
**UNIVERSIDAD DE CASTILLA-LA MANCHA**

**ESCUELA SUPERIOR DE INGENIERÍA INFORMÁTICA**

Departamento de Sistemas Informáticos


**MÁSTER EN FORMACIÓN PERMANENTE EN CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN**

**TRABAJO FIN DE MÁSTER**

# Análisis de la Seguridad en Tecnologías de Identificación y Control de Acceso: Banda Magnética, RFID y NFC


Autor: Isidro Benítez Zapico

Director: Álvaro Núñez Romero Casado


**Junio, 2026**

# Abstract

This Master's Thesis presents a technical and practical analysis of vulnerabilities in magnetic stripe, RFID, and NFC-based card technologies, commonly used in financial, access control, transportation, and identification systems. The study examines the architectural evolution from passive static storage media to embedded devices with computational and cryptographic capabilities and analyzes how this evolution has reshaped the attack surface rather than eliminating risk.

A structured framework is adopted to classify vulnerabilities into structural, protocol-level, and implementation-related weaknesses. A realistic adversary model is defined, assuming capabilities such as wireless interception, replay and relay of communications, temporary physical access, and the use of commercially available tools, while excluding advanced cryptanalytic attacks against robust algorithms.

Beyond theoretical analysis, this work evaluates the practical exploitability of identified weaknesses and includes controlled exploitation scenarios to demonstrate real operational impact. The research focuses particularly on threats affecting authenticity and integrity, such as functional cloning, credential emulation, protocol manipulation, and cryptographic key extraction derived from flawed implementations. In addition, relay attacks are discussed from a theoretical perspective as a relevant threat in RFID and NFC environments.

The thesis also critically assesses the limits of cryptographic protection in smart cards and NFC systems. While dynamic authentication mechanisms mitigate traditional cloning attacks, many real-world compromises stem from design assumptions, poor key management, protocol weaknesses, or implementation errors rather than from fundamental cryptographic breaks.

Finally, based on the experimental findings, security improvements and mitigation strategies are proposed to reduce practical exploitability and strengthen future card-based system deployments.

# Resumen

Este Trabajo Fin de Máster aborda un análisis técnico y experimental de las vulnerabilidades presentes en tecnologías de tarjetas basadas en banda magnética, RFID y NFC, ampliamente utilizadas en sistemas de pago, control de acceso, transporte e identificación. El estudio pone especial énfasis en la evolución de estos sistemas, desde soportes pasivos de almacenamiento estático hasta dispositivos inteligentes con capacidades de procesamiento y mecanismos criptográficos, evidenciando que dicha evolución no elimina los riesgos, sino que transforma la superficie de ataque.

Para ello, se adopta un enfoque estructurado que clasifica las vulnerabilidades en función de su origen, distinguiendo entre debilidades estructurales, fallos a nivel de protocolo y errores de implementación. Asimismo, se define un modelo de adversario realista, considerando capacidades como la interceptación inalámbrica, la repetición y retransmisión de comunicaciones, el acceso físico temporal y el uso de herramientas accesibles.

Más allá del análisis teórico, el trabajo incorpora una evaluación práctica de la explotabilidad de estas vulnerabilidades mediante experimentación en entornos controlados, desarrollando escenarios de ataque que permiten demostrar su impacto real, centrándose principalmente en amenazas que comprometen la autenticidad y la integridad, como la clonación funcional, la emulación de credenciales, la manipulación de protocolos y la recuperación de claves, incorporando además el análisis teórico de vectores como los ataques de relay. Del mismo modo, se analizan los límites de la protección criptográfica en tarjetas inteligentes y sistemas NFC, evidenciando que muchos ataques exitosos no se deben a la ruptura de algoritmos, sino a decisiones de diseño, una gestión inadecuada de claves o errores de implementación.

Finalmente, a partir de los resultados obtenidos, se proponen medidas orientadas a reducir la explotabilidad de estas tecnologías y reforzar la seguridad en futuros sistemas basados en tarjetas.

# Agradecimientos

En primer lugar, me gustaría agradecer a mi tutor, **Álvaro Núñez Romero Casado**, su tiempo, interés y dedicación a lo largo de este trabajo, así como la confianza depositada en mí.

A la **Universidad de Castilla-La Mancha**, por ofrecer una formación tan extensa y avanzada que, gracias a **INCIBE**, ha podido llegar a muchas personas.

También quiero agradecer al equipo de **ciberseguridad del Centro de Gestión de Servicios Informáticos (CGSI)**, durante mi paso por la Beca Talentum de Telefónica, por hacerme sentir parte del equipo y permitirme compatibilizar mis prácticas con mis estudios. En especial, a **Pablo**, mi tutor, por ayudarme siempre que lo he necesitado, y a **Jessica**, mi responsable en el equipo durante la beca, por tenerme siempre en cuenta y fomentar mi iniciativa.

Agradezco con mucho cariño a **Bego**, por apoyarme siempre a lo largo de este camino y alimentar todas y cada una de mis alocadas ideas. No podría sentirme más afortunado.

A mi familia, en especial a **Cris** y a **mis padres**, por creer en mí cada día y estar siempre presentes en mi vida. Y a **Kira**, mi gata, por su compañía y amor incondicional durante todos estos años.

Finalmente, a mi amigo **Isra**, con quien compartí unos cuantos años jugando con las tarjetas MIFARE *Classic* del Consorcio de Transportes de Asturias (CTA). Todos esos momentos han sido la inspiración y el empujón final para realizar este trabajo.

**Gracias a todos por haber formado parte de este camino.**

# Índice de contenidos

# Índice de figuras

# Nota de Responsabilidad

Este trabajo tiene un propósito puramente académico y de investigación en el ámbito de la ciberseguridad. En ningún caso se promueve, recomienda ni justifica el uso de técnicas de clonación u alteración de tarjetas, carding, skimming u otras formas de fraude con fines ilícitos, fraudulentos o malintencionados. Se han analizado diversas tecnologías de identificación por banda magnética, radiofrecuencia y comunicación de campo, sus nombres y detalles específicos han sido deliberadamente censurados para evitar su promoción o distribución indebida.

Todos los ejemplos incluidos en este trabajo han sido modificados o anonimizados con el objetivo de presentar únicamente vulnerabilidades de diferentes sistemas, sin facilitar su implementación práctica. Es importante recordar que las prácticas de suplantación de identidad y fraude u otros tipos de engaños son ilegales en muchas jurisdicciones y pueden constituir delitos penales. Se recomienda a cualquier persona interesada que consulte la legislación vigente en su país antes de intentar cualquier implementación práctica.

# 1. Introducción

Desde su adopción masiva en la década de 1970, la banda magnética (basada en la norma ISO/IEC 7811) ha constituido el pilar fundamental de los sistemas de identificación financiera, autenticación y control de acceso en entornos corporativos, comerciales y gubernamentales. Su simplicidad estructural, bajo coste de fabricación y facilidad de integración con infraestructuras existentes favorecieron su rápida estandarización y expansión global. Durante décadas, este modelo permitió la interoperabilidad entre entidades bancarias, sistemas de pago y control físico sin requerir capacidades de procesamiento en el propio soporte.

Sin embargo, dicha simplicidad implica limitaciones estructurales significativas, la banda magnética se basa en un almacenamiento estático de datos, donde la información se registra de forma permanente y se transmite sin mecanismos de cifrado o autenticación. Esta arquitectura facilita ataques de lectura no autorizada, clonación y reproducción, dado que la seguridad depende principalmente de controles externos al medio físico. En consecuencia, la protección se traslada a los sistemas internos, dejando expuesto el canal físico frente a adversarios con capacidades relativamente modestas.

La creciente digitalización de servicios financieros y la evolución de las diferentes amenazas impulsaron la transición hacia tecnologías basadas en radiofrecuencia, especialmente RFID (*Radio Frequency Identification*) y, posteriormente, NFC (*Near Field Communication*). A diferencia de la banda magnética, estas tecnologías introducen un modelo de interacción basado en comunicación inalámbrica bidireccional, permitiendo no solo la lectura de datos sino también la ejecución de protocolos de autenticación y, en determinados casos, operaciones criptográficas en tiempo real dentro del propio dispositivo.

Esto representa un cambio de concepto donde se pasa de un soporte pasivo de almacenamiento a un sistema embebido con capacidad computacional.

Las tarjetas inteligentes y los dispositivos sin contacto (*contactless)* modernos incorporan microcontroladores, memoria protegida y módulos criptográficos capaces de implementar algoritmos simétricos y asimétricos, autenticación mutua y generación de códigos dinámicos permitiendo mitigar amenazas clásicas asociadas a la clonación directa.

Sin embargo, la incorporación de capacidad computacional no elimina el riesgo, sino que transforma la superficie de ataque. Las vulnerabilidades dejan de centrarse exclusivamente en la copia física de datos para trasladarse al análisis de protocolos, a la implementación criptográfica, a la gestión de claves y a ataques de canal lateral o *relay*. En este contexto, la seguridad ya no depende únicamente del medio físico, sino del diseño integral del sistema, incluyendo *firmware*, estándares de comunicación, infraestructura interna y modelo de amenazas considerado.

La coexistencia actual de sistemas de banda magnética, tarjetas inteligentes con contacto, RFID de distintas frecuencias y soluciones NFC en entornos financieros y de control de acceso genera un ecosistema heterogéneo donde conviven distintos niveles de protección y exposición. Analizar sus fundamentos técnicos, sus mecanismos de seguridad y sus vulnerabilidades inherentes permite evaluar de forma objetiva el grado real de resiliencia frente a ataques contemporáneos.

## 1.1. Motivación

Los fraudes financieros como el robo y clonación de tarjetas de crédito, conocidos como *carding* y *skimming* existen desde la implantación de las primeras tarjetas de crédito y acceso en sistemas de seguridad físicos como medio de autenticación generalizado.

Actualmente, algunos de los usos más habituales en las tarjetas y dispositivos basados en estas tecnologías se utilizan en:

- **Sector financiero**: tarjetas de crédito/débito con banda magnética, chip EMV y pagos contactless.

- **Transporte público**: abonos y billetes inteligentes (metro, autobús, tren).
- **Control de accesos físicos**: credenciales corporativas, universitarias y hoteleras, así como sistemas de acceso residencial en portales de viviendas, urbanizaciones privadas y comunidades de propietarios.
- **Sanidad**: tarjetas sanitarias electrónicas con datos de identificación del paciente.
- **Identificación gubernamental**: DNI electrónicos y documentos oficiales.
- **Sistemas de fidelización y retail**: tarjetas de cliente para acumular puntos y descuentos.
- **Control horario laboral y sistemas de presencia.**
- **Peajes y aparcamientos automatizados.**
- **Sistemas IoT y domótica:** la autenticación por proximidad se integra con infraestructuras inteligentes.

Esta amplia presencia en sectores cotidianos hace que cualquier vulnerabilidad en estas tecnologías pueda tener consecuencias económicas, operativas y reputacionales. Además, la coexistencia de sistemas heredados con soluciones más modernas provoca que la seguridad global dependa, en muchas ocasiones, del componente más débil de la infraestructura.

Por este motivo, el presente trabajo se motiva por la necesidad de analizar el funcionamiento, los mecanismos de protección y las vulnerabilidades de la banda magnética, RFID y NFC desde una perspectiva técnica y práctica. El objetivo es evaluar su grado real de seguridad frente a amenazas como la lectura no autorizada, la clonación funcional, la emulación de credenciales, la manipulación de protocolos y la recuperación de claves, proponiendo finalmente medidas que permitan reducir su exposición.

## 1.2. Alcance y objetivos del trabajo

El presente trabajo tiene como alcance el estudio técnico y de seguridad de las tecnologías de banda magnética, RFID y NFC, ampliamente utilizadas en sistemas de identificación, autenticación y pago. El análisis se centra en los fundamentos físicos y electrónicos, en los modelos de almacenamiento de datos, sus protocolos de comunicación y en los mecanismos de protección incorporados en cada arquitectura.

Se abordará la evolución conceptual desde soportes de almacenamiento estático hasta dispositivos con capacidad computacional y criptográfica, evaluando cómo se ha modificado la superficie de ataque y el modelo de amenazas asociado.

El objetivo principal es analizar de forma sistemática las vulnerabilidades inherentes a cada tecnología, identificando sus debilidades, errores de diseño y posibles fallos de implementación. Se estudiarán los vectores de ataque más relevantes, incluyendo técnicas de clonación, lectura no autorizada, emulación de credenciales, manipulación de protocolos, extracción de claves y explotación de deficiencias en la gestión criptográfica. Adicionalmente, se analizarán de forma teórica amenazas avanzadas como los ataques de relay, debido a su relevancia en sistemas RFID y NFC modernos.

El enfoque no se limita a describir las vulnerabilidades, sino que examina los principios técnicos que permiten su explotación, con el fin de comprender el impacto real que pueden tener en entornos operativos. Asimismo, el trabajo persigue establecer medidas y recomendaciones orientadas a la securización de sistemas basados en estas tecnologías. Para ello, se analizarán diferentes estrategias de mitigación tanto a nivel de diseño arquitectónico como de configuración e integración en infraestructuras más amplias.

El propósito final es determinar el grado de seguridad que ofrecen estos sistemas frente a las amenazas actuales y evaluar si su adopción responde a criterios sólidos de resiliencia o a inercias tecnológicas heredadas.

# 2. Estado del Arte

Es fundamental comprender el contexto histórico, el funcionamiento técnico y la evolución de las tecnologías de banda magnética, identificación por radiofrecuencia (RFID) y comunicación de campo cercano (NFC) para poder analizar de manera rigurosa y fundamentada las vulnerabilidades inherentes a cada una de ellas.

## 2.1. Arquitectura y limitaciones de la Banda Magnética

La tecnología de banda magnética es uno de los primeros sistemas de almacenamiento portátil utilizado masivamente en entornos financieros, comerciales y de control de acceso. Normalizado bajo el estándar ISO/IEC 7811 (*ISO/IEC 7811-1*, s. f.) tiene interoperabilidad internacional entre los diferentes emisores, lectores y sistemas de procesamiento. Esto ha favorecido su adopción global desde la década de 1970.

El principio de funcionamiento se basa en el almacenamiento de información mediante variaciones de flujo registradas a lo largo de distintas pistas longitudinales integradas en la tarjeta. Dichas variaciones representan datos binarios conforme a esquemas de codificación definidos en el estándar correspondiente.

Una de las características más relevantes de esta tecnología es su naturaleza pasiva, las tarjetas de este tipo no poseen capacidad de procesamiento, memoria dinámica ni mecanismos criptográficos. Únicamente almacena información de forma estática y se transmite al lector sin ningún tipo de cifrado o autenticación. Como consecuencia la seguridad reside en los mecanismos de validación de los sistemas *backend*.

### 2.1.1. Limitaciones estructurales

Diferentes investigaciones y análisis técnicos (Svigals, 2012) han demostrado que las vulnerabilidades en la banda magnética no tienen como origen errores de implementación sino fallos inherentes a nivel de diseño. Entre las principales vulnerabilidades destacan las siguientes:

- **Almacenamiento estático de datos:** la información no varía entre transacciones.
- **Ausencia de autenticación mutua:** el lector no verifica criptográficamente la autenticidad de la tarjeta.
- **Transmisión en claro:** los datos pueden ser capturados sin necesidad de romper mecanismos criptográficos.
- **Dependencia de controles externos:** la protección se traslada a sistemas antifraude posteriores a la transacción.

Estas características facilitaron la aparición de técnicas como la clonación directa (Scaife et al., 2018), el robo de información y la reproducción de credenciales. Diversos estudios (Sakharova, 2012) han demostrado que la captura de datos requiere únicamente acceso físico al canal, con dispositivos de bajo coste y conocimientos técnicos moderados.

### 2.1.2. Impacto en el sistema financiero y transición tecnológica

El incremento del fraude asociado a tarjetas de banda magnética motivó el desarrollo de soluciones con capacidades criptográficas, dando lugar a la adopción de tarjetas inteligentes bajo el estándar EMV (Europay, Mastercard y Visa) (*Enabling Seamless and Secure Payments Worldwide*, s. f.).

La transición respondió únicamente a la necesidad de incorporar autenticación dinámica, sino también a la creciente sofisticación de los ataques. Sin embargo, la coexistencia de sistemas heredados y arquitecturas modernas generó nuevos escenarios de riesgo, como los mecanismos de retroceso hacia la banda magnética cuando el chip no puede ser procesado. Diversos estudios (Murdoch et al., 2010) han señalado que esta convivencia tecnológica introduce superficies de ataque híbridas, donde la seguridad global queda condicionada por el componente más débil del sistema.

## 2.2. Arquitectura y limitaciones de RFID

La tecnología de identificación por radiofrecuencia (Radio Frequency Identification) se consolidó como una evolución de los sistemas de identificación automática sin contacto físico, ampliando las capacidades de la banda magnética al permitir lectura remota y, en algunos casos, interacción con el dispositivo.

Su adopción se ha extendido a entornos como logística, transporte, control de acceso y pagos electrónicos, aprovechando su facilidad de integración y bajo coste de implementación. Los estándares internacionales ISO/IEC 14443 de corto alcance (*ISO/IEC 14443-1:2018 - Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics*, s. f.) e ISO/IEC 15693 largo alcance (*ISO/IEC 15693-1*, s. f.), han garantizado la interoperabilidad entre lectores, etiquetas y sistemas *backend*.

Desde el punto de vista funcional, un sistema RFID se compone de una etiqueta y un lector, comunicándose mediante un enlace inalámbrico, basado en acoplamiento inductivo. Las etiquetas pueden ser pasivas, obteniendo energía únicamente del campo del lector, o activas, incorporando una fuente de alimentación propia que permite un mayor alcance y almacenamiento de datos. La información se transmite mediante técnicas de modulación, como *Amplitude Shift Keying* (ASK), y mediante retrodispersión (*backscatter*) para las etiquetas pasivas.

### 2.2.1. Vulnerabilidades y limitaciones de seguridad

Está documentado por diversos estudios (Grover & Berghel, s. f.) que los sistemas RFID presentan diferentes limitaciones que pueden ser explotadas por atacantes:

- **Ausencia de cifrado por defecto:** muchas etiquetas básicas transmiten información sin protección criptográfica.
- **Falta de autenticación mutua:** el lector no valida de manera robusta la identidad de la etiqueta.

- **Exposición a ataques inalámbricos:** es posible interceptar la comunicación (*eavesdropping*) o retransmitirla mediante ataques de relay.
- **Dependencia del *backend*:** la seguridad depende del procesamiento centralizado, no de la propia etiqueta.

Estas limitaciones evidencian que, aunque RFID ofrece ventajas frente a la banda magnética, su seguridad depende en gran medida del diseño del sistema y de la infraestructura de soporte.

## 2.3. NFC: Principios y desafíos

La comunicación de campo cercano *Near Field Communication* (NFC) surge como una evolución de los sistemas RFID de alta frecuencia, orientada a entornos que requieren interacción rápida, segura y de muy corto alcance. Su diseño está optimizado para distancias inferiores a 10 centímetros, lo que reduce la superficie de exposición inalámbrica en comparación con otras tecnologías de radiofrecuencia.

NFC se fundamenta en los estándares ISO/IEC 14443 y en las especificaciones promovidas por el NFC Forum [12], garantizando interoperabilidad entre dispositivos móviles, tarjetas inteligentes y terminales de pago. Su integración en smartphones ha impulsado su adopción masiva en pagos electrónicos, transporte público, control de accesos y servicios digitales. A diferencia de RFID convencional, NFC permite una comunicación bidireccional más flexible, lo que amplía sus posibilidades funcionales y su integración en ecosistemas digitales complejos.

### 2.3.1. Modos operativos y modelo funcional

NFC define tres modos principales de funcionamiento:

- **Modo lector/escritor:** el dispositivo actúa como lector de etiquetas NFC.
- **Modo emulación de tarjeta:** el dispositivo se comporta como una tarjeta inteligente sin contacto.
- **Modo *peer-to-peer* (P2P):** dos dispositivos intercambian información directamente.

Desde el punto de vista arquitectónico, NFC puede implementar entornos de ejecución protegidos dentro del dispositivo o delegar la lógica de emulación en el sistema operativo. Esta flexibilidad funcional convierte a NFC en una tecnología más compleja que RFID tradicional, al depender no solo del medio físico de comunicación, sino también del ecosistema software y de la infraestructura.

### 2.3.2. Limitaciones y riesgos

A pesar de las mejoras incorporadas respecto a tecnologías anteriores, existen diferentes vulnerabilidades en la tecnología NFC:

- **Ataques de *relay*:** retransmisión de la comunicación para extender artificialmente la distancia entre tarjeta y lector.
- **Intercepción de comunicaciones:** aunque el alcance es reducido, la señal puede ser capturada con equipamiento especializado.
- **Dependencia del entorno *software*:** vulnerabilidades en el sistema operativo o en la implementación del protocolo pueden afectar la seguridad global.
- **Compatibilidad con infraestructuras heredadas:** la interacción con sistemas menos robustos puede introducir riesgos indirectos.

Los estudios (Veniamin Ginodman & Azhari, 2014) coinciden en que la seguridad de NFC no depende únicamente del corto alcance físico, sino del diseño integral del sistema, incluyendo la gestión criptográfica, la arquitectura del dispositivo y la configuración del backend.

## 2.4. Criptografía

La criptografía es un componente vital en la seguridad de las tecnologías de identificación y pago modernas, especialmente en sistemas que incorporan capacidad computacional, como tarjetas inteligentes EMV y dispositivos NFC. Su función es proteger la confidencialidad, integridad y autenticidad de la información, mitigando riesgos asociados a la captura, reproducción o manipulación de datos.

Dependiendo de la forma en que se gestionan las claves, los algoritmos criptográficos se dividen en simétricos, que utilizan la misma clave para cifrar y descifrar, y asimétricos, que emplean pares de claves públicas y privadas para proteger la información.

### 2.4.1. Algoritmos simétricos

Son aquellos que utilizan la misma clave para cifrar y descifrar la información. Tienen uso en sistemas de pago y control de acceso para autenticar transacciones, generar códigos de un solo uso (OTP) y proteger la comunicación entre la tarjeta y lector. Su principal ventaja es su velocidad y bajo coste computacional, aunque requieren de un mecanismo seguro para la distribución y almacenamiento de claves.

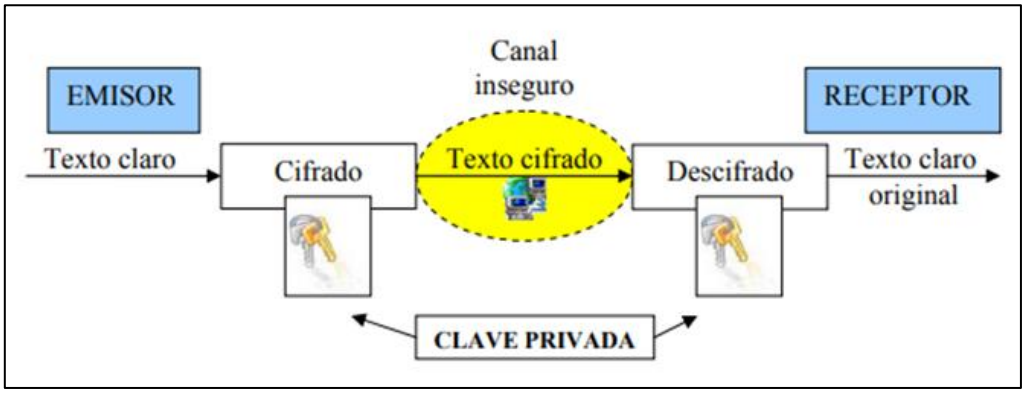


*Ilustración 1: Uso de clave simétrica*
***Nota.*** *Reproducido de INCIBE (2019).*

El cifrado simétrico se clasifica principalmente **en cifrado por bloques y cifrado por flujo,** según cómo procesan la información:

**1) Cifrado por bloques**

El cifrado por bloques procesa los datos en bloques de tamaño fijo, típicamente de 64 o 128 bits, transformando cada bloque mediante funciones matemáticas complejas que dependen de la clave. Los algoritmos más conocidos en tarjetas inteligentes incluyen **DES, 3DES y AES**.

Cada bloque se cifra de manera estructurada, y el resultado depende de la clave y, en la mayoría de los modos de operación, de los bloques previos.

Esto permite mantener la seguridad incluso cuando el mensaje contiene patrones repetidos. Para manejar mensajes más largos que un solo bloque y aumentar la seguridad, se emplean modos de operación:

- **ECB** (*Electronic Codebook*): cada bloque se cifra de manera independiente. Es rápido pero inseguro ante patrones repetidos.
- **CBC** (*Cipher Block Chaining*): cada bloque se combina con el bloque cifrado anterior antes de aplicar la clave, de modo que un cambio en un bloque afecta a todos los siguientes.
- **CFB** (*Cipher Feedback*) y OFB (*Output Feedback*): convierten el cifrado por bloques en un flujo pseudoaleatorio, útil para aplicaciones en tiempo real.
- **CTR** (*Counter Mode*): genera un flujo pseudoaleatorio sumado al valor en claro mediante XOR, permitiendo cifrado y descifrado paralelos y optimizando velocidad en dispositivos NFC y RFID.

En modos como CBC, CFB, OFB o CTR, se utiliza un **vector de inicialización (IV)**, un valor aleatorio que introduce entropía al primer bloque de cifrado. Su función es evitar que al cifrar dos mensajes iguales con la misma clave, el resultado sea el mismo y así se pueda adivinar la información por patrones repetidos. El IV no necesita ser secreto, pero si debe ser único para cada transacción.

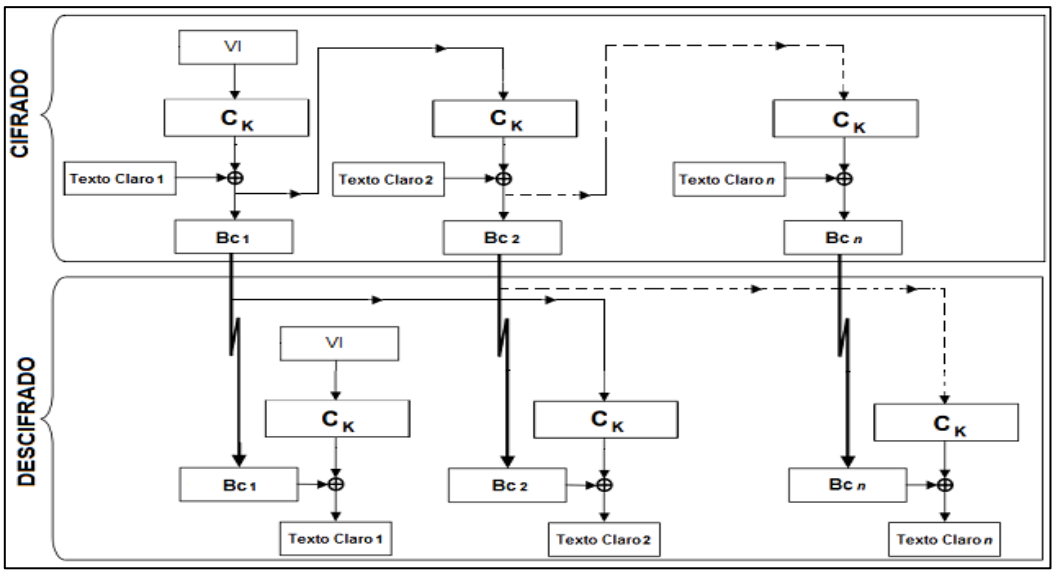


*Ilustración 2: Esquema de cifrado y descifrado por bloques CFB*
***Nota.*** *Reproducido de Numerentur.org (s. f.).*

El cifrado por bloques permite generar códigos de transacción únicos y dinámicos como en EMV o pagos *contactless* y es resistente a ataques de repetición si se combina con un vector de inicialización.

**2) Cifrado por flujo**

El cifrado por flujo procesa los datos bit a bit o byte a byte, a diferencia del cifrado por bloques que opera sobre bloques de tamaño fijo (64 o 128 bits). Este enfoque es especialmente útil en dispositivos embebidos y sistemas de comunicación de bajo consumo, como tarjetas RFID pasivas, lectores NFC y sistemas de pago *contactless*.

Se utiliza un generador pseudoaleatorio controlado por la clave secreta y en muchos casos un IV. Este flujo de bits, llamado *keystream*, tiene la misma longitud que el mensaje que se desea cifrar. Cada bit o byte del valor a cifrar o *plaintext*, se combina con un bit o byte del keystream mediante una operación XOR dando lugar al valor cifrado o *ciphertext*:

$$Ciphertext = Plaintext \oplus Keystream$$

Tanto el emisor como el receptor deben generar exactamente el mismo *keystream* para descifrar correctamente los datos. En sistemas RFID/NFC, esto se asegura mediante el uso de IV o contadores sincronizados para inicializar el generador.

Existen dos tipos de cifrados por flujo atendiendo a si usan retroalimentación o no:

- **Cifradores de flujo sin retroalimentación** (*synchronous stream cipher*):
  El *keystream* se genera de forma independiente del *plaintext* o *ciphertext*.
  La seguridad depende de que el *keystream* sea impredecible y no repetido.
  Un ejemplo sería el algoritmo RC4, aunque actualmente ha quedado obsoleto por diversas vulnerabilidades que fueron descubiertas con el tiempo.

- **Cifradores de flujo con retroalimentación** (*self-synchronizing / ciphertext-feedback stream cipher*)

  El keystream depende de los bits cifrados previamente, permite que el receptor se resincronice automáticamente si se pierde parte de la comunicación. Un ejemplo sería el CFB aplicado a un cifrador por bloques.

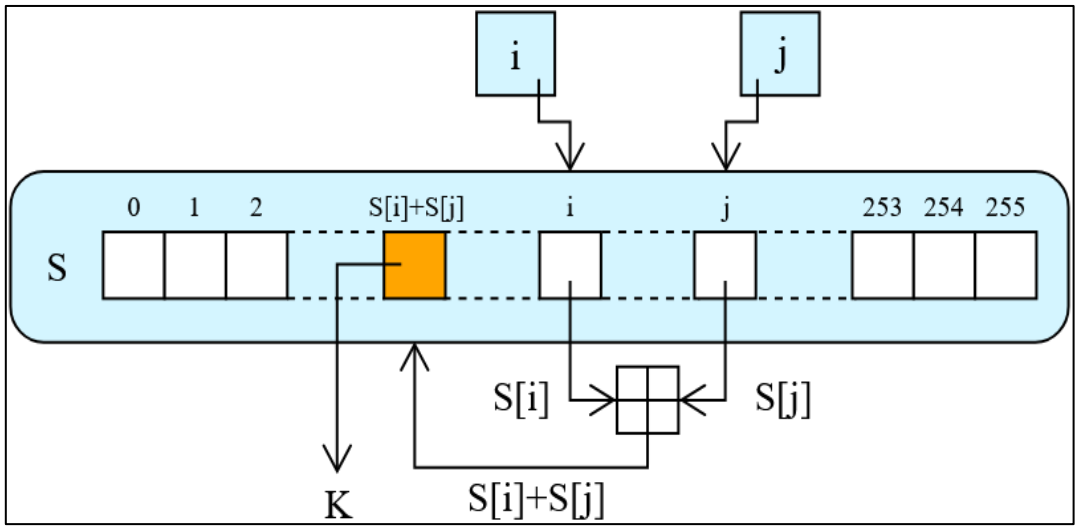


*Ilustración 3: Esquema de cifrado de flujo del algoritmo RC4*
***Nota.*** *Reproducido de Wikipedia (2025).*

### 2.4.2. Algoritmos asimétricos

La criptografía asimétrica, también llamada de clave pública, es un tipo de cifrado que utiliza dos claves distintas, pero matemáticamente relacionadas:

- **Clave pública:** se puede compartir libremente y se utiliza para cifrar información o verificar firmas digitales.
- **Clave privada:** se mantiene secreta en el dispositivo (por ejemplo, una tarjeta inteligente) y se utiliza para descifrar información o generar firmas digitales

Su principal ventaja es que no es necesario compartir previamente las claves privadas entre emisor y receptor, reduciendo el riesgo de que una clave sea interceptada o robada.

La criptografía asimétrica permite dos operaciones principales:

- **Cifrado de información**
  1) El emisor cifra el mensaje con la clave pública del receptor.
  2) Solo el receptor, que posee la clave privada, puede descifrarlo y recuperar el mensaje original.

     Esto garantiza la confidencialidad, ya que nadie más puede leer el mensaje aunque lo intercepte.

- **Autenticación mediante firma digital**
  1. El emisor firma un mensaje usando su clave privada.
  2. Cualquier receptor puede verificar la firma con la clave pública del emisor.

     Esto garantiza la integridad (el mensaje no ha sido modificado) y la autenticidad (proviene del emisor legítimo).

En la práctica, es habitual combinar la seguridad de la criptografía asimétrica con la rapidez de la simétrica. Primero, el emisor genera una **clave de sesión simétrica** para cifrar de manera eficiente la comunicación. Esta clave se protege cifrándola con la **clave pública del receptor**, de modo que solo el receptor, con su clave privada, pueda descifrarla. Una vez compartida de forma segura, ambos utilizan la misma clave de sesión para cifrar y descifrar todos los datos posteriores, garantizando la **confidencialidad y autenticidad** de la comunicación.

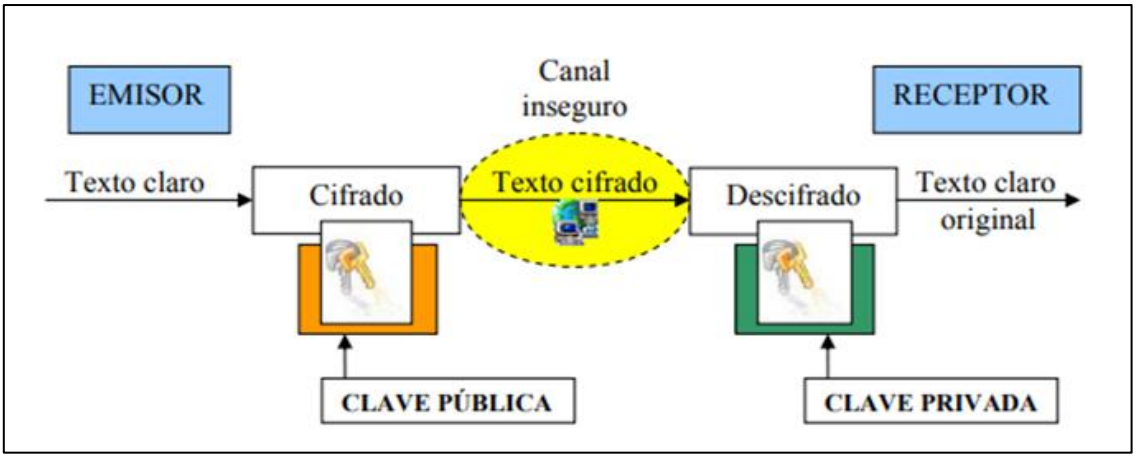


*Ilustración 4: Esquema de cifrado asimétrico*
***Nota.*** *Reproducido de INCIBE (2019).*

### 2.4.3. Funciones Hash

Las funciones *hash* criptográficas son algoritmos matemáticos que transforman una entrada de datos de longitud variable en una salida de longitud fija, denominada valor *hash* o resumen digital. A diferencia del cifrado simétrico o asimétrico, las funciones *hash* no utilizan claves para cifrar ni permiten recuperar el mensaje original, ya que están diseñadas como funciones unidireccionales. Su propósito principal no es la confidencialidad, sino garantizar la integridad de la información.

Una función *hash* toma un mensaje (por ejemplo, los datos de una transacción) y aplica una serie de operaciones matemáticas que producen un valor de tamaño fijo.

Si el mensaje cambia, aunque sea en un solo bit, el valor *hash* resultante cambia completamente. Este comportamiento se conoce como efecto avalancha. Aunque los mensajes son muy similares, el resultado es completamente distinto.

- **Propiedades de seguridad**

Para que una función *hash* sea considerada segura debe cumplir:

  - Resistencia a la preimagen: dado un *hash*, debe ser computacionalmente inviable obtener el mensaje original.
  - Resistencia a la segunda preimagen: dado un mensaje, no debe poder encontrarse otro mensaje distinto con el mismo *hash*.
  - Resistencia a colisiones: no debe ser factible encontrar dos mensajes diferentes que produzcan el mismo valor hash.

- **Aplicaciones en sistemas de pago y autenticación**

  En tecnologías como NFC o sistemas EMV, las funciones *hash* se utilizan para:

  - Verificación de integridad: comprobar que los datos transmitidos no han sido modificados.
  - Firmas digitales: antes de firmar un mensaje con criptografía asimétrica, normalmente se calcula primero su *hash* y se firma ese resumen.

- Almacenamiento seguro de contraseñas: en sistemas *backend*, se almacenan hashes en lugar de contraseñas en texto claro.
- Generación de códigos OTP y mecanismos de autenticación.

Algunos de los algoritmos *hash* más utilizados son **SHA-256 y SHA-512**, pertenecientes a la familia SHA-2 y SHA-3, el estándar más reciente con estructura diferente. Anteriormente se usaban MD5 y SHA-1, actualmente considerados inseguros debido a vulnerabilidades de colisión. A diferencia del cifrado, las funciones *hash* no permiten descifrado, ya que su objetivo no es ocultar la información sino garantizar que esta no ha sido alterada. Por ello, constituyen un componente fundamental en la construcción de sistemas seguros, especialmente cuando se combinan con criptografía simétrica y asimétrica.

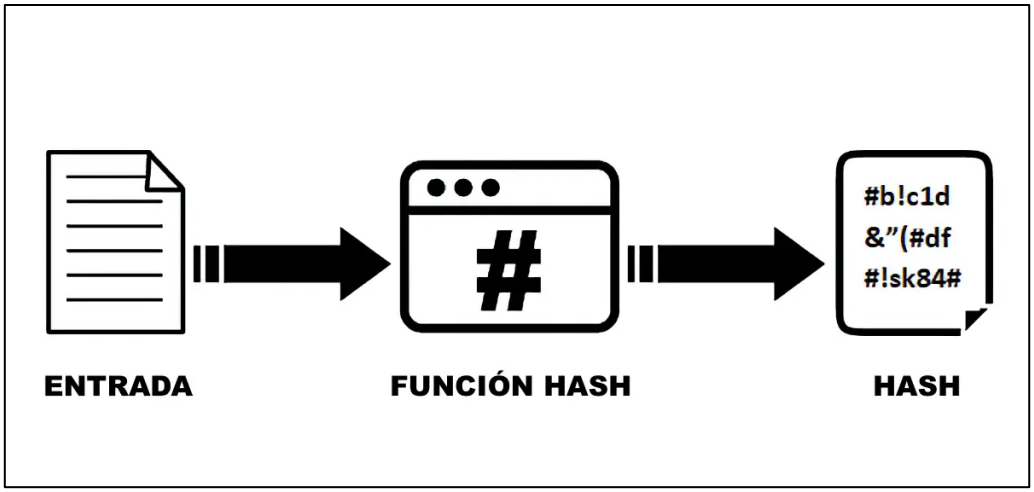


*Ilustración 5: Función de hashing*
***Nota.*** *Reproducido de Dongee (2024).*

## 2.5. Cibercrimen, fraudes y ataques asociados a tarjetas

El uso extendido de tarjetas de banda magnética, RFID y NFC ha generado diversas oportunidades para el crimen organizado. Estos ataques no solo explotan vulnerabilidades técnicas, sino también escenarios operativos donde el usuario y el sistema son engañados. Se distinguen diferentes tipos de fraudes, relacionados con la captura de datos, la suplantación de identidad y la manipulación de canales de comunicación.

### 2.5.1. Fraudes por captura de información

Buscan obtener datos sensibles almacenados o transmitidos por el dispositivo:

- ***Skimming***: consiste en capturar la información de tarjetas de banda magnética de forma general mediante lectores falsos instalados en cajeros automáticos o terminales de pago. El atacante obtiene los datos para crear duplicados y/o realizar transacciones no autorizadas.
- ***Eavesdropping* en RFID/NFC**: interceptación de la comunicación entre la tarjeta y el lector, típicamente en sistemas de transporte o control de acceso, para acceder a identificadores únicos.
- **Captura remota de identificadores**: ataques a sistemas de pago *contactless* o tarjetas de transporte donde los datos son recolectados sin contacto físico.

Estos ataques iniciales de captura de información sientan las bases para la suplantación de identidad y manipulación de transacciones descritas en las secciones siguientes.

### 2.5.2. Fraudes por reproducción o suplantación

Usan la información capturada para hacerse pasar por el titular legítimo:

- **Clonación de tarjetas**: creación de una copia funcional de la tarjeta o dispositivo original para realizar pagos o acceder a instalaciones restringidas.
- ***Spoofing* de dispositivos**: suplantación de tarjetas o dispositivos ante lectores, por ejemplo, para acceder a zonas restringidas o realizar pagos sin autorización.
- **Emulación no autorizada de credenciales digitales**: los dispositivos móviles pueden ser usados para simular tarjetas de pago o transporte, aprovechando credenciales digitales vulnerables.

En este tipo de fraude, la vulnerabilidad técnica se combina con la explotación de escenarios operativos donde el sistema confía en la autenticidad de la credencial.

### 2.5.3. Fraudes por manipulación del canal

Interfieren con la comunicación legítima entre tarjeta y lector, modificando el flujo de datos y comprometiendo la integridad de la transacción:

- **Ataques de *relay***: en pagos *contactless* o control de accesos, la señal puede ser retransmitida para extender el rango de la transacción.
- **Manipulación de protocolos y ataques de *downgrade***: la comunicación entre sistemas heredados y modernos puede permitir que se use un mecanismo menos seguro (por ejemplo, retroceder a banda magnética cuando el chip falla).

Estos ataques muestran que la seguridad no solo depende de la tarjeta, sino de la infraestructura y protocolos asociados.

### 2.5.4. Fraudes avanzados en implementación y gestión criptográfica

Explotan errores internos de los sistemas con capacidad computacional:

- **Extracción de claves**: ataques que comprometen secretos criptográficos usados para autenticar transacciones.
- **Fallos en la gestión de credenciales**: malas prácticas en la generación, almacenamiento o actualización de claves pueden facilitar fraudes.
- **Vulnerabilidades en firmware o software**: errores en la programación de dispositivos móviles o lectores pueden permitir accesos no autorizados o duplicación de credenciales.

Este tipo de fraudes es relevante principalmente en NFC y tarjetas inteligentes EMV, donde la seguridad depende de la correcta implementación de la arquitectura completa. En conjunto, el análisis de las tecnologías y los fraudes asociados muestra que la seguridad depende no solo de la robustez de la tarjeta o dispositivo, sino de todo el ecosistema: infraestructura, protocolos, firmware y comportamiento del usuario.

# 3. Marco teórico

## 3.1. Enfoque del análisis de vulnerabilidades

El análisis de vulnerabilidades en tecnologías de tarjetas no se limita a identificar fallos aislados, sino que requiere comprender cómo interactúan la arquitectura del sistema, el protocolo de comunicación y la implementación concreta. Una misma tecnología puede ser criptográficamente sólida y, sin embargo, resultar explotable debido a decisiones de diseño, supuestos físicos incorrectos o errores en la gestión de claves.

Desde el punto de vista técnico, una vulnerabilidad puede afectar a una o varias de las siguientes propiedades de seguridad:

- **Confidencialidad**: exposición de datos almacenados o transmitidos.
- **Integridad**: alteración no autorizada de información o transacciones.
- **Autenticidad**: suplantación de identidad o validación fraudulenta.
- **Disponibilidad**: interrupción del servicio o denegación operativa.

El análisis posterior se centrará especialmente en aquellas vulnerabilidades que afectan a la autenticidad y a la integridad, dado que son las más críticas en este tipo de sistemas.

## 3.2. Clasificación de vulnerabilidades en tecnologías de tarjeta

Las tecnologías analizadas presentan diferentes debilidades en función de su arquitectura. En rasgos generales, pueden distinguirse tres grandes categorías:

**1) Vulnerabilidades estructurales**

Son aquellas debilidades que derivan directamente en cómo está diseñada la arquitectura del sistema y no en su implementación. Aparecen cuando el propio modelo de funcionamiento carece de mecanismos de protección suficientes. En estos casos, la explotación no requiere técnicas avanzadas, sino aprovechar cómo está concebido el sistema.

En tecnologías de tarjetas, este tipo de vulnerabilidad suele manifestarse cuando:

- Los datos almacenados son estáticos.
- No existe autenticación mutua entre lector y tarjeta.
- La información se transmite sin cifrado.
- La validación depende exclusivamente de un sistema externo.

El ejemplo habitual es la banda magnética, donde la tarjeta actúa como un soporte pasivo que almacena datos legibles y replicables. La ausencia de generación dinámica de valores hace que la clonación sea trivial una vez capturada la información. En este tipo de escenario, la explotación no rompe ningún mecanismo de seguridad, simplemente aprovecha que dicho mecanismo no existe.

**2) Vulnerabilidades de protocolo**

Un protocolo define la secuencia de mensajes, las reglas de validación y el contexto de una sesión entre tarjeta y lector. Aunque la criptografía sea robusta, el protocolo puede introducir debilidades si permite que mensajes válidos se utilicen fuera de contexto. En RFID y NFC, muchas explotaciones modernas no atacan el algoritmo criptográfico, sino la lógica de la comunicación.

Este tipo de vulnerabilidad puede producirse cuando:

- Un mensaje válido puede registrarse y reutilizarse posteriormente (*replay*).
- El sistema asume que la corta distancia implica presencia legítima.
- No se valida correctamente el estado interno de la sesión.
- Se permite operar en modos menos seguros por compatibilidad.

En un ataque de *relay*, la comunicación entre tarjeta y lector se retransmite en tiempo real a mayor distancia. La criptografía sigue funcionando correctamente, pero el protocolo no detecta que la tarjeta no está físicamente próxima al lector. Es decir, se manipula el flujo de comunicación sin necesidad de descifrarlo.

**3) Vulnerabilidades de implementación**

En este caso la implementación concreta no reproduce fielmente el diseño teórico del sistema o introduce fallos técnicos. A diferencia de las vulnerabilidades estructurales, aquí sí existe un mecanismo de seguridad previsto, pero está mal implementado o configurado. En tarjetas inteligentes y sistemas NFC pueden incluir:

- Generadores pseudoaleatorios con baja entropía.
- Reutilización de valores aleatorios o contadores.
- Gestión insegura de claves criptográficas.
- Errores en el *firmware*.
- Ausencia de protección frente a análisis físico (*side-channel*).

En estos casos, el algoritmo criptográfico puede ser matemáticamente sólido, pero su implementación reduce su seguridad real. Por ejemplo, si un generador de números aleatorios produce valores predecibles, puede reconstruirse una clave sin necesidad de romper el algoritmo subyacente. Su explotación se basa en identificar desviaciones entre el diseño teórico y el comportamiento real del sistema.

## 3.3. Modelo de adversario adoptado

Para que el análisis sea coherente, es necesario definir las capacidades del atacante consideradas en este trabajo. Se asume un modelo de adversario con las siguientes capacidades:

- Interceptar comunicaciones inalámbricas.
- Registrar y reproducir intercambios de datos.
- Modificar o retransmitir mensajes.
- Acceso físico temporal a dispositivos.
- Uso de herramientas comerciales de laboratorio.

No se presupone la capacidad de romper algoritmos criptográficos robustos mediante ataques matemáticos avanzados.

La mayoría de los compromisos reales documentados en sistemas de tarjetas no derivan de debilidades matemáticas fundamentales, sino de:

- Mala implementación.
- Gestión deficiente de claves.
- Errores de diseño.
- Manipulación del canal físico.

Este modelo de adversario se alinea con escenarios realistas de fraude y pruebas experimentales controladas.

## 3.4. Superficie de ataque comparada

La superficie de ataque permite analizar cómo evoluciona el riesgo a medida que las tecnologías de tarjetas pasan de sistemas simples y pasivos a dispositivos complejos con capacidad computacional y comunicación bidireccional. La superficie de ataque no solo depende de los canales físicos o inalámbricos, sino también de la lógica interna, la gestión de datos y la interacción con sistemas externos.

| Tecnología | Canal | Datos / Lógica | Capacidad computacional | Observaciones |
|---|---|---|---|---|
| Banda magnética | Físico | Estáticos | Ninguna | Vulnerable a clonación y *skimming*; seguridad dependiente de sistemas externos |
| RFID básico | Inalámbrico | Identificadores transmitidos | Limitada | Dependencia del *backend*; vulnerable a *eavesdropping* y *relay* |
| NFC / Tarjetas inteligentes | Inalámbrico bidireccional | Valores dinámicos | Completa (*firmware* y criptografía) | Reduce vulnerabilidades simples, introduce riesgos de implementación y protocolo; integración con móviles y *backend* aumenta complejidad |

Como se observa en la tabla, la evolución tecnológica ha permitido mitigar vulnerabilidades simples, como la clonación directa o transmisión de datos en claro, presentes en la banda magnética. Sin embargo, esta evolución ha generado un sistema más complejo, donde los vectores de ataque se desplazan hacia errores de implementación, fallos en la gestión criptográfica y vulnerabilidades protocolarias, como ataques de *relay* o *downgrade*.

Comprender esta superficie de ataque es fundamental para identificar no solo las vulnerabilidades de cada tecnología, sino también los escenarios de su explotación, que podrían comprometer la integridad, autenticidad y confidencialidad de la información.

## 3.5. Explotabilidad práctica

No toda vulnerabilidad es automáticamente explotable, para que una debilidad tenga relevancia operativa deben cumplirse tres condiciones:

1) **Accesibilidad**: el atacante puede interactuar con el componente vulnerable.
2) **Controlabilidad**: puede influir en su comportamiento.
3) **Impacto demostrable**: la acción produce una alteración medible.

En el contexto de este trabajo, la explotación puede materializarse en:

- Clonación funcional.
- Suplantación de identidad.
- Autenticación fraudulenta.
- Manipulación de transacciones.
- Obtención de secretos criptográficos.

Este enfoque permite diferenciar entre vulnerabilidades teóricas y con impacto real en entornos operativos.

## 3.6. Criptografía y límites de la protección

La incorporación de criptografía en las tarjetas inteligentes y sistemas NFC añade autenticación dinámica y protección frente a ataques de repetición (*replay*). Sin embargo, la seguridad real depende de la coherencia entre diseño, implementación y contexto de uso, no solo de la robustez matemática del algoritmo. Entre los factores que condicionan la protección se incluyen:

- Robustez y tipo de algoritmo (simétrico o asimétrico).
- Longitud y manejo de claves.
- Entropía efectiva de los generadores de números aleatorios.
- Correcta sincronización de valores dinámicos.
- Protección frente a ataques físicos o de canal lateral.

La práctica muestra que los ataques más relevantes no suelen romper la criptografía de manera directa, sino que explotan fallos de implementación o supuestos erróneos en el entorno real, como:

- Reutilización de valores dinámicos.
- Errores en la sincronización de transacciones.
- Suposiciones físicas incorrectas (la proximidad en un ataque de relay).
- Vulnerabilidades en firmware o software del lector o dispositivo móvil.

Por tanto, un análisis de explotación efectivo se centra en evaluar cómo la implementación y el contexto operativo pueden socavar la protección criptográfica, más que en cuestionar la solidez teórica de los algoritmos.

# 4. Análisis Experimental

## 4.1. Objetivo del laboratorio

El objetivo de este laboratorio es evaluar de manera controlada la explotabilidad de vulnerabilidades en tecnologías de tarjetas magnéticas, RFID y NFC, y determinar cómo los factores de diseño, implementación y protocolo afectan la seguridad real. La intención no es comprometer sistemas reales, sino demostrar el impacto de vulnerabilidades conocidas y proponer mejoras que aumenten la resiliencia de estos sistemas. Se prioriza la seguridad, la reproducibilidad de los experimentos y la observación de resultados medibles. Todas las pruebas se realizan en un entorno controlado, con dispositivos de laboratorio, emuladores, lectores y tarjetas.

## 4.2. Metodología general

Para garantizar consistencia en las pruebas se sigue el siguiente enfoque:

1. **Selección de dispositivos**: se utilizan tarjetas magnéticas antiguas, etiquetas RFID pasivas y activas, y tarjetas inteligentes NFC típicas del mercado.
2. **Preparación del entorno**: lectores controlados, analizadores de tráfico, generadores de señal y *software* de captura de datos.
3. **Tipos de pruebas**:
    - **Lectura y captura de datos**: verificación de accesibilidad y exposición de información.
    - **Clonación y emulación funcional**: evaluación de la posibilidad de replicar la funcionalidad del dispositivo.
    - **Manipulación de comunicación**: reproducción de mensajes válidos y estudio teórico de ataques de *relay*.
    - **Explotación criptográfica**: análisis de debilidades en la gestión de claves y protocolos.
4. **Registro de resultados**: se documenta cada intento de explotación, éxito o fracaso, y el impacto potencial en la integridad y autenticidad del sistema.

Se mantiene un enfoque ético y académico: todos los experimentos se realizan en dispositivos propios o emuladores, sin afectar sistemas de terceros.

## 4.3. Banda magnética

En la banda magnética se almacena información de forma estática y carecen de capacidad computacional. Generalmente se componen de tres pistas longitudinales donde se codifican datos legibles por cualquier lector compatible.


*Ilustración 6: Pistas de una tarjeta de banda magnética con dos pistas*
***Nota.*** *Reproducido de Magspoof (2015).*

### A. Pista 1

- **Formato:** Alfanumérico (hasta 79 caracteres).
- **Contenido habitual en tarjetas de crédito:** Número de tarjeta (PAN), nombre del titular, fecha de expiración, código de servicio.
- **Contenido en tarjetas en general:** Identificador de tarjeta o usuario, nombre o ID asociado al titular, código de acceso o tipo de servicio.
- **Observaciones:** La pista 1 permite incluir información alfanumérica, lo que la hace útil para sistemas que requieren datos completos del titular.

### B. Pista 2

- **Formato:** Numérico (hasta 40 caracteres).
- **Contenido habitual en tarjetas de crédito:** Número de tarjeta (PAN). fecha de expiración, código de servicio.

- **Contenido en tarjetas en general:** Identificador numérico único, fecha de validez, información de control o seguridad para sistemas automáticos.
- **Observaciones:** Esta pista es más compacta y estandarizada, siendo la más utilizada en cajeros automáticos y terminales de pago.

**C. Pista 3**

- **Formato:** Numérico o alfanumérico (hasta 107 caracteres).
- **Contenido habitual en tarjetas de crédito:** Información adicional del emisor, como datos de control interno o auditoría, datos específicos de aplicaciones especiales de la tarjeta.
- **Contenido en tarjetas en general:** Control de acceso avanzado, registro de actividad o historial del titular, datos propios del sistema emisor.
- **Observaciones:** La pista 3 es opcional en la mayoría de las tarjetas de crédito, pero puede ser relevante en tarjetas corporativas, de transporte o sistemas de control de acceso donde se requiere información adicional para la gestión interna.

### 4.3.1. Hardware

En el ámbito de la banda magnética existen diversas alternativas *hardware* que permiten la interacción con tarjetas, abarcando desde dispositivos comerciales hasta implementaciones experimentales. Estas soluciones pueden clasificarse en tres categorías de forma principal; lectura, escritura y emulación.

Los **lectores de banda magnética** constituyen la opción más básica, permitiendo la captura de los datos almacenados en las pistas de la tarjeta. Estos dispositivos suelen funcionar como interfaces tipo *keyboard wedge*, transmitiendo automáticamente la información leída al sistema anfitrión. Son ampliamente utilizados en entornos comerciales como terminales de punto de venta.

*Ilustración 7: Lector de banda magnética MS90*
***Nota**. Reproducido de Amazon (2026).*

En segundo lugar, los **lectores/escritores de banda magnética** amplían estas capacidades al permitir no solo la lectura, sino también la escritura y modificación de datos en tarjetas regrabables. Dispositivos como el Osayde MSR606E representan una solución estándar en entornos de laboratorio, al ofrecer soporte para múltiples pistas y diferentes tipos de coercitividad. Este tipo de *hardware* resulta fundamental para la evaluación de ataques de clonación.


*Ilustración 8: Lector Osayde MSR606E y tarjetas*
***Nota**. Elaboración propia.*

En un contexto distinto, vinculado a actividades ilícitas, destacan los dispositivos conocidos como *skimmers*, ampliamente utilizados en fraudes como el *skimming* en cajeros automáticos y terminales de pago. Dispositivos diseñados específicamente para la captura encubierta de datos de tarjetas de banda magnética sin conocimiento del usuario, constituyendo una de las principales herramientas empleadas por redes de delincuencia organizada en el ámbito financiero.

Los *skimmers* pueden adoptar diferentes formas según su modo de instalación: dispositivos superpuestos (*overlay*) **colocados sobre el lector original**, dispositivos insertables en el interior del lector (*insert skimmers*) o soluciones integradas en la cadena de comunicación (*inline*). Su objetivo es interceptar la señal generada durante el proceso de lectura de la tarjeta, obteniendo el contenido de las pistas de forma transparente para el usuario.


*Ilustración 9: Skimmer en un cajero automático*
***Nota**. Reproducido de Kaspersky (2015).*

En muchos casos, estos dispositivos **incorporan memoria interna** para almacenar los datos capturados o módulos de comunicación inalámbrica que permiten su transmisión remota, facilitando la explotación posterior de la información para la clonación de tarjetas y la realización de transacciones fraudulentas.

La existencia y uso extendido de este tipo de *hardware* en escenarios reales de delincuencia evidencia la debilidad inherente de la banda magnética, donde la información es capturada sin necesidad de vulnerar mecanismos criptográficos, debido a la ausencia de protección en el propio canal físico.

Por último, existen soluciones orientadas a la **emulación de tarjetas**, basadas en microcontroladores de bajo coste, entre las que destaca **MagSpoof** (kamkar, 2015/2026) una implementación experimental desarrollada para reproducir el comportamiento de tarjetas de banda magnética mediante hardware simple como **ATtiny85** o **Arduino**.

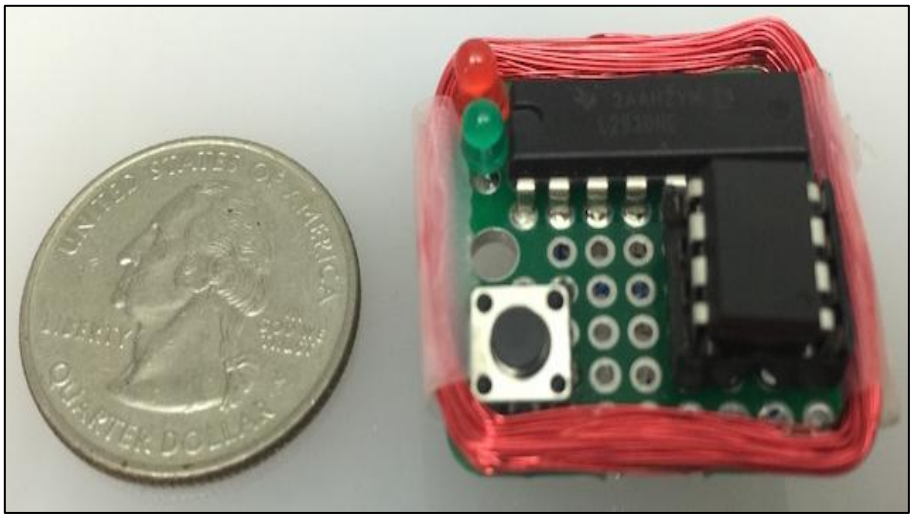

*Ilustración 10: Magspoof con ATtiny85 comparado con una moneda*
***Nota**. Reproducido de Magspoof (2015).*

Este tipo de dispositivos permite replicar el comportamiento de una tarjeta de banda magnética sin necesidad de un soporte físico. En lugar de almacenar la información en una banda, estos sistemas generan directamente el campo magnético que un lector espera recibir, emitiendo de forma controlada la secuencia de señales electromagnéticas correspondiente al contenido de las pistas.

En algunos casos, estas implementaciones pueden complementarse con dispositivos multifunción como Flipper Zero, que permiten integrar capacidades de emulación dentro de plataformas portátiles orientadas a pruebas de seguridad.


*Ilustración 11: Flipper Zero con MagSpoof*
***Nota**. Reproducido de ElectronicCats (2026).*

De forma complementaria, en entornos de investigación avanzada pueden emplearse **cabezas lectoras magnéticas junto con circuitos de acondicionamiento de señal**, lo que permite trabajar a nivel de señal analógica y profundizar en los procesos de codificación y decodificación (por ejemplo, F2F o *Aiken Biphase*).

En conjunto, estas alternativas reflejan la simplicidad del ecosistema de banda magnética, donde la interacción con tarjetas puede realizarse mediante dispositivos de bajo coste y fácil acceso, facilitando su análisis en entornos experimentales.

### 4.3.2. Software

El *software* asociado a tecnologías de banda magnética se centra en la gestión, interpretación y manipulación de los datos contenidos en las pistas, existiendo tanto soluciones comerciales desarrolladas por fabricantes como herramientas *open source* orientadas a investigación.

Por un lado, los **programas propietarios proporcionados por fabricantes** de dispositivos lectores/escritores, como el asociado al Osayde MSR606E (*Software Download*, s. f.) que permiten realizar operaciones básicas como la lectura, escritura, borrado y verificación de tarjetas. Estas herramientas suelen incluir interfaces gráficas que facilitan la visualización del contenido de las pistas en formato legible, así como la edición manual

de los datos. Su uso es habitual en entornos comerciales y de laboratorio debido a su facilidad de uso y compatibilidad directa con el *hardware*.

Por otro lado, existen **herramientas open source y utilidades de análisis** (egginabucket, 2023/2026) orientadas a la interpretación de los datos de banda magnética. Estas soluciones permiten descomponer la información conforme a los estándares definidos en ISO/IEC 7811, identificando campos como delimitadores, códigos de servicio o identificadores. Además, en entornos de investigación es común el desarrollo de scripts propios en lenguajes como *Python* o *C* para procesar datos, generar secuencias o analizar señales capturadas.

### 4.3.3. Vulnerabilidades probadas

- Clonación directa mediante lectura de pistas.
- Validación dependiente de *backend* externo.

Para analizar las distintas vulnerabilidades se empleó un lector/escritor de tarjetas de banda magnética **Osayde MSR606E**, con el objetivo de comprobar si el sistema dependía de un *backend* externo. Además, se utilizaron tarjetas en blanco regrabables, lo que permitió evaluar la posibilidad de realizar clonaciones directas a partir de la lectura de las diferentes pistas de la banda magnética y el software del fabricante.

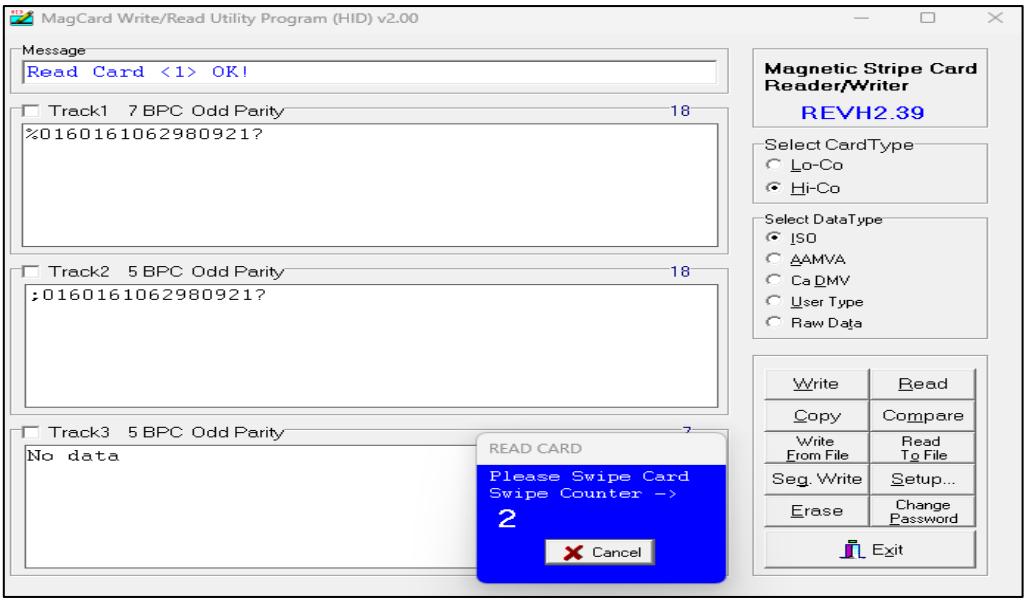


*Ilustración 12: Lectura de una tarjeta de fidelización*
***Nota**. Elaboración propia.*

En primer lugar, se procedió a la lectura del contenido de una tarjeta de fidelización con el objetivo de analizar la información almacenada en sus pistas. Posteriormente, dichos datos fueron escritos en una tarjeta en blanco regrabable, permitiendo así comprobar si era posible generar una copia funcional de la tarjeta original.

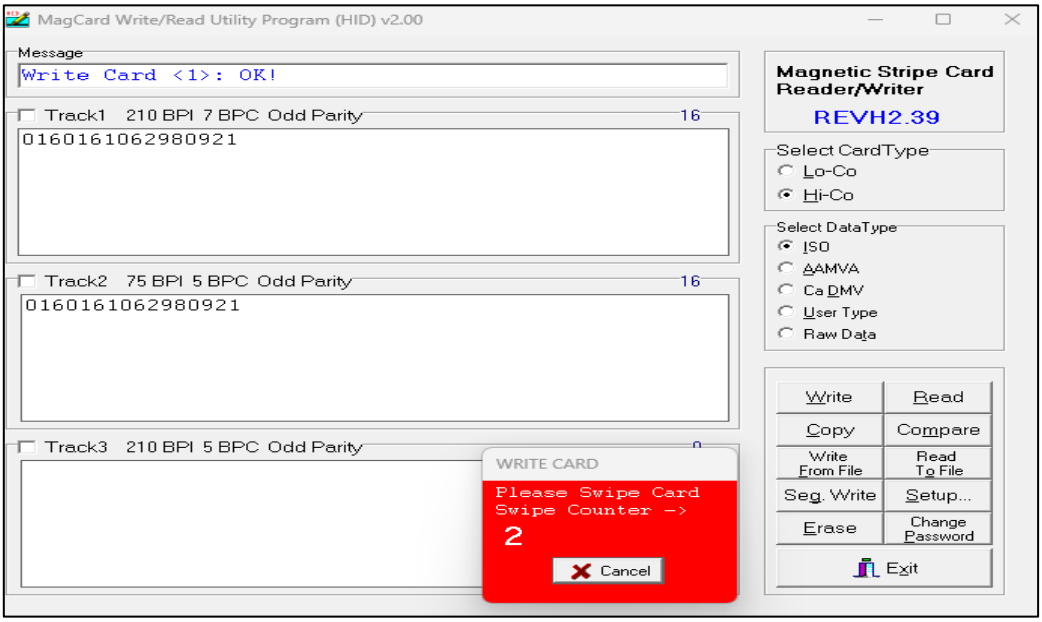


*Ilustración 13: Escritura de una copia en una tarjeta blanca*
***Nota**. Elaboración propia.*

Tras el análisis de los datos obtenidos, se observó que la tarjeta únicamente almacena un identificador, en este caso 0160 1610 6298 0921. Por tanto, la gestión de la información asociada a la tarjeta se realiza en un sistema *backend* externo, encargado de vincular dicho identificador con los datos del usuario y validar su uso dentro del sistema.

### 4.3.4. Resultados

Durante las pruebas realizadas se comprobó que la lectura de la información contenida en la banda magnética puede realizarse sin ningún tipo de autenticación o protección criptográfica. Del mismo modo, los datos obtenidos pueden escribirse directamente en una tarjeta en blanco regrabable, generando una copia funcional que reproduce el mismo identificador que la tarjeta original. Esto evidencia la debilidad inherente de este tipo de tecnologías cuando se utilizan como único mecanismo de identificación.

- La **captura y replicación de datos** fue sencilla y reproducible con dispositivos básicos.
- La **ausencia de autenticación y cifrado** hace que cualquier dato leído pueda generar una tarjeta funcional.

### 4.3.5. Lecciones y mejoras

- Migración a sistemas **EMV con autenticación dinámica** reduce considerablemente el riesgo de clonación.
- Incorporar mecanismos de **detección de lectura anómala y monitoreo de transacciones** ayuda a mitigar fraudes.

## 4.4. Radio Frecuency Identification

La tecnología **RFID (*Radio Frequency Identification*)** es un sistema de identificación inalámbrica que permite la comunicación entre una **etiqueta** (*tag*) y un **lector** mediante el uso de radiofrecuencia. A diferencia de la banda magnética, donde la lectura requiere contacto físico, RFID permite la transmisión de datos sin contacto, utilizando los campos electromagnéticos.

La etiqueta puede ser **pasiva**, obteniendo energía del campo generado por el lector, o **activa**, incorporando una fuente de alimentación propia que permite un mayor alcance y capacidad de almacenamiento.

La comunicación RFID se basa en modulación y retrodispersión (*backscatter*), donde la etiqueta responde reflejando la señal del lector. Funcionalmente, permite leer identificadores y, en algunos casos, escribir datos o aplicar mecanismos básicos de autenticación. No obstante, muchas implementaciones de bajo coste siguen usando identificadores estáticos sin protección criptográfica. RFID engloba distintas tecnologías, frecuencias y niveles de seguridad; por ello, en este trabajo se diferencia de NFC, entendido como una evolución específica de RFID de alta frecuencia con capacidades criptográficas más avanzadas.

### 4.4.1. Hardware

Existen diferentes dispositivos para interactuar con tecnologías RFID, que permiten la lectura, escritura, emulación y análisis de la comunicación entre etiquetas y lectores.

En primer lugar, los **lectores RFID** constituyen el componente fundamental del sistema, siendo responsables de generar el campo electromagnético y gestionar la comunicación con las etiquetas. **Es habitual que trabajen en baja frecuencia, LF - 125/134 kHz** y están ampliamente desplegados en sistemas de control de acceso físico, como edificios, parkings o sistemas industriales.


*Ilustración 14: Lector RFID y etiquetas regrabables*
***Nota**. Elaboración propia.*

En segundo lugar, es fundamental distinguir entre diferentes tipos de **etiquetas RFID**, ya que sus capacidades determinan directamente el nivel de seguridad del sistema:

- **Etiquetas de solo lectura (*Read-Only*)**:

  Contienen un identificador único programado en fábrica que no puede modificarse. Son habituales en sistemas de bajo coste y su seguridad se basa únicamente en la unicidad del identificador, sin mecanismos de autenticación.

- **Etiquetas regrabables (*Read/Write*)**:

  Permiten modificar su contenido, incluyendo el identificador o datos adicionales. Son relevantes en entornos de laboratorio, ya que facilita la evaluación de escenarios de clonación y reproducción de credenciales.

En el ámbito de RFID de baja frecuencia (LF), es común el uso de tecnologías ampliamente extendidas como:

- **EM4100 / EM4102**: etiquetas de solo lectura con identificador fijo, muy utilizadas en sistemas de acceso.
- **T5577 (regrabable)**: etiqueta programable capaz de emular distintos formatos RFID, ampliamente utilizada en pruebas de clonación.

No obstante, existen también sistemas RFID que operan en **alta frecuencia, HF - 13.56 MHz**, los cuales introducen mayores capacidades de almacenamiento, comunicación y, en algunos casos, mecanismos básicos de autenticación. Estas tecnologías suponen un punto intermedio entre RFID clásico y sistemas más avanzados, aunque en este trabajo su análisis se abordará en la sección correspondiente a **NFC**, donde se estudian arquitecturas con capacidades criptográficas más desarrolladas. En conjunto, el *hardware* RFID se caracteriza por su diversidad y por la coexistencia de soluciones muy básicas, sin mecanismos de seguridad, junto con otras más avanzadas. En el caso de RFID clásico, la ausencia de capacidades criptográficas hace que la seguridad dependa en gran medida del diseño del sistema y del *backend*.

### 4.4.2. Vulnerabilidades probadas

- Captura, reutilización de identificadores y fallos de autenticación mutua.

Para la realización de las pruebas experimentales se empleó un dispositivo Flipper Zero junto con una etiqueta RFID de tipo EM4100 integrada en una pulsera deportiva.


*Ilustración 15: Lectura de una etiqueta EM4100 con un Flipper Zero*
***Nota**. Elaboración propia.*

En primer lugar, se procedió a la **lectura de la etiqueta**, capturando el identificador transmitido por la misma. Dado que este tipo de tecnología no incorpora mecanismos de cifrado, la información se obtuvo de forma directa mediante proximidad.


*Ilustración 16: Emulación de etiqueta con Flipper Zero*
***Nota.** Elaboración propia.*

Posteriormente, el identificador capturado fue **almacenado en el dispositivo**, y se llevó a cabo la **emulación de la etiqueta** utilizando el propio dispositivo, reproduciendo el identificador previamente capturado. Esta emulación permitió simular el comportamiento de la etiqueta original frente a un lector, demostrando la posibilidad de realizar una suplantación funcional en sistemas que basan su validación únicamente en identificadores estáticos. Este comportamiento reproduce un escenario de clonación funcional en entornos RFID, equivalente al observado en la banda magnética, pero trasladado al canal inalámbrico.

### 4.4.3. Resultados

Durante las pruebas realizadas se comprobó que las etiquetas RFID de baja frecuencia transmiten identificadores sin **ningún tipo de cifrado** o protección criptográfica, lo que permite capturarlos fácilmente con dispositivos de bajo coste. Además, se observó que estos **identificadores pueden reutilizarse para emular la etiqueta**, reproduciendo su comportamiento frente a un lector sin necesidad de disponer de la tarjeta original. Esto demuestra que, en sistemas basados en identificadores estáticos, la seguridad depende únicamente del *backend*, lo **que permite la suplantación de identidad de forma similar a lo que ocurre en la banda magnética.**

- Etiquetas pasivas **transmiten identificadores sin cifrado**, lo que facilita la interceptación.
- Las etiquetas activas con autenticación básica muestran resistencia parcial, pero los ataques de *relay* continúan siendo posibles.

### 4.4.4. Lecciones y mejoras

- Implementar cifrado simétrico y autenticación mutua robusta.
- Introducir valores dinámicos (*nonces*) para cada transacción.
- Monitorización de patrones de comunicación para detectar anomalías de proximidad.

## 4.5. Near Field Communication

La tecnología **NFC (Near Field Communication)** es una evolución de los sistemas RFID de alta frecuencia, operando en la banda de 13.56 MHz y basada en estándares como ISO/IEC 14443 e ISO/IEC 18092. A diferencia de RFID de baja frecuencia, donde muchas etiquetas se limitan a transmitir identificadores estáticos, las tarjetas y dispositivos NFC incorporan microcontroladores, memoria protegida y mecanismos criptográficos, permitiendo ejecutar protocolos de autenticación, intercambio seguro de datos y, en determinados casos, aplicaciones complejas como pagos, transporte o control de acceso avanzado.

Desde el punto de vista funcional, NFC permite tres modos principales: **lector/escritor**, **emulación de tarjeta** y ***peer-to-peer***. Esta flexibilidad amplía considerablemente su superficie de ataque, ya que la seguridad no depende únicamente del soporte físico, sino también del lector, del software intermedio, del protocolo, de la gestión de claves y de la infraestructura *backend*. En consecuencia, mientras que en banda magnética y RFID clásico predominan ataques de captura y clonación de identificadores, en NFC las vulnerabilidades suelen concentrarse en la implementación del protocolo, la gestión criptográfica, la validación del contexto y la configuración de lectores y dispositivos móviles.

### 4.5.1. Hardware

Existen diferentes dispositivos para interactuar con tecnologías NFC, incluyendo **etiquetas**, **tarjetas inteligentes**, **lectores** y **herramientas de laboratorio**. A diferencia del RFID clásico, el ecosistema hardware en NFC es más heterogéneo, abarcando **desde etiquetas de memoria sin protección hasta tarjetas inteligentes con capacidades criptográficas avanzadas** y sistemas de emulación mediante dispositivos móviles. Con el objetivo de estructurar esta diversidad y facilitar su análisis, a continuación se presenta una clasificación de las principales tecnologías utilizadas en entornos reales y de laboratorio, atendiendo a sus capacidades y nivel de seguridad.

| Tipo de tecnología | Familia | Capacidades | Nivel de seguridad |
|---|---|---|---|
| **Tarjetas de memoria (Type 2)** | NTAG21x (NTAG213/215/216), MIFARE Ultralight | Memoria EEPROM, sin autenticación o protección mínima | Bajo |
| **MIFARE Classic** | MIFARE Classic 1K / 4K | Memoria segmentada, autenticación propietaria (Crypto-1) | Bajo–Medio |
| **MIFARE DESFire** | DESFire EV1 / EV2 / EV3 | Microcontrolador seguro, sistema de ficheros, AES/3DES, autenticación mutua | Alto |
| **Tarjetas EMV contactless** | VISA, MasterCard, etc. | Criptogramas dinámicos, validación backend | Alto |
| **Tarjetas HID (acceso físico)** | HID iCLASS, iCLASS SE, Seos | Autenticación propietaria o basada en estándares, control de acceso | Medio–Alto |
| **Tarjetas vicinity (HF largo alcance)** | ICODE SLIX, SLIX2 (ISO15693) | Mayor distancia de lectura, inventario masivo, comunicación simplificada | Bajo–Medio |

| | | | |
|---|---|---|---|
| **Tarjetas de laboratorio (magic cards)** | MIFARE Classic modificadas (Gen1A, backdoor) | Modificación de UID y acceso a memoria sin autenticación | Muy bajo |
| **Credenciales virtuales (emulación NFC)** | Apple Pay, Google Pay | Emulación de tarjeta EMV, tokenización, autenticación en dispositivo | Muy alto |

Además de las etiquetas y dispositivos NFC, el ecosistema *hardware* incluye una variedad de lectores y herramientas que permiten interactuar con estas tecnologías tanto en entornos productivos como en escenarios de investigación y análisis de seguridad. A diferencia de RFID clásico, estos dispositivos no se limitan a la lectura de identificadores, sino que permiten la ejecución de pruebas activas sobre el protocolo, lo que los convierte en elementos clave para la evaluación de vulnerabilidades.

En primer lugar, los **lectores NFC comerciales**, como el ACR122U, representan la opción más accesible y extendida en entornos de laboratorio. Su principal ventaja radica en su bajo coste, facilidad de uso y compatibilidad con estándares como ISO14443 A/B e ISO18092, así como su integración con librerías como *libnfc*. Estos dispositivos permiten realizar operaciones de lectura, escritura e interacción mediante comandos APDU, siendo adecuados para el desarrollo de aplicaciones y pruebas iniciales.

Desde el punto de vista económico, se sitúan en un rango de **bajo coste (aproximadamente 30–60 €)**, lo que facilita su adopción. Aunque no proporcionan acceso a bajo nivel ni capacidades avanzadas de análisis de señal, pueden ser utilizados con herramientas software para explotar vulnerabilidades conocidas. En el caso de tecnologías como *MIFARE Classic*, es posible recuperar claves, leer y modificar la memoria mediante ataques criptográficos (Almeida, s. f.) utilizando este tipo de lectores, lo que los hace suficientes para la explotación de sistemas con mecanismos de seguridad débiles.


*Ilustración 17: Lector ACR122U y tarjetas mágicas*
***Nota**. Elaboración propia.*

En segundo lugar, herramientas especializadas como el Proxmark3 constituyen la referencia en investigación de seguridad NFC. A diferencia de los lectores convencionales, este dispositivo permite un control completo sobre la capa de comunicación, incluyendo capacidades de *sniffing*, emulación avanzada y ejecución de ataques activos. Facilita la ejecución de ataques como *darkside*, *nested* o *hardnested*, así como el análisis de nonces y procesos de autenticación.

Es necesario diferenciar entre las distintas variantes, las versiones de bajo presupuesto, como Proxmark3 Easy de fabricación no oficial (clones), se sitúan en un rango aproximado de **30–60 €**, lo que reduce significativamente la barrera de entrada a este tipo de análisis, mientras que versiones avanzadas como Proxmark RDV4 alcanzan costes en torno a los **300–400 €**, ofreciendo mayores capacidades, estabilidad y soporte. Como contrapartida, este tipo de herramientas presenta una curva de aprendizaje elevada y requiere conocimientos técnicos avanzados para su uso efectivo.


*Ilustración 18: Proxmark3 Easy y llaveros NFC Mifare Classic 1K*
***Nota.*** *Elaboración propia.*

De forma complementaria, dispositivos multifunción como el Flipper Zero permiten la interacción con tecnologías NFC en entornos portátiles. Su principal ventaja es la facilidad de uso y portabilidad, lo que lo convierte en una herramienta adecuada para demostraciones prácticas y pruebas rápidas en campo. Permite la lectura, almacenamiento y emulación de determinadas credenciales, facilitando la evaluación de sistemas vulnerables a clonación o basados en identificadores estáticos.

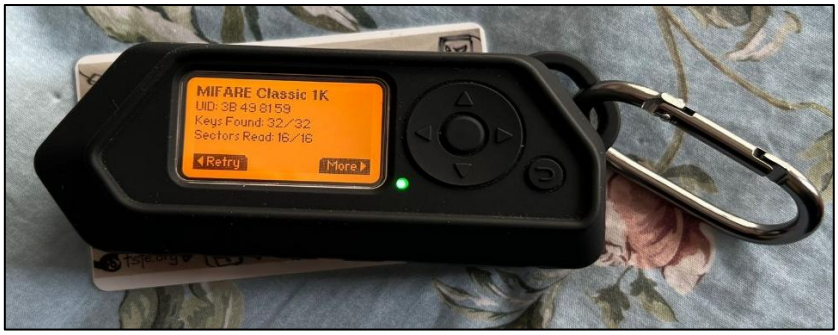


*Ilustración 19: Flipper Zero en lectura NFC*
***Nota.*** *Elaboración propia.*

Su coste se sitúa en un rango **medio (aproximadamente 200–250 €)**. Sin embargo, sus capacidades de análisis a bajo nivel son más limitadas en comparación con herramientas especializadas como el proxmark, por lo que no resulta adecuado para el estudio detallado de protocolos ni para la ejecución de ataques complejos, quedando principalmente orientado a escenarios prácticos de emulación y validación.

Por otro lado, los **dispositivos móviles con capacidades NFC**, especialmente aquellos basados en *chipsets* de ***NXP Semiconductors***, representan una plataforma ampliamente utilizada tanto en entornos reales como en pruebas de seguridad. En el caso de **Android**, los smartphones permiten operar en modo lector/escritor y en modo emulación de tarjeta mediante ***Host Card Emulation*** **(HCE)**, lo que facilita el análisis de aplicaciones reales y sistemas basados en credenciales virtuales.

No obstante, la compatibilidad depende directamente del *chipset* NFC utilizado, siendo los dispositivos basados en NXP los que ofrecen un soporte más amplio para tecnologías como **MIFARE**. En otros terminales con *chipsets* distintos, este soporte se encuentra limitado o directamente no está disponible, condicionando su uso.

En **dispositivos Apple**, por el contrario, el acceso a NFC ha estado tradicionalmente más restringido mediante ***Core NFC***, lo que limita su utilidad para análisis a bajo nivel. Como limitación adicional, además de la dependencia del *chipset*, las APIs del sistema operativo restringen el acceso a bajo nivel, lo que dificulta su uso.

Finalmente, en entornos de laboratorio se emplean módulos como PN532, integrados en plataformas como Arduino o Raspberry Pi. Estos dispositivos permiten implementar lectores personalizados y construir entornos de prueba controlados, siendo útiles para la simulación de escenarios específicos y el desarrollo de herramientas propias.

Su coste es **muy bajo (aproximadamente 10–30 €)**, lo que los convierte en una opción accesible para experimentación. No obstante, requieren conocimientos técnicos adicionales y su uso está más orientado al desarrollo y pruebas específicas que a la explotación directa de vulnerabilidades complejas.

En conjunto, el *hardware* NFC presenta un equilibrio entre coste, facilidad de uso y capacidades de análisis. Mientras que los lectores comerciales permiten interacciones básicas, herramientas especializadas como Proxmark3 ofrecen acceso avanzado al protocolo, y dispositivos como Flipper Zero o smartphones facilitan la reproducción de escenarios reales en entornos prácticos.

### 4.5.2. Software

El análisis y la explotación de tecnologías NFC no dependen únicamente del hardware utilizado, sino también del software asociado, que permite interactuar con los dispositivos NFC, interpretar su contenido y ejecutar pruebas sobre protocolos vulnerables. En este contexto, existe un amplio conjunto de herramientas orientadas tanto al uso legítimo como a la investigación en seguridad, muchas de ellas centradas en la explotación de debilidades conocidas.

En entornos Linux destacan herramientas como ***mfoc* (*MIFARE Classic Offline Cracker*)** y ***mfcuk* (*MIFARE Classic Universal ToolKit*)**, habitualmente utilizadas de forma conjunta en la recuperación de claves de tarjetas MIFARE Classic.

La herramienta *mfcuk* permite obtener claves iniciales explotando vulnerabilidades en el algoritmo criptográfico *Crypto*-1, mediante ataques como *darkside* o *nested*, incluso en ausencia de información previa. A partir de estas claves iniciales, *mfoc* puede emplearse para completar el proceso mediante ataques basados en diccionarios, derivando el resto de claves necesarias para acceder a la memoria completa de la tarjeta. Este enfoque combinado permite optimizar el proceso de recuperación de claves, reduciendo el tiempo de ataque y aumentando la probabilidad de éxito.

Ambas herramientas se integran habitualmente con lectores compatibles como ACR122U mediante librerías como *libnfc*, que proporcionan una interfaz de comunicación con dispositivos NFC y facilitan el desarrollo de herramientas personalizadas. Esta combinación constituye una de las metodologías más extendidas en pruebas de seguridad sobre MIFARE Classic, poniendo de manifiesto la debilidad de esta tecnología y su inadecuación para entornos que requieren mecanismos de seguridad.

Por otro lado, el software asociado a dispositivos como el **Proxmark3** constituye una de las plataformas más completas para el análisis de tecnologías NFC. Su cliente permite ejecutar comandos avanzados para la captura de comunicaciones, identificación NFC, emulación, análisis de protocolos y ejecución de ataques específicos. Entre sus capacidades destacan la posibilidad de realizar *sniffing* en tiempo real, analizar

intercambios entre lector y tarjeta y automatizar ataques complejos contra sistemas vulnerables. Esta herramienta representa el estado del arte en análisis de bajo nivel, siendo ampliamente utilizada en investigación y auditorías de seguridad.

Por otra parte, en el ámbito de dispositivos móviles Android, existen aplicaciones específicas como **MIFARE Classic Tool** (Klostermeier, 2013/2026), ampliamente utilizadas para la lectura, gestión y validación de tarjetas MIFARE *Classic*. Estas herramientas permiten la carga de diccionarios de claves, lectura de sectores y la comprobación de credenciales, constituyendo una de las soluciones más extendidas en entornos prácticos.

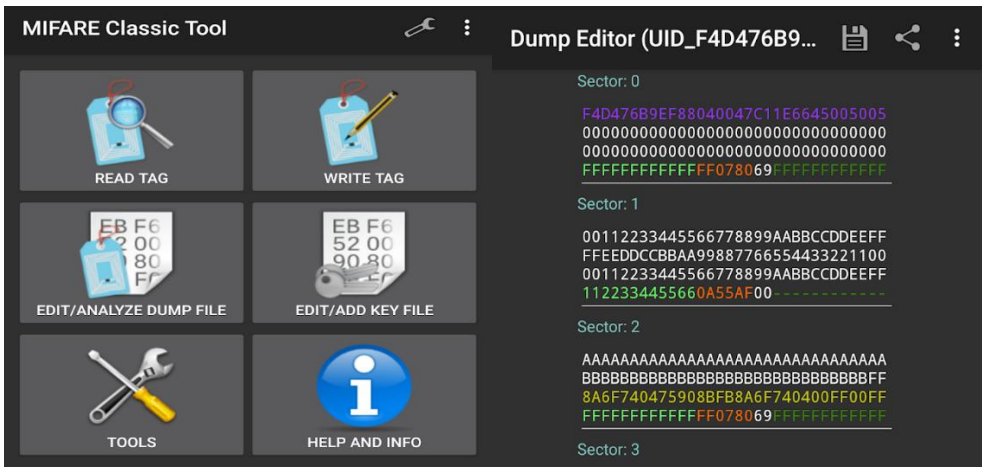


*Ilustración 20: Interfaz de la aplicación Android Mifare Classic Tool*
***Nota.*** *Elaboración propia.*

De forma complementaria, dispositivos como Flipper Zero incorporan su propio software, que incluye aplicaciones específicas para la interacción con tecnologías NFC. Su aplicación NFC permite la **lectura**, **almacenamiento** y **emulación** de credenciales, facilitando la reproducción de escenarios prácticos de clonación en entornos controlados.

Adicionalmente, el uso de aplicaciones extendidas, como *NFC Magic* (*Flipper Lab*, s. f.), amplía estas capacidades, permitiendo la escritura y manipulación de etiquetas avanzadas, incluyendo como *magic cards*.

Estas funcionalidades resultan especialmente relevantes en escenarios de prueba, donde se requiere no solo la emulación, sino también la modificación directa del contenido de las tarjetas. Aunque estas capacidades son más limitadas en comparación con dispositivos como el Proxmark3, su facilidad de uso y portabilidad convierten al Flipper Zero en una herramienta especialmente útil para demostraciones prácticas y validación rápida de configuraciones en entornos reales.

### 4.5.3. Vulnerabilidades probadas

En primer lugar, se evaluaron vulnerabilidades en tarjetas MIFARE *Classic* 1K, centradas en la debilidad del algoritmo propietario Crypto-1. Para ello, se utilizaron herramientas como **mfcuk** y **mfoc**, junto con dispositivos como el **ACR122U** y el **Proxmark3**, permitiendo ejecutar distintos ataques conocidos.

El ataque *darkside* se empleó con el lector ACR122U para obtener claves válidas explotando debilidades en el proceso de autenticación y en la generación de *nonces*. Este ataque no requiere información previa, siempre que la tarjeta permita autenticaciones repetidas. Su ejecución se realizó mediante la herramienta mfcuk, utilizando el comando **mfcuk -C 1 -v 3 -R 0:A -s 50 -S 50**.

En este comando, **-C 1** activa el modo de recuperación de una clave inicial, mientras que **-R 0:A** define como objetivo la clave A del sector 0. Los parámetros **-s** y **-S** ajustan los intentos y ciclos del ataque, condicionando su duración y probabilidad de éxito. El procedimiento se basa en repetir autenticaciones y analizar los *nonces* generados por la tarjeta, aprovechando debilidades del generador pseudoaleatorio de Crypto-1 para reducir el espacio de búsqueda hasta recuperar una clave válida.

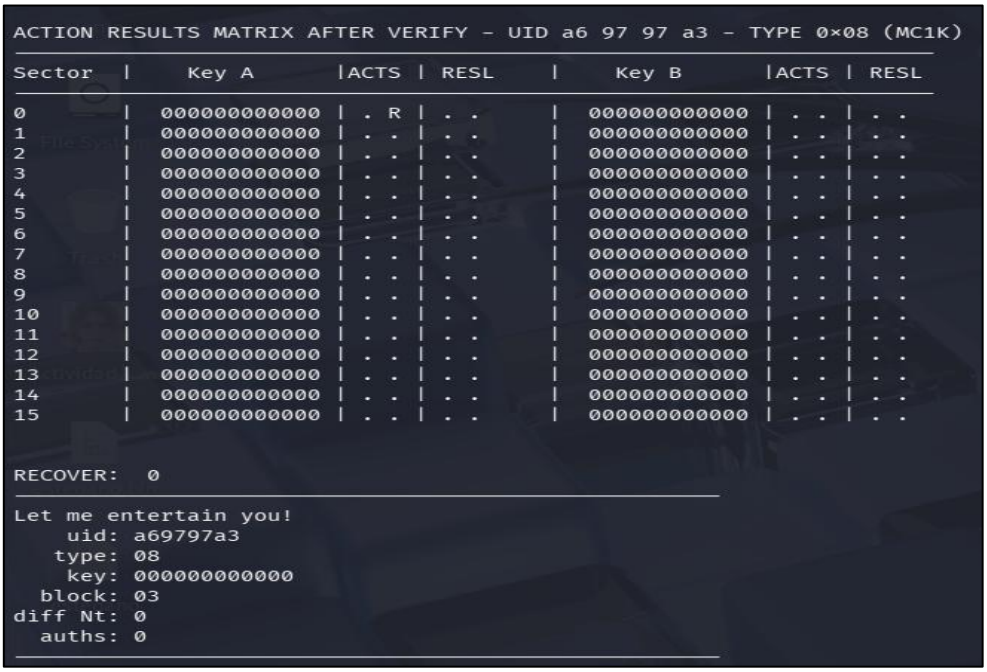


*Ilustración 21: Ataque darkside con Mfcuk y ACR122U*
***Nota**. Elaboración propia.*

En este caso concreto, el proceso de recuperación de claves se realizó solo con la herramienta *mfcuk*, obteniéndose las claves necesarias para acceder a los distintos sectores de la tarjeta. Posteriormente, la herramienta *mfoc* se utilizó únicamente para la lectura y volcado completo de la memoria con el comando **mfoc -f claves.txt -O dump.mfd** en lugar de recuperar las claves mediante el ataque *nested*.

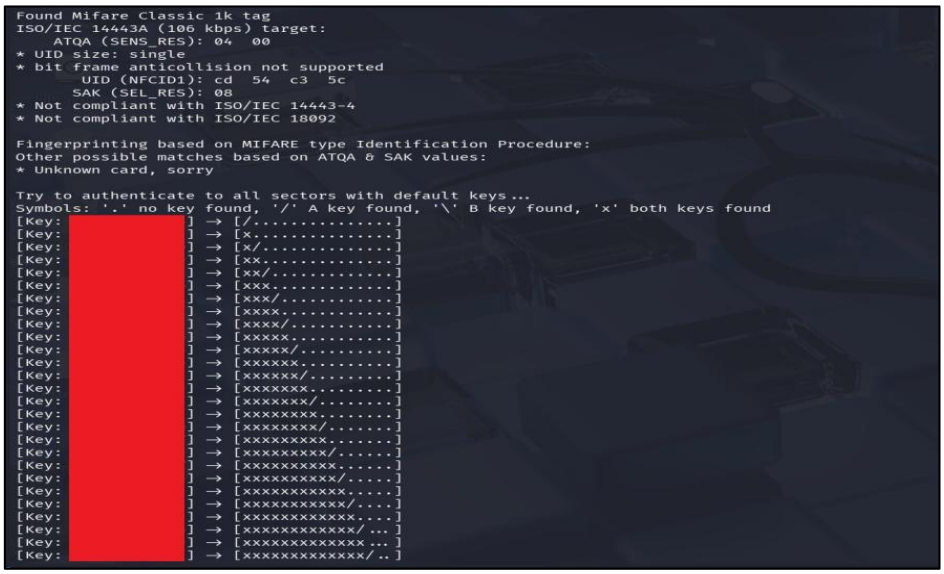


*Ilustración 22: Lectura de tarjeta con mfoc*
***Nota**. Elaboración propia.*

En caso de utilizar el proxmark tenemos varios comandos disponibles que permiten multitud de opciones, para conocer el tipo de tarjeta NFC que estamos leyendo basta con utilizar el comando **hf mf info**

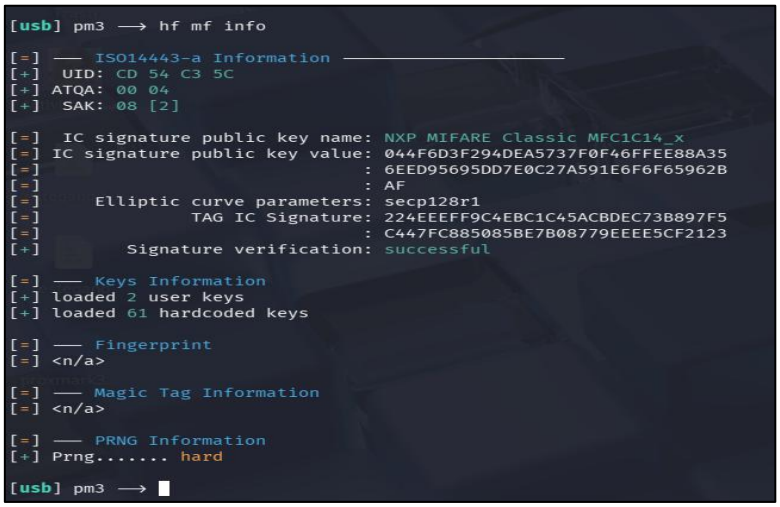


*Ilustración 23: Obtención de información con proxmark*
***Nota**. Elaboración propia.*

Además, el proxmark incluye un comando capaz de realizar ataques de forma automática para *Mifare Classic*, ***hf mf autopwn*****,** al ejecutarlo, el dispositivo identifica la tarjeta como MIFARE *Classic* EV1 y realiza una búsqueda de claves mediante diccionario, obteniendo claves válidas para determinados sectores sin aplicar técnicas de fuerza bruta.

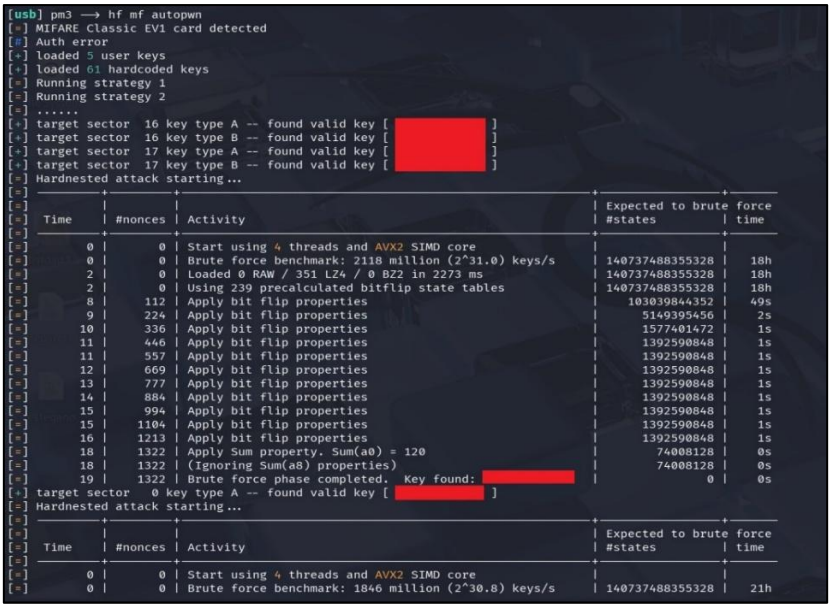


*Ilustración 24: Ataque hardnested con proxmark*
***Nota.** Elaboración propia.*

Posteriormente, el sistema inicia el ataque *hardnested*, una variante optimizada del ataque *nested*, diseñada para entornos donde este último no resulta efectivo. Este ataque se basa en el análisis de los valores de *nonce* generados durante el proceso de autenticación, explotando debilidades en el algoritmo criptográfico Crypto-1.

A diferencia de enfoques tradicionales, el ataque *hardnested* aplica técnicas de reducción del espacio de búsqueda, como el uso de propiedades de *bit flipping* y precomputación de estados, lo que permite disminuir de forma significativa el número de combinaciones a evaluar. En el ejemplo observado, el espacio inicial de búsqueda se reduce progresivamente hasta hacer viable la obtención de la clave en un tiempo reducido.


*Ilustración 25: Obtención de claves con proxmark*
***Nota**. Elaboración propia.*

Como resultado, el sistema logra recuperar claves válidas adicionales, incluyendo la clave del sector 0, permitiendo escalar el acceso a la memoria completa de la tarjeta. Este proceso demuestra la eficacia del Proxmark3 en escenarios donde herramientas como *mfoc* no resultan efectivas, evidenciando la capacidad de ataques avanzados para comprometer la seguridad de tarjetas MIFARE *Classic* incluso en configuraciones más restrictivas. En el caso del dispositivo Flipper Zero, se aplicó un ataque de tipo *nested* sobre la misma tarjeta, logrando recuperar claves válidas y acceder a su contenido.

Este resultado demuestra que el dispositivo es capaz de explotar vulnerabilidades en MIFARE *Classic* en escenarios prácticos, especialmente cuando se dispone de información previa o configuraciones débiles.


*Ilustración 26: Ataque Nested con Flipper Zero*
***Nota**. Elaboración propia.*

No obstante, en comparación con herramientas como Proxmark3, sus capacidades son más limitadas, tanto en velocidad como en control sobre el protocolo, por lo que su uso queda orientado principalmente a la reproducción de ataques y validación de escenarios, más que al análisis avanzado. Esto evidencia que dispositivos accesibles como Flipper Zero permiten ejecutar ataques reales en entornos NFC, reduciendo la barrera técnica necesaria para su explotación.

Por último, se analizaron configuraciones vulnerables en sistemas reales donde la validación se basa exclusivamente en el UID o en datos estáticos. En estos casos, herramientas como Proxmark3 o dispositivos como Flipper Zero, junto con aplicaciones extendidas como *NFC Magic*, permiten realizar ataques de emulación o clonación sin necesidad de explotar directamente el protocolo criptográfico.

Estos ataques demuestran que las vulnerabilidades en NFC no se limitan a fallos criptográficos, sino que afectan también a la implementación del protocolo, la generación de valores aleatorios y la lógica de validación del sistema.

Es importante destacar que los ataques descritos no afectan de igual forma a todas las tecnologías NFC. Mientras que en tarjetas simples como NTAG21x o MIFARE Ultralight es posible la lectura y clonación directa, y en MIFARE Classic la recuperación de claves es viable debido a debilidades en Crypto-1, en tecnologías más avanzadas como MIFARE DESFire o EMV *contactless* la criptografía impide el acceso a la memoria y la obtención de claves.

No obstante, estas tarjetas siguen siendo vulnerables a ataques de tipo *relay*, así como a fallos de implementación o configuraciones débiles. En sistemas de control de acceso (HID) o tecnologías *vicinity* (ISO15693), el riesgo depende del uso de identificadores estáticos y de la validación en *backend*, pudiendo permitir ataques de suplantación mediante emulación. En conjunto, la seguridad en NFC depende no solo de la criptografía, sino del diseño global del sistema.

### 4.5.4. Consideraciones sobre ataques de *relay*

Aunque los ataques de *relay* constituyen una amenaza relevante en sistemas RFID y NFC, en este trabajo no se ha realizado una implementación práctica de este vector. Su inclusión se aborda desde una perspectiva teórica, dado que requiere un escenario experimental específico, mayor control sobre lector y credencial, y condiciones que podrían afectar a sistemas reales si no se ejecutan en un entorno completamente aislado. En este tipo de ataque, el adversario no necesita conocer las claves criptográficas ni clonar físicamente la tarjeta, sino retransmitir la comunicación entre una credencial legítima y un lector, extendiendo artificialmente la distancia entre ambos.

Por ello, los ataques de *relay* evidencian que la autenticación criptográfica por sí sola no garantiza necesariamente la presencia física del usuario.

Como mitigación, se recomienda el uso de mecanismos de verificación de proximidad, como técnicas de *distance bounding*, controles contextuales, límites temporales estrictos en el intercambio de mensajes y validaciones adicionales en el *backend*.

### 4.5.5. Resultados

Durante las pruebas realizadas se comprobó que las tarjetas MIFARE *Classic* presentan vulnerabilidades críticas derivadas del uso del algoritmo criptográfico propietario Crypto-1, permitiendo la recuperación de claves y el acceso completo a la memoria mediante diferentes técnicas de ataque.

En primer lugar, se verificó que el ataque *darkside*, ejecutado con **mfcuk** y un lector ACR122U, permite la obtención de claves iniciales sin necesidad de información previa, siempre que el sistema permita múltiples intentos de autenticación. A partir de estas claves, fue posible acceder a determinados sectores de la tarjeta.

Posteriormente, se comprobó que la recuperación completa de claves puede realizarse utilizando exclusivamente **mfcuk**, sin necesidad de aplicar ataques *nested* con **mfoc**. En este escenario, **mfoc** se empleó únicamente para el volcado completo de la memoria, utilizando las claves previamente obtenidas.

En segundo lugar, mediante el uso de Proxmark3 se observó una mayor eficacia en la recuperación de claves, gracias a la ejecución automatizada de ataques y al uso de técnicas avanzadas como *hardnested*. Este dispositivo permitió obtener claves adicionales incluso en escenarios donde **mfoc** no resultaba efectivo, reduciendo significativamente el tiempo de ataque mediante optimización del espacio de búsqueda.

Por otro lado, el uso de Flipper Zero permitió reproducir ataques de tipo *nested* de forma práctica, logrando acceder al contenido de la tarjeta. No obstante, se observaron limitaciones en comparación con Proxmark3, tanto en velocidad como en capacidad de análisis, confirmando su orientación a escenarios de validación y demostración más que a análisis avanzado.

En conjunto, los resultados evidencian que:

- La seguridad de MIFARE *Classic* es insuficiente frente a ataques conocidos
- La recuperación de claves puede realizarse con herramientas accesibles y de bajo coste.

- Herramientas avanzadas como Proxmark3 permiten comprometer incluso configuraciones más restrictivas.
- La existencia de dispositivos portátiles como Flipper Zero reduce significativamente la barrera de entrada para la explotación de estas vulnerabilidades.

### 4.5.6. Lecciones y mejoras

- Implementar mecanismos de verificación de proximidad (*distance bounding*) para mitigar ataques de *relay*, junto con el uso de canales cifrados y restricciones temporales estrictas en la autenticación.
- Sustituir tecnologías obsoletas como MIFARE *Classic* por soluciones basadas en criptografía robusta (AES), como MIFARE DESFire o sistemas equivalentes.
- Evitar el uso del UID como único mecanismo de identificación, incorporando autenticación mutua y credenciales dinámicas.
- Realizar auditorías periódicas de *firmware*, lectores y configuraciones, así como aplicar actualizaciones de seguridad de forma continua.
- Implementar validaciones adicionales en *backend*, incluyendo control de contexto, detección de anomalías y gestión segura de claves.
- Limitar el número de intentos de autenticación y aplicar mecanismos de protección frente a ataques de fuerza bruta o repetición.
- Promover la concienciación del usuario y del personal técnico sobre riesgos asociados al uso de tecnologías *contactless*.

# 5. Conclusiones

El presente Trabajo Fin de Máster ha abordado el análisis técnico y experimental de vulnerabilidades en tecnologías de tarjeta basadas en banda magnética, RFID y NFC. A lo largo del trabajo se ha estudiado la evolución de estos sistemas desde soportes pasivos de almacenamiento estático hasta dispositivos con capacidad computacional y mecanismos criptográficos, evidenciando que dicha evolución no elimina por completo los riesgos de seguridad, sino que transforma la superficie de ataque.

El análisis realizado permite concluir que la seguridad de estas tecnologías no depende únicamente del medio físico empleado, sino del diseño global del sistema en el que se integran. Factores como la autenticación mutua, la gestión de claves, la robustez criptográfica, la configuración del *backend*, la existencia de mecanismos antifraude y la eliminación de compatibilidades heredadas resultan determinantes para evaluar el nivel real de protección ofrecido.

Mientras que las tecnologías más simples, como la banda magnética o ciertas etiquetas RFID de baja frecuencia, presentan debilidades estructurales asociadas al almacenamiento estático de datos, las tecnologías más avanzadas introducen nuevos riesgos relacionados con protocolos, criptografía, implementación y gestión operativa. Por tanto, la incorporación de mecanismos criptográficos no debe entenderse como una solución absoluta, sino como una capa más dentro de un modelo de seguridad que debe ser correctamente diseñado, desplegado y mantenido

## 5.1. Cumplimiento de los objetivos

Los objetivos planteados al inicio del trabajo se han cumplido mediante el estudio teórico y experimental de banda magnética, RFID y NFC. En el primer caso, banda magnética, se ha comprobado que su principal debilidad es estructural.

Al almacenar información estática y no disponer de mecanismos criptográficos propios, resulta especialmente vulnerable a ataques de lectura, copia y reproducción. Su seguridad depende casi por completo de controles externos al propio soporte.

En RFID, se ha observado que muchas implementaciones simples siguen basándose en identificadores estáticos o en mecanismos de autenticación muy limitados. Esto permite que, en determinados escenarios, una etiqueta pueda ser leída, emulada o reproducida funcionalmente si el sistema no incorpora validaciones adicionales.

En NFC, el análisis se ha centrado especialmente en tarjetas MIFARE *Classic*, donde se ha visto que la existencia de criptografía no garantiza por sí sola la seguridad. El uso de algoritmos obsoletos, claves débiles o configuraciones inseguras puede permitir la recuperación de claves y el análisis del contenido de la tarjeta en entornos controlados.

Por tanto, el trabajo permite confirmar la idea inicial, la evolución tecnológica no elimina los riesgos, sino que los transforma. Se pasa de ataques sencillos basados en la copia de datos a ataques más complejos relacionados con protocolos, claves, configuración e implementación.

## 5.2. Conclusiones técnicas

La banda magnética representa el caso más claro de debilidad por diseño. Su funcionamiento se basa en almacenar y entregar información sin autenticación ni cifrado, por lo que no debería utilizarse como mecanismo principal de seguridad en sistemas actuales.

RFID mejora algunos aspectos funcionales, pero no siempre mejora la seguridad. En etiquetas simples, el identificador puede actuar prácticamente como una “contraseña fija”, con todos los problemas que eso implica. Si el lector acepta únicamente ese identificador como prueba de autenticidad, el sistema queda expuesto a ataques de emulación o clonación funcional.

NFC y las tarjetas inteligentes ofrecen mayores capacidades de protección, pero también introducen más complejidad. Esta complejidad puede ser positiva cuando se utilizan algoritmos robustos, claves bien gestionadas y autenticación mutua, pero también puede generar vulnerabilidades si se emplean tecnologías antiguas o configuraciones inseguras.

Una conclusión importante del trabajo es que muchos ataques no dependen de romper algoritmos criptográficos modernos, sino de aprovechar malas decisiones de diseño, claves por defecto, compatibilidad con sistemas heredados o validaciones insuficientes en el *backend*.

## 5.3. Medidas de mejora

A partir de los resultados obtenidos, se pueden plantear varias medidas generales para reducir el riesgo en sistemas basados en tarjetas.

En primer lugar, debería evitarse el uso de tecnologías basadas en datos estáticos como único mecanismo de autenticación. Siempre que sea posible, es recomendable emplear sistemas con autenticación dinámica y validaciones criptográficas.

En segundo lugar, es importante implementar autenticación mutua entre tarjeta y lector, de forma que el sistema no se limite a comprobar un identificador, sino que pueda verificar que la credencial es legítima.

También resulta fundamental una correcta gestión de claves. Deben evitarse claves por defecto, claves compartidas entre múltiples tarjetas y configuraciones heredadas. La diversificación de claves reduce el impacto si una credencial queda comprometida.

Por último, los sistemas deberían apoyarse en controles adicionales en el *backend*, como detección de anomalías, límites temporales, revocación de credenciales y validación del contexto de uso. La seguridad no debería depender únicamente de la tarjeta.

## 5.4. Consideraciones éticas y legales

Todas las pruebas realizadas en este trabajo se han llevado a cabo con fines académicos y de investigación, utilizando material propio o destinado a experimentación. El objetivo no es promover el uso indebido de estas técnicas, sino comprender las debilidades de estas tecnologías para poder proponer medidas de protección.

Las técnicas descritas solo deben aplicarse en entornos controlados y autorizados. Su uso sobre tarjetas, sistemas de transporte, medios de pago, controles de acceso o infraestructuras de terceros sin permiso puede ser ilegal y causar perjuicios económicos u operativos.

Por este motivo, el trabajo evita proporcionar datos sensibles de sistemas reales y limita la experimentación a escenarios seguros y reproducibles.

## 5.5. Limitaciones y ampliaciones

El trabajo se ha desarrollado en un entorno de laboratorio, utilizando dispositivos, tarjetas y etiquetas propias o destinadas a experimentación. Esto permite analizar las vulnerabilidades de forma controlada y segura, aunque también limita el alcance de los resultados, ya que los sistemas reales pueden incorporar mecanismos adicionales de validación, monitorización, detección de fraude, listas de revocación o controles en *backend*.

Otra limitación es que el análisis se ha centrado principalmente en la tarjeta o etiqueta como elemento de identificación, sin profundizar en todos los componentes del sistema que intervienen en la toma de decisiones. En muchos casos, la seguridad real no depende únicamente de si una credencial puede ser leída, clonada o emulada, sino de cómo responde el lector, qué comprueba el *backend* y si existen controles para detectar usos anómalos o credenciales comprometidas.

Asimismo, algunos vectores avanzados, como determinados ataques de relay o ataques de canal lateral, no se han implementado de forma práctica. Estos escenarios requieren un entorno experimental más específico y un mayor control sobre todos los elementos del sistema, por lo que en este trabajo se han tratado únicamente de forma teórica.

Como ampliación futura, sería interesante construir un laboratorio completo de control de accesos, integrando credenciales, lectores, *backend* y gestión de usuarios. Esto permitiría estudiar no solo la seguridad de la tarjeta, sino también la lógica de validación, la revocación de permisos, la detección de usos anómalos y la respuesta ante intentos de emulación o clonación funcional.

También sería interesante extender el análisis a otros mecanismos de identificación y acceso que comparten problemas similares, como códigos QR, códigos de barras y sistemas de radiofrecuencia empleados en accesos físicos, parkings, barreras o mandos remotos. En el caso de QR y códigos de barras, se podrían comparar credenciales estáticas y dinámicas, evaluando riesgos como la copia mediante fotografía, la reutilización de capturas de pantalla, el reenvío a terceros o una validación insuficiente en *backend*.

En sistemas de radiofrecuencia, una posible ampliación sería comparar mecanismos de códigos fijos, códigos variables y esquemas de desafío-respuesta, analizando su resistencia frente a ataques de captura, repetición, emulación e interferencia. Esto permitiría ampliar el trabajo desde el análisis de tarjetas concretas hacia un estudio más general de sistemas de acceso.

# Referencias bibliográficas

Almeida, M. (s. f.). *Hacking Mifare Classic Cards*.

*Cifrado en bloque I – Numerentur.org*. (s. f.). Recuperado 11 de junio de 2026, de https://numerentur.org/cifrado-en-bloque/

*¿Cuáles son las Dos Funciones de Hash Comunes?* (2024, abril 21). Tutoriales Dongee. https://www.dongee.com/tutoriales/cuales-son-las-dos-funciones-de-hash-comunes/

egginabucket. (2026). *Egginabucket/openmsr* [Go]. https://github.com/egginabucket/openmsr (Obra original publicada en 2023)

*Enabling Seamless and Secure Payments Worldwide*. (s. f.). EMVCo. Recuperado 27 de febrero de 2026, de https://www.emvco.com/

*Flipper Lab*. (s. f.). Recuperado 12 de abril de 2026, de https://lab.flipper.net/apps/nfc_magic

Grover, A., & Berghel, H. (s. f.). *A Survey of RFID Deployment and Security Issues*.

*ISO/IEC 7811-1:2018*. (s. f.). ISO. Recuperado 27 de febrero de 2026, de https://www.iso.org/standard/73637.html

*ISO/IEC 14443-1:2018—Cards and security devices for personal identification—Contactless proximity objects—Part 1: Physical characteristics*. (s. f.). Recuperado 27 de febrero de 2026, de https://www.iso.org/standard/73596.html

*ISO/IEC 15693-1:2018*. (s. f.). ISO. Recuperado 27 de febrero de 2026, de https://www.iso.org/es/contents/data/standard/07/08/70837.html

kamkar, samy. (2026). *Samyk/magspoof* [C]. https://github.com/samyk/magspoof (Obra original publicada en 2015)

Klostermeier, G. (2026). *Ikarus23/MifareClassicTool* [Java]. https://github.com/ikarus23/MifareClassicTool (Obra original publicada en 2013)

*Lector de Tarjetas magnéticas, Lector de Tarjetas de Banda magnética USB MSR90, 3 Pistas Mini mag Hi-Co Swiper, para POS, Banca, Lealtad, Control de Acceso, Verificación de Identidad: Amazon.es: Oficina y papelería*. (s. f.). Recuperado 11 de junio de 2026, de https://www.amazon.es/Regun-Lector-Tarjetas-Banda-magn%C3%A9tica/dp/B08DYBY3NM

Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and PIN is Broken. *2010 IEEE Symposium on Security and Privacy*, 433-446. https://doi.org/10.1109/SP.2010.33

*Radiografía de un Skimmer: ¿Cómo Trabajan? | Blog oficial de Kaspersky*. (2015, enero 21). https://latam.kaspersky.com/blog/radiografia-de-un-skimmer-como-trabajan/4837/

RC4. (2025). En *Wikipedia, la enciclopedia libre*. https://es.wikipedia.org/w/index.php?title=RC4&oldid=165866315

*¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet? | Ciudadanía | INCIBE*. (s. f.). Recuperado 11 de junio de 2026, de https://www.incibe.es/ciudadania/blog/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. *2012 IEEE International Conference on Intelligence and Security Informatics*, 227-234. https://doi.org/10.1109/ISI.2012.6284315

Scaife, N., Peeters, C., Velez, C., Zhao, H., Traynor, P., & Arnold, D. (2018). The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. *2018 IEEE Symposium on Security and Privacy (SP)*, 1063-1076. https://doi.org/10.1109/SP.2018.00042

*Software Download*. (s. f.). Osayde.Com. Recuperado 10 de abril de 2026, de https://www.osayde.com/pages/software-download

Svigals, J. (2012). The long life and imminent death of the mag-stripe card. *IEEE Spectrum*, *49*(6), 72-76. https://doi.org/10.1109/MSPEC.2012.6203975

Veniamin Ginodman, M., Ms. Natalya Obelets, Mr Ram Herkanaidu, & Azhari, F. (2014). Quick detection of NFC vulnerability: Implementation weakness exploitation. *Information Management & Computer Security*, *22*(2), 134-140. https://doi.org/10.1108/IMCS-09-2013-0067