UNIVERSIDAD NACIONAL DE SAN MARTÍN

Escuela de Ciencia y Tecnología

Proyecto Final Integrador

Desarrollo e implementación de un sistema de bicicletero seguro basado en tecnología LoRa para el campus Miguelete de la Universidad Nacional de General San Martín

Autores

Moira Rocio Acher Moranchel

Lucio Javier Ibero

Carrera

Ingeniería en Telecomunicaciones

Tutor

Lucas Gabriel Lopez Ardura

Docentes

Ing. Marcelo Romeo

Dra. en Ingeniería María Claudia Abeledo

2024

Índice

Resumen

El objetivo principal de este proyecto es el estudio y diseño de un sistema de bicicleteros seguros a implementarse en la Universidad Nacional de General San Martín, particularmente, en el campus Miguelete. Se pretende dar soluciones al personal docente y no docente y estudiantes, facilitando su transporte y seguridad a la hora de dejar las bicicletas en el predio.

El sistema consta de un dispositivo llamado candado electrónico ubicado en el bicicletero, y otro dispositivo transceptor ubicado dentro de la Escuela de Ciencia y Tecnología de la Universidad Nacional de General San Martín. Además, como parte del proyecto, se incluye una aplicación móvil que permite a la comunidad educativa hacer uso de los candados, mediante la generación de una clave única que permite bloquear y desbloquear los mismos.

Para lograr la implementación, se estudió acerca de tecnologías de las telecomunicaciones que pudieran servir para la implementación de dichos bicicleteros seguros. Finalmente se tomó la decisión de utilizar la tecnología de Largo Alcance LoRa para la comunicación entre el candado y el transceptor, para lograr por ejemplo la apertura y cierre del pestillo de seguridad, mediante la transmisión y recepción de la clave única.

Por otro lado, el sistema está sustentado en la utilización de una base de datos que almacena la información de los usuarios y los candados electrónicos. El dispositivo transceptor debe comunicarse con la base de datos para consultar acerca del estado del candado. Para ello, se establece una comunicación a través del estándar 802.11n.

Se seleccionó este proyecto debido a su estrecha relación con la Ingeniería en Telecomunicaciones, donde se involucra el estudio e implementación de una comunicación LoRa y una comunicación bajo el estándar 802.11n. Además, es un proyecto que aporta a la idea de un campus inteligente, sustentable y donde toda la comunidad académica se sienta segura de transitar.

Introducción

Para el desarrollo del Proyecto Final Integrador de la carrera Ingeniería en Telecomunicaciones, se tomó la decisión de desarrollar e implementar un sistema de bicicleteros seguros basados en tecnología LoRa para el campus Miguelete de la Universidad Nacional de General San Martín, desde ahora UNSAM.

El campus Miguelete de la UNSAM es un terreno de aproximadamente 1 kilómetro de extensión, donde se pueden encontrar diferentes Escuelas o Facultades. El campus cuenta además con múltiples instalaciones de investigación, administrativas y un sector de aulas donde se cursa el ingreso a las carreras, además de otras materias.

Los medios de acceso al campus más comunes son:

- Líneas de colectivo que transitan por la Av. 25 de Mayo
- Automóvil (el campus cuenta con amplias zonas de estacionamiento)
- Tren Línea Mitre ramal José León Suárez, estaciones Miguelete y San Martín. Cada estación se encuentra a pocas cuadras de las extremos del campus.

Además, la Universidad cuenta con un sistema de bus interno que permite a la comunidad universitaria moverse de una punta del campus, hacia la otra.

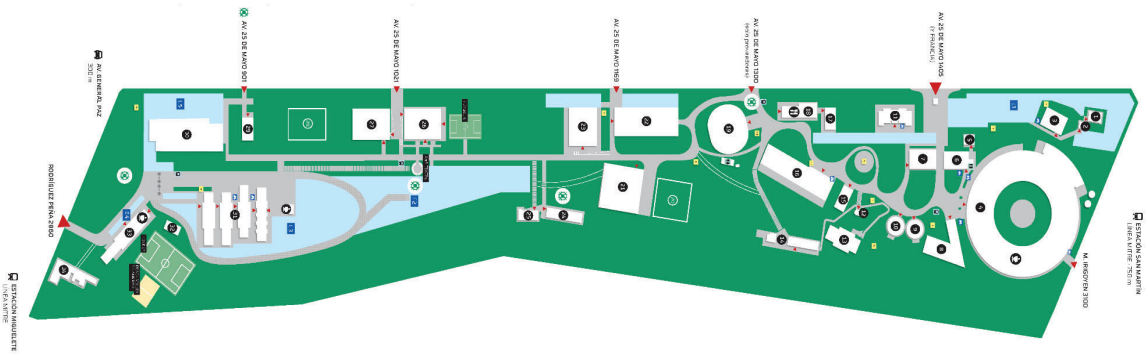

Imagen 1. Diagrama del campus Miguelete.

Ahora bien, habiendo hecho un repaso general de la infraestructura del campus y del acceso al mismo, se plantea la problemática actual la cual lleva al propósito del proyecto.

El bus cuenta con horarios bastante específicos, que no cubren el horario académico de forma completa, y con capacidad muy limitada. Sumado a eso, hay días en los que no se encuentra en funcionamiento. Consecuentemente, las probabilidad de poder alcanzar el bus, son bajas. Finalmente, termina sucediendo que tanto los alumnos, docentes y no docentes se quedan con la opción de caminar o de utilizar una bicicleta como medio de transporte interno.

En cuanto a la opción de caminar, tal cómo se mencionó, el campus tiene una extensión de 1 kilómetro por lo que trasladarse de una punta hacia la otra resulta tedioso. Sumado a esto, suele suceder que los alumnos, docentes y no docentes, ya sea por inconvenientes con el transporte o cuestiones de índole laboral llegan con poco márgen de tiempo para el inicio de sus actividades académicas, por lo que caminar 1 kilómetro, insume entre 15 y 20 minutos extra.

Imagen 2. Campus Miguelete en visto desde Google Maps Satelital donde se aprecia la distancia entre extremos.

Por otro lado, el tren, uno de los medios de acceso más comunes al campus, cuenta con furgones que permiten a los pasajeros llevar de forma cómoda la bicicleta. De esta manera, es muy común ver un gran porcentaje de la comunidad académica utilizando dicho medio de transporte dentro del campus.

Si bien a lo largo del predio universitario se pueden ver “bicicleteros”, lo cierto es que no son más que caños metálicos sin ningún tipo de seguridad, más que el candado que puede llevar el dueño de la bicicleta.

Como consecuencias, en primer lugar, siendo la Universidad un lugar de acceso público, como cualquier ente Nacional, no es poco común escuchar historias de robos de bicicletas. En segundo lugar, muchos tienden a dejar su medio de transporte en un lugar más “seguro”, es decir dentro de los edificios, en los pasillos y en las aulas. Esto último no solo es molesto para transitar, sino que también va contra las normas de seguridad.

Finalmente, se llega al propósito del proyecto: candados electrónicos que puedan ser instalados a lo largo del campus y que cuenten con los métodos de seguridad correspondientes para no ser adulterados. La idea es poder agilizar la movilidad dentro del campus, minimizando los tiempos de traslado. De esta manera, se contribuye a la idea de un campus inteligente, donde la tecnología permita mejorar la calidad educativa en cuanto al acceso y la movilidad dentro del mismo.

Se propone instalar bicicleteros a lo largo del campus dotados de una cantidad de candados electrónicos de manera que cualquier persona perteneciente a la comunidad educativa pueda ingresar con su bicicleta propia y estacionarla sin preocupación alguna. Para ello, el usuario deberá descargarse una aplicación, de ahora en más App, desarrollada también como parte del proyecto. En dicha App se encontrará con un mapa del campus Miguelete, en cual podrá visualizar las estaciones disponibles. Al seleccionar una estación, podrá además visualizar los candados disponibles y seleccionar uno para su uso.

La selección del candado generará un token el cual permitirá bloquear el pestillo de seguridad del candado, quedando la bicicleta estacionada. Cuando el usuario quiera retirarse del campus, deberá volver a loguearse en la App y simplemente ingresa el código de desbloqueo que se indica en pantalla, el cual será únicamente visible al usuario que haya hecho el bloqueo en primer lugar.

A nivel constructivo, aunque se presenta con mayor detalle en próximos capítulos del informe, el prototipo se construirá con dos dispositivos, uno ubicado en la estación de bicicletas (bicicletero) y otro ubicado en la Escuela de Ciencia y Tecnología. Ambos constan de un módulo LoRa, un módulo IEEE 802.11n y un microprocesador ESP32.

Del lado del candado, el dispositivo se conectará a un teclado matricial, el cual permitirá al usuario ingresar el token. Además, se conectará a un servomotor que permitirá mover el pestillo de seguridad. Del lado de la Escuela de Ciencia y Tecnología, el dispositivo se conectará a través del estándar 802.11n a una Base de Datos que almacena la información del usuario y el estado del candado. Entre ambos dispositivos se comunicarán a través de LoRa para transmitir dicha información. Para mayor claridad sobre el sistema de comunicación entre el candado, el dispositivo de usuario, la base de datos y la aplicación, se puede consultar la imagen de la sección *2.3 Tecnologías Implementadas* del presente documento (Img. 3)

El informe está organizado en cuatro capítulos. El primero, se encuentra destinado a lo que se conoce como Anteproyecto. En dicha sección se realiza el desglose preliminar de lo que conlleva el desarrollo del proyecto presentado en cuanto a costos, riesgos y la gestión de tiempos y tareas a realizar.

En el segundo capítulo se introducen los conceptos básicos de la comunicación por radiofrecuencia. Se estudiarán las tecnologías existentes y su factibilidad para el desarrollo del proyecto, presentando a LoRa como la elegida, gracias a sus características. Hablaremos de su modulación, su codificación y los mecanismos y políticas de seguridad empleadas.

El capítulo número tres está dedicado puramente al proyecto, en él se realiza el análisis y diseño de la solución. Desde el establecimiento de la comunicación, la construcción del candado electrónico, los materiales utilizados, la programación detrás del mismo, el armado de la base de datos y el desarrollo de la aplicación.

Finalmente, en el cuarto capítulo, se comparten las consideraciones y sugerencias de implementación futura junto con las conclusiones obtenidas a lo largo de la realización del proyecto. Al final del documento se incluyen los códigos empleados y la bibliografía consultada.

1. Anteproyecto

1.1 Acta constitutiva del proyecto

ACTA CONSTITUTIVA		
Título del proyecto		
Desarrollo e implementación de un sistema de bicicletero seguro basado en tecnología LoRa para el campus Miguelete de la UNSAM. Nombre comercial: UNSAM Bicis Seguras		
Estudiantes	**Legajos**	**Firmas**
Lucio Javier Ibero Moira Rocio Acher Moranchel	CYT-9098 CYT-9249	
Fecha de Inicio	**Fecha tentativa de finalización**	
21 de marzo de 2023	21 de marzo de 2024	
Objetivo General		
Mitigar el riesgo de robo de bicicletas dentro del campus Miguelete de la UNSAM con la implementación y armado de un bicicletero seguro.		
Objetivos Específicos		
Desarrollar e implementar un sistema de bicicletero seguro en el campus Miguelete de la UNSAM, con el fin de mitigar el riesgo de robo de bicicletas. Esto se logrará mediante el armado de un candado electrónico utilizando tecnología LoRa, junto con la integración de una aplicación móvil y una base de datos. El objetivo es proporcionar a los usuarios una solución confiable y conveniente para proteger sus bicicletas, fomentando así el uso de este medio de transporte sostenible en la comunidad universitaria.		
Descripción del producto o servicio que generará el proyecto – Entregables finales del proyecto		
El proyecto a realizar consiste en el armado de un bicicletero seguro en el campus Miguelete de la UNSAM. El mismo consta de 5 componentes principales que conforman al sistema de comunicación entre el punto A (Transmisor LoRa ubicado en el candado) y el punto B (Receptor LoRa ubicado en el CIDI): un candado electrónico, un transceptor con módulo 802.11n que actúe como nexo con Firebase, una Base de datos (Firebase), una aplicación móvil y el lugar físico para colocar el candado. La idea es que el usuario pueda desbloquear el candado mediante una clave única generada aleatoriamente mediante la aplicación. Para ello vamos a desarrollar el armado de la base de datos, la aplicación, el prototipo de candado y el establecimiento de la comunicación entre		

los sitios.

Justificación o propósito del Proyecto (Aportes y resultados esperados)

- Incremento de la seguridad: El principal aporte de este proyecto es proporcionar un sistema de almacenamiento de bicicletas seguro para los estudiantes, profesores y personal de la UNSAM. Al implementar un candado electrónico con comunicación LoRa y una aplicación móvil, se facilita el acceso y se espera reducir significativamente los casos de robo de bicicletas en la UNSAM, brindando tranquilidad a los usuarios y promoviendo el uso de la bicicleta como medio de transporte sostenible
- Mejora de la experiencia de usuario: El proyecto busca brindar a los usuarios una solución conveniente y confiable para proteger sus bicicletas. La generación de una clave única mediante la aplicación móvil permitirá a los usuarios desbloquear el candado de forma rápida y sencilla, eliminando la necesidad de llevar consigo su propio candado o cadena.
- Innovación tecnológica: La implementación de tecnologías implica una incorporación de soluciones tecnológicas avanzadas en la infraestructura de la UNSAM. Esto demuestra el compromiso de la institución con la vanguardia tecnológica y la adaptación a las necesidades actuales, contribuyendo a la construcción de un "campus Inteligente".

Supuestos

- Se contará con los recursos financieros necesarios para adquirir los materiales requeridos para el armado del prototipo de candado y la implementación del sistema en general.
- Se conseguirán los componentes adecuados para el armado del prototipo de candado.
- Se contará con los conocimientos necesarios para la realización del proyecto.
- Se contará con el tiempo suficiente para llevar a cabo todas las etapas del proyecto.
- Se contará con el respaldo de la Institución, autoridades y profesores para llevar a cabo el proyecto.
- Se contará con el apoyo de un Tutor adecuado para el proyecto.
- Como alumnos, se tendrán todas las materias necesarias regularizadas y con sus respectivos finales aprobados.
- Se espera que exista una comunicación fluida y una colaboración efectiva entre los miembros del equipo.

Restricciones

- Existe un límite de presupuesto, lo cual implica que se deben tomar decisiones de adquisición de materiales y recursos dentro de un marco financiero que permita que el proyecto sea factible.
- Existe una restricción de tiempo sujeta a lo establecido en el reglamento institucional, por lo que el proyecto debe ser completado dentro de un plazo determinado.
- El equipo encargado del proyecto tiene una cantidad limitada de miembros, por lo que se debe realizar una adecuada distribución de tareas.
- Se deben tener en cuenta las limitaciones físicas propias de las bicicletas y los bicicleteros en los que se instalarán los candados (infraestructura disponible).
- Se deben cumplir con todas las regulaciones, normativas y leyes aplicables en relación con la protección de datos personales, la seguridad de la información, la propiedad intelectual y cualquier otro aspecto relevante para el desarrollo y la implementación del proyecto.

Dirigido por	Lucas Gabriel Lopez Ardura	**Firma**	
Co-dirigido por		**Firma**	
Aprobado por		**Firma**	

1.2 Work Breakdown Structure (WBS)

1. Investigación de las bases del proyecto
    1.1 Investigación de la tecnología a utilizar para la comunicación.
    1.2 Investigación sobre el armado de una base de datos
    1.3 Investigación del cifrado/generación de claves aleatorias y seguras
    1.4 Investigación desarrollo de la aplicación
    1.5 Investigación sobre LoRa, LoRaWAN
    1.6 Registro/documentación de los avances.

2. Investigación sobre el armado del prototipo de candado
    2.1 Alimentación, materiales a utilizar (modelos, tamaño, consumo)
    2.2 Investigación sobre el robo/corte del candado
    2.3 Compra de los materiales
    2.4 Registro/documentación de los avances.

3. Análisis de costos y comunicación
    3.1 Investigación sobre el establecimiento de la comunicación
    3.2 Análisis de costos y factibilidad de la implementación futura.
    3.3 Registro/documentación de los avances
    3.4 Presentación resultados (29/6/2023)

4. Desarrollo
    4.1 Desarrollo de la aplicación (Java, Android)
        4.1.1 Diseño de dashboards e interfaces
        4.1.2 Vinculación con Firebase para registro y autenticación
        4.1.3 Generación de tokens seguros
    4.2 Desarrollo del script del transceptor del CIDI
    4.3 Desarrollo del script del candado electrónico
    4.4 Elaboración de diagramas de conexionado
    4.5 Armado del prototipo
    4.6 Registro/documentación de los avances

5. Puesta a prueba inicial

5.1 Establecimiento de la comunicación
5.2 Registro/documentación de los avances
5.3 Presentación resultados (24/11/2023)

6. Implementación del sistema de cierre y apertura
   6.1 Construcción física del sistema
   6.2 Integración del sistema de cierre y apertura al script del candado.
   6.3 Registro/documentación de los avances

7. Implementación del sistema de alarma
   7.1 Construcción física del sistema de alarma
   7.2 Integración de la alarma al script del candado.
   7.3 Adición de la alarma a la aplicación (notificación)
   7.4 Registro/documentación de los avances
   7.5 Presentación resultados (24/12/2023)

8. Puesta a prueba final
   8.1 Prueba del sistema de cierre y apertura
   8.2 Prueba del sistema de alarma
   8.3 Registro/documentación de los avances

9. Presentación final del proyecto
   9.1 Armado de la presentación en formato PowerPoint
   9.2 Entrega del informe final del proyecto.
   9.3 Disertación final del proyecto. (21/03/2024)

1.3 Gestión de tiempos

Para la realización del proyecto se dividió el tiempo en fases de trabajo (sprints) de 1 semana cada uno. En la tabla a continuación se presenta el tiempo aproximado dedicado a cada tarea en cantidad de horas.

Actividad	Tiempo en Horas
Investigación de las bases del proyecto	**108**
1.1 Investigación de la tecnología a utilizar para la comunicación.	15
1.2 Investigación sobre el armado de una base de datos	15
1.3 Investigación del cifrado/generación de claves aleatorias y seguras	10
1.4 Investigación desarrollo de la aplicación	48
1.5 Investigación sobre LoRa, LoRaWAN	10
1.6 Registro/documentación de los avances.	10
Investigación sobre el armado del prototipo de candado	**55**
2.1 Alimentación, materiales a utilizar (modelos, tamaño, consumo)	20
2.2 Investigación sobre el robo/corte del candado	20
2.3 Compra de los materiales	5
2.4 Registro/documentación de los avances.	10
Análisis de costos y comunicación	**78**
3.1 Investigación sobre el establecimiento de la comunicación	48
3.2 Análisis de costos y factibilidad de la implementación futura.	20
3.3 Registro/documentación de los avances	10
3.4 Presentación resultados (29/6/2023)	-
Desarrollo	**2184**
4.1 Desarrollo de la aplicación (Java, Android)	260
4.1.1 Diseño de dashboards e interfaces	60
4.1.2 Vinculación con Firebase para registro y autenticación	100
4.1.3 Generación de tokens seguros	100
4.2 Desarrollo del script del transceptor del CIDI	400
4.3 Desarrollo del script del candado electrónico	700
4.4 Elaboración de diagramas de conexionado	4
4.5 Armado del prototipo	720
4.6 Registro/documentación de los avances	100
Puesta a prueba inicial	**100**
5.1 Establecimiento de la comunicación	80
5.2 Registro/documentación de los avances	20
5.3 Presentación resultados (24/11/2023)	-
Implementación del sistema de cierre y apertura	**238**
6.1 Construcción física del sistema	168
6.2 Integración del sistema de cierre y apertura al script del candado.	50

6.3 Registro/documentación de los avances	20
Implementación del sistema de alarma	**214**
7.1 Construcción física del sistema de alarma	120
7.2 Integración de la alarma al script del candado	50
7.3 Adición de la alarma a la aplicación (notificación)	24
7.4 Registro/documentación de los avances	20
7.5 Presentación resultados (24/12/2023)	-
Puesta a prueba final	**68**
8.1 Prueba del sistema de cierre y apertura	24
8.2 Prueba del sistema de alarma	24
8.3 Registro/documentación de los avances	20
Presentación final del proyecto	**240**
9.1 Armado de la presentación en formato PowerPoint	72
9.2 Armado del informe final del proyecto.	168
TOTAL	**3285**

Tabla 1. Cuadro con la distribución de tareas y su duración medida en horas

La cantidad de horas son estimadas y es necesario tener en cuenta que varias tareas se pudieron paralelizar. Por otro lado, siendo ambos estudiantes activos de la carrera de Ingeniería en Telecomunicaciones al momento de realizar el proyecto, hubo tiempos “muertos” en los que ambos nos encontramos rindiendo exámenes parciales y finales de otras materias. Además, por cuestiones administrativas de correlatividades, se retrasó también un poco la entrega y desarrollo del proyecto final. Este último punto será tenido en cuenta en el análisis de riesgos hechos a continuación.

1.4 Análisis de riesgos

Para realizar un análisis de riesgos, es necesario establecer ciertos parámetros sobre los cuales basar dicho análisis. Se deben establecer los niveles de severidad, la probabilidad de ocurrencia y además identificar los umbrales por los cuales se tomará la decisión de armar o no un plan de mitigación.

Severidad	S
Insignificante	1
Menor	2
Moderado	3
Mayor	4
Crítico	5

Probabilidad de Ocurrencia	O
Raro	1
Muy baja	2
Baja	3
Media	4
Alta	5

Casos	
RPN <= 10	No hay plan de mitigación
RPN > 10	Hay plan de mitigación
RPN >= 20	Se debe buscar uno o más planes de mitigación y hacer especial seguimiento
RPN* <= 10	Se logra reducir el riesgo
RPN* > 10	No se logra reducir tanto el riesgo, por lo que habrá que prestar especial atención, o recurrir a otros planes de contingencia

A continuación, en base a los criterios establecidos, se presenta una tabla conteniendo todos los riesgos asociados al proyecto, junto con un plan de mitigación en caso que el RPN supere los 10 puntos.

Riesgo	Descripción	S	O	RPN	S*	O*	RPN*
Riesgo 1	Mala planificación e identificación de las tareas necesarias para el cumplimiento en tiempo y forma del proyecto **Plan de mitigación** Dedicarle tiempo y atención al proceso de identificación de tareas y planificación, considerando que ambos estudiantes tenemos otras obligaciones con las cuales cumplir	4	3	12	4	2	8
Riesgo 2	Errores en el análisis de costos **Plan de mitigación** RPN < 10 por lo que no hay plan de mitigación	2	3	6	---	---	---
Riesgo 3	Mala elección de los materiales / software **Plan de mitigación** Investigar acerca de las diferentes opciones de materiales para la construcción del candado y el desarrollo de la aplicación, antes de embarcarse en el armado en sí. Consultar a personas con experiencia de ser necesario.	4	4	16	4	2	8
Riesgo 4	Problemas para adquirir los materiales necesarios para la construcción del candado **Plan de mitigación**	5	4	20	5	2	10

	Al momento de investigar, tratar de tener opciones alternativas para los materiales. Consultar a conocidos si pueden prestarnos materiales propios. Consultar a la facultad						
Riesgo 5	Falta de documentación de los componentes para el candado o del software de la aplicación a utilizar **Plan de mitigación** RPN < 10 por lo que no hay plan de mitigación	4	2	8	---	---	---
Riesgo 6	Demoras a la hora de desarrollar la aplicación por falta de experiencia en actividades similares **Plan de mitigación** Consultar con expertos. De ser necesario tomar algún curso corto de desarrollo de aplicaciones para principiantes	3	5	15	2	3	6
Riesgo 7	Demoras a la hora de construir el candado por falta de experiencia en actividades similares **Plan de mitigación** Consultar con expertos	3	5	15	3	3	9
Riesgo 8	Surgimiento de tareas no previstas **Plan de mitigación** RPN < 10 por lo que no hay plan de mitigación	4	2	8	---	---	---
Riesgo 9	Demoras en la entrega del proyecto final integrador por cuestiones administrativas de la facultad **Plan de mitigación** Hablar con autoridades correspondientes para solucionar los problemas administrativos con antelación	5	4	20	5	3	15

Tabla 2. Riesgos del proyecto en conjunto con su plan de mitigación en caso que correspondiese.

El riesgo 9 el cual habla de demoras en la entrega del proyecto final por problemas administrativos, sigue teniendo un alto RPN. Entiéndase por problemas administrativos cuestiones ajenas a los estudiantes como ser no poder presentar un examen final o realizar la Práctica Profesional Supervisada por alguna exención de correlatividad no dada. Habrá que estar en contacto permanente con las autoridades en caso que surja algún inconveniente del estilo.

1.5 Análisis de costos

A continuación se presenta una tabla con los costos de los materiales.

Materiales	Descripción	Cantidad	Costo unitario (ARS)	Costo Total (ARS)
Protoboard	830 puntos	1	$3.300,00	$3.300,00
Heltec WiFi LoRa 32 V3	Placa de Desarrollo	2	$20.949,00	$41.898,00
Teclado	Membrana matricial 4x4	1	$1.900,00	$1.900,00
Display 1602 I2C	Pantalla LCD 16x2 azul	1	$9.000,00	$9.000,00
Servomotor MG90S	Actuador (cerradura)	1	$6.100,00	$6.100,00
Buzzer	Sonido de alerta (hurto)	1	$3.916,00	$3.916,00
Sensor HC-SR04	Sensor para la detección del corte del pestillo de seguridad	1	$1.533	$1.533
Batería	Alimentación	1	$7.020,00	$7.020,00
Cables jumper	Macho Hembra 10cm	1 paquete (10)	$993,00	$993,00
	Macho Macho 10cm	1 paquete (10)	$993,00	$993,00
	Hembra Hembra 10cm	1 paquete (10)	$993,00	$993,00
Estructura + pestillo	Cuerpo del candado + pestillo de seguridad + estructura del transceptor	1	$15.000,00	$15.000,00
TOTAL			**$71.697,00**	**$92.646,00**

Tabla 3. Materiales a utilizar con su costo en pesos argentinos.

En cuanto al costo total de $92.646 (pesos argentinos), si bien es una suma elevada considerando la coyuntura económica del país, en dólares, el costo calculado para el mes de Abril del 2024 utilizando la cotización del dólar oficial, es de $101 USD (dólares americanos). Este costo se considera razonable, teniendo en cuenta que el dispositivo tiene una vida útil que permite que sea utilizado múltiples veces, por múltiples usuarios.

Se presupone que el costo podría reducirse si se hiciese una producción de candados electrónicos al por mayor para cubrir todo el campus. En este caso, el

costo calculado es para un solo dispositivo. De esta manera, consideramos que la realización de este proyecto a gran escala podría ser rentable para la Universidad.

2. Marco teórico - Tecnologías

En el presente capítulo se estudiarán las tecnologías necesarias para el desarrollo del proyecto. Se introducirán los conceptos básicos sobre el enlace, las posibles soluciones a la hora de implementar un sistema de comunicación inalámbrico como el deseado y los mecanismos y políticas de seguridad a tener en cuenta al implementar el sistema de comunicación.

2.1 Conceptos básicos

Tal como se mencionó en la introducción, el presente trabajo se basa en el estudio, diseño y desarrollo de un sistema de bicicleteros seguros con candados electrónicos para el campus Miguelete de la UNSAM. El objetivo es el de mitigar el riesgo de robo de bicicletas, a la vez de motivar la movilidad sostenible y reducir los tiempos de traslado dentro del predio.

Además, como también se mencionó, el proyecto requiere de la aplicación de tecnologías de las comunicaciones, las cuales fueron seleccionadas mediante un estudio minucioso de todas las posibles técnicas a implementar en la solución. Resulta de gran importancia comprender y aplicar una serie de conceptos clave relacionados con las telecomunicaciones. A continuación, se presenta una breve descripción de estos conceptos fundamentales que serán abordados a lo largo de este proyecto.

Las telecomunicaciones abarcan al conjunto de técnicas, sistemas y dispositivos que permiten la transmisión y recepción de información a través de un medio. En el contexto del presente proyecto, las telecomunicaciones se aplicarán para establecer una comunicación inalámbrica efectiva entre los usuarios y el sistema de bicicleteros, así como entre los diversos componentes del sistema.

El control de acceso se refiere a los métodos utilizados para gestionar quién tiene permiso para utilizar el servicio. En el sistema de bicicleteros, la autenticación de usuarios se realizará mediante códigos token únicos, garantizando que solo la persona autorizada pueda retirar su bicicleta.

Se utilizará una base de datos para almacenar y gestionar la información relacionada con el uso del sistema, incluyendo los datos de los usuarios y los registros de acceso. Esto facilitará la gestión y el seguimiento de las actividades en el sistema de bicicleteros.

Además, se empleará una aplicación móvil que funciona como interfaz de usuario, la misma permite un acceso sencillo y una experiencia amigable para que los usuarios interactúen con el sistema.

Estos conceptos clave proporcionan la base sobre la cual se construirá el proyecto del candado electrónico. A lo largo de este trabajo, se explorará en profundidad cada uno de estos conceptos, aplicándolos de manera específica para cumplir con los objetivos de mejorar de la movilidad y la seguridad en el campus Miguelete de la Universidad Nacional de General San Martín.

2.2 Posibles implementaciones

Para el armado de un sistema de comunicación inalámbrico hay varias tecnologías que se pueden utilizar. Entre las opciones más comunes se pueden mencionar Bluetooth, el estándar 802.11 definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en inglés) , Identificación por Radiofrecuencia (RFID), Comunicación de campo cercano (NFC) y Técnica de Largo Alcance (LoRa). A continuación se hará un breve repaso por cada una de ellas, y se justificará la elección hecha.

Para el armado de un sistema de comunicación inalámbrico hay varias tecnologías que se pueden utilizar. Entre las opciones más comunes se encuentran:

2.2.1 Bluetooth

Bluetooth es una tecnología de radiofrecuencia (RF) que utiliza la banda de frecuencias ISM (Industrial, Científica, Médica) correspondientes al espectro de 2.4 GHz. Esto significa que trabaja bajo el rango de frecuencias que no requieren licencia, y por lo tanto no existen gastos asociados a su uso.

Es utilizada para la conectividad inalámbrica de baja potencia y de corto alcance entre dispositivos tales como teléfonos celulares, equipos de audio, periféricos, máquinas de fax, computadoras, impresoras, etc. y permite la transferencia de datos y/o voz entre ellos.

La distancia de conexión más común suele ser de hasta 10 metros por lo que suele ser utilizado en redes residenciales o en pequeñas oficinas, es decir, en lo que se conoce como Redes de Área Personal Inalámbricas o Wireless Personal Area Network (WPAN), ofreciendo la posibilidad de crear pequeñas redes inalámbricas que permitan la sincronización de datos entre equipos personales.

Es fundamental destacar que como las señales de RF pueden atravesar paredes los dispositivos no necesitan estar “a la vista”, y el aspecto inalámbrico soluciona el problema de puede conllevar la conexión por cable.

La tecnología Bluetooth utiliza la modulación por desplazamiento de frecuencia gaussiana o Gaussian Frequency Shift Keying (GFSK), una de las variantes de la modulación por desplazamiento de frecuencia (FSK). De hecho, pueden utilizarse los mismos moduladores, con un filtro gaussiano pasabajos en la entrada. Este tipo de modulación permite una reducción en el ruido de la señal.

Para que un dispositivo sea compatible con Bluetooth debe contar con un software adecuado para controlar la transferencia de datos, así como con un chip Bluetooth que dispone de una unidad transmisora y otra receptora, y que está integrado en el hardware. También se puede conectar un adaptador Bluetooth en el puerto USB de un dispositivo para así añadir esta función.

En cuanto a la utilidad de Bluetooth para el presente proyecto, podría ser una buena opción para comunicar a los dispositivos móviles de los usuarios con el candado electrónico, aunque no así entre el candado y el dispositivo transceptor. Esto último se debe al corto alcance que tiene la tecnología mencionada.

2.2.2 802.11

El estándar 802.11 es un conjunto de normas creadas por el Instituto de Ingenieros Eléctricos y Electrónicos o Institute of Electrical and Electronics Engineers (IEEE) para la conexión de dispositivos de forma inalámbrica. En el mundo de la informática y las telecomunicaciones, se denomina red inalámbrica a un tipo de conexión que permite conectar distintos nodos sin ningún tipo de cableado o dispositivo alámbrico. La conexión entre sistemas se da mediante la propagación de ondas electromagnéticas en el aire. La transmisión y recepción de éstas, se realiza a través de puertos. A diferencia de lo que se cree comúnmente, WiFi no es un acrónimo, sino el nombre comercial que se le dió a los diferentes estándares 802.11.

El primer protocolo fue el 802.11-1997 el cual especificaba dos velocidades de transmisión teóricas de 1 y 2 Mbits/s, a través de señales de infrarrojo. Luego, a lo largo de los años se fue dando una sucesión de estándares del 802.11, que varían las velocidades de transmisión, como también la banda de frecuencias utilizadas.

Tiene un alcance de menos de 100 metros sin obstáculos o de aproximadamente 50 metros efectivos según la infraestructura del lugar. Además, permite la transmisión de datos a velocidades muy altas y la conexión de múltiples dispositivos simultáneamente.

El uso de WiFi podría ser una buena opción para el candado electrónico ya que permitiría controlar y monitorear al mismo desde una ubicación remota a través de una interfaz de usuario en línea. Pero, además, podría usarse el módulo WiFi como cliente y enviar los datos directamente a la base de datos a través de internet.

Como aspecto negativo, el uso de esta tecnología puede consumir mucha energía y reducir la duración de la batería del candado electrónico rápidamente.

2.2.3 Identificación por Radiofrecuencia

La Identificación por Radiofrecuencia (RFID) es una tecnología que permite la detección e identificación de objetos a distancia. Se basa en el uso de etiquetas electrónicas (tags) que contienen información acerca del elemento que se esté monitoreando. Dichos tags se componen de una antena y un chip. Por otro lado, un sistema basado en RFID cuenta con un dispositivo controlador que puede actuar tanto de lector como escritor, y es quien, mediante el envío de ondas de radiofrecuencia, se comunica con el tag y obtiene información.

Cabe destacar que al utilizar radiofrecuencia, no es necesario que haya línea de vista directa para capturar la información de las etiquetas o tags. Ambos dispositivos, la etiqueta y el dispositivo de lectura/escritura deben estar sintonizados a la misma frecuencia. El lector/escritor envía una señal de RF y éstos responde enviando la información que tienen almacenada.

En el caso de un candado electrónico, se podría utilizar esta tecnología para permitir el acceso solo a personas autorizadas que tengan una etiqueta RFID válida. El candado debería contar con un dispositivo lector.

Como lo que se buscaba era una implementación a nivel general, la tecnología RFID tendría dificultades de implementación en el campus Miguelete ya que necesitaríamos de una gran cantidad de etiquetas, las cuales deberían ser distribuidas y mantener un control sobre la entrega a los usuarios. Además, se correría el riesgo de la clonación ó pérdida de las mismas, lo que podría comprometer la seguridad del sistema.

2.2.4 Comunicación de Campo Cercano

NFC es una tecnología que permite la comunicación entre dispositivos inalámbricos que se ubican a una muy corta distancia el uno del otro (pocos

centímetros). NFC trabaja en la banda de frecuencias altas, específicamente en los 13.56 MHz y es capaz de transferir datos a una velocidad aproximada de 420 kilobits por segundo (kbps).

Los dispositivos se comunican gracias a la generación de un campo electromagnético. De hecho, se pueden mencionar dos modos de funcionamiento en un sistema que utiliza tecnología NFC: activo y pasivo. En el primer modo, los dos dispositivos generan una señal, permitiendo una comunicación bidireccional. En el segundo, por el contrario, un solo dispositivo produce el campo electromagnético, y el otro se “aprovecha” de dicho campo para el intercambio de información. En este caso se tiene una comunicación unidireccional.

Para utilizar esta tecnología de comunicación se requiere de dos dispositivos que incorporen la funcionalidad NFC. Como se mencionó anteriormente, el alcance es de unos pocos centímetros y además, similarmente al RFID se requiere del uso de etiquetas. Si bien podría haberse utilizado para gestionar los candados, consideramos que había mejores tecnologías disponibles.

2.2.5 Largo Alcance (LoRa)

LoRa es una tecnología de comunicación inalámbrica de largo alcance que se puede utilizar para transmitir datos a largas distancias con un consumo de energía muy bajo, permitiendo comunicar dispositivos que se encuentran a una distancia de hasta 20 kilómetros en campo abierto.

Esta tecnología utiliza un protocolo de comunicación de Acceso Múltiple con Detección de Portadora (CSMA) y Modulación de Espectro Ensanchado (Spread Spectrum), lo que le permite tolerar ruido y caminos múltiples de señal (multipath) mientras mantiene muy bajo el consumo de energía.

Con LoRa, se podría establecer una conexión inalámbrica entre el candado electrónico y otro dispositivo LoRa que proporcione acceso a Internet, permitiendo el control remoto del candado y así establecer una comunicación de larga distancia garantizando una larga duración de la batería.

2.3 Tecnologías implementadas

Imagen 3. Esquema básico de comunicación

Luego de estudiar las tecnologías de comunicación disponibles para el armado del sistema de comunicación (Img. 3), finalmente se seleccionaron las tecnologías LoRa en conjunto con el estándar 802.11 para los diferentes estadíos de comunicación dentro del sistema.

Teniendo en cuenta que el proyecto consistió en implementar un sistema que sea apto para cualquier sitio dentro del campus y no en todos ellos existe cobertura WiFi, se llegó a la conclusión de que LoRa era la mejor opción para la comunicación entre el dispositivo candado electrónico y el transceptor.

En particular, la tecnología WiFi fue empleada de manera estratégica para establecer el vínculo entre el sistema desarrollado y la base de datos que alberga información esencial, como usuarios y claves de acceso. A través de este enfoque, se logró crear una solución de conectividad que ofrece una comunicación eficiente y segura, fundamental para el funcionamiento exitoso del sistema de bicicleteros seguros en el campus Miguelete de la UNSAM.

En las secciones siguientes se profundizará acerca de los detalles técnicos de ambas tecnologías proporcionando información y los aspectos fundamentales que respaldaron la elección de las mismas para el sistema de comunicación del proyecto “UNSAM Bicis Seguras”.

2.3.1 LoRa - Comunicación entre extremos

Como se mencionó anteriormente, LoRa es una tecnología de comunicación inalámbrica de largo alcance que se puede utilizar para transmitir datos a largas distancias con un consumo de energía muy bajo.

Fue desarrollada por la empresa Semtech en 2012 y desde entonces ha ganado una gran popularidad en el mercado para aplicaciones de Internet de las Cosas (IoT), donde entre las más comunes se encuentran el monitoreo remoto de sensores, la telemetría, el seguimiento de activos y la automatización de edificios.

Esta tecnología utiliza un protocolo de comunicación CSMA y modulación Spread Spectrum, siendo capaz de resistir interferencias, tolerando ruido y caminos múltiples de señal, lo que mejora la fiabilidad y la calidad de la transmisión de datos. Esto es especialmente útil en aplicaciones de IoT donde los dispositivos pueden estar expuestos a una amplia variedad de condiciones ambientales, donde por ejemplo, los candados electrónicos, al ubicarse en los espacios abiertos del campus, van a estar expuestos a la lluvia. Tanto el protocolo como la modulación son explicadas en próximos apartados.

Utiliza un esquema de modulación de espectro ensanchado para transmitir datos a través de la banda de frecuencia libre de licencia de 915-928 MHz en Argentina. Además, permite el uso de canales múltiples y admite una capacidad de red escalable para conectividad en áreas urbanas, suburbanas y rurales.

Una de las principales ventajas de LoRa es su gran alcance, que puede superar varios kilómetros en áreas rurales y hasta varios cientos de metros en áreas urbanas densamente pobladas; y cómo esta tecnología requiere muy poca energía para transmitir y recibir datos, la hace ideal para dispositivos alimentados por batería que necesitan funcionar durante largos períodos de tiempo sin necesidad de mantenimiento, como es el caso del proyecto presentado.

Cabe destacar la existencia de la técnica de Largo Alcance para Redes de Área Amplia (LoRaWAN®), un protocolo de red de acceso múltiple por división de

tiempo (TDMA) y control de acceso al medio (MAC) basado en la tecnología de modulación inalámbrica LoRa, que permite que dispositivos IoT se comuniquen de forma segura y eficiente con la red. En forma simple, LoRaWAN® hace referencia a una red de nodos basados en tecnología LoRa, que se comunican a través de dichos gateways, y que son gestionados por un servidor.

En ese sentido, LoRaWAN® es un estándar global abierto para comunicaciones inalámbricas, muy utilizado y difundido en industrias con múltiples dispositivos conectados entre ellos y gestionados por un mismo servidor. Permite tener datos analíticos del funcionamiento de dichos dispositivos, a la vez de datos en tiempo real que permiten por ejemplo, localizarlos. De esta manera, el protocolo LoRaWAN® está pensado para redes amplias con dispositivos IoT, donde existe la necesidad de cubrir grandes distancias, tener la capacidad de transmitir incluso en lugares con gran cantidad de obstáculos físicos.

Las redes que LoRaWAN® se despliegan con una arquitectura del tipo estrella-de-estrellas, donde la estación base o gateway transmite mensajes entre los nodos LoRa (dispositivos de IoT generalmente) y el servidor de red. Es decir, los gateways toman las señales de RF, y las convierte en paquetes IP que envía al servidor para que este se encargue de los procesos de gestión de la red.

Por otro lado, si bien a la larga LoRaWAN® promete reducir costos en las industrias que lo aplican, a la vez de fomentar procesos de automatización, la implementación de un sistema de este tipo, no solo es complejo, sino que también es costoso en cuanto al uso del gateway y en cuanto al tiempo de implementación. De esta manera, debido al alcance del proyecto presentado, donde no hay multiplicidad de dispositivos interactuando, la distancia máxima es de 1 kilómetro, no se requiere de toma de datos analíticos en tiempo real y donde además el proyecto fue costeado en su totalidad por los estudiantes, se decidió utilizar directamente la tecnología LoRa en su modo más básico, sin necesidad del armado de una red compleja.

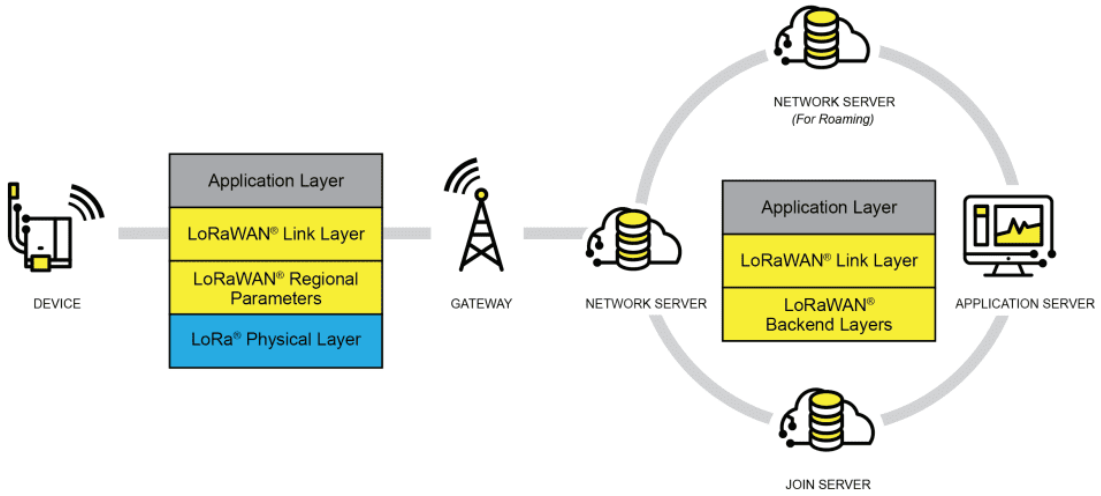

Imagen 4. Arquitectura de una red que utiliza protocolo LoRaWAN®

A continuación, a modo de resumen, se presenta una comparativa de la tecnología LoRa y el protocolo de red LoRaWAN®:

Funcionalidad	LoRa	LoRaWAN®
Tipo de tecnología	Técnica de modulación	Protocolo de comunicación completo
Arquitectura de Red	Punto a Punto (P2P), Punto a Multipunto (P2MP) y malla	Topología estrella de estrellas
Seguridad	Básica	Avanzada
Escalabilidad	Despliegues de redes chicas	Despliegues de redes grandes
Interoperabilidad	No estandarizado. Implementaciones según el proveedor	Estandarizado por LoRa Alliance.

Tabla 4. Diferencias entre LoRa y LoRaWAN®

De esta manera, para la realización del proyecto se optó por establecer una conexión inalámbrica entre el candado electrónico y el transceptor mediante LoRa, donde este último se va a comunicar con la base de datos mediante el módulo incorporado que proporciona acceso a Internet, generando la consulta de token que permite la apertura del candado.

En las secciones siguientes se profundizará acerca de los detalles técnicos de LoRa, siendo los aspectos fundamentales que respaldaron la elección de esta tecnología para establecer la comunicación entre los extremos del proyecto.

Modulación de Espectro Ensanchado

La modulación por espectro ensanchado o Spread Spectrum en inglés, refiere a un sistema de modulación en el cual la señal modulada tiene un ancho de banda mucho mayor al de la señal en banda base. Este tipo de modulaciones vienen acompañadas de ciertos beneficios como mayor resistencia a interferencias y transmisiones multitrayectorias.

Asimismo, las señales de espectro ensanchado no tienen picos definidos en frecuencia, por lo que son señales más achatadas. De esta manera, la señal se vuelve más difícil de interceptar debido a su cercanía en frecuencia al ruido. Es por este motivo que una de las aplicaciones más importantes del Spread Spectrum se da en el ámbito militar.

En particular, la tecnología LoRa se basa en la modulación Chirp Spread Spectrum (CSS), la cual consiste en modular el mensaje por medio de una señal que varía continuamente y de manera lineal en frecuencia. CSS es una técnica ampliamente difundida en sistemas de comunicación inalámbrica de larga distancia. Proporciona una alta resistencia a interferencias, se caracteriza por el bajo consumo de potencia y que fue diseñada para operar en la banda de 2.4GHz.

La tasa de chirp o de símbolo en la tecnología CSS y por ende en LoRa, se controla mediante el Factor de Esparcimiento (SF). A menor SF, se obtiene una velocidad de transmisión más rápida y por ende se incrementa la tasa de transmisión. Por otro lado, el rango en el que se produce la trasmisión, se acorta. Esto se debe a que el factor de esparcimiento en esencia lo que hace es regular el la duración del símbolo en el aire.

El SF además de tener relación con la velocidad de transmisión, se asocia al control de congestión o de colisiones en un canal de comunicación. Asimismo, se relaciona a la duración del símbolo y por ende a su capacidad de atravesar

obstáculos y su inmunidad al ruido. Consecuentemente, el SF influye en la capacidad de detectar una portadora en un canal compartido.

Para el proyecto a desarrollar se debían cumplir ciertos requisitos básicos: el alcance debía incluir a todo el campus Miguelete, se debía tener un bajo consumo de energía y por último, una buena inmunidad a ruido e interferencias ya que el candado estaría ubicado en el exterior. De esta manera, teniendo en cuenta que LoRa se basa en la tecnología Chirp y por ende conlleva todos los beneficios explicados anteriormente, se pudo concluir que es la mejor tecnología para el desarrollo del candado electrónico.

Acceso Múltiple con Detección de Portadora

LoRa es un protocolo ampliamente utilizado para IoT donde muchos dispositivos se comunican a través del mismo medio. El proyecto presentado se trata de una comunicación inalámbrica entre un dispositivo transceptor y varios otros dispositivos distribuidos a lo largo del campus Miguelete, donde el medio de transmisión compartido es el aire. Consecuentemente, contar con un buen protocolo de acceso al medio, resulta algo clave.

CSMA refiere a un protocolo de acceso al medio que permite regular un sistema de comunicaciones donde se producen transmisiones simultáneas de forma descentralizada, sobre un mismo medio. La manera de lograr dicho control de acceso al medio es haciendo que cada nodo, previo a transmitir, verifique la ausencia de tráfico en los canales de comunicación que tiene disponibles en el medio de transmisión.

A alto nivel, el protocolo CSMA se basa en dos aspectos fundamentales, como su nombre lo indica:

- Carrier Sense

Los dispositivos que quieren transmitir verifican que el canal no esté ocupado. En caso de estarlo, esperan un tiempo para luego volver a verificar y poder transmitir

la información. Es decir, los dispositivos escuchan y detectan la presencia de portadoras de otros dispositivos.

- Multiple Access

Muchos dispositivos utilizan un mismo medio de comunicación, por lo que se debe regular de cierta manera el acceso para evitar colisiones o pérdidas de paquetes.

Las colisiones se dan cuando dos dispositivos transmiten información en la misma frecuencia, al mismo tiempo y con el mismo factor de esparcimiento. Channel Activity Detection (CAD) es el proceso mediante el cual un dispositivo verifica la ocupación de un canal. En la tecnología LoRa que implementa CSMA, se pueden distinguir dos fases o periodos de tiempo claves: DIFS (Distributed Inter-Frame Space) y Back-Off. El primero, refiere al tiempo que espera un dispositivo para transmitir información luego que se haya marcado el canal como desocupado. Durante este tiempo el dispositivo realiza CAD para asegurarse que efectivamente no haya actividad en el canal.

El segundo tiempo o fase clave, Back-Off (BO), representa un tiempo aleatorio durante el cual el dispositivo sigue realizando la verificación CAD. Se puede pensar como un doble chequeo de actividad que permite decrementar la posibilidad de colisiones. Suponiendo que varios dispositivos activan su proceso DIFS al mismo tiempo, al finalizar el período de espera, todos transmitirán y se producirán colisiones de paquetes. Al tener el agregado del BO, se evita que este escenario suceda, ya que la segunda espera es aleatoria.

2.3.2 802.11n - Nexo con la base de datos

En el mundo actual, la conectividad a Internet se ha convertido en la columna vertebral de una amplia variedad de aplicaciones y sistemas. La capacidad de acceder y compartir información de manera inalámbrica se ha vuelto esencial para la eficiencia, la comodidad y la seguridad en diversas áreas de la vida cotidiana.

WiFi, abreviatura de "Wireless Fidelity", es una tecnología inalámbrica que ha revolucionado la forma en que nos comunicamos y compartimos datos. Su capacidad para proporcionar conexiones de alta velocidad y confiables en entornos diversos lo convierte en un elemento central en la infraestructura de comunicación moderna.

El estándar 802.11 es un conjunto de normas creadas por el Institute of Electrical and Electronics Engineers (IEEE). El primer protocolo fue el 802.11-1997 el cual especificaba dos velocidades de transmisión teóricas de 1 y 2 Mbits/s, a través de señales de infrarrojo. Luego, a lo largo de los años se fue dando una sucesión de estándares del 802.11, que varían las velocidades de transmisión, como también la banda de frecuencias utilizadas.

Para el caso de aplicación, el módulo WiFi utilizado es apto para los estándares 802.11b, 802.11g o 802.11.n. Teniendo en cuenta que no es el objetivo de este trabajo profundizar sobre conceptos de WiFi en sí, en este apartado únicamente se tratará el estándar 802.11n.

El estándar 802.11n, comercializado como WiFi 4, es una propuesta de modificación al estándar IEEE 802.11-2007 que mejora significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Si bien se basa en estándares previos de 802.11, dos grandes beneficios del WiFi 4 es la incorporación del uso de la tecnología Multiple Input-Multiple Output (MIMO) y unión de interfaces de red (Channel Bonding).

MIMO es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información (cuidando la coherencia) que al utilizar una sola antena. La tecnología MIMO depende de señales multiruta las cuales son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión ha sido recibida. En una red no basada en MIMO, como son las redes 802.11b/g, las señales multiruta

son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multirutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Channel Bonding, también conocido como 40 MHz o unión de interfaces de red, es la segunda tecnología incorporada al estándar 802.11n. La misma, permite utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente. La unión de interfaces de red incrementa la cantidad de datos que pueden ser transmitidos. Se utilizan dos bandas adyacentes de 20 MHz cada una, por eso el nombre de 40 MHz. Esto permite doblar la velocidad de la capa física disponible en un solo canal de 20 MHz.

La especificación para WiFi 4 plantea el uso de la modulación QAM, específicamente 64-QAM. A su vez, las técnicas de acceso empleadas en esos estándares es la de OFDM (Orthogonal Frequency-Division Multiplexing) combinado con la tecnología MIMO.

Modulación QAM

La modulación QAM o Quadrature Amplitude Modulation, es un tipo de modulación digital donde la información está contenida en la amplitud y en la fase de la señal transmitida. Consiste en modular dos señales portadoras de la misma frecuencia en amplitud (ASK), desfasadas entre sí por 90°. La señal modulada de QAM es el resultado de sumar las dos señales moduladas en ASK.

Dependiendo de la cantidad de bits utilizados, la modulación puede ser 8-QAM, 16-QAM, 64-QAM, o genéricamente m-QAM, siendo 2N = m donde N representa la cantidad de bits por símbolo.

Para representar los estados de modulación, se utiliza un diagrama de constelación. Cuanto más separados estén dichos estados, mayor inmunidad al ruido tendrá la señal. Asimismo, al estar alejados se reduce la interferencia intersimbólica (ISI). Cuanto mayor sea la cantidad de bits por símbolo, es decir

una modulación QAM de mayor grado, si bien aumenta la tasa de transmisión de bits, la interferencia e inmunidad al ruido disminuyen (los bits están más dispersos y cercanos entre sí).

Multiplexación por División de Frecuencias Ortogonales

La modulación OFDM (multiplexación por división de frecuencias ortogonales), consiste en enviar información a través de portadoras de distintas frecuencias moduladas en QAM o PSK, por un mismo canal de transmisión. Es decir, divide el flujo de datos permitiendo utilizar en una forma más eficiente el espectro, a través de la implementación de un sistema multiportadora.

La información se divide en varias portadoras, por lo tanto si cualquiera de ellas sufre problemas de interferencia, los datos enviados pueden recuperarse implementando técnicas de corrección de errores. Estas señales portadoras, de bajas tasas de transmisión de datos, se combinan en el receptor, recuperando la alta velocidad de transmisión y la información original. El uso de este tipo de señales portadoras ayuda a minimizar los efectos de distorsión multitrayecto en la transmisión, así como también reduce la interferencia intersimbólica (ISI) y la interferencia de otras señales del mismo espectro de frecuencia, o cercano.

Por otro lado, las señales que llegan contribuyen de manera positiva en el receptor, por lo que existe la posibilidad de crear redes de radiodifusión sin interferencia. Por último ofrece un desempeño excelente frente al problema de multitrayectorias generado por la reflexión, difracción y dispersión de las señales de RF, debido a que los símbolos se encuentran separados en el dominio del tiempo, lo suficiente como para no interferirse entre ellos.

Lo primero que uno puede pensar de este sistema de modulación multi-portadora es que se necesitan tantos transmisores y receptores como portadoras tenga el múltiplex. Sin embargo, las portadoras se pueden modular y demodular todas a la vez, a través de la transformada rápida de Fourier (FFT), algoritmo muy simple de implementar de manera digital. Luego, no solo se soluciona el problema de las

multitrayectorias, sino que también el proceso de modulación y demodulación no se hace complicado como se puede tender a pensar.

Una desventaja de la modulación OFDM para sistemas WiFi es que un único usuario ocupa todas las subportadoras al mismo tiempo. En estándares posteriores de WiFi, se introduce la modulación OFDMA utilizando técnicas como TDMA y/o FDMA (Multiplexación por División de Tiempo o Frecuencia), que permite dividir las subportadoras en múltiples usuarios.

2.4 Seguridad

Como la comunicación podría ser vulnerable a ataques externos, cualquiera sea el tipo de tecnología que se utilice resultó fundamental implementar medidas de seguridad adecuadas como la autenticación de usuarios y la encriptación de datos para proteger la integridad y la privacidad de los datos transmitidos.

Para el presente proyecto se investigaron diversas maneras de obtener claves aleatorias criptográficamente seguras. El objetivo era poder generar un número aleatorio que fuera extremadamente difícil de predecir, incluso para un atacante bien informado y motivado. De esta manera, se lograría que el candado y el mecanismo de claves sean lo suficientemente seguros para hacer el producto atractivo para los usuarios, y que opten por emplear el candado en vez de la típica cadena de bicicletas.

Para la generación del token se utilizó “SecureRandom”, una clase de Java perteneciente al paquete “java.security”. La misma es utilizada para generar números aleatorios criptográficamente seguros.

SecureRandom permite generar diferentes tipos de números aleatorios, como enteros, bytes y secuencias de bytes. También es posible especificar un algoritmo específico para la generación de números aleatorios.

Pero, no sólo existen posibles ataques al enlace, sino que también se tuvo que tener en cuenta que el candado podría ser vulnerado físicamente. Como medida para intentar prevenir el hurto de la bicicleta se tuvo la idea de implementar un

sistema de alarma. El mismo implica la detección de algún intento de manipulación o fuerza bruta en el candado mediante un sensor de distancia. Sumado a esto, se dispara una alarma sonora y se da aviso al usuario mediante una notificación push de la app “UNSAM Bicis Seguras”.

El sistema de alarma está conformado por un buzzer y un sensor ultrasónico HC-SR04 colocado en la zona del candado donde entraría la rueda de bicicleta. La detección de un posible intruso que quiera vulnerar la cerradura se logra a partir de la interrupción del eco enviado por el sensor para medir una distancia preestablecida que cubre la longitud completa del candado. Cuando el pestillo de seguridad se encuentre cerrado, si el sensor midiese una distancia menor a la preestablecida, entonces se activará la alarma sonora, suponiendo que hay un intento de quitar la bicicleta.

El buzzer, estará conectado a un pin de salida digital de la placa de desarrollo Heltec WiFi 32 LoRa V3, y a este último se lo programará de manera tal que cuando detecte una intrusión en la distancia medida, dispare la alarma sonora y la notificación en la aplicación móvil del respectivo usuario.

Para lograr esto último, cuando se detecta una situación de alarma, como un intento de robo o una apertura no autorizada, el candado enviará una alerta a través de LoRa al transceptor, el cual, a través de una conexión WiFi, actualiza la base de datos en tiempo real de Firebase con la información sobre la alarma.

Luego, Firebase enviará la notificación en tiempo real a la aplicación móvil del usuario correspondiente, permitiéndole tomar medidas inmediatas en respuesta a la alarma del candado.

Es importante tener en cuenta que, aunque una alarma sonora puede ser un elemento disuasivo para los ladrones, no garantiza que la cerradura no pueda ser manipulada. Por lo tanto, es fundamental utilizar materiales resistentes para la construcción del candado, intentando que el sistema sea lo más robusto posible.

3. Proyecto

En el presente capítulo se especifican las bases del proyecto.

Como se estuvo mencionando en capítulos anteriores, el proyecto presentado consistió en el armado de un bicicletero seguro para el campus Miguelete de la UNSAM. El mismo consta de 5 componentes principales que conforman al sistema de comunicación entre el punto A (Transmisor LoRa ubicado en el candado) y el punto B (receptor LoRa ubicado en el tornavías, específicamente en el Centro de Investigación y Desarrollo en Informática)

- Candado electrónico
- Transceptor con módulo 802.11n que actúe como nexo con Firebase
- Base de datos (Firebase)
- Aplicación móvil.
- Lugar físico para colocar el candado (bicicletero)

En las próximas secciones de este apartado, se explicarán los procedimientos realizados para el ensamble de los cinco puntos mencionados, que hicieron al funcionamiento del prototipo de Bicicletero Seguro.

3.1 Establecimiento de la comunicación

La comunicación entre los sitios es bidireccional, esto quiere decir que se logró que los dispositivos ubicados en el candado y en el CIDI, actúen tanto de transmisores como receptores en el sistema de comunicación LoRa.

Para dar un poco de contexto al esquema presentado en el apartado referente a las tecnologías de comunicación implementadas (Img. 3), a continuación se dará una breve explicación. En las próximas subsecciones se dará más detalle.

Dado que Firebase es una base de datos alojada en la nube, la opción de conexión directa a la base de datos no era posible, por lo que se necesitó un microcontrolador que posea un módulo WiFi y que actuase como “intermediario”.

Este microcontrolador forma parte de la placa o dispositivo que se ubicó en el CIDI. Para poder acceder a la Base de Datos e interactuar con la misma para el alta de usuarios y asignación de Tokens, se utilizó una biblioteca específica, “FirebaseESP32.h”.

En cuanto a la comunicación, la biblioteca “LoRaWan_APP.h” nos permitió recibir y envíar la información necesaria para el bloqueo y desbloqueo del candado (Tx-Rx y validación de tokens). Además, se utilizó una biblioteca particular de los módulos adquiridos, “heltec.h”, junto a otras bibliotecas que permitieron establecer por ejemplo la conexión al teclado matricial y al LCD.

Finalmente, como la aplicación fue diseñada para intercambiar información directamente con Firebase (autenticando a los usuarios y generando una colección en Realtime Database con el valor del token seguro y aleatorio), el candado electrónico es capaz de leer el valor generado por la aplicación móvil y compararlo con el ingresado mediante teclado, produciéndose la apertura del sistema si ambos coinciden.

3.1.1 Candado electrónico

En esta sección se detalla la construcción del candado electrónico desarrollado para nuestro proyecto. Este dispositivo se concibió con el propósito de brindar una solución segura y efectiva para el resguardo de las bicicletas en el Campus Miguelete de la Universidad Nacional de San Martín.

El candado realizado es un sistema que consta de dos bloques fundamentales: la parte electrónica y la parte mecánica. El bloque electrónico cuenta con los componentes listados a continuación.

- Kit de desarrollo “HTIT-WB32LA_V3”

También llamado “WiFi LoRa 32 V3”, es una placa de desarrollo IoT diseñada y producida por Heltec Automation.

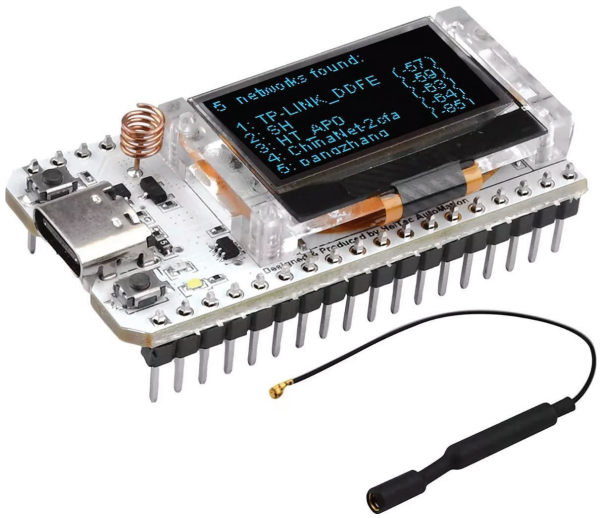

Imagen 5. Kit de desarrollo empleado.

Compuesto por el microprocesador ESP32-S3FN8 (procesador Xtensa® 32-bit LX7 de doble núcleo, estructura de rack de tuberías de cinco etapas, frecuencia de hasta 240 MHz) y el chip LoRa SX1262, lo vuelven la pieza fundamental para el desarrollo del proyecto.

El ESP 32 es un microcontrolador que tiene capacidad suficiente para realizar el proceso de entrada de código, comunicarse con el módulo LoRa y controlar el actuador que abre o cierra la cerradura.

El chip LoRa SX1262 implementa la comunicación de radiofrecuencia utilizando la modulación LoRa. De esta manera, permite transmitir y recibir datos de manera inalámbrica a largas distancias con un consumo de energía reducido. Puede operar en diferentes frecuencias de radio, en un rango que va desde 863 MHz hasta 928 MHz, lo que permite adaptarse a los requisitos específicos del sistema. En nuestro caso, hemos seleccionado la frecuencia de 915 MHz, que pertenece a la banda de Frecuencias Industriales, Científicas y Médicas (ISM) en Argentina. La banda ISM es una porción de espectro de radio que se designa como libre de licencia y está reservada para dispositivos y aplicaciones de uso no regulado, como las comunicaciones LoRa, lo que la hace ideal para nuestro propósito.

Para ello, según datasheet, la potencia máxima de transmisión es de (21 ± 1) dBm, y la sensibilidad máxima a la hora de la recepción está dada por la siguiente tabla:

Signal Bandwidth/[KHz]	Spreading Factor	Sensitivity/[dBm]
125	SF12	-134
125	SF10	-130
125	SF7	-122

Tabla 5. Sensibilidad de recepción. Fuente: Hoja de datos del microcontrolador (Ver Bibliografía)

El kit HTIT-WB32LA_V3 posee una interfaz USB tipo C con regulador de tensión completo, protección contra descargas electrostáticas (ESD), protección contra cortocircuitos y blindaje RF. Además, cuenta con una interfaz de batería SH1.25-2 integrada, sistema de gestión de batería de litio integrado (gestión de carga y descarga, protección contra sobrecarga, detección de energía de la batería, conmutación automática entre USB/batería).

Cuenta con una pantalla OLED con backlight azul de matriz de 128x64 puntos de 0.96 pulgadas integrada que permite mostrar información de depuración, nivel de batería y demás datos. Además, posee el chip CP2102 USB a puerto serie integrado, que puede ser de utilidad para descargar programas e imprimir información de depuración.

En cuanto a las conexiones de red integradas, la antena de resorte metálico permite la utilización de WiFi, Bluetooth y LoRa, según necesidades del usuario.

Además, el kit incluye dos tiras de pines y un cable con ficha JST, piezas que permiten conectarlo a una protoboard y alimentarlo con una batería de litio.

Todo lo mencionado, sumado a sus pequeñas dimensiones (50.2mm x 25.5mm x 10.2mm) y peso (0.0247 kg), la vuelven una placa de desarrollo con buen diseño de circuito RF y bajo consumo de energía, fundamental para el candado.

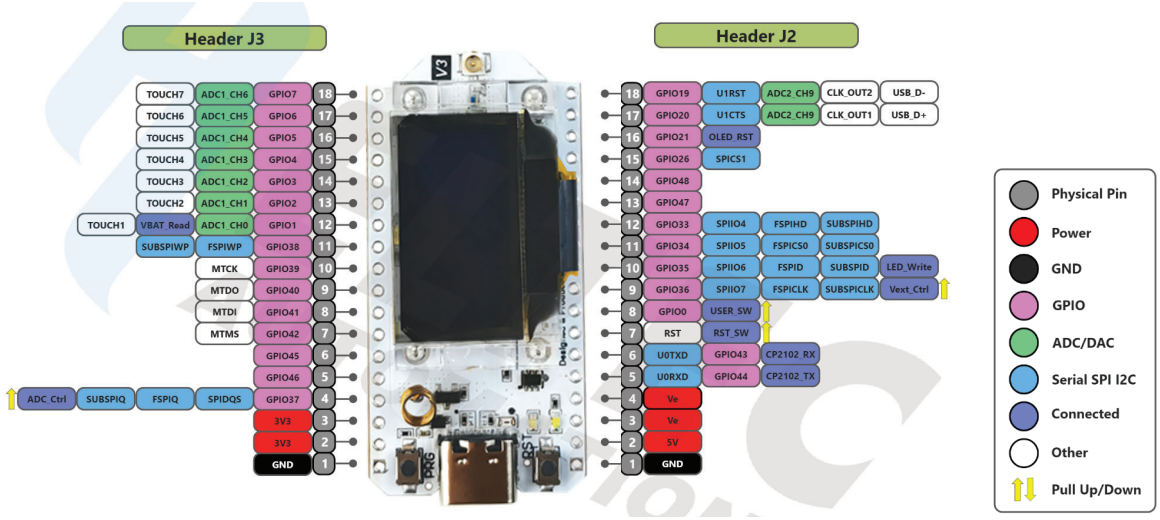

Imagen 6. Pin Map del kit de desarrollo

- Protoboard de 830 puntos

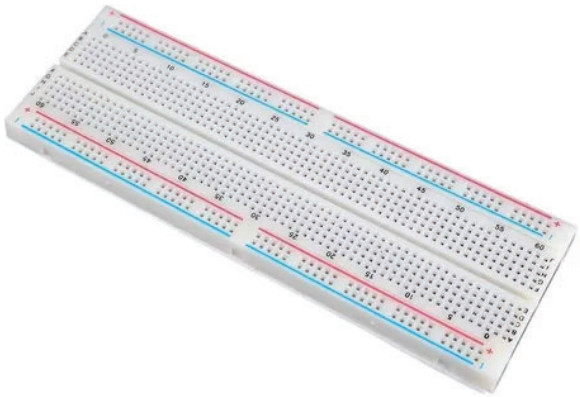

Imagen 7. Protoboard genérica 830 puntos.

La protoboard fue utilizada para el armado del prototipo funcional supliendo la necesidad de una placa PCB. Cuenta con 4 líneas de energía, 63 columnas y 10 filas para un total de 830 puntos de inserción que nos alcanzan para el montaje de los demás componentes del candado. Su vida útil es de más de 10.000 inserciones, y sus dimensiones son: 165mm x 55mm x 8mm.

- Teclado de membrana matricial 4x4

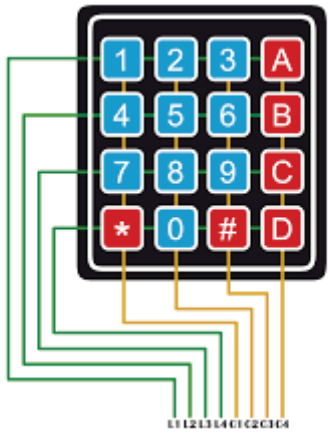

Imagen 8. Teclado Matricial 4x4

Es un dispositivo de entrada que consta de cuatro filas y cuatro columnas de botones, cantidad suficiente para ingresar los 10 dígitos (0,1,2,3,4,5,6,7,8,9) posibles para el desbloqueo del candado. Ofrece resistencia al agua y al polvo, lo cual es positivo ya que los candados se ubicarán en el exterior. Sus dimensiones son 70 mm x 80 mm y presenta una expectativa de vida de 1.000.000 de operaciones

- Display LCD 16x2 azul 1602 I^2C

Imagen 9. Display LCD 16x2

Es una pantalla de cristal líquido que puede mostrar 16 caracteres en cada una de sus 2 líneas, lo que es suficiente para mostrar los caracteres necesarios para el código de desbloqueo. Sus dimensiones son 80 mm x 36 mm x 12 mm, y su alimentación es de 5V.

- Batería (Alimentación)

Dado que el candado no irá enchufado a la corriente eléctrica porque parte de los requerimientos del proyecto es que el mismo puede ser utilizado en cualquier punto del campus.

Para un primer acercamiento y elaboración del prototipo se utilizó una batería de litio recargable que sea compatible con el kit de desarrollo y que tenga suficiente capacidad para alimentar todo el circuito que compone al candado.

- Sistema de alarma - Sensor HC-SR04

Implica la detección y emisión de una alarma sonora ante un intento de manipulación o fuerza bruta en el candado. Al dispararse la alarma sonora, se da aviso al usuario mediante una notificación push de la app “UNSAM Bicis Seguras”.

El sistema de alarma está conformado por un buzzer y un sensor ultrasónico HC-SR04 que mide distancias. El mismo emite pulsos ultrasónicos y mide el tiempo que tarda en recibir el eco de esos pulsos. Luego, utiliza la información para calcular la distancia al objeto más cercano. Se utilizará para establecer umbrales de distancia en los que debe o no sonar la alarma y enviar la notificación de alerta de robo al usuario.

Imagen 10. Sensor ultrasónico HC-SR04

- Componentes complementarios

Además de todo lo mencionado, para construir el circuito y conectar los componentes entre sí se emplearon cables jumper del tipo Macho-Hembra, Macho-Macho y Hembra-Hembra.

En cuanto al bloque mecánico, se pueden mencionar dos partes fundamentales:

- Estructura + Pestillo

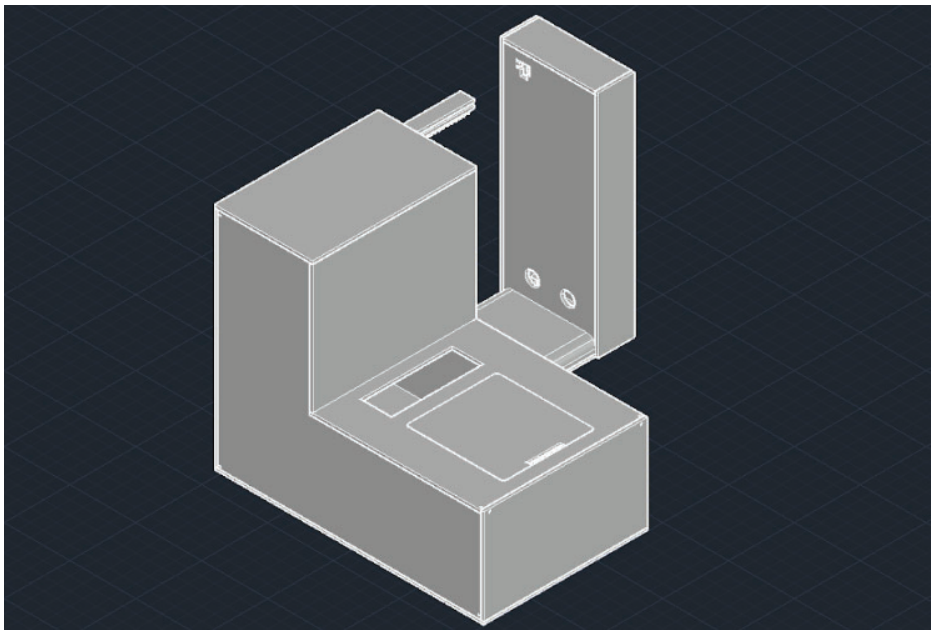

Imagen 11. Estructura del candado modelada en AutoCad.

El cuerpo del candado, es decir, la estructura que contenga a todos los materiales mencionados, se realizó de impresión 3D utilizando el filamento de ácido poliláctico (PLA). El diseño se realizó en AutoCad y a partir del mismo se confeccionó el archivo para pasar a la impresora. Tanto el cuerpo del candado como el pestillo fueron impresos en 3D.

En caso de que el proyecto sea implementado a lo largo del campus, para la transformación del prototipo al producto final es necesario reemplazar la estructura por algún material metálico que pueda resistir a la intemperie y afrontar condiciones climáticas desfavorables. De la misma manera, se debería diseñar un sistema de aislamiento para los componentes electrónicos y considerar la implementación de energía solar para alimentar los candados.

- Servomotor

Para poder generar el movimiento del pestillo, se decidió utilizar un servomotor modelo MG90S. Éste cuenta con un torque de 1.8Kg y funciona con una tensión

de 5V, lo que lo volvió una elección muy acertada para la necesidad. El pestillo, como se mencionó anteriormente, fue impreso en PLA, por lo que no se requiere de un motor de gran torque para moverlo.

A continuación, se presenta el esquemático del conexionado de los componentes a los pines de la placa de desarrollo Heltec.

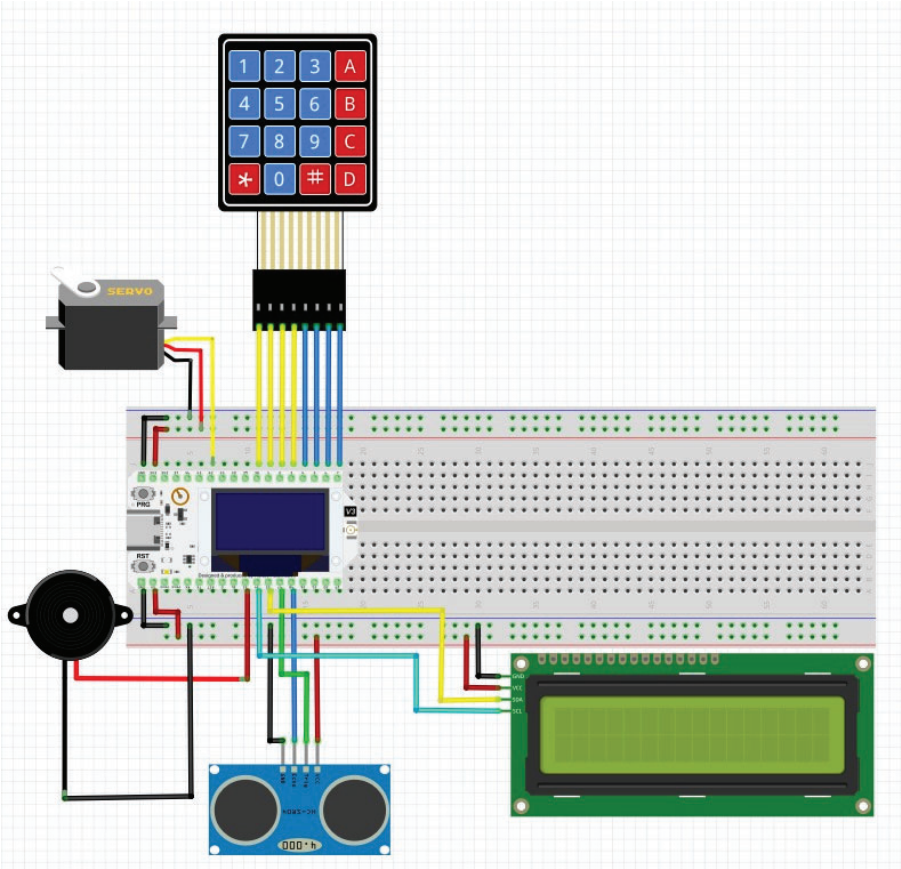

Imagen 12. Esquema del prototipo de candado.

Para el prototipo, las decisiones de diseño fueron fundamentales para lograr un equilibrio entre costo y utilidad. Algunas de las decisiones clave incluyen:

- Elección de materiales

Se eligieron componentes económicos y de fácil accesibilidad en el mercado. Los componentes utilizados son componentes básicos de la electrónica, sencillos de utilizar. No se requirió de soldaduras complejas, ni tampoco una programación a muy bajo nivel.

- Gestión de la energía

Se buscó prolongar la vida útil de la batería del candado electrónico, para ello se empleó la tecnología LoRa, la cual implica un bajo consumo.

- Regulaciones y frecuencias permitidas

En Argentina, la banda de frecuencia ISM (Industrial, Scientific, and Medical), reservada para dispositivos de uso no regulado comprende las frecuencias que van desde los 915 MHz hasta los 928 MHz. Los kits de desarrollo utilizados en el proyecto están equipados con el chip LoRa SX1262, el cual permite la operación en esta banda específica.

Según lo establecido por ENACOM (Ente Nacional de Comunicaciones), la entidad encargada de regular y supervisar las telecomunicaciones, incluida la gestión del espectro de radiofrecuencia en Argentina, no se requiere una licencia de radiofrecuencia para la utilización de dispositivos en esta banda de frecuencia.

La elección de operar dentro de la banda ISM garantiza que el candado electrónico cumpla con las regulaciones locales y funcione dentro de un rango de frecuencia permitido sin la necesidad de requerir licencias adicionales. Esto simplifica la implementación del sistema y evita posibles obstáculos legales, asegurando que el candado pueda ser utilizado de manera legal y efectiva en el entorno argentino.

El diseño del candado electrónico se centra en ofrecer seguridad y facilidad de uso. La combinación de una cerradura resistente y la parte electrónica garantizará la protección de las bicicletas y un acercamiento al mundo IoT.

3.1.2 Transceptor

En esta sección se brinda información sobre el transceptor que se ubicó en el Tornavías, específicamente en el CIDI (Centro de Investigación y Desarrollo en Informática) del Campus Miguelete de la Universidad Nacional de San Martín.

Este dispositivo se concibió con el propósito de brindar una comunicación LoRa con el candado electrónico, realizando el intercambio de claves token y su validación mediante la conexión con la base de datos. El sistema incluye los componentes detallados a continuación.

- Kit de desarrollo “HTIT-WB32LA_V3”

Se trata de la misma placa utilizada para la construcción del candado (ver apartado 4.1.1.), estableciendo mediante LoRa la comunicación de RF con el mismo. Además, gracias a su conectividad WiFi, este kit de desarrollo nos permitió realizar las validaciones y consultas correspondientes con la base de datos.

- Cable USB tipo C

Como el transceptor se encuentra ubicado en un entorno controlado y de baja exposición, la alimentación del mismo se realiza vía USB tipo C, evitando cualquier tipo de problema de consumo.

3.2 Tablas de materiales

Candado electrónico		
Materiales	**Descripción**	**Cantidad**
Protoboard	830 puntos	1
Heltec WiFi LoRa 32 V3	Placa de Desarrollo HTIT-WB32LA_V3 (ESP32+SX1262)	1
Teclado	Membrana matricial 4x4	1
Display 1602 I2C	Pantalla LCD 16x2 azul	1
Batería	Alimentación del candado electrónico	1
Servomotor MG90S	Actuador para mover el pestillo de seguridad	1
Sensor HC-SR04	Sensor utilizado para el sistema de alarma	1
Buzzer	Sonido de alerta (hurto)	1
Estructura + Pestillo	Estructura y pestillo de seguridad hechos en 3D	1
Cables jumper	Cables para conectar los elementos entre sí y a la protoboard (M-M, H-M, H-H)	30

Tabla 6. Materiales para la construcción del prototipo de candado electrónico.

Transceptor ubicado en el CIDI		
Materiales	**Descripción**	**Cantidad**
Heltec WiFi 32 LoRa V3	Placa de Desarrollo HTIT-WB32LA_V3 (ESP32+SX1262)	1
Alimentación	Cable USB tipo C	1
Estructura	Impresión 3D	1

Tabla 7. Materiales para la construcción del transceptor ubicado en el CIDI.

3.3 Construcción del Prototipo

Tanto para el candado electrónico como el dispositivo transceptor, se necesitó fabricar una estructura que dentro contenga los componentes electrónicos que hacen al funcionamiento del sistema. Para ello, se tomó la decisión de realizar dichas estructuras en termoplástico de ácido poliláctico (PLA), es decir impresión 3D. Esta decisión se tomó considerando que el sistema es un prototipo y que además el haber hecho una estructura metálica hubiese elevado los costos.

Se pidieron presupuestos a diferentes fabricantes de estructuras de PLA, los cuales eran muy variables y no había un rango fijo de precio. Sumado a esto, conseguimos acceso a una impresora 3D prestada. De esta manera, se tomó la decisión de adquirir un rollo de filamento PLA y hacer la impresión nosotros mismos, con ayuda del tutor.

En línea de tiempo, en primer lugar se diseñó la estructura del candado electrónico en el programa de diseño AutoCad. A partir del diseño generado, se construyó el archivo necesario para la impresión 3D (archivos de extensión .stl).

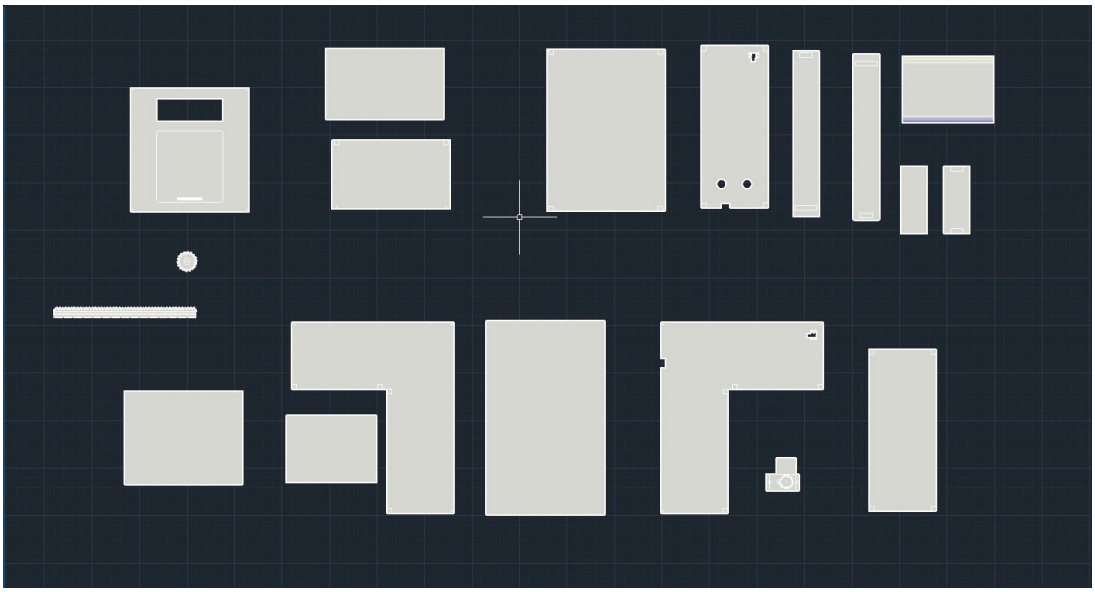

Imagen 13. Partes de la estructura del candado electrónico.

Por otro lado, en cuanto a la construcción del circuito del candado electrónico, como se mencionó anteriormente, el mismo fue realizado utilizando una protoboard como base para las conexiones. De esta manera, no fue necesario realizar ningún proceso complejo, más que configurar los pines de la placa de desarrollo para que funcionen adecuadamente con los dispositivos conectados (teclado, pantalla, servomotor, sistema de alarma)

Respecto a la estructura del dispositivo transceptor, se encontró una plantilla gratuita[1] en línea la cual se adaptó perfectamente a lo buscado.

Finalmente se obtuvieron ambos prototipos, tanto para el candado electrónico como para el dispositivo transceptor. Cómo se puede observar en la imagen a continuación (Img. 14), todo el circuito y conexionado se encuentra por dentro de la estructura azul de PLA. El usuario únicamente puede interactuar con el teclado, y observar el código ingresado en el LCD. Además, puede observar el movimiento del pestillo para ubicar su bicicleta correctamente.

[1] Se puede encontrar la plantilla en el Anexo

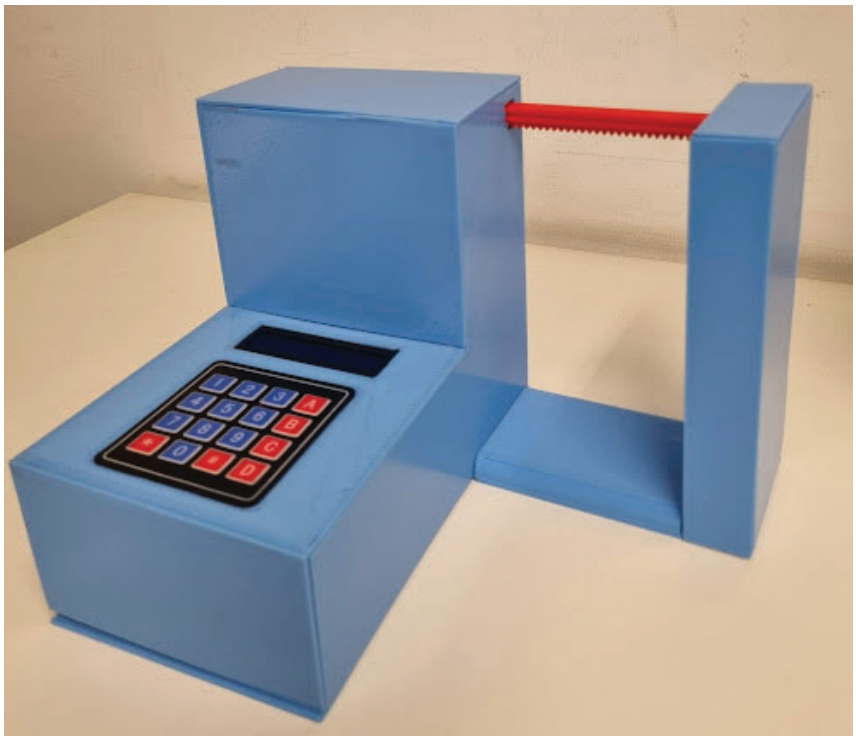

Imagen 14. Prototipo final del candado electrónico

El dispositivo transceptor se encuentra dentro de su pequeña estructura y se puede observar que lo único que sobresale es la antena que permite establecer la comunicación LoRa.

Imagen 15. Prototipo final dispositivo transceptor.

3.4 Programación

Para el desarrollo del proyecto se estableció un sistema de comunicación LoRa entre los dos módulos Heltec LoRa 32 V3, uno de ellos el que llamamos “Candado electrónico” y el otro es el “Transceptor”.

Para comenzar a utilizar los kits de desarrollo fue necesario configurar un entorno de desarrollo integrado (IDE) que permitiera escribir y cargar el código en los microcontroladores. Si bien existen varios IDE disponibles para el ESP32, incluyendo Arduino IDE, PlatformIO, y Espressif IDF, se empleó el primero de los mencionados.

Para programar los kits, se estableció una conexión en serie con la PC, instalando el driver correspondiente y verificando al puerto COM al que se encontraba conectado.

La documentación del HTIT-WB32LA_V3 brinda un conjunto de herramientas y configuraciones que permiten programar el kit de desarrollo. De manera que se

instaló el “Heltec ESP32 & ESP8266 Series Arduino Develop Environment”, un entorno de desarrollo de Heltec basado en Arduino, para interactuar con las características y periféricos del kit, facilitando la programación y el desarrollo del proyecto. El mismo contiene una serie de bibliotecas, funciones y abstracciones que brindan el acceso a las características particulares del kit (desde controladores para la pantalla OLED, funciones para la gestión de la conectividad WiFi, acceso a sensores integrados, y más.)

A grandes rasgos, el sistema completo del proyecto se puede dividir en 4 pasos secuenciales:

1. **Generación del token**: Cuando un usuario de la aplicación móvil genera un token para desbloquear el candado, el mismo se almacena en Realtime Database junto con la información del usuario.

2. **Lectura y envío del token**: El transceptor se conecta vía WiFi con Firebase y lee el token correspondiente. Luego, lo envía por LoRa hacia el dispositivo receptor, en este caso, el candado.

3. **Comparación del token**: El candado compara el token recibido por LoRa con el ingresado por teclado. Si coinciden, se abre el mecanismo para guardar la bicicleta.

4. **Retiro de la bicicleta:** Cuando el usuario desbloquea el candado se detiene la generación de tokens. Cuando quiera dejar de utilizarlo, basta con que ingrese el token que se observa en la pantalla de la aplicación para retirar su bicicleta.

Además de elegir la frecuencia correspondiente para el intercambio de tokens (915 MHz) entre ambos kits fue fundamental definir ciertos aspectos del sistema de radio. Los parámetros a continuación son compartidos por las funciones de Recepción y Transmisión en LoRa.

Nombre	Descripción
modem	Este parámetro indica el modo de modulación que se utilizará. En este caso, se utiliza el modo de modulación LoRa
bandwidth	En general, los anchos de banda comunes en aplicaciones LoRa suelen ser 125 kHz, 250 kHz y 500 kHz. Para el sistema postulado, como no se necesita transmitir grandes datos, se empleó un ancho de banda de 125 kHz, ya que proporciona una mayor distancia de transmisión, mayor inmunidad al ruido y menor consumo energético, a expensas de una menor velocidad de datos.
spreadingFactor	El Spreading Factor (factor de expansión) determina cómo se extiende la señal en el tiempo. Se representa generalmente como un número entero, y un valor más alto significa una mayor expansión de la señal. Es decir, cada símbolo se envía a una velocidad más lenta y ocupa un período de tiempo más largo. Esto hace que la señal sea más resistente al ruido y a las interferencias, lo que permite una mayor distancia de transmisión, pero a costa de una velocidad de transferencia de datos más baja.
codingRate	Este parámetro define la tasa de codificación utilizada en la comunicación LoRa, es decir, la relación entre la cantidad de bits de datos transmitidos y la cantidad de bits en el flujo de datos total, incluyendo bits de redundancia o corrección de errores. Típicamente se expresa como una fracción que indica cuántos bits de redundancia se agregan a los datos para garantizar una comunicación más confiable. En LoRa, las tasas de codificación suelen ser 4/5, 4/6, 4/7 ó 4/8, donde el primer número (4, en este caso) se refiere a la cantidad de bits de datos transmitidos, y el segundo número (5, 6, 7 u 8) representa la cantidad total de bits en la transmisión, incluyendo bits de redundancia. Una tasa de codificación más alta proporciona una mayor resistencia al ruido, a costa de una menor velocidad de datos, ya que una mayor cantidad de bits debe ser transmitida para representar la misma cantidad de información. Con esto en mente, para el proyecto se seleccionó la tasa más alta posible.
preambleLength	Este parámetro define la longitud del preámbulo en la comunicación LoRa. El preámbulo es una secuencia de bits utilizada para sincronizar los receptores antes de recibir los datos. Algunos valores típicos de longitud de preámbulo son: 8, 12, 16, 20 o 24 símbolos. Un valor más alto del preámbulo puede aumentar la robustez de la comunicación, pero también puede afectar la eficiencia y la velocidad de transferencia. Se eligieron 8 símbolos.
fixLength	Este parámetro indica si se debe usar una longitud fija para los paquetes de datos. Se setea en True o False dependiendo de la aplicación. En este caso como se envían y reciben paquetes de diferentes tipos de datos, se decidió configurar el parámetro en false para la Recepción y Transmisión.
iqInversionOn	Este parámetro controla la inversión de la señal en cuadratura (IQ) durante la modulación y demodulación. En los sistemas de comunicación digital, la modulación de amplitud en cuadratura (QAM) y otras formas de modulación suelen implicar el uso de dos componentes de señal, conocidos como I (in-phase) y Q (cuadratura). La inversión de IQ invierte la fase de una de estas

	señales. Algunos módulos LoRa pueden requerir inversión de IQ para funcionar correctamente debido a la configuración de hardware específica. Por otro lado, dependiendo de la configuración específica del sistema y del entorno de comunicación, la inversión de IQ puede afectar el rendimiento de la comunicación. Se eligió dejarlo en false.
crcOn	Indica si se utiliza CRC (Cyclic Redundancy Check) para la detección de errores. Se puede establecer en false o true sólo si fixLenght está deshabilitado. Se estableció en true. On
freqHopOn	Controla si se utiliza salto de frecuencia. Este parámetro no aplica (N/A), por lo que se establece en 0.
hopPeriod	Define el período de salto de frecuencia. Este parámetro no aplica (N/A), por lo que se establece en 0.

Tabla 8. Parámetros compartidos para la transmisión y recepción por LoRa

Los parámetros exclusivos de la función de recepción, que se suman a los mencionados anteriormente, se listan a continuación.

Nombre	Descripción
bandwidthAfc	Este parámetro se utiliza para controlar el ancho de banda en el circuito de control automático de frecuencia (AFC, por sus siglas en inglés: Automatic Frequency Control) en algunos dispositivos LoRa. El AFC es una función que ajusta automáticamente la frecuencia del receptor para mantenerse sincronizado con la frecuencia del transmisor, lo que ayuda a compensar las desviaciones de frecuencia. De acuerdo a la documentación, el parámetro No Aplica (N/A), por lo que se deja configurado en 0. La función debe recibir el parámetro por compatibilidad.
symbTimeout	Este parámetro define la cantidad máxima de símbolos que el receptor espera recibir antes de considerar que la recepción del paquete ha finalizado. Cuando el dispositivo LoRa está configurado en modo de recepción continua, el tiempo de espera se basa en el número de símbolos en lugar de en un tiempo específico. Para ello, se establece en 0 el parámetro.
payloadLen	Este parámetro especifica la longitud de la carga útil en bytes cuando el paquete LoRa no tiene una longitud de carga útil fija predefinida. En otras palabras, si fixLength está desactivado, el receptor debe conocer la longitud de la carga útil del paquete para poder interpretar correctamente los datos recibidos. Los valores van de 0 a 255
rxContinuous	Indica si la recepción es continua o única (solo un paquete). Este paŕametro se estableció en true para indicar que la recepción es contínua.

Tabla 9. Parámetros para la recepción por LoRa

Los parámetros exclusivos de la función de transmisión, que se suman a los mencionados anteriormente, se listan a continuación.

Nombre	Descripción
power	Este parámetro indica la potencia de transmisión utilizada para enviar la señal LoRa. La potencia de transmisión se mide en dBm y representa la potencia de salida del transmisor en la antena. Es crucial en la comunicación inalámbrica, ya que afecta la distancia de transmisión y la robustez de la señal. Un valor más alto de potencia de transmisión puede permitir una mayor distancia de comunicación y una mejor penetración a través de obstáculos, pero también puede consumir más energía. Se configuró en 14, pero podría reajustarse de ser necesario.
fdev	Este parámetro especifica la desviación de frecuencia utilizada en la modulación LoRa. La desviación de frecuencia es la magnitud máxima en la cual la frecuencia de la portadora puede variar respecto a su frecuencia central. De acuerdo a la documentación, este parámetro se tiene que configurar en 0.
timeout	Este parámetro especifica el tiempo de espera máximo para la transmisión antes de que se cancele.

Tabla 10. Parámetros para la transmisión por LoRa

3.4.1 Transceptor

A nivel código del dispositivo transceptor se definieron 12 funciones:

- setup

La función setup() es una función especial que se ejecuta una vez al inicio del programa. Es utilizada para realizar la inicialización y la configuración de hardware y software antes de que el bucle principal (loop()) comience a ejecutarse. Junto a las declaraciones iniciales se encarga de inicializar el módulo LoRa y llamar a “WIFI_Firebase_Setup” para realizar la conexión con RealTimeDatabase, permitiendo acceder al proyecto de Firebase para que luego se pueda operar en él utilizando las credenciales de administrador.

- loop

La función loop() es otra función especial que se ejecuta de forma continua después de que la función setup() haya terminado. Contiene la lógica principal del programa y se ejecuta repetidamente mientras el sistema está alimentado. Dentro

del código, se utiliza para verificar si hubo cambios en el campo ‘token’ de la base de datos de Firebase, de ser así, se envía el valor por LoRa.

- WIFI_Firebase_Setup

Como se mencionó, el módulo transmisor debe conectarse con Firebase para obtener el token generado por la aplicación. Para poder conectarse a Firebase se necesita una conexión a Internet. Para el armado de la función se utilizó la biblioteca “WiFi.h”

- OnTxDone

Es un callback que se ejecuta cuando se ha completado la transmisión LoRa con éxito. Luego, pone el módulo en modo de recepción. Los paquetes transmitidos son los tokens que se obtienen de la base de datos.

- OnRxDone

Se ejecuta cuando se ha completado la recepción LoRa. Almacena el paquete recibido en el buffer, entre las opciones de paquetes que pueden recibirse están: la señal para bloquear el candado, la señal para activar la alarma o el token de desbloqueo.

- isBloqueo

Verifica si el paquete recibido es el string ‘block’, es decir, se introdujo correctamente el token en el candado.

- mandarBloqueo

Si se recibió el bloqueo, se actualiza la base de datos de Firebase marcando el flag ‘tokenvalidado’ como ‘true’. Es decir, bloquea y detiene el envío de tokens.

- isAlert

Verifica si el paquete recibido es el string ‘Alerta’, es decir, hubo un intento de hurto en el candado electrónico.

- mandarAlerta

Si se recibió la alerta, se actualiza la base de datos de Firebase marcando el flag ‘alarma’ como ‘true’. La aplicación, al leer este cambio, hace que se dispare la notificación push al usuario del candado para informarle que el candado fue vulnerado y que su bicicleta corre peligro.

- liberarBicicleta

Verifica si el paquete recibido es el string ‘Liberada’, es decir, se introdujo correctamente el token de desbloqueo en el candado. La lógica detrás de la función hace que se “limpien” los campos y el candado esté nuevamente disponible para que otro usuario pueda utilizarlo.

- mandarTokens

Implementada dentro del loop. Si ocurre un cambio en el valor del campo ‘token’ de la base de datos, se envía el nuevo valor vía LoRa.

- leerTokenDB

Implementada dentro del loop. Obtiene el token actual desde Firebase.

Por otro lado, para que el código funcione, se debieron importar las siguientes bibliotecas:

- heltec.h
- WiFi.h
- FirebaseESP32.h
- LoRaWan_APP.h

En resumen, este código controla el sistema de comunicación LoRa del Transceptor, se conecta a Firebase para gestionar el envío de tokens y verificar el estado del candado, permitiendo el control lógico del mecanismo de apertura y cierre y, de ser necesario, dar el aviso para que se dispare la notificación push ante un caso de hurto.

3.4.2 Candado electrónico

A nivel código del candado electrónico se definieron 9 funciones:

- setup

Como se mencionó, la función setup() es una función especial que se ejecuta una vez al inicio del programa. Es utilizada para realizar la inicialización y la configuración de hardware y software antes de que el bucle principal (loop()) comience a ejecutarse. Junto con las declaraciones iniciales, se encarga de configurar los pines, encender la pantalla LCD y establecer la radio LoRa con los parámetros necesarios para la recepción y transmisión.

- loop

Como se mencionó anteriormente, la función loop() es otra función especial que se ejecuta de forma continua después de que la función setup() haya terminado. Contiene la lógica principal del programa y se ejecuta repetidamente mientras el sistema está alimentado. Dentro del código, detecta la entrada del teclado y muestra en la pantalla LCD el código ingresado. Si se ingresan 6 dígitos, compara lo ingresado con el código recibido por LoRa y realiza acciones correspondientes en consecuencia.

- OnRxDone

Es una función de callback que se ejecutará cuando se haya completado la recepción de datos vía LoRa. Verifica el contenido del paquete recibido y almacena el token para su posterior comparación con el ingresado vía teclado.

- liberarBici

Implementada dentro del loop. Si el candado está en uso y el usuario ingresa en el teclado matricial el código de desbloqueo de forma correcta, esta función hace que se abra el mecanismo para que pueda retirar su bicicleta. Además envía el mensaje ‘Liberada’ al transceptor, el cual implementará la lógica necesaria para que otro usuario pueda utilizar nuevamente el candado.

- OnTxDone

Es un callback que se ejecuta cuando se ha completado la transmisión LoRa con éxito. Luego, pone el módulo en modo de recepción. Entre las opciones de paquetes que pueden enviarse están: la señal para bloquear el candado, la señal para liberar la bicicleta o la señal para activar la alarma.

- enviarBloqueo

Función implementada dentro del loop que envía el mensaje ‘block’. Con él, se le indica al Transceptor que se ingresó el código correcto y que el candado estará en uso por el usuario. Con esta información, el Transceptor detiene la generación de tokens en la base de datos y permite que solamente el usuario actual pueda desbloquearlo.

- verificarAlarma

Función implementada dentro del loop una vez que el candado está en uso por un usuario. Verifica si la distancia mesurada actual es próxima a la distancia que había antes de la ocupación. Para ello, se consideró el valor más bajo mesurado por el sensor en estado vacío (8,5 cm) con una tolerancia de 1 cm. Si el valor actual es mayor o igual a 7,5 cm indica un posible hurto, en consecuencia se dispara la alarma sonora y se envía la alerta al transceptor.

- sensarDistancia

Implementada dentro de verificarAlarma(). Contiene la lógica para que el sensor ultrasónico mida la distancia hasta la obstrucción más cercana.

- enviarAlarma

Implementada dentro de verificarAlarma(). Envía por LoRa el paquete ‘Alerta’, es decir, hubo un intento de hurto en el candado electrónico.

Por otro lado, para que el código y los componentes funcionen, se debieron importar varias bibliotecas:

- heltec.h
- "LoRaWan_APP.h"
- Wire.h
- Keypad.h
- LiquidCrystal_I2C.h
- ESP32Servo.h

En resumen, este código controla el sistema de comunicación LoRa del lado del Candado, permitiendo el desbloqueo/bloqueo del mismo. Siendo la parte física con la que interactúa el usuario final.

3.5 Base de datos

El desarrollo del proyecto “UNSAM Bicis Seguras” requirió del armado de un sistema de tokens, es decir, la generación de claves aleatorias, únicas y seguras que serán utilizadas para el bloqueo y desbloqueo del candado. Las mismas deben ser almacenadas por el tiempo que el usuario utilice el bicicletero.

Por otro lado, la interfaz de usuario se basa en una aplicación móvil, por lo que se requirió además contar con un sistema de autenticación que dé lugar al registro e inicio de sesión.

Por lo mencionado entonces, se decidió utilizar Firebase para diseñar una base de datos que permita realizar ambas cosas: claves y usuarios. A continuación se detalla información acerca de Firebase y la base de datos seleccionada.

3.5.1 Firebase

Es una plataforma diseñada para el desarrollo de aplicaciones web y móviles de forma rápida y eficiente. Ofrece tres productos o soluciones para la implementación, el lanzamiento y el monitoreo de las apps:

- Compilación

Armado del backend. Utiliza Firestore o Realtime Database como base de datos, y además cuenta con un sistema de autenticación.

- Lanzamiento y supervisión

Permite mejorar la calidad de las aplicaciones con un bajo esfuerzo. Integra herramientas para el monitoreo de performance de la app, así como también facilita la distribución de la misma. Además cuenta con un Test Lab, el cual permite testear la app previo a su lanzamiento.

- Participación

Permite aumentar la participación de los usuarios con estadísticas, pruebas y campañas. Cuenta con un módulo de In-App Messaging, el cual permite interactuar con los usuarios. Además, cuenta con un módulo para cambiar el aspecto de la app sin necesidad de actualizarla.

En lo que respecta al proyecto presentado, el énfasis estuvo puesto en el módulo de compilación que ofrece Firebase para realizar el armado del backend, ya que ofrece diferentes funcionalidades que contribuyen al desarrollo de las bases del proyecto, siendo “Firebase Authentication” y “Realtime Database” los servicios más interesantes para la construcción de la app “UNSAM Bicis Seguras”.

Realtime Database

La Realtime Database de Firebase es un servicio de almacenamiento en la nube en tiempo real. Permite almacenar y sincronizar datos en tiempo real entre clientes y servidores. Utiliza una estructura de datos de árbol JSON y proporciona un conjunto de APIs que permiten la sincronización automática de datos en todos los dispositivos conectados en tiempo real. Esto significa que cualquier cambio en los datos se refleja instantáneamente en todos los dispositivos que están escuchando esos datos.

Por otro lado, utiliza una arquitectura de cliente-servidor en la que los clientes se conectan directamente al servidor de Firebase para leer o escribir datos. Los datos almacenados en forma de árbol JSON además se organizan en nodos. Cada nodo tiene una clave única y puede contener datos o más nodos secundarios. Al ser en tiempo real, permite escuchar cambios en los nodos de interés y recibir las actualizaciones en el momento que se producen cambios en esos nodos.

Firebase Authentication

Para que la comunidad educativa pueda acceder al uso de los candados, debe registrarse como usuario en la app e iniciar sesión al querer usarla. De esta manera, si algo sucediese con los candados, se puede obtener registro del usuario que lo utilizó por última vez.

Para ello, Firebase ofrece un sistema de autenticación fácil de implementar tanto para el backend, como así también cuenta con bibliotecas de UI (User Interface) ya elaboradas para que el usuario pueda registrarse. Ofrece registro mediante contraseñas, números de teléfono e incluso proveedores de identidad como Facebook, Google, Twitter.

Por otro lado, el SDK (Software Development Kit) de Firebase Authentication maneja el envío de correos electrónicos para el restablecimiento de la contraseña, en caso que un usuario se la olvide.

Cuando un usuario se autentica a través de Firebase Authentication, se genera un token de acceso que se puede utilizar para autorizar las operaciones de lectura o escritura en la base de datos. Esto permite establecer reglas de seguridad basadas en el usuario autenticado, lo que garantiza que solo los usuarios autorizados puedan acceder y modificar los datos.

De esta manera, Firebase Authentication se integra con la base de datos en tiempo real permitiendo establecer reglas de seguridad personalizadas para determinar quién puede leer y escribir en los diferentes nodos de la base de datos, y Firebase Authentication se encargará de gestionar la autenticación de los usuarios y proporcionar los tokens de acceso necesarios.

3.6 Desarrollo de la aplicación

El desarrollo del proyecto “UNSAM Bicis Seguras”, requiere el armado de un sistema que permita el ingreso de usuarios y la generación de claves aleatorias y únicas para el bloqueo y desbloqueo del candado. Para ello se decidió utilizar Firebase Realtime Database como base de datos y Android Studio como entorno de desarrollo, a través de java.

3.6.1 Android Studio

Android Studio es un entorno de desarrollo integrado (IDE, por sus siglas en inglés) diseñado para la creación de aplicaciones móviles para el sistema operativo Android. Es desarrollado por Google y es el entorno de desarrollo recomendado para crear aplicaciones en Android.

Algunas de las principales características de Android Studio son:

- Interfaz de usuario intuitiva y fácil de usar

La interfaz de usuario de Android Studio está diseñada para ser fácil de usar, con herramientas intuitivas y accesibles para los desarrolladores.

- Herramientas de desarrollo

Incluye herramientas de desarrollo, como un editor de código completo, depurador, simulador de dispositivos y una gran cantidad de herramientas de prueba y análisis.

- Múltiples lenguajes de programación

Android Studio admite múltiples lenguajes de programación, incluyendo Java, Kotlin y C++, lo que lo hace una herramienta versátil y adaptable a las necesidades de los desarrolladores.

- Integración con otras herramientas de Google

Android Studio se integra con otras herramientas de Google, como Firebase, lo que permite a los desarrolladores agregar fácilmente características de la nube a sus aplicaciones.

- Herramientas de Android SDK

El IDE permite compilar el código, junto con los archivos de recursos y datos, en un APK (paquete de Android, que es un archivo de almacenamiento con el sufijo .apk). Un archivo APK incluye todos los contenidos de una aplicación de Android y es el archivo que usan los dispositivos con tecnología Android para instalar la aplicación.

- Compatibilidad con una amplia gama de dispositivos

Android Studio permite a los desarrolladores crear aplicaciones para una amplia gama de dispositivos Android, lo que garantiza que sus aplicaciones puedan llegar a la mayor cantidad posible de usuarios.

- Mejora en la calidad de la aplicación

Proporciona una amplia gama de herramientas de prueba y análisis que ayudan a los desarrolladores a identificar y solucionar problemas de la aplicación, lo que puede mejorar significativamente la calidad de la aplicación final.

En cuanto al uso para la app de Bicis Seguras, los dos primeros puntos son bastante beneficiosos. Por un lado, el hecho de que proporcione herramientas para simplificar el proceso de desarrollo, es un plus considerando que no contamos con grandes conocimientos de programación ni de armado de aplicaciones.

Por otro lado, el hecho de que sea una aplicación compatible con todos los dispositivos Android, es beneficioso para el uso de la aplicación, ya que consideramos que la mayoría de las personas que conforman la comunidad

académica de la UNSAM, cuentan con este tipo de dispositivos. Para el alcance de este proyecto, no consideramos que sea necesario adaptar la aplicación a IOS.

En resumen, Android Studio es una herramienta de gran utilidad para cualquier desarrollador que desee crear aplicaciones para dispositivos Android, y se combina perfectamente con varios lenguajes de programación para hacer que el proceso de desarrollo sea lo más fácil y eficiente posible.

3.6.2 Java

- Java fue el lenguaje de programación empleado para el desarrollo de la app. Si bien cada lenguaje de programación tiene sus ventajas y desventajas, se pueden destacar ciertos beneficios de utilizar Java con Android Studio.

- Java es uno de los lenguajes de programación más populares y cuenta con una gran comunidad de desarrolladores y una amplia gama de recursos y herramientas disponibles. Además, Android Studio está optimizado para Java y ofrece una amplia documentación y soporte.

- Por otro lado, el lenguaje, además de estructurado y sencillo de aprender, es compatible con una amplia variedad de plataformas y dispositivos, lo que lo hace ideal para el desarrollo de apps móviles. Además, Android Studio ofrece una amplia gama de herramientas y bibliotecas para el desarrollo de apps móviles en Java, debido a su gran desempeño en la ejecución de aplicaciones

3.6.3 SHA-1

SHA-1 (Secure Hash Algorithm 1) es una función hash criptográfica utilizada para garantizar la integridad de los datos. En el desarrollo de una app con Android Studio y Firebase, SHA-1 se utiliza para autenticar la app y permitir el acceso a los servicios de Firebase, como la base de datos en tiempo real, el almacenamiento en la nube y la autenticación de usuarios.

En primer lugar, se debe generar un hash SHA-1 para la app mediante la herramienta "keytool" de Java, que está incluida en el kit de desarrollo de Java (JDK). Esta clave se utiliza para registrar la app en Firebase Console y generar un archivo de configuración "google-services.json" que contiene información de configuración para la app.

Luego, en el código de la app, se debe agregar la dependencia de Firebase a través de Gradle, que es el sistema de construcción de Android Studio. Una vez que se agrega la dependencia, se puede utilizar Firebase SDK para acceder a los servicios de Firebase en la app.

En resumen, SHA-1 se utiliza en el proceso de autenticación de la app en Firebase, permitiendo el acceso a los servicios de Firebase y garantizando la seguridad y la integridad de los datos en la app.

3.6.4 “UNSAM Bicis Seguras”

La aplicación desarrollada para dispositivos Android representa una solución efectiva para que los usuarios puedan utilizar el sistema propuesto.

Una de las características esenciales de esta aplicación es la generación de "tokens", unas claves aleatorias, únicas y altamente seguras que desempeñan un papel fundamental en el proceso de bloqueo y desbloqueo de los candados. Los usuarios pueden acceder a estos tokens de manera conveniente a través de la aplicación móvil, lo que garantiza un acceso rápido y confiable a los bicicleteros.

Como la seguridad y la privacidad son una prioridad en "UNSAM Bicis Seguras", se ha implementado un sistema de autenticación que permite a los usuarios registrarse e iniciar sesión de manera segura. Los datos personales, como nombre, correo electrónico, teléfono y contraseña, se gestionan mediante Firebase Realtime Database, una solución robusta y escalable. La integración con Android Studio y el desarrollo en Java permiten una interfaz de usuario intuitiva y un flujo de trabajo eficiente para los usuarios de la aplicación.

La aplicación diseñada presenta cuatro bloques principales, lo que simplifica la experiencia del usuario:

- Autenticación

Los usuarios pueden registrarse e iniciar sesión de manera segura. Aquí se recopilan los datos como nombre, correo electrónico, teléfono y contraseña, fundamentales para realizar un seguimiento de los usuarios de los candados.

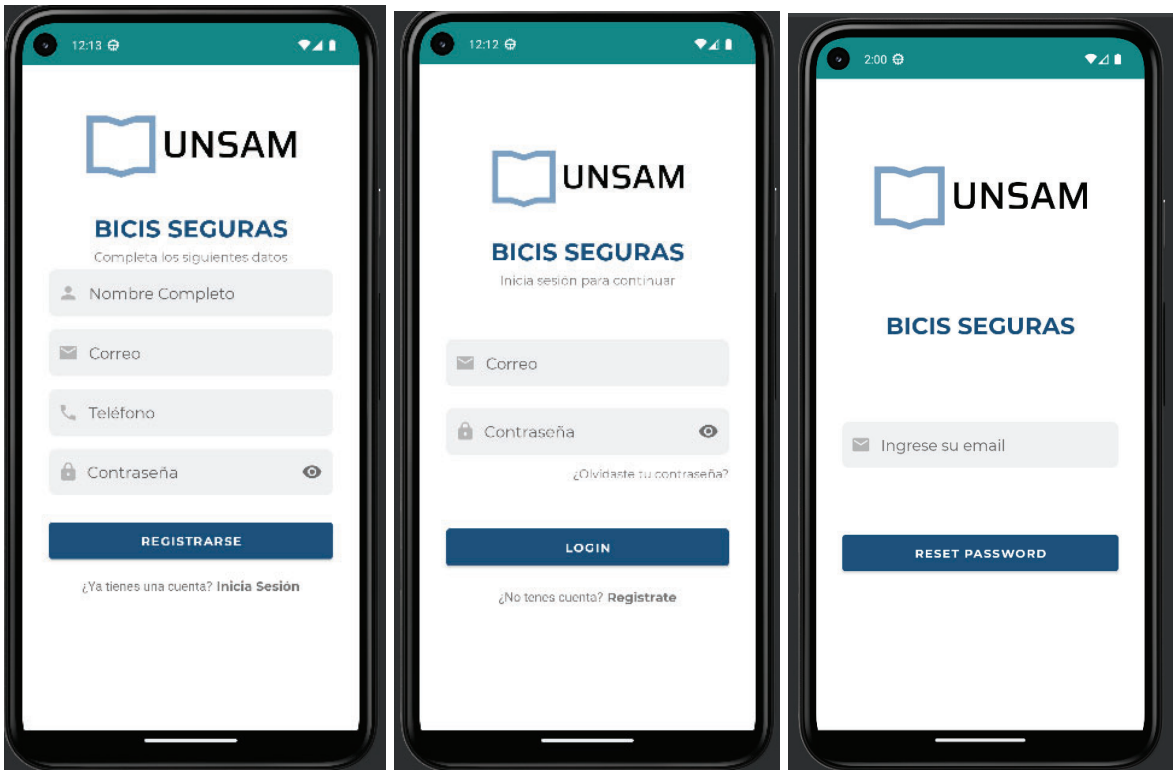

Imagen 16. De izquierda a derecha: Dashboard de “Registro”, “Inicio de sesión”, “Olvidé mi contraseña”

- Gestión de bicicleteros

Al acceder a este dashboard, los usuarios pueden ver un mapa del campus que muestra la ubicación de los bicicleteros disponibles, lo que facilita la planificación de rutas para optimizar tiempo y la elección de una ubicación de estacionamiento conveniente.

Imagen 17. Dashboard “Bicicleteros disponibles”

- Gestión de candados

Al seleccionar un bicicletero disponible en el mapa, los usuarios pueden acceder a información detallada del mismo, observando los candados disponibles.

Imagen 18. Dashboard “Candados disponibles”.

- Tokens

Una vez que los usuarios eligen un candado específico, se genera un token único que se puede utilizar para el bloqueo y desbloqueo del candado. En pantalla se muestra el token generado y una barra de tiempo de 30 segundos, plazo para introducirlo en el candado.

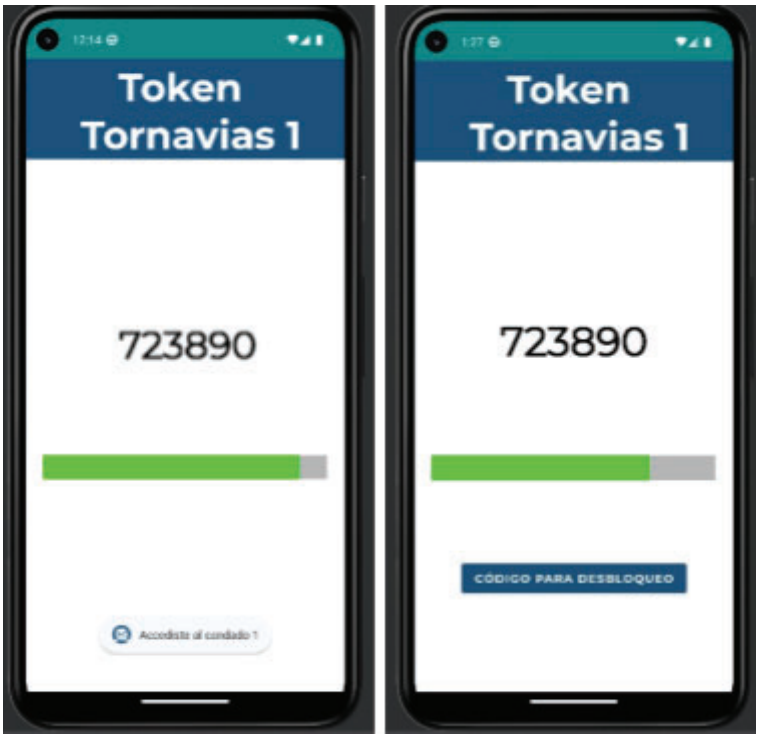

Imagen 19. Dashboard “Token”. A la izquierda, la generación de tokens. A la derecha se observa la pantalla que se muestra una vez que el candado está siendo utilizado por el usuario.

"UNSAM Bicis Seguras" es la combinación de tecnología y practicidad, con un diseño intuitivo y una preocupación por la seguridad, destinada a mejorar la vida de la comunidad universitaria. En ese sentido, además de poder generar un token único por cada candado y cada usuario, el mismo permanece guardado en la base de datos, de manera tal que el usuario pueda recuperar su bicicleta sin memorizar la cadena de números. Para ello, al ingresar a la app, el usuario podrá ver su candado y el código que debe utilizar para el desbloqueo y la liberación de la bicicleta.

- Notificación de alerta

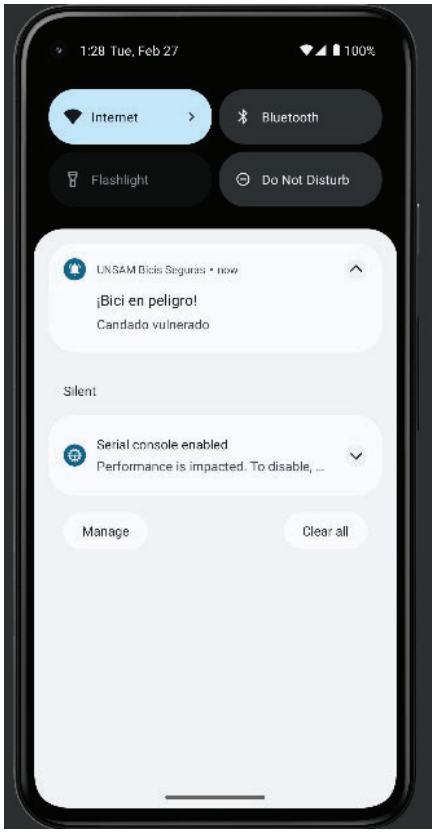

Imagen 20. Notificación de “Bici en Peligro”

Ante un intento de vulneración del candado y robo de la bicicleta, el candado electrónico disparará no sólo una alarma sonora disuasiva que podría ser escuchada por el personal de seguridad o transeúntes, sino que mediante la aplicación se le dará aviso al usuario y dueño de la bicicleta. Este aviso se envía en forma de notificación al instante que se detecta la vulneración del candado.

4. Conclusiones

En el presente capítulo se especifican las consideraciones y sugerencias para una implementación futura. Además, se realiza el análisis final del proyecto, detallando por qué el sistema desarrollado representa una solución efectiva tanto para mejorar la seguridad de las bicicletas en el campus Miguelete como para promover la movilidad sostenible.

4.1 Implementación futura

La distribución de los bicicleteros actuales ubicados en el Campus Miguelete de la Universidad Nacional de San Martín permite el resguardo de 10 bicicletas cada uno.

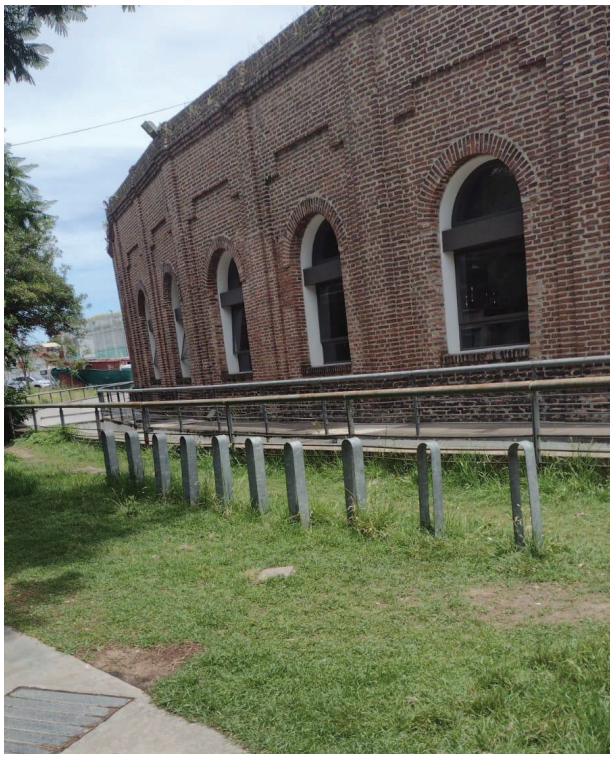

Imagen 21. Bicicleteros actuales

Para el proyecto se realizó un único prototipo de candado electrónico, por lo que si se desea replicar e implementar en el campus Miguelete, se estima una cantidad de 9 candados para el primer acercamiento. De esta manera se podrían ubicar tres candados en cada uno de los puntos estratégicos: el Tornavías, el Circo y el Aulario. Con ello, los usuarios podrían comenzar a familiarizarse con el mecanismo y “tomar confianza” para su uso.

Si bien lo ideal sería que en caso de que la implementación sea exitosa todo el campus transforme los bicicleteros actuales en “bicicleteros inteligentes”, consideramos que es precipitado una cantidad mayor para un primer acercamiento.

Una de las principales causas es la compatibilidad, ya que para lanzar la aplicación de forma oficial en “Google Play Store” se debe crear un perfil en “Google Play Console”, donde se realiza un registro como desarrollador y se paga por única vez la suma de 25 USD. Con ello, cualquier persona que tenga un dispositivo con sistema operativo Android, ya sea celulares, relojes inteligentes o tablets, podrán descargar y utilizar de forma gratuita la aplicación “UNSAM Bicis Seguras”.

Cuando se trata de iOS, el costo por tener un perfil que permite publicar aplicaciones en la “App Store” es de 100 dólares anuales, motivo por el que para la realización del prototipo funcional, se decidió desarrollar la aplicación para Android, sin lanzarla oficialmente al mercado, abaratando los costos.

Además, el temor a lo desconocido juega un papel crucial ante cualquier cambio. Si bien el proyecto incentiva a avanzar hacia un campus inteligente, se debe ganar la confianza de los futuros usuarios acostumbrados a dejar sus bicicletas atadas con lingas y cadenas. Por lo que, en primera instancia, consideramos que lo mejor es tener un esquema “híbrido” hasta que todo el mundo esté familiarizado y le dé una oportunidad al sistema de candados electrónicos.

A continuación se presentan sugerencias a tener en cuenta si se desea llevar a cabo el proyecto a futuro no como un prototipo, sino una implementación final del mismo.

- Escalabilidad

A la hora de realizar una implementación a gran escala es importante obtener sugerencias por parte de los usuarios, por lo que consideramos que la cantidad planteada anteriormente es adecuada para la primera etapa. Esto permitiría tener un mayor control en cuanto a su funcionamiento, brindando la posibilidad de realizar mejoras gracias a la retroalimentación recibida.

Además, algunas personas no disponen de un dispositivo Android que les de acceso a los mismos, y otros pueden preferir no utilizarlos, sintiéndose más

cómodos de proteger su medio de transporte con instrumentos típicos, ya que siempre hay un temor hacia lo desconocido.

En cuanto a la escalabilidad además entra en juego una mejora en la base de datos utilizada. Firebase en su versión gratuita permite almacenar hasta 1 GB de datos, con 100 conexiones en simultáneo, lo que podría no ser suficiente considerando el alto tránsito de personas que hay en la Universidad. Es necesario realizar pruebas de performance que permitan tomar la decisión adecuada acerca de si seguir utilizando Firebase en su sistema pago, o si cambiar a una base de datos relacional como MySQL o PostgreSQL.

- Compatibilidad para todos los dispositivos

Tal como mencionamos anteriormente, nuestro proyecto se desarrolló para dispositivos Android, por lo que se podría realizar una posible expansión a iOS para que cualquier persona perteneciente a la universidad pueda utilizar el sistema. Además, sería necesario lanzar las aplicaciones al mercado para que puedan ser descargadas oficialmente por los usuarios.

- Sustitución del display

Para la construcción del prototipo se empleó un “Display LCD”, el mismo podría sustituirse por una pantalla OLED, ya que tiene mejores características en términos de brillo, ángulo de visión y menor consumo de energía, a costas de ser una opción menos económica.

- Mejora en los materiales

La estructura completa del prototipo de candado se realizó con impresión 3D. La misma podría sustituirse por materiales resistentes a la intemperie y más duraderos para garantizar la longevidad del candado, siendo el hierro una de las opciones más factibles para garantizar mayor robustez y seguridad, a costa de ser una opción menos económica y más pesada.

Sin importar el tipo de metal utilizado, es muy importante tener en cuenta que se generaría una jaula de Faraday, aislando la antena LoRa de la placa de desarrollo

ubicada en el interior de la estructura del candado. Si esto sucediese, el sistema completo dejaría de funcionar ya que nunca podrían comunicarse entre dispositivos generando que no exista una recepción de los tokens. Para resolver este punto de forma simple, se propone agregar a la estructura metálica algún tipo de salida pequeña que permita salir a la antena.

- Implementación de paneles solares

Para la construcción del prototipo se empleó una batería de litio, suficiente para demostrar su funcionamiento. En el caso de replicar los candados se deberían incluir paneles solares ubicados en los bicicleteros actuales, los cuales permitirían brindar un flujo de energía permanente a todos los candados de un mismo bicicletero.

- Circuito impreso

En caso de querer replicar el sistema, la fabricación del candado podría optimizarse desarrollando un circuito impreso, evitando la utilización de una protoboard.

- Fijación del candado

En caso de implementar la solución en todo el campus, se recomienda que la parte inferior de la estructura del candado sea modificada para poder fijarla al terreno, de manera que el mismo no pueda ser desplazado o hurtado.

- Comunicación LoRa

Para el prototipo, el dispositivo Transceptor realiza periódicamente consultas a la base de datos para actuar ante el cambio de alguno de los parámetros definidos en ella. Además, se encuentra en constante situación de “escucha” en su canal de LoRa. Esto resulta en que el dispositivo nunca se encuentra en un estado de reposo, sino que siempre está realizando algún procesamiento.

Al haber elegido placas de desarrollo más centradas en el funcionamiento de LoRa, el desempeño de la misma frente a la cantidad de consultas a la base de

datos que debe realizar por el uso de un sólo candado electrónico, se ve deteriorado. Consideramos que para una implementación donde haya varios dispositivos candados comunicándose al transceptor, es realmente necesario hacer un cambio. Como sugerencia o idea, se podría reemplazar el transceptor por una Raspberry Pi a la cual se le pueda adicionar un módulo LoRa para la comunicación.

La sugerencia del uso de una Raspberry Pi deviene de que la misma es una computadora de una sola placa que son económicas y de bajo consumo energético, aunque lo suficientemente potentes para ejecutar una gran cantidad de aplicaciones en simultáneo. Soportan diferentes sistemas operativos y cuentan con los puertos de conexión necesarios para anexarles el módulo LoRa. De esta manera, se podría optimizar mucho el desempeño del dispositivo transceptor.

Por otro lado, tal como se mencionó anteriormente en el informe, se podría implementar el proyecto utilizando el protocolo de red LoRaWAN® . Se debe tener en cuenta que dicho protocolo está pensado para redes de gran escala y que además requiere el uso de estaciones base o gateway, y de un servidor de red que actué de gestor de los nodos. Además, se debe considerar que la implementación es más costosa que la realizada utilizando la tecnología LoRa base como método de comunicación.

En caso que se quiera realizar la mejora utilizando LoRaWAN®, se podría realizar una integración del presente proyecto con el trabajo de tesis de grado realizado por los Ingenieros recibidos de la Escuela de Ciencia y Tecnología de UNSAM Ing. Bullian, L. E. e Ing. Urbina,C. acerca de la implementación de una red LoRa en el ámbito de la Universidad Nacional de San Martín[2].

Utilizar el protocolo de red LoRaWAN® traería una mejora en la escalabilidad del proyecto, pudiendo comunicar múltiples candados electrónicos ubicados a lo largo del campus. Además, utilizar dicho protocolo garantizaría una mejor seguridad en

[2] Se puede encontrar el informe de dicha Tesis de Grado en la Bibliografía.

la transmisión de paquetes, dado que el mismo brinda dos capas de seguridad utilizando dos claves encriptadas para la comunicación entre nodos y el servidor.

- Reubicación del Transceptor

Para el prototipo, el dispositivo Transceptor fue ubicado en el Centro de Investigación y desarrollo en Informática (CIDI) ya que nos resultó un lugar de acceso permitido como estudiantes de la Escuela de Ciencia y Tecnología. El CIDI permitió resguardar de la intemperie al dispositivo, además de conectarlo a una red WiFi privada y alimentarlo vía USB. Debido a que el CIDI se encuentra dentro del Tornavías, para lograr una mejor cobertura y garantizar la comunicación a lo largo de toda la extensión del campus universitario, lo ideal sería reubicarlo en un punto céntrico del campus Miguelete de la UNSAM.

4.2 Análisis final

El desarrollo e implementación de un sistema de bicicletero seguro basado en tecnología LoRa para el campus Miguelete de la Universidad Nacional de General San Martín representa una solución tecnológica efectiva para mejorar la seguridad y promover la movilidad sostenible en la comunidad universitaria.

A lo largo de este proyecto, hemos explorado diversos conceptos y tecnologías clave en el campo de las telecomunicaciones. Desde el establecimiento de la comunicación entre los sitios mediante LoRa, la construcción del candado electrónico, el armado de la base de datos, el desarrollo de la aplicación que permita al usuario interactuar con el sistema y toda la programación involucrada en cada etapa, aportaron conocimientos y un valor adicional a nuestra formación.

El prototipo de candado electrónico desarrollado representa un acercamiento a la solución efectiva para garantizar la seguridad de las bicicletas de la comunidad universitaria. La combinación de una cerradura resistente y la electrónica detrás del “sistema de alarma” proporcionará un nivel de protección que será capaz de disuadir intentos de hurto y manipulación.

Por otro lado, el diseño del candado se centra en la comodidad y la facilidad de uso para los usuarios. La aplicación móvil, mediante una interfaz muy amigable, les permite bloquear y desbloquear sus bicicletas de manera conveniente, eliminando la necesidad de llevar lingas o sus propios mecanismos de seguridad.

La implementación de un sistema de comunicación de bajo consumo es la clave fundamental para la gestión de energía, permitiendo prolongar la vida útil de la batería del candado electrónico. Esto, garantiza una experiencia sin interrupciones para los usuarios y contribuye a la sostenibilidad del sistema.

La introducción de este sistema de bicicleteros seguros tendrá un impacto positivo en la vida de los miembros de la comunidad universitaria. Facilitará el transporte en bicicleta al campus, promoviendo la movilidad sostenible, al tiempo que proporcionará tranquilidad en cuanto a la seguridad de las bicicletas.

Si bien este proyecto representa un paso significativo hacia la mejora de la seguridad y la movilidad en el campus, queda espacio para la mejora continua. Se podría considerar la expansión del sistema a otras sedes o la incorporación de características adicionales para adaptarse a las necesidades cambiantes de la comunidad universitaria.

En conjunto, este proyecto de estudio y diseño del candado electrónico demuestra cómo la combinación de tecnología, seguridad y eficiencia energética puede traducirse en soluciones prácticas que benefician a la comunidad. La seguridad de las bicicletas y la promoción de un estilo de vida más sostenible son objetivos que siguen siendo prioritarios para la Universidad Nacional de San Martín, y este proyecto se alinea estrechamente con esas metas.

Queda claro que el camino hacia un campus más seguro y sostenible implica la incorporación de tecnologías innovadoras como el candado electrónico, y estamos emocionados por el impacto positivo que este proyecto puede traer a la vida de nuestra comunidad universitaria.

4.3 Cierre del Proyecto

De la misma manera en la que al inicio del proyecto se realizó el Anteproyecto, corresponde finalizar el presente informe dando el cierre. El objetivo es analizar qué tan asertivo fue el estudio hecho previo a dar comienzo al inicio del proyecto, en cuanto a la gestión de tareas, análisis de tiempos y de riesgos. De esta manera, se podrá tener un registro que sirva para el desarrollo de futuros proyectos, que conlleven actividades similares.

En cuanto a la distribución de tareas detalladas en el Work Breakdown Structure (WBS), se podría decir que si bien la descripción de cada una de ellas es correcta, en algunos casos el orden secuencial en las que fueron presentadas no se dió de la misma manera a la hora de llevar el proyecto a la práctica. Por ejemplo, la compra de los materiales (tarea 2.3), no se realizó en forma unitaria, es decir todos los materiales en una misma compra, sino que a medida que se fue construyendo el candado, se investigaron los materiales más adecuados y se adquirieron.

Por otro lado, en el WBS se estimaron algunas fechas de entregas intermedias e incluso la entrega final que no pudieron ser cumplidas debido a demoras en la finalización de la Práctica Profesional Supervisada, en conjunto también con el receso de verano en el mes de Enero. Esto mismo afectó la gestión de tiempos planificada. En este caso, la estimación de tiempos de las tareas fue adecuada, pero algunos plazos estimados no pudieron cumplirse.

En cuanto al análisis de riesgos, a continuación se presenta una tabla con los riesgos analizados, y un breve comentario en cuanto a si realmente fueron mitigados, si su RPN fue bien calculado y si el plan de contingencia fue adecuado, en caso que correspondiese. En la tabla se especifica el número de riesgo. Para mayor información, se puede ir a la tabla de la sección 1.4 del presente documento.

Riesgo	RPN	RPN*	Comentarios
1	12	8	El riesgo estaba asociado a la mala planificación e identificación de tareas. Al ser el RPN mayor a 10, se eligió un plan de contingencia que incluía dedicarle tiempo y atención al armado de tareas y gestión de tiempos. Si bien se le dedicó tiempo a la tarea, tal como se comentó anteriormente, hubo algunos contratiempos. De todas formas, el tiempo por demás que se demoró hasta la entrega del Proyecto no fue de gravedad.
2	6	–	Este riesgo refería errores en el análisis de costos. No hubo problemas con el costo de materiales, por lo que no se presentó este riesgo a lo largo del Proyecto.
3	16	8	Este riesgo se refería a la mala elección de materiales o de software. Al tener un RPN mayor a 10, se pensó un plan de mitigación que incluía investigar diferentes opciones para los materiales y para el desarrollo de la aplicación, sumado a la consultoría con expertos. A lo largo del proyecto nos adherimos al plan de mitigación consultando a nuestro tutor, compañeros, amigos y colegas acerca de entornos de desarrollo para la aplicación, y opiniones para el armado del candado. Este riesgo fue mitigado y no tuvo impacto negativo.
4	20	10	Este riesgo se refería a problemas para conseguir los materiales necesarios. Al tener un RPN mayor a 10 se diseñó un plan de contingencia que incluía tener alternativas de materiales. Contrario a lo esperado, dado el contexto económico de la Argentina, no tuvimos inconvenientes a la hora de adquirir los materiales necesarios. Este riesgo no tuvo impacto negativo.
5	8	–	Este riesgo estaba asociado a la falta de documentación de los componentes a utilizar en el candado y para el desarrollo del software. No se encontraron problemas de documentación, por lo que este riesgo no impactó en el proyecto.
6	15	6	Este riesgo se asociaba a demoras en el desarrollo de la aplicación por falta de experiencia. Al tener el RPN mayor a 15, se diseñó un plan de contingencia que incluía consultar expertos. Nos adherimos a dicho plan, además de consultar en Internet, por lo que el riesgo fue mitigado.
7	15	9	Este riesgo se refería a demoras a la hora de construir el candado por falta de experiencia. Al tener un RPN mayor a 10, se diseñó un plan de contingencia que incluía consultar con expertos. Nos adherimos al dicho plan, incluyendo la ayuda de nuestro tutor, por lo que el riesgo fue mitigado.
8	8	–	Este riesgo estaba asociado al surgimiento de tareas no previstas. En este caso, el RPN era menor a 10 por lo que no hubo plan de contingencia. No surgieron tareas no previstas.
9	20	15	Este riesgo estaba asociado a demoras en la entrega final por cuestiones administrativas de la facultad. Este riesgo tenía un RPN mayor a 20, incluso con el plan de contingencia. En este caso

			estuvimos acertados en marcar este punto como el más riesgoso, ya que el plan de contingencia tampoco funcionó. Los plazos establecidos se vieron modificados por demoras en la Práctica Profesional Supervisada, el período de receso en Enero (tanto nosotros como personal docente no pudo acudir a la facultad) y además por la entrega de otro Proyecto Final Integrador, previo al nuestro, que generó demoras en la corrección del informe.

Tabla 11. Análisis de los riesgos al cierre del proyecto

5. Agradecimientos

El Proyecto Final Integrador no podría haber sido realizado de no ser por la cooperación y por el apoyo recibido. En ese sentido, se agradece a la Universidad Nacional de General San Martín por haber brindado una educación gratuita y de excelencia en la carrera de Ingeniería en Telecomunicaciones.

Se agradece también al director de la carrera Ingeniería en Telecomunicaciones, Mgt.Ing. Rodolfo Salvatore por el acompañamiento y apoyo brindado a lo largo de todo nuestro desarrollo académico.

Se agradece por otro lado a los docentes que nos acompañaron a lo largo de la carrera, especialmente en la realización del Proyecto Final Integrador, el Ing. Marcelo Romeo y la Dra. en Ingeniería María Claudia Abeledo. Se suma al agradecimiento nuestro tutor de tesis Lucas Gabriel Lopez Ardura y a nuestro compañero de la carrera Ingeniería Electrónica, docente de la asignatura Proyecto III, Pablo Daniel Bilocopetiuc por el apoyo dado.

Por último, se agradece a nuestros familiares, amigos y parejas quienes nos acompañaron en nuestra carrera universitaria y especialmente en el desarrollo del proyecto con palabras de aliento a cada paso del camino.

Esta tesis fue lograda por todos ustedes, que hicieron posible que nunca afloje: Rubén, Marta, Rocío, Victoria, Hernán, Lisandro, Olga, Ari, Andy, Fede, Fran, Caro, Matias, Luz, Tomás, Edu, Sol y Tefy. Gracias a todos, los quiero. Lucio.

Quiero agradecer a mis padres Andrea y Fernando, a mis hermanos Alejo y Bautista, a mi abuela Titi por el aguante en los últimos 7 años de esta larga

carrera. También agradecer a Fer por bancarme en cada “no entiendo nada” y darme una mano con todo. A mi pareja Lucas, por bancarme en los momentos más críticos y esperarme con un plato de comida después de largas horas de cursada. Agradezco también a mi amiga incondicional que está desde los 6 años a mi lado y siempre me dio palabras de aliento y festejó todos mis logros, Cande.

Bibliografía

Enlaces Externos

Qué es y para qué sirve el NFC - Telefónica

Red Inalámbrica - Qué es, tipos, ventajas, desventajas y ejemplos

Esquemas de detección y corrección de errores en WiFi 802.11 | by Fabricio Quiros-Corella

IEEE SA - IEEE 802.11n-2009

Different Wi-Fi Protocols and Data Rates

sistema de identificación por radiofrecuencia (rfid)

Bluetooth Technology Overview

Cuánto cuesta publicar una aplicación en Google Play Store y App Store - Infobae

Documentación de Firebase

Establish Serial Connection — main latest documentation

Heltec ESP32+LoRa Series Quick Start

Chirp Spread Spectrum (CSS) for Positioning | Inpixon.

Spreading Factors | The Things Network

TR013-1.0.0 Carrier Sense Multiple Access (CSMA)

Radio Driver Reference Guide | Renesas

https://developer.android.com/studio/intro?hl=es-419

What is Java technology and why do I need it?

LoRa Alliance

Understanding the Differences: LoRa vs LoRaWAN | by Macnman | Medium

Firebase ESP32 Client - Arduino Reference

https://github.com/mobizt/Firebase-ESP32

Getting started with ESP32 and Firebase | by Fabrice Beya

https://ri.unsam.edu.ar/bitstream/123456789/1806/1/TING%20ESCYT%202018%20BLE-UC.pdf

Datasheets

Kit de desarrollo “HTIT-WB32LA_V3”: WiFi LoRa 32(V3) – Heltec Automation

Protoboard de 830 puntos: Protoboard De 830 Puntos

Teclado membrana matricial 4x4: 4x4 Matrix Membrane Keypad (#27899)

Display LCD 16x2 azul 1602 I2C: https://pdf1.alldatasheet.com/datasheet-pdf/view/431751/LUMEX/LCM-S01602DTR-M.html

Servo Motor MG90S: MG90S Datasheet (PDF)

Sensor HC-SR04: HCSR04 Datasheet (PDF)

Anexo

Repositorio con los códigos empleados: https://github.com/UnsamBicisSeguras/Bicis-Seguras

Carpeta de Google Drive con los archivos de AutoCad y los .stl para la impresión: https://drive.google.com/drive/folders/1IoU9OvishL6JkZDBGXFFsMWkN1Ghf_kl?usp=sharing

Copyright. Modelado de la estructura para el transceptor: Heltec V3 OLED LoRa Case by adamziegler - Thingiverse