UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Dispositivo NFC para autenticación de usuarios en Linux

TRABAJO FIN DE MÁSTER

Máster en Ingeniería Informática

Autor: D. Josué Gutiérrez Durán

Tutor: Dr. José Ismael Ripoll Ripoll

Curso 2019-2020

Resum

En aquest Treball Fi de Màster es presenta una proposta per facilitar l'autenticació en diferents equips informàtics utilitzant per a això claus Near Field Communication (NFC).

Aprofitant el suport estàndard d'autenticació de Linux Plugable Authentication Module (PAM), el qual permet definir nous mecanismes d'autenticació de forma modular, es desenvoluparà un nou mòdul per integrar l'ús de les claus NFC com un element més d'identificació de usuaris.

Paraules clau: Mòdul PAM, NFC, RFID, Comunicació Xifrada, AES, ESP32

Resumen

En este Trabajo Fin de Master se presenta una propuesta para facilitar la autenticación en distintos equipos informáticos utilizando para ello llaves NFC.

Aprovechando el soporte estándar de autenticación de Linux PAM, el cual permite definir nuevos mecanismos de autenticación de forma modular, se desarrollará un nuevo módulo para integrar el uso de las llaves NFC como un elemento más de identificación de usuarios.

Palabras clave: Módulo PAM, NFC, RFID, Comunicación Cifrada, AES, ESP32

Abstract

In this Master's Final Project a proposal is presented to facilitate authentication in different computer equipment using keys NFC.

Taking advantage of the standard Linux PAM authentication support, which allows defining new authentication mechanisms in a modular way, a new module will be developed to integrate the use of ac NFC keys as another element of identification of users.

Key words: PAM Module, NFC, RFID, Encrypted Communication, AES, ESP32

Agradecimientos

Y de nuevo, el pequeño 'chispas', aquí se encuentra, poniendo fin a otra etapa que definirá mi persona tanto personal como profesionalmente. Siempre se ha dicho que las segundas partes nunca fueron buenas, pero, aún con los alti-bajos que ha podido tener esta película, ha sido otra gran etapa en mi vida. Mi familia siempre me ha demostrado ser el mejor apoyo, y si nunca pusieron límites a mi imaginación y fueron trampolín de mis ideas, ahora fueron ellos los que me animaron a seguir, a correr y a lanzarme a por todo lo que se me pusiera delante.

Muchos han sido los profesores y maestros que han contribuido a mi formación, y en concreto quiero reconocer la labor de aquellos con los que he tenido la suerte de cruzarme en esta última etapa, gracias. A José Ismael Ripoll, por enseñarnos y por darme un voto de confianza y creer que lo que teníamos entre manos podía llegar a buen puerto.

Gracias también a todos los compañeros y amigos que han sido apoyo y su ayuda, incluso cuando no tenían porque darla. Todos habéis aportado para que este proyecto sea una realidad.

Gracias a ti lector, me gustaría que mi trabajo sirva para satisfacer tu curiosidad, potenciar tus ideas y de paso, proteger y que tengas en mente la seguridad que tanto hace y hará falta en este mundo, cada vez más digital.

Por último, gracias a mi ahora mujer, Cristina. De la que aprendo cada día, no sería lo que soy hoy sin ti.

Jefe, por muchas tormentas que acechen, sigues y seguirás teniendo el timón en tus manos, sabiendo que no hay más capitán que nos pueda salvar.

... porque Jehová tu Dios estará contigo en dondequiera que vayas.

Josué Gutiérrez Durán.

Muchas veces las personas no saben lo que quieren, hasta que se lo enseñas.
Steve Jobs.

Índice general

Índice de figuras

Índice de cuadros

Listado de acrónimos

BBDD	Base de Datos
F.C.I.D.	Fiabilidad, Confiabilidad, Integridad y Disponibilidad
FIDO	Fast Identity Online
HDD	Hard Disk Drive
HF	High Frequency
IoT	Internet of Things
IPO	Interacción Persona-Ordenador
IS	Ingeniería del Software
LF	Low Frequency
MIT	Massachusetts Institute of Technology
MPIu+a	Modelo de Proceso de la Ingeniería de la usabilidad y de la accesibilidad
NFC	Near Field Communication
OTP	One Time Password
P2P	Peer to Peer
PAM	Plugable Authentication Module
PCB	Printed Circuit Board
PWM	Pulse Width Modulation
RFID	Radio Frequency Identification
SRAM	Static Random Access Memory
SUS	System Usability Scale
U2F	Universal 2nd Factor
UHF	Ultra High Frequency
USB	Universal Serial Bus

CAPÍTULO 1
Introducción

En pleno siglo XXI, nadie duda de la importancia que han adquirido los sistemas informáticos en nuestras vidas. Ya sea desde complejos sistemas industriales, a simples equipos personales, los ordenadores están presentes a lo largo y ancho de nuestra sociedad.

Desde que en 1970, con el Kenbak-1 [Bla73] (Figura 1.1), se contemplara la idea de que estas máquinas pudieran utilizarse en un entorno personal y doméstico, los ordenadores personales han ido evolucionando tanto en características como la velocidad, capacidad y seguridad.

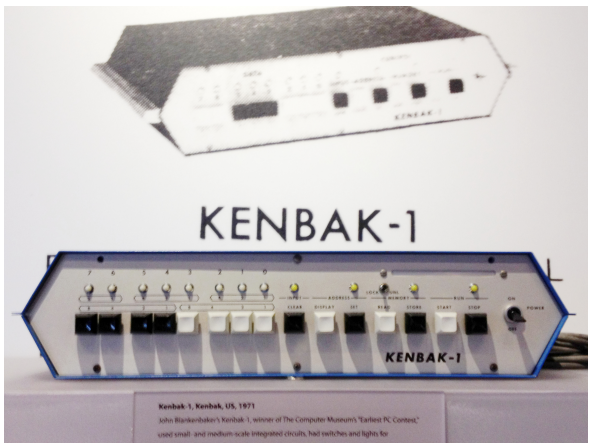


Figura 1.1: Kebank-1, 1971

Lamentablemente, estas características han ido mejorando a distintos ritmos [Tra03], centrándonos en la velocidad de procesamiento, mejora de calidad de imagen o aumento en la capacidad de almacenamiento, características como la seguridad de nuestra información y equipos queda en un segundo plano [RílMS17].

Además, la seguridad queda también supeditada al propio usuario del sistema, por lo que añade un elemento nuevo de riesgo, nuestra propia naturaleza.

El esquema más habitual de autenticación es el nombre de usuario y contraseña, un conjunto de caracteres que actúan de llave para aquel que los conozca. Si analizamos la mente humana y sus limitaciones, podemos observar que para la mayoría de la sociedad es más fácil recordar palabras o algunas fechas a recordar complejas secuencias de números, letras en mayúsculas y minúsculas y algún que otro carácter especial.

Añadida a la complejidad de encontrar una contraseña robusta para uno de nuestros servicios cotidianos, está la buena práctica de asignar una contraseña distinta para el resto de los servicios que utilizamos.

Todos estos impedimentos y el aumento de la capacidad de cómputo de los equipos informáticos, hacen arriesgados los métodos de autenticación tradicionales [RVOG16].

Gracias a la evolución tecnológica, surgen nuevas formas de autenticación. En concreto, y a parte del método tradicional ya explicado, cabe destacar la Autenticación One Time Password (OTP), Token USB, Soluciones Biométricas y Llaves NFC

Autenticación OTP
: En este método de autenticación, el usuario pose un generador de contraseñas válidas que tienen un periodo de vida limitado. Este método es muy efectivo contra ataques de fuerza bruta, ya que cada vez la contraseña se cambia de forma dinámica y los intentos realizados para romper la contraseña son inútiles, pues a cada cambio, se debería de repetir el ataque desde el inicio.

Token USB
: En este caso, el usuario dispone de un dispositivo físico que admite contraseñas de un solo uso, cifrado y autenticación por clave pública y la implementación del protocolo Universal 2nd Factor (U2F). De esta forma, se permite al usuario iniciar sesión de forma segura al emitir contraseñas de un solo uso o al usar un par de claves publico/privadas basadas en Fast Identity Online (FIDO). Además, estos dispositivos también permiten almacenar contraseñas estáticas para poder hacer uso del mismo en sitios o sistemas que no admiten contraseñas de un solo uso.

Soluciones Biométricas
: Se usan lectores biométricos para controlar accesos físicos. No existe una gran variedad de proveedores de lectores biométricos por lo que este tipo de soluciones se utilizan en general dentro de empresas para proteger aplicaciones y datos sensibles.

  Actualmente, no existen estándares aplicados a navegadores que permitan controlar estos accesos a través de PC en Internet. Además, el almacenamiento y gestión de estos datos puede suponer problemas legales, dependiendo de qué países, debido a la protección del individuo, ya que no se autorizan bases de datos centrales para el almacenamiento de dichos datos biométricos.

Llaves NFC
: Las soluciones basadas en tecnologías NFC aplican el protocolo RFID para identificar al usuario sin necesidad de un contacto físico directo. El usuario posee una llave que permite la identificación cuando este la pasa por el lector. Esta opción es muy útil debido a la amplia personalización que permite (distancia de detección, acciones a aplicar en la entrada o salida del usuario, al existir varios usuarios, etc.).

En este TFM se presenta una propuesta para facilitar la gestión y autenticación en distintos equipos informáticos compartidos. Este sistema, mediante llaves NFC será capaz de conceder acceso al equipo a aquellas llaves que estén registradas como autorizadas.

En la Figura 1.2 tenemos un diagrama general que ejemplifica el cambio de concepto, de como un usuario introduce una contraseña para poder acceder a un equipo o como utiliza una llave NFC para acceder a los sistemas a los que tiene acceso.

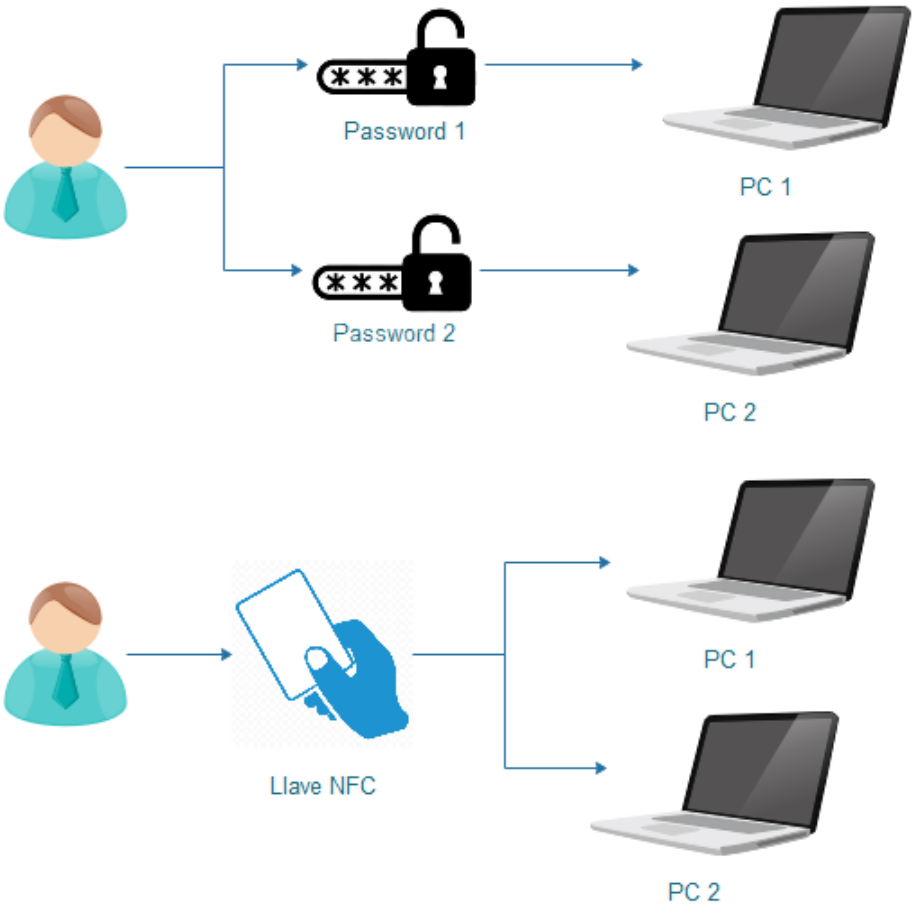


Figura 1.2: Diagrama general comparativo de métodos de autenticación.

1.1 Objetivos

El objetivo general del proyecto es facilitar el desbloqueo y acceso al ordenador, mediante un elemento de identificación único como es una llave NFC.

La consecución del objetivo antes descrito, conlleva la definición de un formato de comunicación entre el equipo y el gestor de llaves NFC. Esta comunicación es realizada cada vez que un usuario intente realizar un acceso con su identificación, siendo el destino quien localmente comprobará la identidad de la persona.

En la Figura 1.3 podemos observar un ejemplo de la idea citada anteriormente, el Usuario (*Azul*) inicia la orden de identificación, siendo el Gestor de Llaves (*Verde*) el que recoge dicha intención y el Modulo Local (*Rojo*) quien procesa dicha orden, y dispone si identificación es lícita o no.

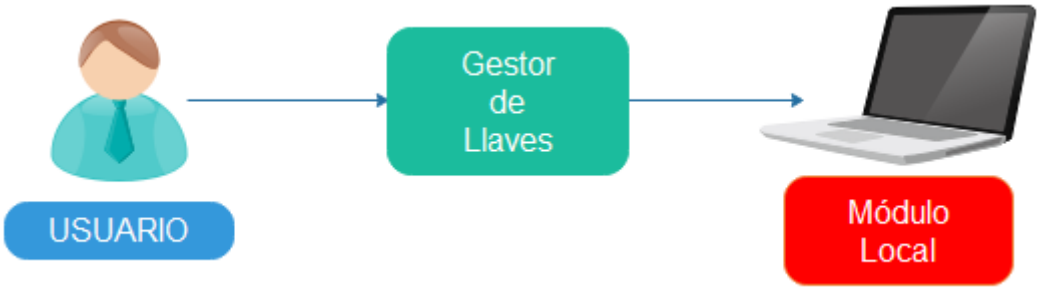


Figura 1.3: Contexto del Sistema.

1.1.1. Objetivos Específicos

Tras definir el objetivo general de este proyecto, se describen los siguientes objetivos específicos.

- Asegurar y garantizar las reglas de Fiabilidad, Confiabilidad, Integridad y Disponibilidad (F.C.I.D.) [LH94].
- Asegurar la escalabilidad y expansión del sistema. Posibilitar la inclusión de nuevas llaves para el desbloqueo del equipo de forma sencilla.
- Asegurar una comunicación cifrada entre el Gestor de Llaves y el módulo local.
- Dotar al Gestor de Llaves de distintos mecanismos (Sonoros, Lumínicos, ...) que permitan al usuario conocer el reconocimiento de su dispositivo personal.
- Estudiar la viabilidad de integrar medidas contra los tipos de ataque comunes en este tipo de entorno (Man-in-the-Middle, Fuerza Bruta, ...).
- Garantizar el registro de acciones. Crear mecanismos de control e histórico que permita conocer las acciones ejecutadas por el sistema.

1.2 Motivación

«Escoge un trabajo que te guste, y nunca tendrás que trabajar ni un solo día de tu vida.» Este TFM concentra conocimientos y técnicas de diversas ramas de la informática. Desde la ciberseguridad hasta dispositivos empotrados o Internet of Things (IoT), pasando por pequeños desarrollos específicos.

Nacido de una necesidad real, la motivación que impulsa este trabajo es el deseo de ver como un «pequeño» cambio puede hacer la vida más fácil y segura a la gente que desee aplicar dicho proyecto.

La mejor tecnología no es la que es ostentosa y vistosa, sino aquella que es posible aplicar y hacer funcionar de forma transparente y oculta para el usuario que no sabe que existe.

Desde que tengo uso de razón siempre me ha gustado explorar y desmontar aparatos, y poder combinarlo con mi carrera profesional y con los mundos de seguridad y IoT en este trabajo es una de las mayores suertes que, por desgracia, no todos tienen el placer de experimentar.

1.3 Estructura del Documento

A continuación, se detallan los capítulos de los que se compone este documento; a ellos, les acompaña una breve descripción de lo que se encontrará en cada uno de ellos.

Capítulo 2: Fundamentos y Antecedentes
Se presenta unos fundamentos básicos para la comprensión de este proyecto y se exponen distintos trabajos desarrollados en este campo de investigación, relaciones entre ambos y sus distintas ventajas e inconvenientes.

Capítulo 3: Metodología y Fases de Trabajo
Se justifica la elección de una metodología de desarrollo a seguir, tras esta valoración, se describe la metodología de trabajo seguida durante el desarrollo del proyecto.

Capítulo 4: Resultados
Se valora la evolución del trabajo resultante, se comprueba el grado de consecución de objetivos planteados y se presentan evaluaciones SUS.

Capítulo 5: Conclusiones
Se exponen las conclusiones, se describen las dificultades encontradas durante el desarrollo y se presentan propuestas de mejora y de trabajos futuros.

CAPÍTULO 2
Fundamentos y Antecedentes

En este capítulo se explica de forma general los conceptos necesarios para el entendimiento del proyecto, una visión sobre el estado actual de las diferentes tecnologías a emplear y los diferentes proyectos que existen a día de hoy en este campo.

2.1 Tecnologías RFID

Esta tecnología fue desarrollada en la década de los 30 por el Massachusetts Institute of Technology (MIT), denominando la tecnología RFID a aquella que permite identificar objetos usando ondas de radio. Tal y como indica el esquema de funcionamiento de la Figura 2.1, un sistema RFID está compuesto por una etiqueta, un lector y una antena. El lector envía mediante ondas de radio una señal a la etiqueta y esta responde con una información única [Fin10].

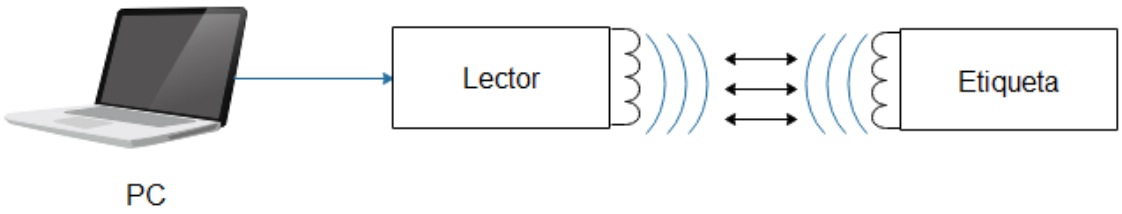


Figura 2.1: Esquema de funcionamiento RFID

Aunque actualmente la tecnología de identificación de objetos más extendida son los códigos de barras, la tecnología RFID presenta una serie de ventajas respecto a estos que podrían hacerlo un claro competidor a corto plazo.

En concreto, las tecnologías RFID no necesitan tener visión directa entre el código y el lector, pueden almacenar una mayor cantidad de información y ser reprogramados con facilidad.

Existen dos grandes tipos de etiquetas en los que se pueden clasificar; Etiquetas Activas y Etiquetas Pasivas.

2.1.1. Etiquetas Activas

Las etiquetas RFID activas contienen su propia fuente de alimentación, por lo que su rango de lectura puede llegar a distancias de incluso 100 metros. Esto las hace muy útiles dentro de sistemas de administración logística [Rod16].

A menudo, estas etiquetas están además dotadas de tecnologías asociadas, tales como GPS o sensores, aunque esto aumenta significativamente su precio con respecto a las etiquetas pasivas.

Este tipo de etiquetas, al estar pensadas para un uso de largo alcance, son diseñadas de forma altamente resistente, ya que están preparadas para trabajar en ambientes hostiles, exteriores o climatológicamente adversos, lo cual las hace muy útiles como sistemas de balizas o de localización.

2.1.2. Etiquetas Pasivas

Las etiquetas RFID no tienen fuente de alimentación propia, por lo que deben de ser alimentadas desde el lector [AFRMGMF06]. Debido a que las ondas de radio deben de ser lo suficientemente fuertes para poder alimentar a las etiquetas, las etiquetas RFID pasivas tienen un rango de lectura de hasta 25 metros de distancia.

Estas etiquetas tienen, generalmente, tres rangos de frecuencia.

- Low Frequency (LF) 125 - 134 KHz
- High Frequency (HF) 13.56 MHz
- Ultra High Frequency (UHF) 856 - 960 MHz

2.2 Llaves NFC

NFC es una tecnología especializada dentro de la familia de las tecnologías RFID. Las llaves NFC (Figura 2.2) operan dentro de la misma frecuencia que las RFID HF (13.56 MHz). Los estándares NFC están basados en los del RFID regidos en la ISO/IEC 14443 [CKP06] y ISO/IEC 18092 [HK05].

Figura 2.2: Llaves NFC

La tecnología NFC toma como ventaja el reducido rango de lectura del RFID HF, por lo que obliga a que llave y lector estén a una pequeña distancia. Esto le ha servido para convertirse en una opción de comunicación segura entre dos dispositivos.

Otro rasgo distintivo de la tecnología NFC es la comunicación Peer to Peer (P2P), ya que los dispositivos NFC son capaces de actuar tanto como lectores o como etiquetas. Gracias a esta tecnología se posibilita la implementación de sistemas de pagos sin contactos.

Además, la inclusión de esta tecnología por parte de los fabricantes y empresas de telefonías móviles permite una rápida extensión y popularización de su uso.

Por último, al igual que las tecnologías RFID, los lectores NFC pueden leer etiquetas pasivas o etiquetas RFID HF que cumplan la ISO 15693 [LZYX06]. Estas etiquetas permiten almacenar comandos específicos como abrir aplicaciones o enlaces que serán ejecutados por el software que las leen.

2.3 Electrónica de Consumo

La Electrónica de Consumo engloba todas las tecnologías y equipos que se usan de forma cotidiana para comunicaciones y ocio. Desde móviles, televisores, electrodomésticos, este tipo de de tecnología ha tenido un aumento notable de la demanda y de su avance tecnológico [MSV17].

El híbrido de estos dispositivos con las tecnologías inteligentes, ha hecho posible un escenario hasta ahora impensable en el que los precios de estos desarrollos han descendido significativamente. Además, es notable destacar las plataformas de hardware libre. Estas plataformas posibilitan el desarrollo de escenarios diseñados a pequeña escala, los cuales permiten interconectar dispositivos que en un inicio eran independientes.

El auge de plataformas tales como Arduino[1], basados en la familia de microcontroladores Atmega, Atmel o Intel; ESP con series como la ESP32 (Figura 2.3) y ESP8266, los cuales añaden el plus de conectividad Wi-Fi y Bluetooth; STM con microprocesadores ARM hacen que cualquiera, por un bajo y competitivo precio, pueda adquirir y montar cualquier sistema que se nos ocurra gracias también a la gran batería de sensores y actuadores disponibles.

Figura 2.3: Microcontrolador ESP32

[1] https://www.arduino.cc/

2.4 Criptografía

Se entiende como criptografía al estudio de algoritmos, protocolos y sistemas usados para dotar de seguridad a comunicaciones, información y entidades que se comunican. El objetivo principal es el diseño, implementación e implantación de sistemas que cumplan con las propiedades F.C.I.D..

Un sistema criptográfico es considerado seguro si un adversario no es capaz de romper esa seguridad en una tarea o punto específico [MT03].

2.5 Linux

Linux es un Sistema operativo open source, lo que significa que su código se puede ejecutar, estudiar, compartir y modificar.

Podemos definir 3 grandes ramas dentro de las funcionalidades que podemos explotar en Linux. Una de ellas es la desunión de los entornos gráficos a las aplicaciones, ya que tanto el sistema operativo, como la mayoría de aplicaciones pueden funcionar tanto en modo consola, como con entorno gráfico. Esto es muy útil para escenarios en los que el entorno gráfico es prescindible, aprovechando mejor así el rendimiento de la máquina.

Otra de las grandes ventajas de Linux es la gran colección de utilidades para la programación. Además de contar con la capacidad de compilar código para múltiples lenguajes de programación como Java, C, C++, Pascal, ADA también soporta las diversas arquitecturas de procesador gracias a la compilación cruzada.

Por último, existe un gran numero de aplicaciones de usuario y con la posibilidad de acceder a dicho software gracias a repositorios oficiales de aplicaciones soportadas, evitando así recurrir a sitios de terceros para obtener las aplicaciones deseadas.

2.6 Módulos PAM

Los Módulos PAM son mecanismos concretos de autenticación flexible que permite a las aplicaciones y software abstraerse del proceso de identificación.

Existen múltiples formas de identificar a un usuario, contraseñas, identificaciones biométricas, claves de un solo uso, etc. Además existen multitud de sistemas que necesitan identificar al usuario que lo maneja (Correo Electrónico, Web, Base de Datos, etc.).

De esta necesidad, surge la idea de estandarizar y delegar la acción de autenticar a un módulo externo (PAM). Una aplicación preparada para usar esta forma de autenticar, delega esa tarea al módulo, de las formas que este disponga (Contraseñas, Tokens, Biometría, etc.) sin necesidad de realizar modificaciones especiales en la propia aplicación.

CAPÍTULO 3
Metodología y Fases de Trabajo

En este capítulo se describe la metodología de trabajo que se ha seguido y el porqué de su elección, se indican las distintas fases realizadas durante el desarrollo del proyecto y se detallan las herramientas utilizadas.

3.1 Metodología MPIu+a

MPIu+a es una metodología de desarrollo de sistemas interactivos que sigue los principios del Diseño Centrado en el Usuario [iS07]. Una de las metas más importantes de esta metodología de proceso es conseguir «casar» el modelo de desarrollo de sistemas interactivos de la Ingeniería del Software con los principios básicos de la Ingeniería de la Usabilidad y los de la accesibilidad proporcionando una metodología que sea capaz de guiar a los equipos de desarrollo durante el proceso de implementación de un determinado sistema interactivo.

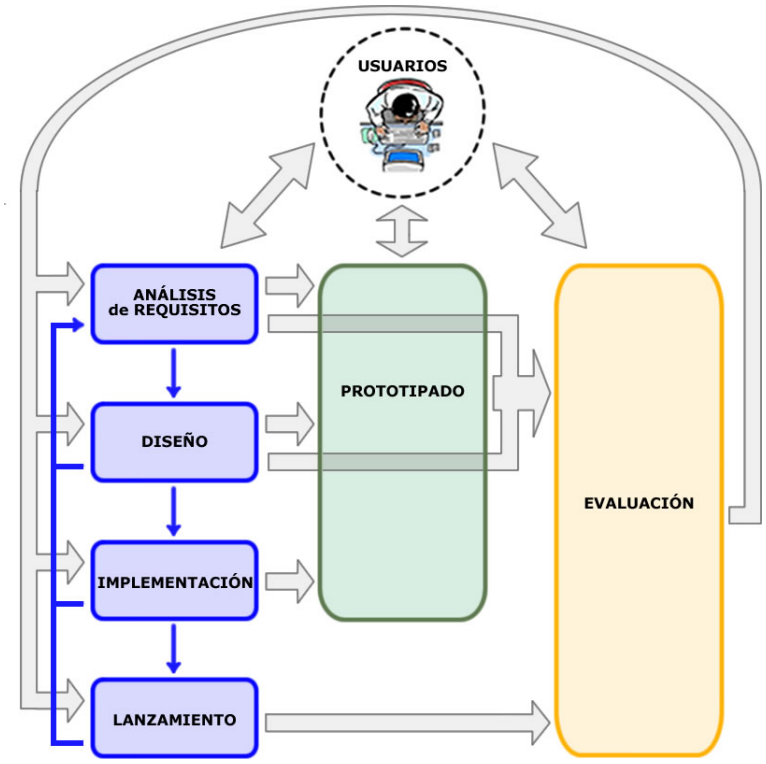


Figura 3.1: Esquema de modelo MPIu+a.

Como podemos observar en la Figura 3.1 esta metodología está organizada en base a una serie de módulos que determinan la fase de desarrollo en la que se encuentra el proyecto y ubica en un nodo concreto la actividad del conocimiento existente en Interacción Persona-Ordenador (IPO). Esto, en definitiva, no hace más que «poner cada cosa en su sitio», dotando de las pautas a seguir durante el diseño de un sistema interactivo.

En la Ingeniería de la Usabilidad y en IPO, en general hay dos conceptos muy importantes que deben realizarse de manera sistemática desde el inicio del desarrollo del proyecto y no pueden cesar hasta la finalización del sistema: El prototipado y la evaluación.

Volviendo a la Figura 3.1 vemos reflejado, con una codificación en colores, estos tres conceptos a modo de tres pilares básicos.

1. **Ingeniería del Software** La Ingeniería del Software, en el formato "clásico" de ciclo de vida en cascada iterativo, marcada en color azul.
2. **Prototipado** El prototipado, como metodología que engloba técnicas que permitirán la posterior fase de evaluación, marcado en color verde.
3. **Evaluación** La evaluación que engloba y categoriza a los métodos de evaluación existentes, marcada en color amarillo.

Podemos por tanto diferenciar las siguientes características en esta metodología:

Centrado en el Usuario

En los modelos de desarrollo actuales los diseñadores y/o los programadores deciden por los usuarios, escogiendo las metáforas, organizando la información y los enlaces, eligiendo las opciones de los menús, etc. Dichas personas incluso, etiquetan sus aplicaciones como amigables al usuario a pesar de que ningún usuario real haya dado su aprobación a tal característica.

Un proceso de Diseño Centrado en el Usuario debe dejar claro de que es así sólo con mirar el esquema la primera vez. Esto es lo que queda reflejado al disponer a éste en la parte central y por encima del resto de etapas todo el modelo de proceso.

Queda claro, pues, que el usuario está en el centro del desarrollo y en las facetas en las que interviene, por lo que durante todo el desarrollo deberá de estar presente.

Iterativo

Establecer procesos repetitivos es un aspecto natural que se da en cualquier otro ámbito de ingeniería, sea de la disciplina que sea. Por poner un ejemplo de otra disciplina, en el mundo de la edificación existe incluso antes de empezar con la excavación del terreno una serie de reuniones (iteraciones) arquitecto-cliente (desarrollador-usuario) para conseguir que el diseño del futuro edificio se adapte a las necesidades de sus inquilinos.

Dicho proceso de repetición aplicado a la Ingeniería del Software también existe, aunque suele producirse en la fase final del proceso. El esquema propuesto dispone de una serie de flechas cuyo objetivo no es otro que visualizar que desde todas las fases se promueve la participación activa de los usuarios, tanto en el análisis de requisitos como en el diseño y en la realización de prototipos y/o su posterior evaluación.

En la Figura 3.2 puede observarse dos tipos de flechas, unas delgadas que se corresponden con el modelo de la Ingeniería del Software (IS), y otras más gruesas que convierten la IS en un verdadero modelo centrado en el usuario. Estas últimas indican, entre otras cosas, donde interviene el usuario en el proyecto.

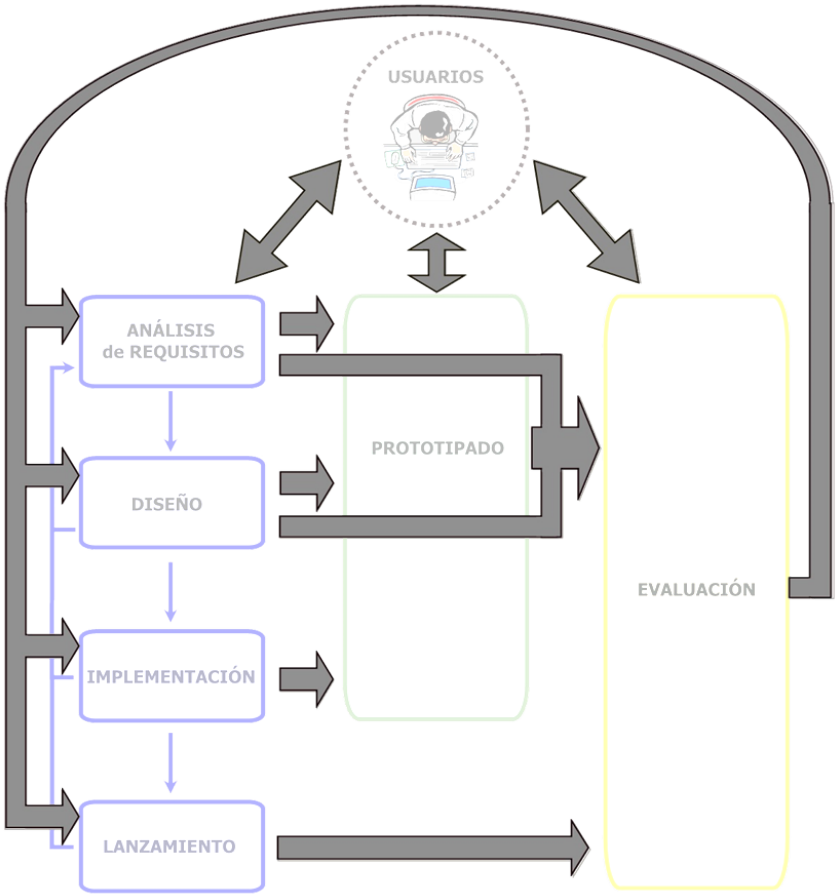


Figura 3.2: Participación del Usuario en el modelo MPIu+a.

Sencillez

En el desarrollo de sistemas interactivos se pretende que la usabilidad sea un factor determinante de los mismos. De igual modo, sus interfaces sin perder su capacidad comunicativa y funcional, deben de ser lo más sencillas y simples posibles.

Con la premisa anterior en mente, debemos proceder con la metodología de trabajo de este proyecto de igual forma. Esta debe de permitir llevar a cabo su trabajo de forma simple y sencilla.

Las representaciones del diseño del proyecto deben, por tanto, ser comprensibles por todos los componentes de los equipos, tanto de desarrollo, como de usuarios. Esto último solo será posible construyendo estas representaciones de forma clara.

Flexibilidad

Cabe destacar que esta metodología no tiene un sentido lineal o restrictivo, sino que fomenta la libre aplicación del mismo, siendo el desarrollador junto a los usuarios y los propios requisitos del sistema y sus particularidades, los que marcaran cuantas iteraciones deben de realizarse el flujo de acciones en cada iteración y cómo deben de hacerse.

3.2 Fases de Trabajo

De acuerdo a lo visto en el apartado anterior, se procede a desarrollar las distintas fases del desarrollo del proyecto.

3.2.1. Análisis de Requisitos

Esta es la fase inicial del proyecto en la cual recogeremos las necesidades del usuario de cara a la elaboración del sistema. Dichos requisitos los clasificaremos según la IS en Requisitos Funcionales y Requisitos No Funcionales, ambos se detallan a continuación.

Requisitos Funcionales

Gestor de Llaves

- El gestor de llaves debe de garantizar el registro de acciones mediante la creación de mecanismos de control e histórico que permitan conocer las acciones ejecutadas.
- El gestor de llaves debe de ser capaz de registrar a varios usuarios.

Módulo Hardware

- Debe de existir una señal visual y sonora para una tarjeta detectada.
- El módulo no debe de almacenar ningún tipo de clave.
- El módulo hardware podrá cancelar la autenticación para dar paso a un método alternativo.

Requisitos No Funcionales

- Los módulos relacionados con el Gestor de Llaves estarán escritos en lenguaje C.
- Los módulos hardware estarán escritos en la variante de C preparada para Arduino.
- En todo momento se usará un sistema de control de versiones.
- El Gestor de Llaves podrá tener registrado a varios usuarios para conceder el acceso a los mismos.
- La comunicación del módulo hardware debe de ser mediante USB.

3.2.2. Diseño

En el transcurso de esta etapa, se elaboran los diseños de los 2 módulos que componen este sistema.

Los bocetos de los modelos electrónicos han sido realizados [RRG+11] con la herramienta Fritzing.

Gestor de Llaves PAM

El Gestor de Llaves o Módulo PAM será el encargado de gestionar el intento de autenticación de los usuarios mediante sus llaves NFC.

El módulo enviará una petición de lectura al módulo hardware y esperará a recibir la respuesta del dispositivo. Esta respuesta puede ser una orden de salida, en cuyo caso se enviará la orden al sistema de autenticación obviada y el sistema pasara a intentar autenticar al usuario mediante el siguiente método PAM disponible.

Otra respuesta a recibir será la identificación de una llave NFC, la cual pasara a ser comparada con el registro de llaves autorizadas. En el caso de que este sea el caso, se procederá a enviar al sistema una autenticación aceptada, en caso contrario, se enviará una autenticación fallida.

Sea como fuere, el módulo dejará constancia en un archivo de histórico para su posterior consulta por parte de un administrador de sistema.

El código del Listing 3.1 describe el funcionamiento del módulo en formato Pseudo-Código.

```
si ( Lectura de nfc.access )
| si ( Apertura de Comunicacion )
| | si (Envio de peticion de login )
| | | *Lectura de Tarjeta
| | |   Existente
| | |     Escritura en log
| | |     Acceso Concedido
| | |   No Existente
| | |     Escritura en log
| | |     Acceso Denegado
| | | *Boton de omision
| | |   Escritura en Log
| | |   Siguiente Metodo PAM
| | sino
| |   Salida y error
| sino
|   Salida y error
sino
  Salida y error
```

Listing 3.1: Pseudo-Codigo de Modulo PAM.

Módulo Hardware

Este módulo será el encargado de realizar la lectura de la llave NFC y de enviar el ID leído al Módulo PAM.

El módulo estará en estado de espera hasta recibir una señal de login, con la cual se iniciará la lectura, indicándolo mediante una señal lumínica (Led Rojo) y con un ligero pitido.

El módulo quedará a la espera de lectura de una tarjeta NFC, esta lectura correcta quedará identificada mediante una señal lumínica (Led Verde) y será enviado el ID de dicha llave al módulo PAM.

En caso de no disponer de una llave NFC, el usuario deberá de pulsar el botón de bypass para ignorar el método de autenticación con llave NFC y proceder a identificar al usuario con el siguiente método definido en la cola de métodos PAM.

En cuanto al diseño electrónico (véase Figura 3.3), el Arduino contará con los dos LEDs citados anteriormente y con un zumbador. Además, es necesario el pulsador para omitir la identificación y el módulo lector NFC.

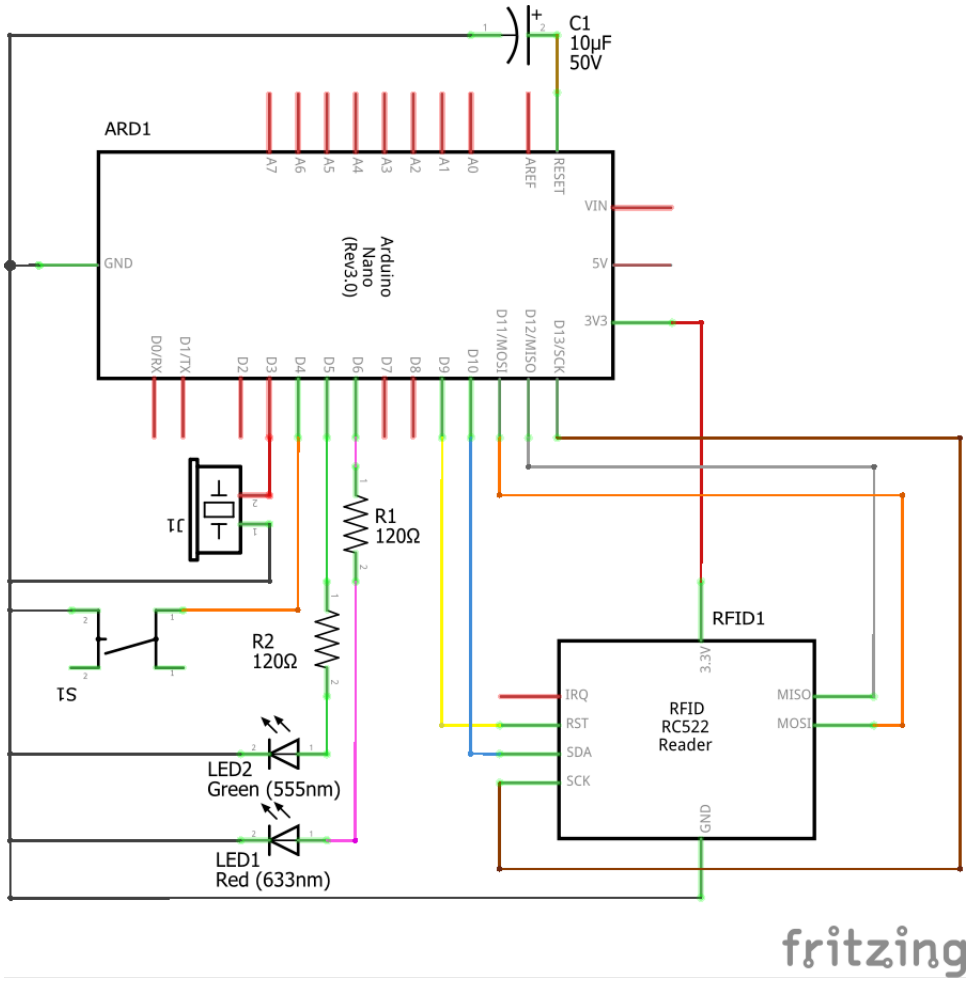


Figura 3.3: Diagrama Esquemático de Lector de llaves NFC

A modo de resumen, podemos ver el diagrama de la Figura 3.4 el cual describe el panorama de comunicación seguido dentro del diseño planteado anteriormente.

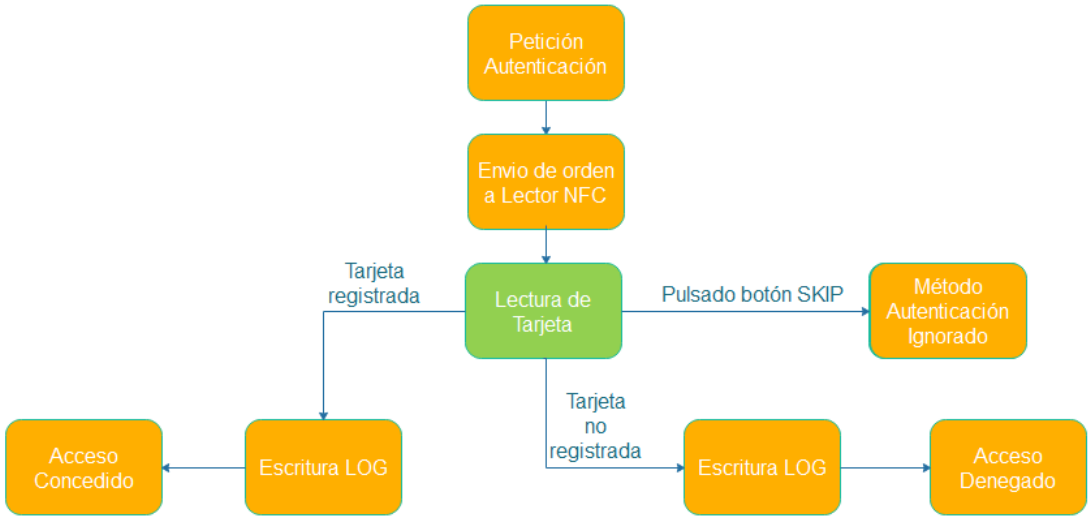


Figura 3.4: Diagrama Esquemático de Lector de llaves NFC

En color naranja podemos observar las acciones ejecutadas por el módulo PAM mientras que en color verde vemos las acciones que efectúa el lector NFC.

3.2.3. Implementación

En esta etapa se comienzan a desarrollar las diferentes funciones de los módulos, con respecto a los requisitos definidos anteriormente en al Apartado 3.2.1.

La implementación de los 2 módulos se ha producido mediante 5 iteraciones o hitos en los cuales se buscaba completar una acción para poco a poco completar las especificaciones finales del proyecto.

Durante todo el desarrollo de ambos módulos se utiliza tecnología *Git*[1] para el control de versiones, haciendo posible la vuelta atrás en una copia de seguridad si existiera algún problema con cambios realizados en el código de la aplicación. La aplicación utilizada para realizar estos controles es *SourceTree*[2].

Para el correcto desarrollo del software del gestor de llaves NFC se usa el entorno de desarrollo de *Arduino*[3].

Iteración 1

En esta primera iteración se diseña el primer prototipo de lector de llaves NFC (Figura 3.5) además, se define un protocolo de comunicación a nivel de aplicación para el lector NFC. De esta manera, se definen dos posibles comandos de entrada el cual el lector espera recibir mediante comunicación serie.

reading La recepción de este comando inicia la orden de lectura de una tarjeta y de envío de la misma de forma normal y sin cifrado adicional. Esta opción es usada cuando se quiere identificar una tarjeta fuera de un proceso de autenticación (Por ejemplo,

[1] `https://git-scm.com/`
[2] `https://www.sourcetreeapp.com/`
[3] `https://www.arduino.cc/`

cuando queremos conocer la numeración de una tarjeta para posteriormente añadirla en la lista de accesos lícitos).

login La recepción de este comando inicia la orden de autenticación con una tarjeta y el envío de la información de la misma. Esta opción es usada cuando el módulo PAM ha iniciado una petición de autenticación y requiere una tarjeta para el proceso.

Además, se define una pequeña aplicación de escritorio en lenguaje *C* para complementar al comando *reading* anteriormente mencionado. De esta forma, es posible leer la numeración de las tarjetas disponibles.

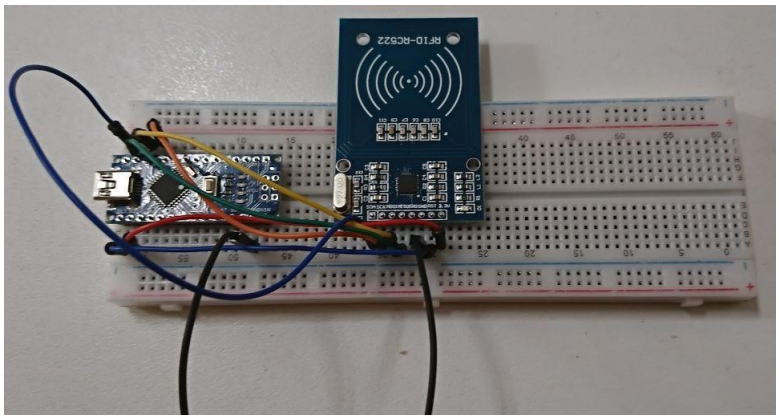


Figura 3.5: Prototipo Lector NFC.

Iteración 2

En esta segunda iteración, se describe el protocolo para la autenticación gracias a la definición del módulo PAM. En esta primera fase del módulo se busca ser capaces de autenticar de forma correcta una numeración de tarjeta predefinida de forma estática.

Como podemos ver en la Figura 3.6, el módulo PAM inicia la comunicación con el lector de llaves NFC el cual le facilita la información de la tarjeta leída. El módulo PAM compara esta información con la lista (estática en esta fase) de tarjetas con acceso para permitir o denegar el acceso al equipo.

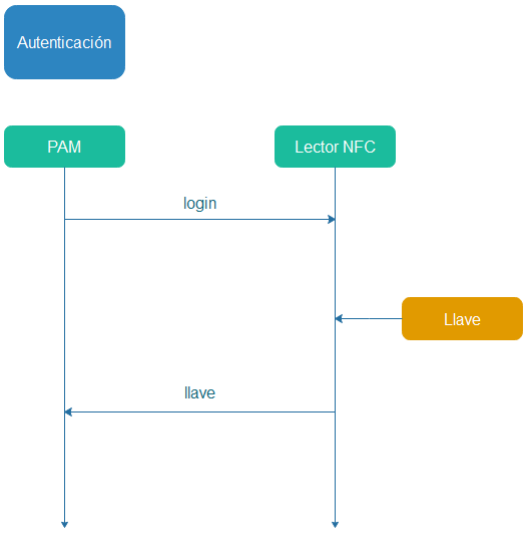


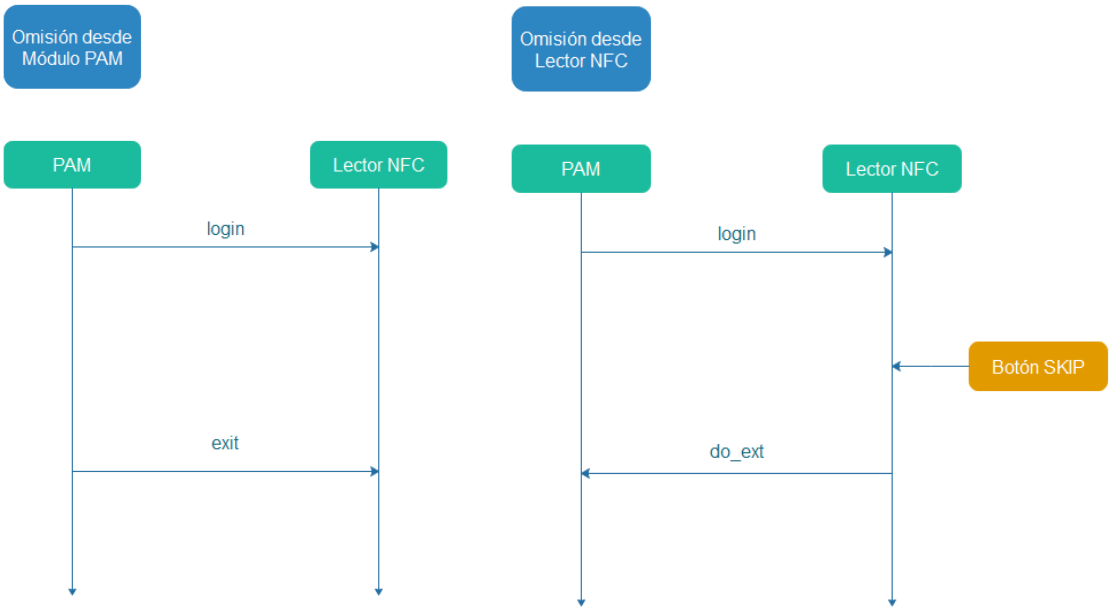
Figura 3.6: Diagrama de Autenticación.

Iteración 3

En la tercera iteración, se definen los protocolos de omisión. De esta forma, ya sea porque el usuario ha cancelado el proceso de autenticación (Figura 3.7a) o porque el usuario a cancelado el lector NFC como método de autenticación (Figura 3.7b).

De esta forma, en el primer caso, es el módulo PAM quien comunica al lector que el proceso de *login* ha finalizado, por lo que debe de volver a estado de espera y debe de cancelar las señales sonoras y lumínicas, ignorando también cualquier tarjeta leída o por leer.

En caso de que el usuario desee obviar el método de autenticación de llaves NFC para proceder a autenticarse con el siguiente método disponible en la cola PAM, deberá de pulsar el botón de *SKIP* situado en la esquina superior derecha del lector de llaves. De esta forma, el lector indicara al módulo PAM que el usuario no desea autenticarse por esta vía por el motivo que sea.



(a) Diagrama omisión desde módulo PAM **(b)** Diagrama omisión desde módulo NFC

Figura 3.7: Diagramas de Omisión.

Iteración 4

En esta iteración se realiza el proceso de gestión de varias tarjetas, pudiendo así personalizar en el archivo de configuración (Figura 3.8) por un lado el puerto en el que el módulo PAM esperara la comunicación del lector de llaves NFC y por otro lado las llaves a las que conceder acceso al sistema.

```
pc@pc:~$ sudo cat /var/nfc.access
/dev/ttyUSB0
B7E93163
39AA94A3
```

Figura 3.8: Ejemplo de archivo de configuración.

Iteración 5

En la última iteración, se realiza el proceso de implementación del sistema de histórico de acciones ejecutadas por el módulo PAM. Este histórico refleja las acciones de autenticación correcta, autenticación fallida y petición de omisión por parte del usuario; pulsando el botón de omisión del lector NFC.

Como se puede observar en la Figura 3.9, el histórico registra el día y la hora en la que se produjo la acción, la acción que se produjo y la numeración de la tarjeta implicada (si procede).

```
pc@pc:~$ sudo cat /var/nfc_access.log
2020-10-06 09:44:58 Access Granted to: B7E93163
2020-10-06 09:45:13 Skip Button Pushed
2020-10-06 09:45:25 Card 44D8DD2E not register
```

Figura 3.9: Ejemplo de archivo de Historial.

3.2.4. Evaluación

Para la evaluación final del proyecto, se elige un modelo de Cuestionario SUS [MP88]. Gracias a su manera fácil de completar, puntuar y de establecer comparaciones cruzadas, así como su uso extendido en evaluaciones de proyectos digitales [Arr04]. El Cuestionario SUS (Véase Anexo B) se realizará a dos grupos de personas, uno familiarizado con entornos informáticos y un segundo grupo que no está relacionado con dichos entornos.

El grupo de personas esta formado por 10 evaluadores, de los cuales 5 son clasificados como personal familiarizado con el contexto tecnológico y los 5 restantes no tienen relación directa con el mundo investigador técnico.

El protocolo seguido ha sido el mismo para ambos grupos. En primer lugar se realiza una prueba funcional del módulo propuesto, realizando una serie de acciones que han sido dirigidas, para después realizar la evaluación de usabilidad de dicho módulo. El cuestionario se divide en un solo módulo de acuerdo con los requisitos requeridos e implementados en capítulos anteriores(Véase Apartado 3.2.1). Los resultados y evaluaciones de dichos cuestionarios pueden verse en detalle en el Capítulo 4.

3.2.5. Dificultades Técnicas

Tras las distintas etapas de diseño e iteraciones, surgen distintas dificultades técnicas de las cuales es significativo destacar las siguientes.

- Debido a la estructura en formato *cola* de los módulos PAM, fue inviable tener dos formas alternativas de autenticarse (contraseña o llave NFC) al mismo tiempo. Esto se intentó paliar de diferentes formas, (Creación de procesos hijos, Comunicación entre módulos, etc.) pero todos los intentos fueron infructuosos. Además, a esto se le suma la complejidad de que los módulos PAM, aunque están escritos en lenguaje *C*, tienen ciertas restricciones debido a la capa de seguridad añadida, por lo que fue imposible usar algunas funciones o estructuras dentro de dicho módulo.
- La comunicación entre módulo PAM y lector de llaves NFC tuvo ciertas complicaciones debido al bajo nivel de programación requerido por el propio módulo PAM y las limitaciones del mismo. Problemas como los reinicios de conexión o tiempos de espera fueron frecuentes hasta que se pudo definir una estructura de conexión

solida para evitar dichos problemas. Además, las limitaciones en las propias comunicaciones series (Imposibilidad de añadir *Sniffers* de testeo o Limitaciones a la hora de realizar tareas de *Debug*) hicieron estas tareas mucho más complicadas.

- Cabe destacar también, una de las dificultades encontradas en el propio diseño hardware de *Arduino*, la cual tuvo un efecto en el software y que se tuvo que solucionar por medios hardware. *Arduino Nano* tiene un reinicia automáticamente la placa cuando hay un cambio en la conexión serie (reinicio de la conexión o salida de la misma). Esto es un problema ya que la conexión se abre y cierra por el módulo PAM cada vez que se realiza un intento de autenticación, por lo que al acabar cada intento de autenticación el lector de llaves sufría un reinicio. Esto fue subsanado añadiendo un condensador electrolítico de 10μF entre los pines *RST* y *GND*.

3.3 Tecnología

A continuación, se describen las tecnologías que fueron necesarias para el correcto desarrollo del proyecto.

3.3.1. Medios Hardware

Los Medios Hardware que han sido necesarios para el correcto desarrollo del proyecto se desarrollan a continuación.

- Fueron necesarios dos equipos informáticos (véase Cuadro 3.1) con un entorno de desarrollo *Arduino*.

Nombre	Procesador	Memoria RAM	Hard Disk Drive (HDD)
Equipo 1	Intel Core i7-6700k 4,01GHz	64,00 Gb DDR4 2133 MHz	SSD 525Gb SATA R: 530Mb/s W: 510MB/s
Equipo 2	Intel Core i7-7700HQ 2,80GHz	16,00 Gb DDR4 2133 MHz	SSD 256Gb SATA 3 R: 534Mb/s W: 178MB/s

Cuadro 3.1: Equipos Informáticos.

- También fueron necesarias varias placas de microcontroladores para las distintas evaluaciones.

	Arduino Uno	**Arduino Nano**	**ESP32**
Microcontrolador	ATmega328	ATmega328	Dual Core Xtensa LX6 32 Bits
Voltaje	5 V	5v	3.3-5 V
Entradas/Salidas Digitales	14 (6 PWM[4])	22 (6 PWM)	36 (16 PWM)
Entradas/Salidas Analógicas	6	8	16
Memoria Flash	32 KB	32 KB	4 MB
Memoria SRAM[5]	2 KB	2 KB	520 KB
Velocidad de Reloj	16 MHz	16 MHz	160-240 MHz
Tamaño	53x75 mm	18x45 mm	24x55mm

Cuadro 3.2: Placas de desarrollo microcontrolador.

- Por último, fueron necesarias distintas llaves NFC para los registros y pruebas del sistema.

Identificador HEX	**Tipo**
B7 E9 31 63	Tarjeta
39 AA 94 A3	Llavero
04 2E 00 F2 A0 65 85	Pegatina

Cuadro 3.3: Llaves NFC.

3.3.2. Medios Software

Los Medios Software que han sido necesarios para el correcto desarrollo del proyecto se desarrollan a continuación.

C *C* es un lenguaje de programación de propósito general de tipo débil y estático, orientado a la implementación de sistemas operativos como *Unix*.

Arduino IDE *Arduino IDE* es el entorno de desarrollo integrado de Arduino, pensado para programar y compilar programas para las placas de desarrollo compatibles.

Fritzing *Fritzing* es un programa libre de automatización de diseños electrónicos utilizado para los diseños de cableados, tanto de los prototipos como de las PCB finales.

Git *Git* es un software de control de versiones, pensando en la eficiencia y la confiabilidad del mantenimiento de versiones de aplicaciones cuando éstas tienen un gran número de archivos de código fuente [Swi08].

LaTex *Latex* es un sistema de composición de textos, orientado a la creación de documentos escritos que presenten una alta calidad tipográfica [Lam94]. La elaboración de la presente documentación fue elaborada en formato *Latex*, con el compilador TeXstudio.

[5]Pulse Width Modulation (PWM)
[5]Static Random Access Memory (SRAM)

Notepad++ *Notepad++* es un editor de texto y de código fuente libre con soporte para varios lenguajes de programación. Este editor fue utilizado para el desarrollo en C del módulo PAM y para labores menores de edición, tales como la web final del producto.

SourceTree *SourceTree* es un cliente gratuito de *Mercurial* y *Git* para *Windows* y *Mac* que ofrece una interfaz gráfica para tus repositorios de *Hg* y *Git*. Mediante este software se gestionó el repositorio en el que está alojado el proyecto.

Balsamiq Mockups 3 Los diferentes diseños de bocetos elaborados a lo largo del desarrollo del proyecto han sido realizados con esta herramienta.

Corel Draw X8 *Corel Draw* es una herramienta de dibujo vectorial, la cual fue utilizada para los diseños de los diferentes logotipos e imágenes comerciales del proyecto.

Adobe Premiere Pro *Adobe Premiere* es una herramienta de edición de vídeo, usada para la creación de animaciones utilizadas como recursos en la pagina web.

Sony Vegas Pro 11 *Sony Vegas* se utilizó en la maquetación de un vídeo promocional para aumentar el impacto del proyecto en redes sociales.

CAPÍTULO 4
Resultados

En este capítulo, se presenta en detalle los resultados obtenidos a lo largo del desarrollo del proyecto. Un pequeño contexto de aplicación del mismo y de los resultados obtenidos para posteriormente entrar en profundidad en la evolución y despliegue del sistema. Por último, se presentan los resultados de la evaluación de usabilidad y un estudio del mismo, al igual que el feedback recogido.

4.1 Contexto

Como ya hemos visto anteriormente en el presente documento, este proyecto se enmarca en el contexto de simplificación de la acción de autenticación de equipos informáticos gracias al uso de dispositivos o llaves NFC.

El módulo encargado de la autenticación es el módulo PAM Este módulo inicia la comunicación con el lector y recibe los datos de la tarjeta leída. Como podemos ver en la Figura 4.1 el módulo además de comprobar si la tarjeta esta autorizada o no, deja constancia en un registro de las acciones ejecutadas por el lector y el propio módulo.

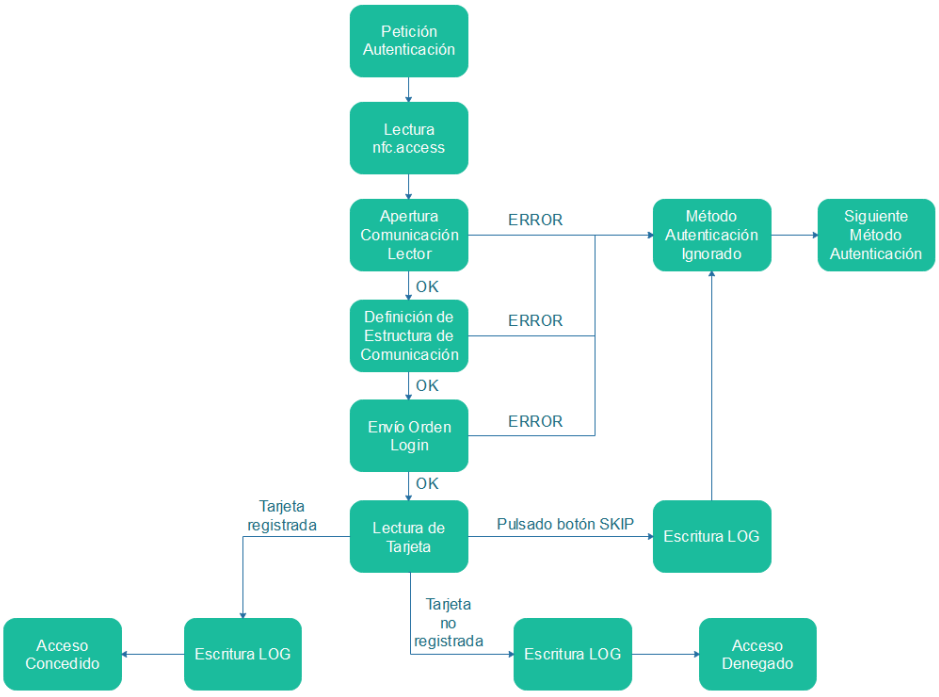
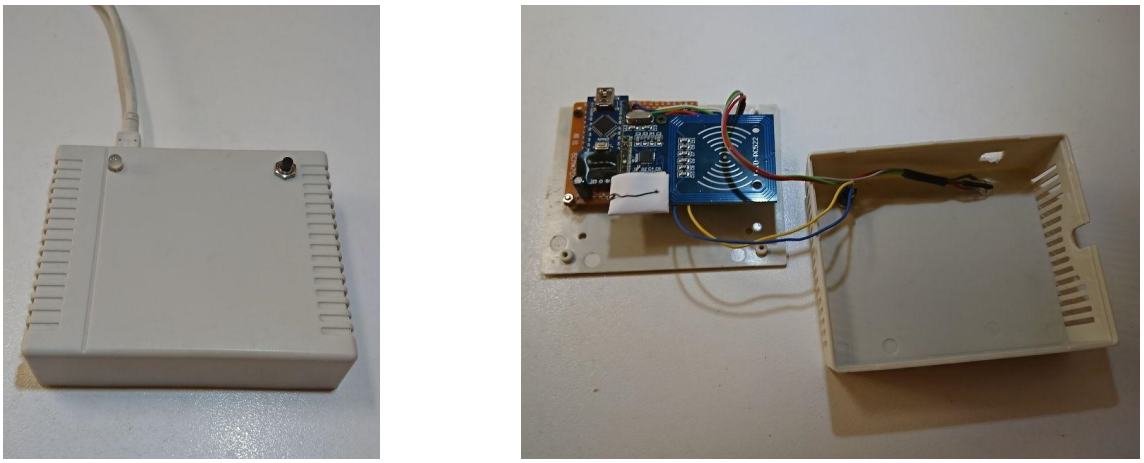


Figura 4.1: Diagrama de acciones del módulo PAM.

El lector de llaves NFC (Figura 4.2) es el encargado de recibir la orden de lectura del módulo PAM y de proceder a la misma, para después, enviar el resultado al módulo. El lector, diseñado a medida, está compuesto por un *Arduino Nano*, un módulo NFC, un zumbador y un LED bicolor. De esta forma, el software ejecutado en el lector ha podido ser diseñado a medida bajo las demandas del módulo PAM.



(a) Vista frontal **(b)** Vista interior

Figura 4.2: Lector de llaves NFC

A modo de conclusión de lo tratado anteriormente en el Capítulo 3, a lo largo del proyecto se ha podido seguir un desarrollo metódico que se ve culminado con el lanzamiento tanto del módulo de autenticación PAM como de la construcción y programación del lector de llaves NFC.

Por último, cabe destacar que gracias a la posibilidad de obtener registros de los intentos de uso y autenticación, es posible encontrar intentos de accesos ilícitos a los sistemas informáticos en los cuales está instalado dicho sistema de autenticación.

4.2 Evaluación de Usabilidad

En total, han sido 10 personas las que han evaluado este proyecto, a continuación se detallarán los resultados obtenidos por cada uno de los grupos de encuestados (Perfil Técnico y Perfil NO Técnico). Tras esto, se procederá a realizar una evaluación global de los resultados.

Ambos grupos de encuestados han seguido el mismo procedimiento. Dado que ninguno conocía de la existencia de este proyecto, a modo de introducción se les ha leído un resumen que a grandes rasgos, cuenta los objetivos a alcanzar por este sistema.

Tras esto, se reparte una hoja de Cuestionario SUS (Véase Anexo B) en los cuales, además de las tablas de puntuación, existen unas pequeñas acciones que el usuario debe de realizar (Intentar identificarse correctamente, de forma incorrecta, etc.) Tras haber *testeado* el sistema, se procede a evaluarlos mediante las tablas de puntuaciones.

Además, se recoge el *feedback* de los encuestados, ya que estos proponen mejoras para el sistema.

4.2.1. Perfil Técnico

Los encuestados técnicos corresponden a personal docente e investigador de la Escuela Técnica Superior de Ingeniería Informática de Valencia y a alumnos de la misma escuela. El 80.0 % de los encuestados son varones, frente al 20.0 % de mujeres. El 80.0 % de los encuestados había usado o usa llaves *NFC* frente a un 20.0 % que no las usa frecuentemente. Las franjas de edad de los encuestados varían entre un 20.0 % de entre 18 y 24 años, un 40.0 % de entre 25 y 34 años, y un 40.0 % entre 35 y 64 años, no siendo ninguno de los encuestados mayor de 65 años.

A continuación se reflejan la nota de cada uno de los módulos por cada encuestado (véase Cuadro 4.1).

ID Encuestado	Media
1	90.0
2	77.5
3	92.5
4	85.0
5	95.0

Cuadro 4.1: Resultado de Cuestionario de Usabilidad a personal técnico.

Realizando la media de estos resultados obtenemos las siguientes puntuaciones (Cuadro 4.2).

Media
88.0

Cuadro 4.2: Media Cuestionario de Usabilidad a personal técnico.

4.2.2. Perfil NO Técnico

Los encuestados no técnicos corresponden a personas o familiares escogidos aleatoriamente. El 40.0 % de los encuestados son varones, frente al 60.0 % de mujeres. El 60.0 % de los encuestados había usado o usa llaves *NFC* frente a un 40.0 % que no lo usa frecuentemente. Las franjas de edad de los encuestados varían entre un 40.0 % de entre 18 y 24 años, un 40.0 % de entre 25 y 34 años, y un 20.0 % entre 35 y 64 años, no siendo ninguno de los encuestados mayor de 65 años.

A continuación se reflejan la nota de cada uno de los módulos por cada encuestado (véase Cuadro 4.3).

ID Encuestado	Media
6	82.5
7	92.5
8	75.0
9	80.0
10	95.0

Cuadro 4.3: Resultado de Cuestionario de Usabilidad a personal no técnico.

Realizando la media de estos resultados obtenemos las siguientes puntuaciones (Cuadro 4.4).

Media
85.0

Cuadro 4.4: Media Cuestionario de Usabilidad a personal no técnico.

4.2.3. Evaluación Global

Como se puede observar, no existe mucha discrepancia entre las notas obtenidas por los dos grupos, dejando la siguiente media (Cuadro 4.5).

Media
86.5

Cuadro 4.5: Media Cuestionario de Usabilidad.

Es importante ver el porcentaje de encuestados que habían utilizado una llave NFC con anterioridad, en concreto, un 70.0 % de personas que sí lo usan o han usado con frecuencia frente a un 30.0 % que no (Véase Figura 4.3).

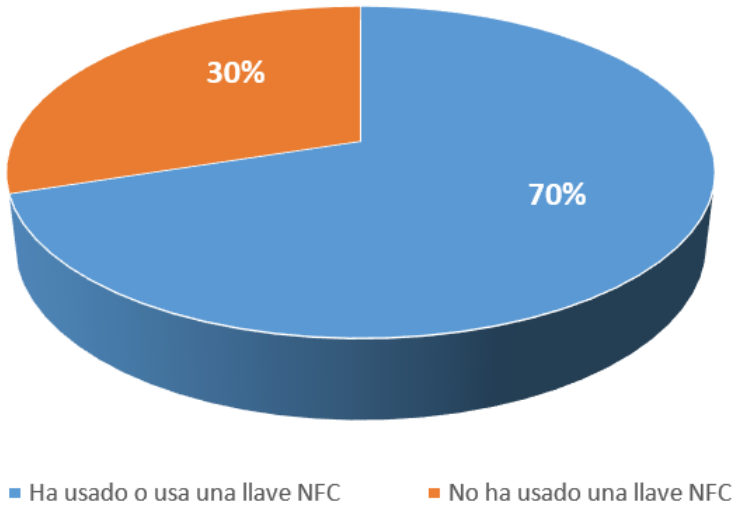


Figura 4.3: Gráfica de Uso de llaves NFC entre los encuestados.

Cabe destacar la lista de sugerencias que los encuestados han ido realizando a lo largo del proceso de evaluación del sistema, a continuación se exponen los diferentes aspectos en los que los usuarios ven puntos de mejora.

- Creación de herramienta para configuración de archivo nfc.access.
- Herramienta para consulta de fichero nfc_access.log
- Repetir señal sonora y lumínica cada cierto tiempo para recordar la espera de una acción por parte del usuario.
- Crear sistemas análogos para entornos Mac o Windows.
- Posibilidad de Usuarios centralizados.

Las sugerencias recogidas, se verán reflejadas en el Apartado de Trabajos Futuros 5.2, el cual, abre la posibilidad de continuar este proyecto por nuevas líneas de trabajo.

CAPÍTULO 5
Conclusiones

PARA acabar, analizamos el grado de consecución de los objetivos planteados al inicio del proyecto. Además, se dan a conocer las propuestas de trabajo futuro con el fin de mejorar y seguir completando el sistema.

5.1 Consecución de Objetivos

A continuación se justifica el cumplimiento de los objetivos específicos descritos en el Capítulo 1. Dichos objetivos han sido completados en su totalidad.

Escalabilidad y Expansión del Sistema El módulo PAM ha sido diseñado para poder permitir el acceso a cuantas llaves NFC estén contenidas en el archivo de configuración. De esta forma es posible añadir o eliminar accesos de forma sencilla.

Reglas F.C.I.D. El sistema de autenticación dentro del módulo PAM es el encargado de comprobar la numeración de una llave NFC y descartar aquellas que no concuerden.

Mecanismos de Reconocimiento El lector de llaves NFC ha sido dotado con diferentes salidas (Sonora y Lumínica) para captar la atención y reconocimiento del usuario cuando sea necesaria una acción por su parte o se tenga el resultado de la misma.

Comunicación La comunicación se establece mediante un bus serie, con el cual, establecemos un lenguaje propio y seguro entre el módulo de lectura de llaves NFC y el módulo de autenticación PAM.

Medidas Adicionales de Seguridad En este caso, se ha optado por dar la posibilidad de un único intento de autenticación mediante el sistema de llaves NFC teniendo además un pequeño retardo entre uso y uso, por lo que se hace inviable el lanzar ataques de, por ejemplo, fuerza bruta.

La consecución de los objetivos específicos antes descritos, llevan al cumplimiento del objetivo principal; **Facilitar el desbloqueo y acceso al ordenador mediante un elemento de identificación único como es una llave NFC**, quedando cumplido con el desarrollo del módulo lector de llaves NFC y el módulo de autenticación PAM.

5.2 Trabajo Futuro

A continuación, se describen las posibles vías de trabajo futuro que podría adoptar el proyecto.

Base de Datos (BBDD) centralizada Ampliando el objetivo de escalabilidad del proyecto, sería viable estudiar la incorporación de una posible BBDD de accesos a usuarios centralizada. De esta manera, al igual que se puede definir un servicio de autenticación con usuario y contraseña para acceder a distintos equipos conectados en red, se podría acceder a dichos equipos a los cuales una llave NFC tuviera acceso.

Generador de llaves NFC La tecnología NFC está implantada a tal nivel que no solo es fácil encontrarnos llaves NFC físicas, sino que son numerosos los fabricantes de dispositivos personales, tales como Dispositivos Móviles o Dispositivos *Wearable* que añaden la tecnología NFC a dichos dispositivos. De esta manera, se podría aprovechar esta capacidad mediante la creación de distintas aplicaciones generadoras de llaves NFC reconocibles por el módulo lector, permitiendo así poder identificarnos con la llave disponible en nuestro móvil o *wearable*.

Inclusión de Tecnologías Debido a que el proyecto tiene una alta carga de seguridad, es imprescindible abordar distintas tecnologías en lo que a esta materia se refiere. Por tanto, se propone incluir tecnologías de seguridad combinadas para hacer el sistema aun más robusto, tales como Llaves Universal Serial Bus (USB), *Tokens* o Sistemas de códigos cambiantes de un solo uso para cifrar contenido.

Bibliografía

[AFRMGMF06] Sadot Alexandres Fernández, Carlos Rodríguez-Morcillo García, and José Daniel Muñoz Frías. Rfid: La tecnología de identificación por radiofrecuencia. 2006.

[Arr04] Martín Arribas. Diseño y validación de cuestionarios. *Matronas profesión*, 5(17):23–29, 2004.

[Bla73] John V Blankenbaker. Kenbak-1 digital computer. *The Journal of Data Education*, 13(4):7–8, 1973.

[CKP06] Dario Carluccio, Timo Kasper, and Christof Paar. Implementation details of a multi purpose iso 14443 rfid-tool. In *Printed handout of Workshop on RFID Security-RFIDSec*, volume 6, 2006.

[Fin10] Klaus Finkenzeller. *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John wiley & sons, 2010.

[HK05] Gerhard P Hancke and Markus G Kuhn. An rfid distance bounding protocol. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 67–73. IEEE, 2005.

[iS07] Toni Granollers i Saltiveri. *MPIu+ a. Una metodología que integra la Ingeniería del Software, la Interacción Persona-Ordenador y la Accesibilidad en el contexto de equipos de desarrollo multidisciplinares*. Universitat de Lleida, 2007.

[Lam94] Leslie Lamport. *LATEX: a document preparation system: user's guide and reference manual*. Addison-wesley, 1994.

[LH94] Jaynarayan H Lala and Richard E Harper. Architectural principles for safety-critical real-time applications. *Proceedings of the IEEE*, 82(1):25–40, 1994.

[LZYX06] Dong-sheng Liu, Xue-cheng Zou, Qiu-ping Yang, and Ting-wen Xiong. An analog front-end circuit for iso/iec 15693-compatible rfid transponder ic. *Journal of Zhejiang University-Science A*, 7(10):1765–1771, 2006.

[MP88] JL Meliá and JM Peiró. *El cuestionario de satisfacción S10/12: Estructura factorial, fiabilidad y validez*. Colegio Oficial de Psicólogos de Madrid, 1988.

[MSV17] Alexander Maier, Andrew Sharp, and Yuriy Vagapov. Comparative analysis and practical implementation of the esp32 microcontroller module for the internet of things. In *2017 Internet Technologies and Applications (ITA)*, pages 143–148. IEEE, 2017.

[MT03] Yran Marrero Travieso. La criptografía como elemento de la seguridad informática. *Acimed*, 11(6):0, 2003.

[RílMS17] Normandi Rocío Tirado Ríos, Elsa Leuvany í lvarez Morales, and Stalin Daniel Carreño Sandoya. Seguridad informática, un mecanismo para salvaguardar la información de las empresas. *Revista Publicando*, 4(10 (2)):462–473, 2017.

[Rod16] Solórzano Andrés Medranda Rodríguez. Tecnología rfid al servicio de la logística. *Revista RETO: Revista Especializada En Tecnologías Transversales De La Organización*, 4(4):77–90, 2016.

[RRG+11] José Matías Rivero, Gustavo Rossi, Julián Grigera, Esteban Robles Luna, and Antonio Navarro. From interface mockups to web application models. In *International Conference on Web Information Systems Engineering*, pages 257–264. Springer, 2011.

[RVOG16] Jose Ramírez, Karina Villao, Omar Orrala, and Juan Garcés. Seguridad informática o seguridad personal, evolucionando con la tecnología. *Revista Científica y Tecnológica UPSE*, 3(2):113–117, 2016.

[Swi08] Travis Swicegood. *Pragmatic version control using Git*. Pragmatic Bookshelf, 2008.

[Tra03] Alejandro Hernández Trasobares. Los sistemas de información: evolución y desarrollo. *Proyecto social: Revista de relaciones laborales*, (10):149–165, 2003.

APÉNDICE A
Diseño Electrónico

Diagrama *Protoboard* de Lector de llaves NFC

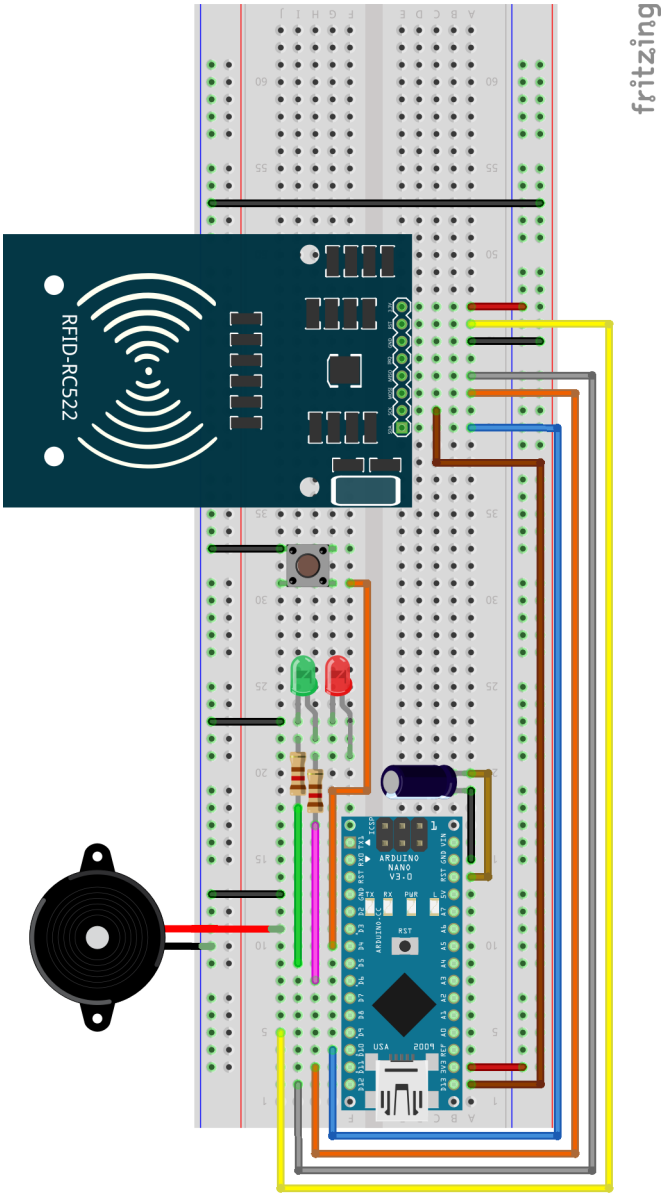


Figura A.1: Diagrama *Protoboard* de Lector de llaves NFC

Diagrama PCB de Lector de llaves NFC

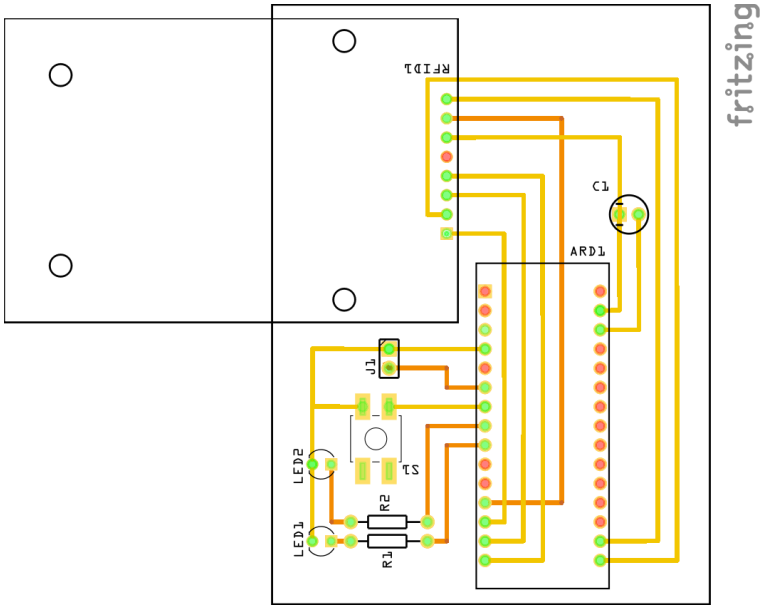


Figura A.2: Diagrama PCB de Lector de llaves NFC

APÉNDICE B

Cuestionario SUS

Dispositivo NFC para autenticación de usuarios en Linux
Proyecto NFCUnlock

Fecha: ____/____/____

Edad:

18 a 24	25 a 34	35 a 64	65 >

Sexo

Hombre	Mujer

Has usado/usas alguna llave NFC:

Si	No

A continuación, encontrará una serie de preguntas destinadas a conocer su opinión sobre diversos aspectos de la usabilidad del Proyecto NFCUnlock.

El cuestionario tiene una sección correspondiente al módulo del Proyecto. Por favor lea las instrucciones al inicio y conteste la alternativa que más se acerca a lo que usted piensa. Sus respuestas son confidenciales y serán reunidas para valorar la usabilidad del sistema. Muchas gracias.

MODULO 1: LECTOR NFC

Su tarjeta de acceso tiene la numeración: B7E93163
Se le pide que además de probar a autenticarse correctamente, simule una autenticación errónea con otra tarjeta (numeración 39AA94A3) y que simule que no dispone de ninguna tarjeta y obvie el método de autenticación con llaves NFC.

Preguntas	Grado de Acuerdo				
	Total desacuerdo	En desacuerdo	Ni acuerdo ni desacuerdo	De acuerdo	Total acuerdo
Usaría este sistema de forma frecuente.	1	2	3	4	5
Veo este sistema demasiado complejo.	1	2	3	4	5
La forma de autenticarse es intuitiva y fácil de usar.	1	2	3	4	5
Creo que necesitaría ayuda (Un técnico o un manual) para usar el sistema.	1	2	3	4	5
Este sistema es para cualquier tipo de persona.	1	2	3	4	5
He necesitado aprender algo para ser capaz de usar este sistema.	1	2	3	4	5
Entiendo el funcionamiento del sistema.	1	2	3	4	5
He tardado mucho en realizar las operaciones indicadas.	1	2	3	4	5
El tiempo de respuesta del sistema es aceptable.	1	2	3	4	5
Veo este sistema innecesario.	1	2	3	4	5

APÉNDICE C
Manual de Usuario

Compilación

En primer lugar, se detallan las instrucciones para la correcta instalación de las librerías necesarias para el proceso de compilación y el proceso mismo.

Ha sido preparado un *script* de instalación para facilitar la tarea mencionada anteriormente. Haciendo uso del comando C.1 se ejecutará dicho proceso.

```
$ ./need_to_compile.sh
```

Listing C.1: Comando de Instalación de Librerias de Compilación.

Una vez listas las librerías de seguridad necesarias, es posible compilar el módulo PAM mediante el comando C.2 siendo también necesario el comando C.3 para poder añadir el módulo PAM compilado a la lista de métodos PAM disponibles.

```
$ gcc -fPIC -fno-stack-protector -c nfc_pam.c
```

Listing C.2: Comando de Compilación Módulo PAM.

```
$ sudo ld -x --shared -o /lib/security/nfc_pam.so nfc_pam.o
```

Listing C.3: Comando de Insercción Módulo PAM en Sistema.

Todo este proceso de compilación y inserción en la lista de módulos PAM del sistema ha sido simplificado con la creación de un *script* (Comando C.4).

```
$ ./only_compile.sh
```

Listing C.4: Comando de Instalación de Librerias de Compilación.

Instalación

A continuación, se detallan los pasos para realizar la instalación del módulo PAM. Para simplificar esta acción, se ha creado un *script* que se ejecutará con el comando C.5.

```
$ sudo ./install.sh
```

Listing C.5: Comando de Insercción Módulo PAM en Sistema.

Por último, debemos de editar la primera línea del archivo */var/nfc.access* . En esta línea debemos de especificar el puerto *ttyUSB* en el que este el lector NFC (Normalmente *ttyUSB0*).

Uso

Por último, se detallan las instrucciones de uso de los diferentes apartados o funcionalidades del sistema.

Gestión de Tarjetas

El archivo */var/nfc.access* visto anteriormente, además de ser el encargado de definir el puerto *ttyUSB* en el que se espera al lector NFC, sirve también para definir las tarjetas que tienen acceso al sistema.

En concreto, a partir de la segunda línea podemos definir tarjetas para que así tengan concedido el acceso (Véase la figura C.1 como ejemplo).

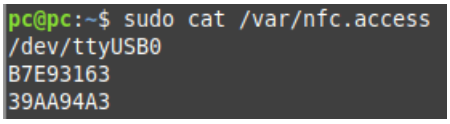


Figura C.1: Ejemplo de configuración archivo */var/nfc.access* .

Autenticación

En caso de que sea necesaria una autenticación (ya sea por inicio de sesión o por necesidad en el equipo o terminal) el primer método configurado tras la instalación sera el método NFC. Una vez se inicie la petición de autenticación y la misma llegue al lector NFC este se iluminará en rojo y emitirá un pitido, indicando así al usuario que espera una acción por su parte.

Llegados a ese punto el usuario puede obviar la autenticación pulsando el botón de omisión (lo que dará paso a un intento de autenticación con el siguiente método disponible en la cola PAM) o acercar una tarjeta a la zona superior del lector NFC. De esta forma, la tarjeta será leída (podrá observarse la luz verde que indica esta lectura) y enviada al módulo de autenticación el cual determinara si la tarjeta es aceptada o no.

En caso afirmativo, la autenticación se resolverá como aceptada y se permitirá el acceso (ya sea desbloquear el equipo o ejecutar la acción determinada), en caso negativo, se avisará de que la tarjeta leída no esta reconocida y se probará el siguiente método de autenticación para intentar resolver la petición.

Consulta de Histórico

En caso de querer consultar el histórico de acciones realizadas (Tanto accesos concedidos, denegados, o omisiones del lector NFC), debemos de tener permisos *root* o de superusuario. Para poder consultar el histórico, simplemente debemos hacer un *cat* al archivo */var/nfc.access* (Comando C.6).

```
1 $ sudo cat /var/nfc.access
```

Listing C.6: Comando de Consulta Histórico.

Ademas, es posible combinar la salida del comando *cat* con otros como el comando *grep* a través del uso de tuberías. De esta forma, podemos filtrar los resultados del histórico por fecha u hora (Figura C.2), por tipo de acción (Figura C.3), o por numeración de tarjeta (Figura C.4).

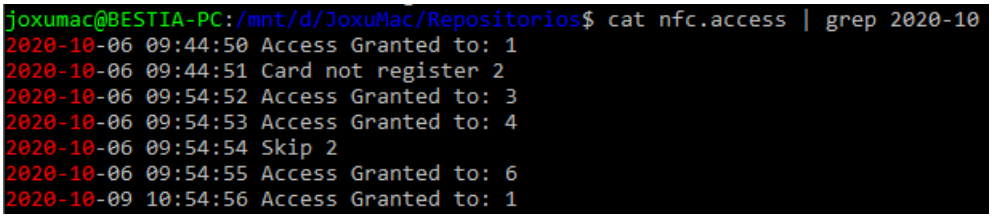


Figura C.2: Ejemplo de filtrado por fecha u hora.

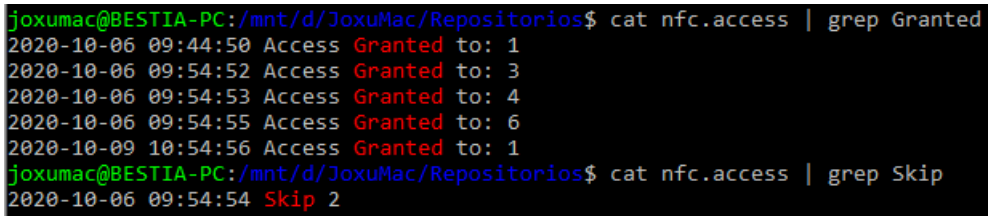


Figura C.3: Ejemplo de filtrado por tipo de acción.

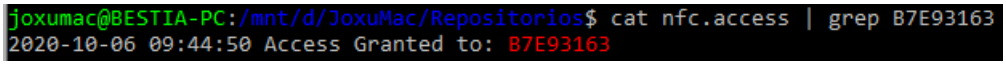


Figura C.4: Ejemplo de filtrado por Tarjeta.

APÉNDICE D
Contenido del CD

Con el presente documento (formato físico) se adjunta un CD que contiene el material desarrollado durante el transcurso del proyecto. En el mismo, se incluye este mismo documento en formato electrónico y códigos fuentes de los diferentes módulos.

A continuación, se lista el contenido proporcionado.

Documentación Electronica El presente documento en formato electrónico.

Diseño Hardware Diseños PCB y esquemas electrónicos para la construcción de un lector NFC.

Módulo PAM Módulo de autenticación PAM para Sistema Operativo *Linux*.

Lector NFC El código fuente del lector NFC basado en *Arduino*.