico'. There are also 'Activar' and 'Desactivar' buttons at the bottom right of the form.

En la Figura 42.- Actualizar información de alumno, muestra lo siguiente:

Eliminar Alumno: Permite a los administradores eliminar registros de alumnos si es necesario. Esto puede incluir una confirmación de eliminación para evitar acciones accidentales.

Figura 43.- Eliminar Alumno

The screenshot shows the 'Eliminar' (Delete) form for a student record. The interface is similar to the previous one, with the same top navigation bar and sidebar. The main form area has the same search bar and action buttons, but the 'Eliminar' button is highlighted with a mouse cursor. The form structure is identical to the 'Actualizar' form, with 'Información Escolar' and 'Información personal' sections and their respective fields. The 'Activar' and 'Desactivar' buttons are also present at the bottom right.

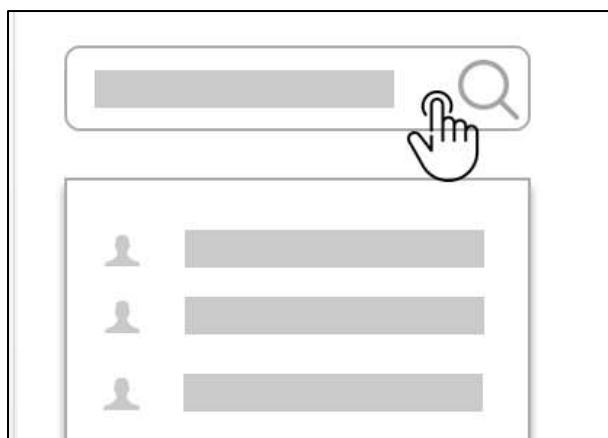
Figura 44.- Mensaje de confirmación Eliminar alumno



En la Figura 44.- Mensaje de confirmación, muestra lo siguiente:

Búsqueda: Agrega opciones de búsqueda en la lista de alumnos para facilitar la localización de estudiantes específicos. Incluye búsqueda por número de control.

Figura 45.- Búsqueda de Alumnos



En la Figura 45.- Búsqueda de alumnos, muestra lo siguiente:

9.9.5 Sección de Accesos

Descripción de los elementos de la sección "Accesos":

Figura 46.- Sección Accesos



En la Figura 46.- Sección de acceso, muestra lo siguiente:

Registro de Accesos en Tiempo Real: Esta sección muestra en tiempo real los registros de acceso de los alumnos al instituto. Utiliza una tabla para mostrar los detalles de cada acceso, como el número de control del alumno, la hora de entrada y salida, y cualquier otra información relevante. Este registro en tiempo real permite a los administradores tener una visión actualizada de los accesos de los alumnos.

Figura 47.- Registro de accesos en tiempo real

Registro de accesos en tiempo real				
	Num. Control	Hora	Ubicación	Acción
	18370990	09:00	Acceso 1	Entrada
	18370991	09:10	Acceso 1	Entrada
	18370945	09:20	Acceso 2	Salida
	18370992	10:00	Acceso 3	Entrada
	18370993	10:10	Acceso 2	Salida
	18370994	10:14	Acceso 1	Entrada
	18370995	11:00	Acceso 1	Salida
	18370996	12:20	Acceso 2	Salida
	12370846	12:21	Acceso 3	Salida
	12345678	13:50	Acceso 3	Entrada
	09876543	14:00	Acceso 4	Salida

En la Figura 47.- Registro de accesos en tiempo real, muestra lo siguiente:

Filtro de Accesos por Día de la Semana: Dentro de la sección de Accesos, se incluye un filtro que permite a los administradores seleccionar un día de la semana específico, como lunes, martes, miércoles, jueves, viernes o sábado. Al seleccionar un día, se mostrarán los registros de acceso correspondientes a ese día en particular. Esto facilita el seguimiento y la revisión de los accesos de los alumnos en días específicos de la semana.

Figura 48.- Filtro de Accesos por Día de la Semana



Número de acc

Entradas

Salidas

En la Figura 48.- Filtro de acceso por día de la semana, muestra lo siguiente:

Detalles de Acceso del Estudiante: Al seleccionar un registro de acceso o buscar un alumno en específico en la lista, se despliegan los detalles específicos de ese acceso en particular. Estos detalles pueden incluir la hora de entrada y salida del alumno, la ubicación o cualquier otra información relevante. Proporcionar estos

detalles permite a los administradores tener una comprensión más completa de los patrones de acceso de cada alumno.

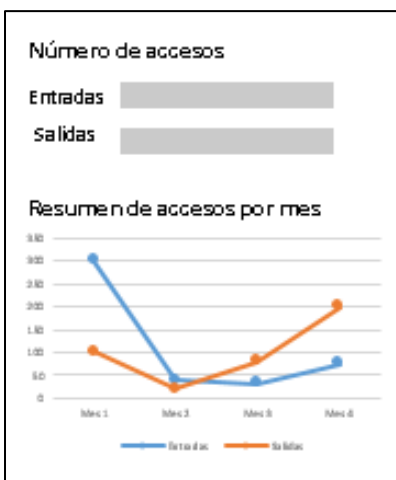
Figura 49.- Detalles de Acceso del Estudiante



En la Figura 49.- Detalles de acceso del estudiante, muestra lo siguiente:

Resumen de Accesos: En la sección de detalles de acceso, se puede incluir un resumen que muestre estadísticas clave sobre los accesos del alumno. Esto puede incluir información como el número total de accesos. Estos resúmenes brindan una visión general rápida y útil de los hábitos de acceso del alumno.

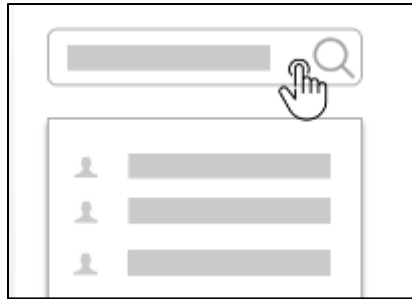
Figura 50.- Resumen de Accesos



En la Figura 50.- Resumen de accesos, muestra lo siguiente:

Búsqueda: Agrega opciones de búsqueda en la lista de alumnos para facilitar la localización de estudiantes específicos. Incluye búsqueda por número de control.

Figura 51.- Búsqueda Acceso



En la Figura 51.- Búsqueda acceso, muestra una manera más fácil de realizar el filtrado de datos para encontrar un alumno en específico.

9.9.6 Perfil de Administrador

Icono de usuario: Utiliza un icono de usuario como indicador visual para acceder al perfil del administrador.

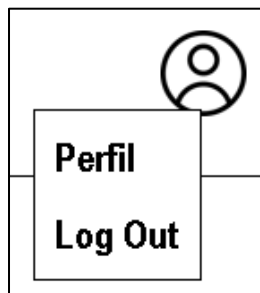
Figura 52.- Icono usuario Administrador



En la Figura 52.- icono de usuario administrador, muestra un acceso rápido para entrar al perfil y administración de los administradores.

Menú desplegable: Al hacer clic en el icono de usuario, muestra un menú desplegable con dos opciones: "Perfil" y "Cerrar sesión".

Figura 53.- Menú desplegable



Perfil: En la Figura 53.- Menú desplegable, muestra que al seleccionar la opción "Perfil", se carga una página o sección donde se muestra la información relevante del administrador, como su nombre, cargo, correo electrónico y cualquier otro detalle pertinente. Puedes incluir también la foto de perfil del administrador, si es aplicable.

Figura 54.- Perfil de Administrador



En la Figura 55-60.-Gestión de los administradores, muestra lo siguiente:

Gestión de administradores: Dentro de la página de perfil, puedes agregar una sección dedicada a la gestión de administradores. Aquí, el administrador tendrá opciones para agregar, eliminar o editar otros perfiles de administradores. Esto le permitirá al administrador tener control sobre quién tiene acceso y privilegios en la plataforma.

Figura 56.- Agregar Administradores



Figura 55.- Mensaje para agregar Administrador

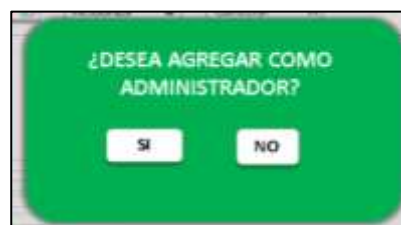
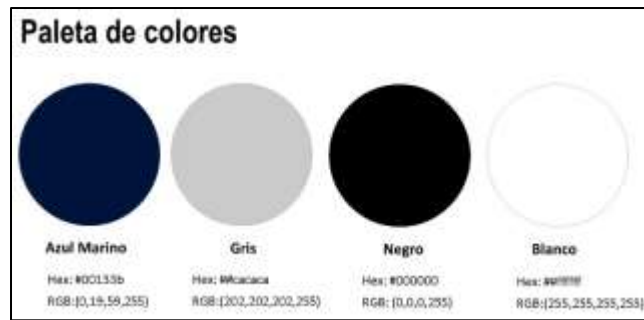


Figura 62.- Paleta de colores Sitio Web



En la Figura 62.- Paleta de colores sitio web, muestra lo siguiente:

Azul marino: El color azul marino transmite confianza, estabilidad y profesionalismo. Es ideal para transmitir seriedad y establecer una atmósfera de confianza en la interfaz de usuario. Según la teoría del color, el azul está asociado con la confianza, la seguridad y la eficiencia en entornos profesionales (Pileckaite, 2020).

Gris: El color gris se asocia con la neutralidad, la sofisticación y la elegancia. Es un color versátil que puede utilizarse como fondo para resaltar otros colores o elementos en la interfaz. Según el significado del color, el gris transmite un sentido de estabilidad, imparcialidad y equilibrio (D'Andrea, 2019).

Negro: El color negro evoca elegancia, autoridad y exclusividad. Utilizado en elementos de texto o como color de contraste, el negro agrega un toque de sofisticación y enfatiza la importancia de la información presentada. Según la teoría del color, el negro se asocia con el poder, la autoridad y la formalidad (Lantrip, 2021).

Blanco: El color blanco representa la pureza, la limpieza y la simplicidad. Es ampliamente utilizado como color de fondo para resaltar otros elementos y proporcionar claridad visual. El blanco crea un aspecto fresco y minimalista, transmitiendo una sensación de orden y simplicidad (Saha, 2019).

En la Figura 64.- Variación de colores, muestra lo siguiente:

Figura 63.- Variación de colores



9.9.8 Tipografía

Se suele recomendar utilizar dos o tres tipografías en un sitio web: una para los encabezados y titulares, otra para el cuerpo del texto y, en algunos casos, una tercera para resaltar elementos especiales como botones o llamadas a la acción.

Al seleccionar las tipografías para tu sitio web, es importante considerar factores como la legibilidad, la coherencia con la identidad de la marca, la combinación de estilos (por ejemplo, una tipografía serif para títulos y una sans-serif para el cuerpo del texto) y la disponibilidad en diferentes dispositivos y navegadores web. Las tipografías elegidas deben ser accesibles y compatibles con diferentes sistemas operativos y navegadores para garantizar una experiencia de usuario consistente.

Es recomendable utilizar servicios de fuentes web como Google Fonts o Adobe Fonts, que ofrecen una amplia variedad de tipografías gratuitas y optimizadas para su uso en sitios web.

9.9.9 Tipografías a implementar

Existen varias tipografías que son ampliamente compatibles entre navegadores y sistemas operativos. A continuación, proporciono tres tipografías comunes y ampliamente aceptadas para implementar en el sitio web:

Figura 64.- Tipografía Arial



En la Figura 64.- Tipografía arial, muestra lo siguiente:

Arial: Arial es una tipografía sans-serif ampliamente utilizada, conocida por su legibilidad y simplicidad. Es una opción popular para aplicaciones digitales y sitios web debido a su amplia disponibilidad y compatibilidad entre diferentes sistemas operativos y navegadores.

Figura 65.- Tipografía Helvetica



En la Figura 65.-Tipografía Helvetica , muestra lo siguiente:

Helvetica: Helvetica es una icónica tipografía sans-serif reconocida por su diseño limpio y moderno. Es ampliamente utilizada en diseño gráfico y diseño web debido a su versatilidad y legibilidad en diferentes tamaños y medios.

Figura 66.- Tipografía Open Sans



En la Figura 66.- Tipografía OpenSans, muestra lo siguiente:

Open Sans: Open Sans es una popular tipografía sans-serif de código abierto que ofrece una excelente legibilidad tanto en pantalla como en impresiones. Es ampliamente utilizada en diseño web debido a su amplia gama de pesos y estilos, así como a su fácil integración con sistemas de diseño responsivo.

10. Estructura y diseño del Look and Feel de la app

10.1 Login

En la Figura 67,68,69.- muestran el inicio de sesión es la primera pantalla que se muestra a los alumnos al abrir la app. Su objetivo principal es autenticar a los usuarios y permitirles acceder a sus datos personales de forma segura. El inicio de sesión requiere que los alumnos ingresen su número de control y contraseña proporcionados por la institución. Esto garantiza que solo los alumnos autorizados puedan acceder a la información protegida por la app.

Figura 69.- Login App



Figura 68.- Mensaje Login credenciales incorrectas



Figura 67.- Mensaje Login credenciales correctas



10.2 Credencial digital

La pantalla de la credencial digital es una representación digital de la identificación física del alumno. Muestra la información personal del alumno, como su nombre completo, fotografía, número de control. Esta sección tiene como objetivo proporcionar un código QR para que pueda escanearlo al momento de querer entrar o salir del instituto esto con el fin de brindar una forma conveniente y rápida de acceder a la información personal del alumno, lo que facilita su identificación y verificación al ingresar a las instalaciones de la universidad u otros servicios relacionados.

Figura 70.- Credencial digital App

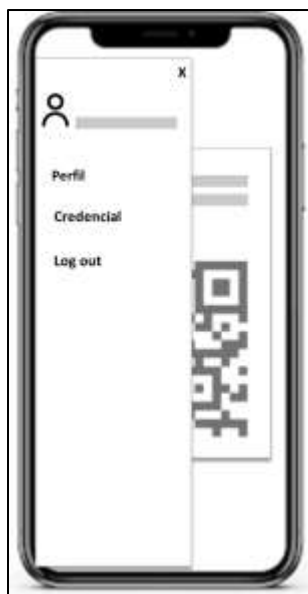


En la Figura 70.- Credencial Digital, muestra la credencial del estudiante el cual tendrá una foto del estudiante, su nombre, carrera y un código QR.

10.3 Menú lateral

El menú lateral es un componente de navegación que se encuentra en la parte izquierda de la pantalla. Proporciona un acceso rápido y fácil a las diferentes secciones de la app para los alumnos. Este menú suele estar representado por un icono de tres líneas horizontales. Al seleccionar el icono, se despliega un panel lateral que muestra las opciones disponibles.

Figura 71.- Menú lateral de la App



En la Figura 71.- Menú lateral de la app, muestra lo siguiente:

Un menú desplegable de izquierda a derecha con los botones de perfil, credencial y log out.

10.4 Perfil del alumno

Muestra información detallada y relevante sobre el alumno, como su nombre, dirección, carrera, entre otros. Esta sección es útil para que los alumnos consulten su información personal y obtengan acceso a cualquier otro detalle importante relacionado con su estancia en la institución educativa.

Figura 72.- Sección Perfil de la App



En la Figura 72.- Sección Perfil de la App, muestra lo siguiente:

La pantalla de Perfil con la información personal e información académica de los estudiantes.

10.5 Cerrar sesión

En la Figura 73.- Log out App, muestra lo siguiente: La opción de cerrar sesión permite a los alumnos finalizar su sesión actual en la app. Al seleccionar esta opción, se cerrará la sesión activa y se eliminará cualquier acceso no autorizado a la información personal del alumno. Esta función es importante para garantizar la privacidad y seguridad de los datos del alumno y asegurarse de que nadie más pueda acceder a ellos en caso de que el dispositivo sea compartido o perdido.

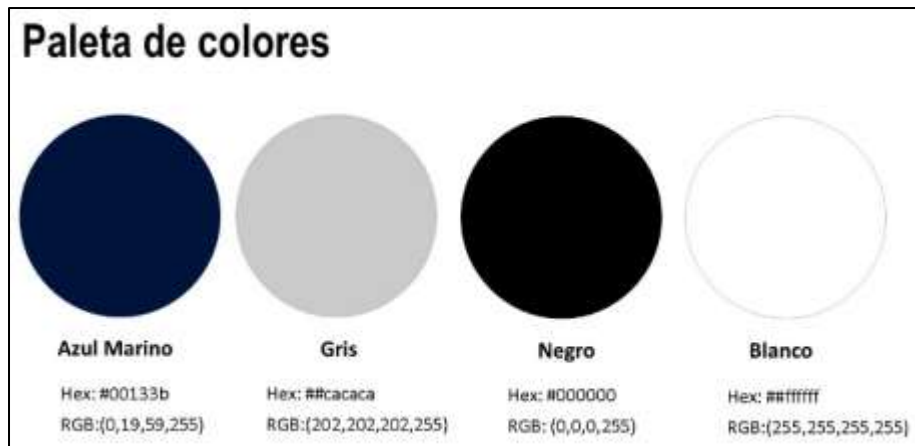
Figura 73.- Log out App



10.6 Paleta de colores

Se utilizarán los mismos colores para la paleta de colores de la app. A continuación, proporciono la descripción de la paleta de colores.

Figura 74.- Paleta de colores App



En la Figura 74.- Paleta de colores, muestra lo siguiente:

Azul marino: Este color se utilizará para elementos principales y destacados en la app. Representa confianza, seriedad y profesionalismo. Puede utilizarse para resaltar botones principales, títulos y elementos de navegación importantes.

Gris: El color gris se utilizará para elementos secundarios y fondos en la app. Aporta neutralidad y equilibrio visual. Puede utilizarse para fondos de pantalla, áreas de texto o secciones informativas.

Negro: El color negro se utilizará para textos y elementos de contraste en la app. Proporciona legibilidad y elegancia. Puede utilizarse para texto principal, descripciones o detalles importantes.

Blanco: El color blanco se utilizará como color de fondo para áreas de contenido y espacios en la app. Aporta claridad y luminosidad. Puede utilizarse para fondos de secciones, áreas de visualización de información o espacios en blanco para mejorar la legibilidad.

Figura 75.- Variación de colores App



En la Figura 75.- Valoraciones de colores app, muestra lo siguiente:

Esta paleta de colores proporcionará una apariencia coherente y profesional en la app, manteniendo la consistencia con el diseño del sitio web. El uso adecuado de

estos colores ayudará a resaltar la información relevante, facilitar la lectura y crear una experiencia visual agradable para los alumnos.

11. Diseño de los servicios a utilizar

El "Diseño de los servicios a utilizar" se refiere a la planificación y diseño de los diferentes servicios o funcionalidades que se ofrecerán a los usuarios en la aplicación o sitio web. Esto implica identificar las necesidades de los usuarios, definir los servicios que se proporcionarán para satisfacer esas necesidades y diseñar la forma en que se presentarán y funcionarán dentro de la plataforma.

11.1 Identifica las necesidades de los usuarios

Realiza un análisis de los usuarios de la aplicación o sitio web, comprende sus objetivos y las tareas que desean realizar. Esto te ayudará a determinar qué servicios son importantes y qué funcionalidades deben ser incluidas.

Necesidades de los administradores:

- Gestionar de manera eficiente la base de datos de alumnos, lo que incluye agregar, editar y eliminar registros de estudiantes.
- Gestionar de manera eficiente la base de datos de administradores, lo que incluye agregar, editar y eliminar registros de administradores.
- Supervisar y monitorear los accesos de los alumnos, permitiendo el registro de entradas y salidas, y generando informes o estadísticas relevantes.
- Realizar búsquedas y filtros avanzados para acceder rápidamente a la información de los alumnos.
- Contar con una interfaz intuitiva y fácil de usar que simplifique las tareas de administración y reduzca la carga de trabajo.

Necesidades de los estudiantes:

- Acceder fácilmente a su credencial digital desde la aplicación móvil, lo que les permite ingresar a la institución de manera rápida y sin depender de una credencial física.
- Verificar su información personal de manera sencilla, como fotografía, datos de contacto o programa académico.

11.2 Prioriza los servicios

Una vez que hayas identificado las necesidades de los usuarios, prioriza los servicios en función de su importancia y relevancia. Esto te permitirá enfocarte en los aspectos más críticos y asegurarte de que se implementen correctamente.

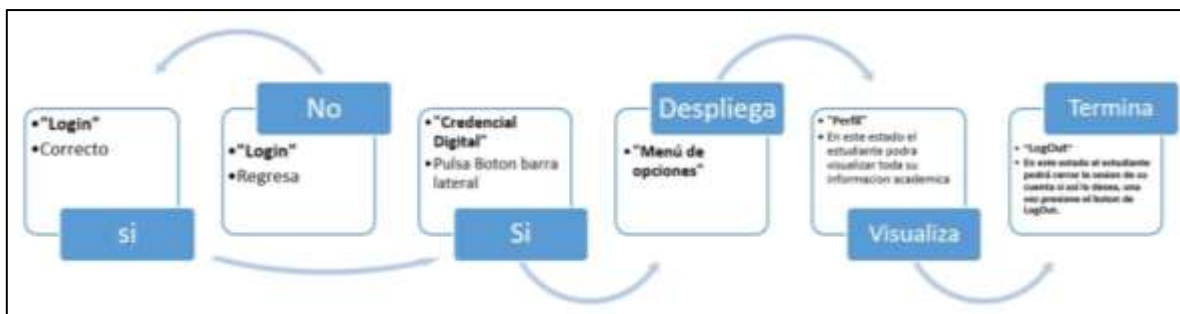
- **Gestión de la base de datos de alumnos y administradores:** Este servicio es de alta prioridad, ya que es fundamental para el funcionamiento del sistema. Permite agregar, editar y eliminar registros de estudiantes y administradores, lo que garantiza la actualización y precisión de la información.
- **Registro y supervisión de accesos de los alumnos:** Este servicio también es prioritario, ya que es esencial para garantizar la seguridad y el control de los accesos a la institución. Permite registrar las entradas y salidas de los alumnos, generando informes y estadísticas relevantes para su supervisión.
- **Generación de informes y estadísticas de accesos:** Este servicio, aunque importante, puede tener una prioridad menor en comparación con los anteriores. Proporciona información detallada sobre los accesos de los alumnos, como horarios, frecuencia y resumen de entradas y salidas. Estos informes y estadísticas son útiles para el monitoreo y la toma de decisiones.
- **Búsqueda y filtros avanzados de información de alumnos:** Este servicio tiene una prioridad media, ya que facilita el acceso rápido y eficiente a la información de los alumnos. Permite realizar búsquedas y aplicar filtros específicos para encontrar rápidamente los registros deseados.
- **Interfaz intuitiva y fácil de usar:** Este servicio, aunque importante, puede considerarse de prioridad menor en comparación con los anteriores. Una interfaz intuitiva y fácil de usar es fundamental para simplificar las tareas de administración y reducir la carga de trabajo. Sin embargo, se espera que el diseño general del sistema y la usabilidad cumplan con altos estándares.

11.3 Diseña la estructura y el flujo de la aplicación

Define cómo se organizarán y presentarán los servicios dentro de la aplicación. Crea un mapa de navegación que muestre cómo los usuarios se moverán de una sección a otra y cómo interactuarán con los diferentes servicios. Crea diseños de pantalla para cada servicio, considerando la usabilidad, la consistencia visual y la experiencia del usuario. Especifica qué acciones podrán realizar los usuarios en cada servicio. Por ejemplo, si hay un servicio de gestión de credenciales, determina si los usuarios podrán ver, editar o actualizar su información personal. Detalla las características específicas de cada servicio para asegurarte de que cumplan con las necesidades de los usuarios.

Diagrama proceso de Login de la aplicación

Figura 76.-Proceso de Login de la aplicación



En la Figura 76.-Proceso de Login de la aplicación, muestra lo siguiente:

El primer diagrama representa el flujo de un proceso de Login con usuario y contraseña, El proceso comienza en el estado inicial, donde el sistema espera que el usuario ingrese su nombre de usuario y contraseña. Desde ese estado, el sistema puede seguir dos caminos. Si el usuario hace clic en el botón "Iniciar sesión" después de ingresar las credenciales, el sistema pasa al estado de verificación de credenciales, donde se verifica si las credenciales son válidas.

Diagrama de proceso CRUD del sistema Administrador

Figura 77.- Diagrama para visualizar un estudiante



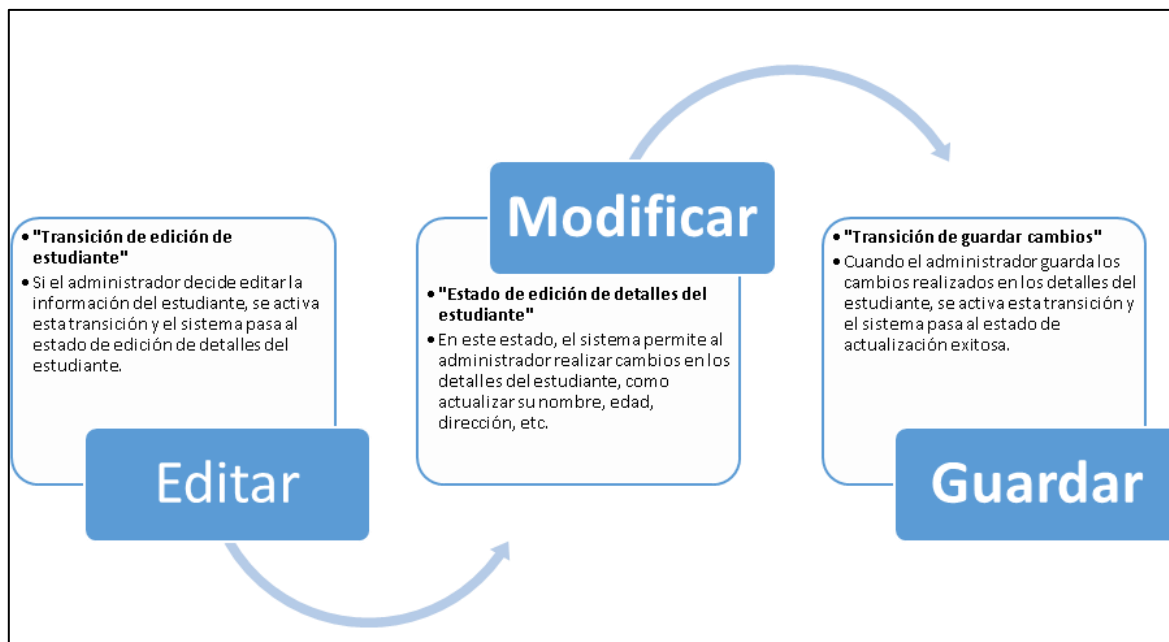
En la Figura 77.- Diagrama para visualizar un estudiante, muestra lo siguiente:

El siguiente diagrama muestra el flujo de un sistema administrativo (admin) para realizar operaciones CRUD (Crear, Leer, Actualizar, Eliminar) de estudiantes. El

proceso comienza en el estado inicial, donde el sistema muestra una lista de estudiantes existentes.

Diagrama de proceso de Editar un estudiante

Figura 78.- Diagrama para Editar un estudiante

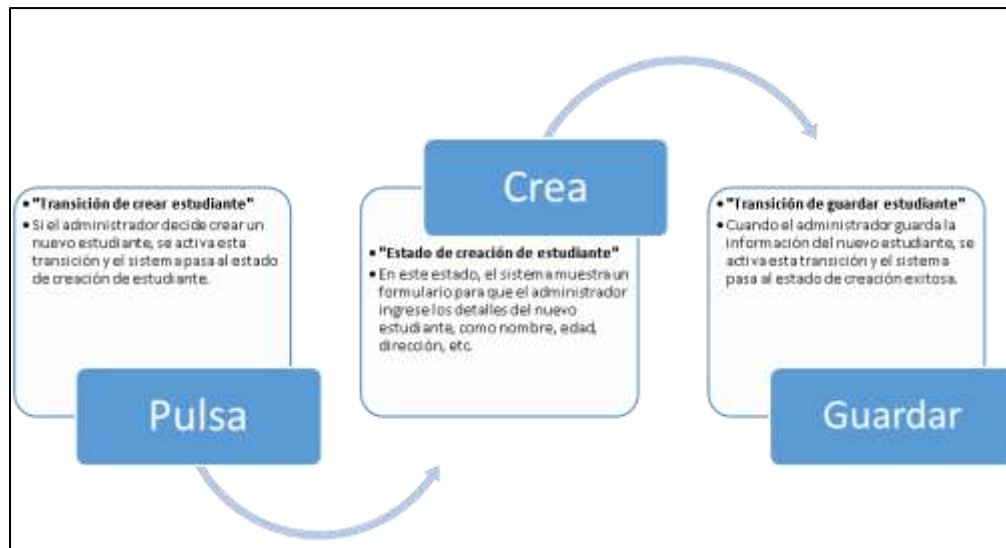


En la Figura 78.- Diagrama para editar un estudiante, muestra lo siguiente:

A partir de este estado, el administrador tiene dos opciones. Puede optar por editar los detalles del estudiante, lo que activa la transición de edición de estudiante y lleva al sistema al estado de edición de detalles del estudiante. En este estado, el administrador puede realizar cambios en la información del estudiante.

Diagrama de proceso de Crear un nuevo estudiante

Figura 79.- Diagrama para Crear un nuevo estudiante

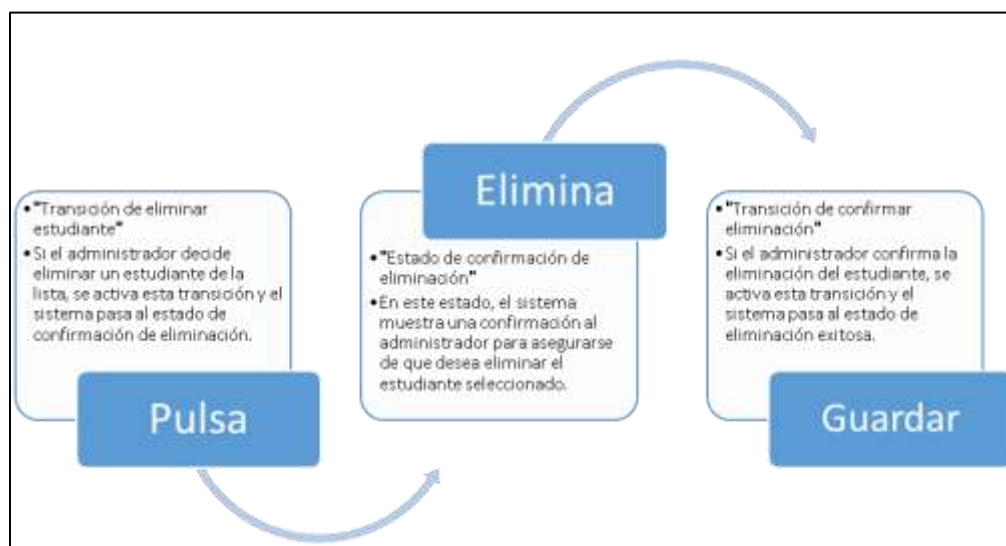


En la Figura 79.- Diagrama para crear un nuevo estudiante, muestra lo siguiente:

En el estado de creación de nuevos estudiantes el administrador podrá crear nuevos usuarios llenando un formulario, que detalla los datos necesarios que se requieren para la creación de uno nuevo, para posteriormente pasar al estado de guardado exitoso.

Diagrama de proceso de Eliminar un nuevo estudiante

Figura 80.- Diagrama para Eliminar un estudiante



En la Figura 80.- Diagrama para eliminar un estudiante, muestra lo siguiente:

Desde el estado de visualización de detalles del estudiante seleccionado, el administrador también tiene la opción de eliminar al estudiante. Al seleccionar la opción de eliminar, se activa la transición de eliminar estudiante, y el sistema pasa al estado de confirmación de eliminación.

12. Conclusiones

El uso de credenciales digitales en lugar de credenciales físicas ofrece una solución más eficiente y segura para la gestión de acceso en el Instituto Tecnológico Nacional de México/Instituto Tecnológico de Apizaco. Esto resuelve los problemas de vulnerabilidad de seguridad asociados con las credenciales de plástico, como pérdida, robo o replicación.

La implementación de una aplicación móvil para estudiantes proporciona un acceso rápido y conveniente a la credencial digital. Esto elimina la dependencia de una credencial física y facilita el ingreso a la institución, mejorando la experiencia del usuario.

En resumen, el proyecto propuesto busca mejorar la seguridad, eficiencia y experiencia del usuario en el acceso y gestión de credenciales en el Instituto Tecnológico Nacional de México/Instituto Tecnológico de Apizaco. La implementación de una aplicación móvil para estudiantes y un sitio web para administradores ofrece soluciones tecnológicas que optimizan los procesos y contribuyen a la modernización de la institución.

12.1 Recomendaciones

Seguridad de datos: Es fundamental garantizar la seguridad de los datos, especialmente al digitalizar las credenciales y manejar información personal de los estudiantes. Implementar medidas sólidas de seguridad, como encriptación de datos, autenticación segura y protección contra ataques cibernéticos, para asegurar la confidencialidad y privacidad de la información.

Pruebas exhaustivas: Antes de lanzar la aplicación y el sitio web, realizar pruebas exhaustivas para asegurar que funcione correctamente y cumplan con todos los requisitos. Realizar pruebas de funcionalidad, seguridad y usabilidad para identificar posibles problemas y corregirlos antes de su implementación final.

Experiencia del usuario: En el diseño tanto de la aplicación como del sitio web, debe dar gran importancia a la experiencia del usuario. Asegurando de que la interfaz sea intuitiva, fácil de usar y atractiva visualmente. Realizaré pruebas de usabilidad con usuarios reales para obtener sus comentarios y realizar mejoras que optimicen su experiencia.

Capacitación y soporte: Una vez que el proyecto esté implementado, proporcionaré una capacitación adecuada y soporte a los usuarios, tanto a los administradores como a los estudiantes. Crearé tutoriales claros, documentación detallada y canales de soporte para resolver cualquier duda o problema que puedan surgir, asegurándome de que todos puedan utilizar el sistema de manera efectiva.

Actualizaciones y mantenimiento: Mantendré el proyecto actualizado y realizaré un mantenimiento regular para garantizar su correcto funcionamiento a lo largo del tiempo. Implementaré actualizaciones de seguridad, corregiré errores y realizaré mejoras adicionales según sea necesario. Estaré atento a las nuevas tecnologías y prácticas en el campo de las aplicaciones móviles y la seguridad digital para mantener el proyecto actualizado y seguro.

12.2 Experiencia profesional adquirida

Participar en el desarrollo del proyecto ACCESO DIGITAL CARD-ITA: ANÁLISIS Y DISEÑO ha sido una experiencia enriquecedora y de gran relevancia en mi desarrollo profesional. Este proyecto me ha permitido adquirir conocimientos y habilidades fundamentales en el diseño de soluciones tecnológicas innovadoras, así como en la gestión eficiente de bases de datos y en la creación de interfaces intuitivas y amigables para los usuarios y me ha permitido aprender de las mejores prácticas en términos de seguridad, usabilidad y escalabilidad.

El desarrollo de este proyecto me dejó los siguientes conocimientos:

1. Análisis de la problemática existente en el uso de credenciales físicas.
2. Investigación de tecnologías y conceptos relacionados, como credenciales digitales, transformación digital, identidad digital y gestión de identidades.
3. Aplicación de metodología de desarrollo de proyectos.
4. Recopilación y análisis de requisitos funcionales y no funcionales.
5. Diseño de la estructura y flujo de la aplicación.
6. Evaluación de factibilidad del proyecto.
7. Definición de requerimientos funcionales y no funcionales.
8. Desarrollo de casos de uso y diagramas correspondientes.
9. Modelado de la base de datos.
10. Creación de diagramas de secuencia y actividad.
11. Selección de herramientas y tecnologías adecuadas.
12. Diseño del look and feel del sitio web y la aplicación móvil.
13. Priorización de servicios según las necesidades de los usuarios.
14. Implementación de la estructura y flujo de la aplicación.
15. Documentación de todos los aspectos del proyecto.
16. Exposición y discusión de los resultados obtenidos.
17. Diseño y creación de interfaces intuitivas y de fácil uso.
18. Implementación de técnicas de seguridad de la información.

19. Trabajo en equipo y colaboración con los diferentes roles involucrados en el proyecto.
20. Adquisición de conocimientos en tecnologías emergentes como Blockchain y códigos QR.
21. Manejo de bases de datos y modelado de entidades y relaciones.
22. Diseño centrado en el usuario y consideraciones de usabilidad.

13. Competencias desarrolladas

Desarrollo de aplicaciones móviles: Al crear una aplicación móvil para sustituir la credencial de plástico, has adquirido habilidades en el desarrollo de aplicaciones móviles, incluyendo el diseño de interfaces, la programación y la integración de funcionalidades.

Seguridad de la información: Al implementar medidas de autenticación y seguridad en la plataforma digital, has adquirido conocimientos y habilidades en el ámbito de la seguridad de la información. Esto puede incluir el uso de cifrado, protección de contraseñas y autenticación multifactor.

Análisis de requisitos: Para identificar las credenciales requeridas y diseñar la plataforma, es probable que hayas realizado un análisis de requisitos. Esto implica identificar las necesidades de los usuarios y traducirlas en funcionalidades y características concretas.

Diseño de bases de datos: Al desarrollar una base de datos para almacenar las credenciales digitalmente, has adquirido habilidades en el diseño de bases de datos, incluyendo la definición de tablas, relaciones y restricciones.

Diseño de interfaces de usuario (UI): Al crear el diseño del look and feel tanto del sitio web como de la aplicación, has adquirido habilidades en el diseño de interfaces de usuario atractivas y funcionales. Esto puede incluir el diseño de elementos visuales, la selección de colores y tipografías, y la organización de la información en la interfaz.

Experiencia de usuario (UX): Al diseñar el look and feel de la aplicación y el sitio web, es probable que hayas tenido en cuenta la experiencia de usuario. Esto implica comprender las necesidades y expectativas de los usuarios y diseñar la interfaz de manera que sea intuitiva y fácil de usar.

Diseño centrado en el usuario: Al desarrollar el diseño del look and feel, es posible que hayas seguido un enfoque centrado en el usuario, teniendo en cuenta las necesidades, preferencias y comportamientos de los usuarios. Esto implica realizar investigaciones, crear prototipos y realizar pruebas de usabilidad para mejorar la experiencia del usuario.

Creatividad y estética: Al diseñar el look and feel, es probable que hayas aplicado tu creatividad y habilidades estéticas para crear una interfaz atractiva y visualmente agradable. Esto implica tomar decisiones de diseño en cuanto a la disposición de los elementos, la selección de colores, imágenes y tipografías, y la creación de una identidad visual coherente.

Diseño de navegación y flujo de usuarios: Al diseñar tanto el sitio web como la aplicación, es probable que hayas tenido en cuenta la navegación y el flujo de los usuarios a través de las diferentes secciones y funcionalidades. Esto implica crear una estructura de navegación clara y lógica, asegurando que los usuarios puedan acceder fácilmente a la información y realizar las acciones deseadas.

Fuentes de información

- Ayuda para pruebas de software. (Dakota del Norte.). Metodologías de prueba de software.
- boyd, d. (2014). It's complicated: The social lives of networked teens. Yale University Press.
- Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. <https://ethereum.org/en/whitepaper/>
- Choi, B. H., & Chung, W. H. (2019). A study on the security improvement of the mobile barcode authentication method using the QR code. Journal of the Korea Institute of Information Security and Cryptology, 29(2), 471-482.
- Consorcio de Aprendizaje Global IMS. (2017). Credencialización digital: conceptos básicos. Recuperado el 12 de marzo de 2023, de <https://www.imsglobal.org/digital-credentialing-basics>
- Cummings, T. G., & Worley, C. G. (2014). Organization development and change (10th ed.). Cengage Learning.
- D'Andrea, M. (2019). The Psychological Effects of Colors: Blue. Retrieved from <https://www.thoughtco.com/psychological-effects-of-color-blue-2795811>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 13(3), 319-340.
- *El modelo en cascada: desarrollo secuencial de software*. (2019, 21 marzo). IONOS Digital Guide. <https://www.ionos.mx/digitalguide/paginas-web/desarrollo-web/el-modelo-en-cascada/>
- GeeksforGeeks. (2022). Waterfall Model. Retrieved March 12, 2023, from <https://www.geeksforgeeks.org/software-engineering-waterfall-model/>
- Graff, M. (2017). Credenciales digitales: una investigación sobre el valor de las insignias digitales y las microcredenciales en la educación superior. Educause. Obtenido de <https://library.educase.edu/resources/2017/6/digital-credentials-an-investigation-into-the-value-of-digital-badges-and-microcredentials-in-higher-education>.
- Instituto de manejo proyectos. (2017). Una guía de los fundamentos de la dirección de proyectos (Guía del PMBOK), sexta edición.
- International Organization for Standardization (ISO). (2019). ISO 9241-11:2018 Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. <https://www.iso.org/standard/63500.html>
- International Organization for Standardization (ISO). (2019). ISO 9000:2015 Quality management systems — Fundamentals and vocabulary. <https://www.iso.org/standard/63712.html>
- International Organization for Standardization. (2015). ISO/IEC 18004:2015 - Information technology - Automatic identification and data capture techniques

- QR Code 2005 bar code symbology specification. Retrieved from <https://www.iso.org/standard/62021.html>
- Investopedia. (2022). Blockchain. Retrieved from <https://www.investopedia.com/terms/b/blockchain.asp>
- ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.
- Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
- Lantrip, L. (2021). The Psychology of Color: A Designer's Guide to Color Association & Meaning. Retrieved from <https://99designs.com/blog/tips/the-psychology-of-color/>
- Laudon, K. C. y Laudon, J. P. (2016). Sistemas de Información Gerencial: Gestión de la Empresa Digital. Pearson Educación limitada.
- Li, X., Li, W., Li, Y., & Zhu, H. (2016). A ubiquitous campus information service system based on QR code. Journal of Ambient Intelligence and Humanized Computing, 7(2), 189-200.
- Liu, H., & Wu, Y. (2017). Design and implementation of campus smart card system based on QR code. Journal of Physics: Conference Series, 946(1), 012010.
- Makridakis, S., Lontou, C. y Barlas, P. (2018). Blockchain: una solución a los problemas de transparencia y confianza en la acreditación y la acreditación. En R. Koussouris, D. Gouscos y E. Bacao (Eds.), Gobierno Abierto: Oportunidades y Desafíos para la Gobernanza Pública (pp. 289-306). Saltador.
- Makridakis, S., Lontou, C., & Barlas, P. (2018). Blockchain: A Solution to Transparency and Trust Issues in Accreditation and Credentialing. In R. Koussouris, D. Gouscos, & E. Bacao (Eds.), Open Government: Opportunities and Challenges for Public Governance (pp. 289-306). Springer.
- Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. Information & management, 38(4), 217-230.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
- National Institute of Standards and Technology. (2011). Guidelines for Managing and Securing Mobile Devices in the Enterprise. Retrieved from <https://nvlpubs.nist.gov/nistpubs/ir/2011/NIST.IR.7298r2.pdf>
- National Institute of Standards and Technology. (2017). Digital Identity Guidelines. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf>
- NIST. (2018). Computer Security Resource Center. Retrieved March 12, 2023, from <https://csrc.nist.gov/topics/cybersecurity>
- O'Brien, J. A. y Marakas, G. M. (2018). Sistemas de Información Gerencial. Educación McGraw-Hill.

- Pileckaite, G. (2020). The Meaning of Colors in Marketing. Retrieved from <https://www.printful.com/blog/the-meaning-of-colors-in-marketing/>
- Priyadarshini, R., & Barua, A. K. (2019). A smart card-based secure attendance system. *Procedia Computer Science*, 165, 286-293.
- Rahman, A., Sarker, S., Islam, S., & Zaman, S. (2019). A Framework for Secure Digital Credentials Management in the Blockchain Era. *IEEE Access*, 7, 1202-1213.
- Revista Internacional de Ciencias de la Computación y Seguridad de la Información. (2017). Diseño de sistemas.
- Revista Internacional de Ciencias de la Computación y Seguridad de la Información. (2017). Implementación.
- Revista Internacional de Ciencias de la Computación y Seguridad de la Información. (2017). Mantenimiento del software.
- Rogers, EM (2003). *Difusión de Innovaciones*, 5ª Edición. Prensa Libre.
- Royce, W. (1970). Gestión del desarrollo de grandes sistemas de software: Conceptos y técnicas. *Actas de la novena conferencia internacional sobre ingeniería de software*, 328-338.
- Saha, S. (2019). The Meaning of Colors: Color Symbolism in Design. Retrieved from <https://uxdesign.cc/the-meaning-of-colors-color-symbolism-in-design-ec6b9b5b8e94>
- Sommerville, I. (2015). *Ingeniería de software*. Pearson.
- Stair, R. M. y Reynolds, G. W. (2019). *Principios de los Sistemas de Información*. Aprendizaje Cengage.
- Sun, X., Chen, J. y Li, Y. (2019). Una revisión de la investigación sobre las credenciales digitales en la educación. *Revista Internacional de Tecnologías Emergentes en el Aprendizaje*, 14(22), 59-75.
- Sun, X., Chen, J., & Li, Y. (2019). A Review of Research on Digital Credentials in Education. *International Journal of Emerging Technologies in Learning*, 14(22), 59-75.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.
- Techopedia. (Dakota del Norte.). *Recopilación de requisitos*.
- Techopedia. (n.d.). *Mobile Application*. Retrieved from <https://www.techopedia.com/definition/29506/mobile-application>
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. Simon & Schuster.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131.

- Typewolf, "Arial Typeface", [En línea]. Disponible en: <https://www.typewolf.com/site-of-the-day/fonts/arial>.
- Van den Hoven, J. (2015). Value sensitive design and responsible innovation. In B. Calvo & T. G. Fjeldberg (Eds.), *The Routledge Handbook of Philosophy of Engineering* (pp. 280-294). Routledge.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*, 46(2), 186-204.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 27(3), 425-478.
- Wattenhofer, R. (2016). The science of the blockchain. https://www.cs.huji.ac.il/~razw/files/BlockchainF12/04_The_Science_of_the_Blockchain.pdf
- Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security*. Cengage Learning.
- Wu, W., & Chen, X. (2019). Research and implementation of the smart campus access control system based on NFC and QR code technology. *Journal of Physics: Conference Series*, 1279(1), 012031.
- Zarei, S., & Saberi, M. (2018). QR code-based student attendance system. *International Journal of Information and Communication Technology Education*, 14(2), 13-28.
- Zeng, L., Huang, Y., Li, Y., & Li, S. (2016). A design of intelligent campus system based on QR code and mobile technology. *Journal of Ambient Intelligence and Humanized Computing*, 7(6), 801-811.

ANEXOS

ANEXO 1 ENCUESTA

Título: Credenciales digitales para el acceso de los estudiantes

Introducción:

Estamos considerando implementar credenciales digitales basadas en dispositivos móviles para reemplazar las credenciales de plástico para el acceso a la universidad. Con este cambio, los estudiantes utilizarían una aplicación móvil para acceder a las instalaciones de la universidad, reemplazando la necesidad de credenciales físicas. Estamos buscando sus comentarios sobre este cambio potencial para ayudarnos a tomar decisiones informadas.

Preguntas de la encuesta:

¿Alguna vez ha enfrentado dificultades o inconvenientes relacionados con el porte de la credencial de plástico ya sea olvidado, perdido o extraviado?

- a) Sí, una vez
- b) Sí, varias veces
- c) No, nunca los he perdido o extraviado

¿Alguna vez perdiste u olvidaste tu credencial de plástico y, de ser así, qué impacto tuvo en tus estudios o rendimiento académico?

- a) Perdí varias horas de clases
- b) Bajo mi promedio por faltas
- c) Llegar tarde a clases por realizar el registro en el libro

En caso de extravió ¿Cuánto tiempo tardas en reponer tu credencial en caso de extravió?

- a) Una semana
- b) Más de una semana
- c) Un mes o más

¿Cuál es el motivo por el que te tardas en reponer tu credencial?

- a) Económico (Costo de reposición)
- b) Falta de tiempo
- c) Desconocimiento del proceso
- d) Tiempo de entrega

¿Actualmente cuentas con un teléfono móvil?

- a) Sí
- b) No

¿Cuál es el sistema operativo de tú teléfono móvil?

- a) Android
- b) IOS

¿Cuentas con acceso a internet y o datos móviles?

- a) Sí

- b) La mayoría de tiempo
- c) Casi Nunca
- d) No

¿Está familiarizado con las credenciales digitales y cómo funcionan?

- a) Sí
- b) No

¿Le resultaría conveniente tener su credencial de plástico de forma digital en una aplicación móvil para acceder al instituto y a sus servicios?

- a) Sí, mucho más conveniente
- b) Sí, algo más conveniente
- c) No, aproximadamente el mismo nivel de conveniencia
- d) No, menos conveniente

¿Qué importancia tiene para usted la seguridad de sus datos a la hora de acceder a las instalaciones universitarias?

- a) Muy importante
- b) Algo importante
- c) Neutro
- d) Poco importante
- e) Nada importante

¿Cómo te sientes con la idea de usar una aplicación móvil para acceder a las instalaciones de la universidad en lugar de usar credenciales de plástico?

- a) Me gusta la idea
- b) Neutro
- c) No me gusta la idea

¿Estaría dispuesto a participar en un programa piloto para probar una aplicación móvil donde tenga tú credencial digital para poder acceder a la institución y los servicios que esta ofrece y, de ser así, qué factores influirían en su decisión de participar?

- a) Sí
- b) No

¿Tiene algún otro comentario o sugerencia relacionada con la implementación de credenciales digitales basadas en dispositivos móviles para el acceso a la universidad?

Gracias por tomarse el tiempo para completar esta encuesta. Sus comentarios nos ayudarán a tomar decisiones informadas sobre la implementación de credenciales.

ANEXO 2 GLOSARIO DE TÉRMINOS

Credenciales: Son datos de identificación utilizados para acceder a un sistema o servicio.

Base de datos: Un conjunto organizado de datos almacenados en una computadora.

Interfaz de usuario: La forma en que los usuarios interactúan con un sistema o una aplicación.

Look and Feel: La apariencia y experiencia general de un sitio web o aplicación.

Usuario: Una persona que utiliza un sistema o servicio.

Administrador: Una persona encargada de gestionar y supervisar un sistema o una aplicación.

Credencial digital: Una versión electrónica de una identificación o tarjeta de acceso.

Accesos: Los registros de entrada y salida de usuarios a un sistema o lugar.

Gráficos: Representaciones visuales de datos utilizando diferentes tipos de gráficos, como barras, líneas o círculos.

Tipografía: El estilo y diseño de las letras utilizadas en un diseño o texto.

Paleta de colores: Un conjunto de colores seleccionados y utilizados en un diseño.

Estructura: La organización y disposición de los elementos en un diseño o sistema.

Diseño de servicios: La planificación y creación de servicios que satisfacen las necesidades de los usuarios.

Necesidades de los usuarios: Los requisitos y deseos de los usuarios en relación con un sistema o servicio.

Mapa de navegación: Una representación visual de la estructura y flujo de un sitio web o aplicación.

Glosario de términos: Una lista de palabras y definiciones utilizadas en un proyecto o conversación.

Registro: Un conjunto de datos relacionados que se almacenan en una base de datos.

Búsqueda: Proceso de encontrar información específica dentro de un conjunto de datos.

Filtro: Una función que permite mostrar solo los datos que cumplan con ciertos criterios predefinidos.

Estadísticas: Datos numéricos y métricas utilizados para analizar y resumir información.

Informes: Documentos o presentaciones que contienen datos organizados y analizados.

Menú lateral: Una barra de navegación vertical que proporciona acceso a diferentes secciones o funciones de una aplicación.

Carga de trabajo: La cantidad de trabajo o tareas que se deben realizar en un período de tiempo determinado.

Smartphone: Un teléfono móvil inteligente que ofrece funciones avanzadas como acceso a Internet, aplicaciones y comunicación.

Identificación: El acto de demostrar o confirmar la identidad de una persona.

Programa académico: Un plan de estudios o conjunto de cursos y asignaturas en un campo educativo específico.

Verificar: Confirmar la autenticidad o exactitud de algo, como la información personal.

Flujo de la aplicación: El recorrido o secuencia de pantallas y acciones que un usuario sigue dentro de una aplicación.

Credencial física: Una tarjeta o documento impreso que se utiliza como identificación o acceso.

Impacto ambiental: El efecto o consecuencias que una acción o proceso tiene en el medio ambiente.

Generar: Crear o producir algo, como informes, estadísticas o documentos.