

# Vulnerabilidades en dispositivos de monitorización continua de glucosa

Análisis técnico del sistema Abbott FreeStyle Libre 14-Day

RF Village HackGDL 2025:

Wulfrano Moreno / [wulfrano@mexbalia.mx](mailto:wulfrano@mexbalia.mx)

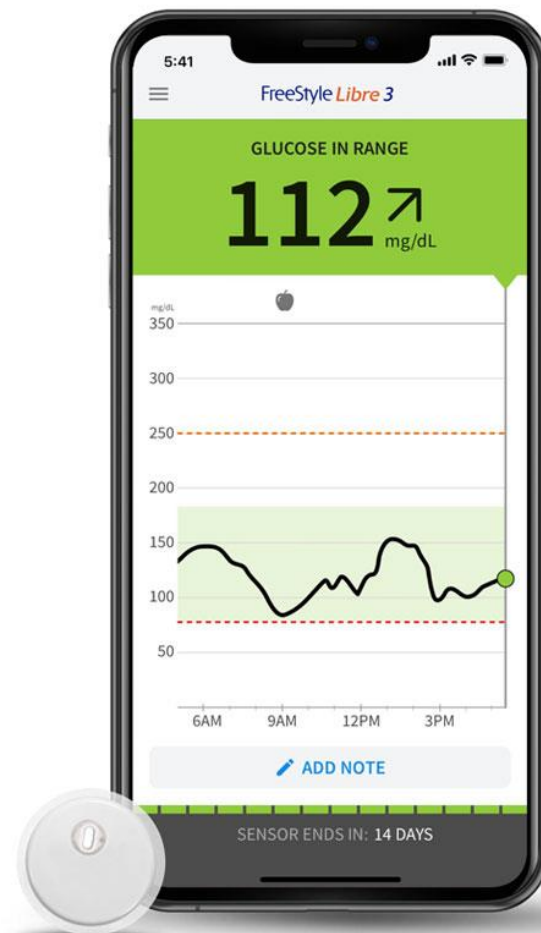


## Acerca de mí

- CTO, empresario, arquitecto empresarial e instructor
- Entusiasta de la ciberseguridad
- 30 años en TI
- 25 años Web/Nube (1,2,3)
- Amplia experiencia en diversos escenarios de integración
- Certificaciones TI
- Creador digital
- OpenEnchilada OG

# Agenda

1. Introducción al sistema FreeStyle Libre
2. Aplicaciones médicas y validación clínica
3. Diseño biomédico y características técnicas
4. Aspectos químicos del sensor
5. Hardware y firmware
6. Vulnerabilidades identificadas
7. Prueba de concepto
8. Demo
9. Implicaciones éticas y médicas
10. Estrategias de mitigación
11. Conclusión



# Introducción al FreeStyle Libre

- Propósito: Monitorización continua de glucosa (CGM) para diabetes.
- Tecnologías clave:
  - Sensor subcutáneo con NFC pasivo (13.56 MHz).
  - Mide glucosa en líquido intersticial (sin punción en dedo).
- Beneficios:
  - Menos invasivo
  - Datos en “tiempo real”
  - Integración de sensores y plataformas digitales



# Aplicaciones médicas y validación clínica

## Uso en diabetes

- Tipo 1 y 2
- Gestacional

## Monitorización remota y telemedicina

## Alta precisión (

- MARD ~9,4%
- Zona A de error

## Aprobaciones



# Diseño biomédico y características técnicas

## Biocompatibilidad y Portabilidad

- Adhesivo hipoalergénico
- Resistente al agua y al sudor

## Mecánica del sensor

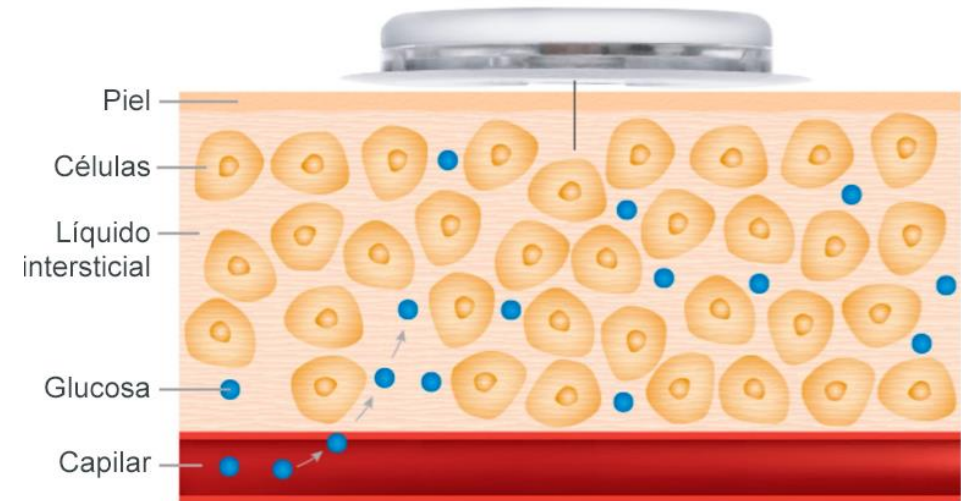
- Microfilamento biocompatible (5 mm bajo la piel).
- Reacción enzimática (glucosa oxidasa → peróxido de hidrógeno → señal eléctrica).

## Transmisión de datos

- NFC 13.56 MHz ISO/IEC 14443 (almacena datos cada 60 segundos, 8 horas de historial).
- Sin batería: alimentado por el lector durante el escaneo.

# Aspectos químicos del sensor

- Cableado enzimático:
  - Uso de glucosa oxidasa (GOx) modificada con polímeros redox (osmio).
  - Transformación de la enzima en un conductor de carga
  - Generación de corriente proporcional a la concentración de glucosa
  - Evolución desde el cableado con ferroceno hasta hidrogeles redox
- Ventajas: No lixiviables, permeables a la glucosa.
- Comparación de mediciones: Retraso de 5-10 minutos vs. glucosa en sangre.





# Hardware y Firmware

- Componentes clave:
  - Chip RF430 TAL TI (procesamiento NFC, memoria FRAM).
  - Sensor de temperatura (termistor para calibración).
  - Antena NFC y batería de respaldo.
- Diseño:
  - Ensamblaje compacto y sellado
  - Protección de memoria mediante CRC16 para integridad de memoria y contraseñas
- Limitaciones: Chip Texas Instruments personalizado sin documentación pública.





# Vulnerabilidades identificadas

- Riesgos en NFC:
  - Ataques de repetición.
  - Inyección de datos.
  - Manipulación de memoria.
- Ejemplos:
  - Alteración del tiempo de uso del sensor.
  - Anulación de bloqueo geográfico.
  - Falta de autenticación mutua.



# Prueba de Concepto (NFC)

- Hardware usado: HunterCat NFC (Electronic Cats)
- Implicaciones en la manipulación de datos y en el estado del sensor
- Pasos:
  - Configuración y conexión hardware
  - Captura y análisis de datos NFC
  - Reproducción de datos para demostrar vulnerabilidades





Demo

0x00000000 23 6A 48 11 01 00 00 00 00 00 00 00 00 00 00  
0x00000010 00 00 00 00 00 00 00 00 62 C2 00 00 00 00 00  
0x00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Header

Data

...  
0x000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000140 26 44 00 01 AB 08 25 51 14 07 96 80 5A 00 ED A6  
0x00000150 00 6A 1A C8 04 AD F9 6A 9E 42 21 83 F2 90 07 00  
0x00000160 06 08 02 24 0C 43 17 3C C2 43 08 08 B2 40 DF 00  
0x00000170 08 08 D2 42 A2 F9 08 08 D2 42 A3 F9 08 08 0C 41  
0x00000180 0C 53 92 12 90 1C 5C 93 03 20 A2 41 08 08 02 3C  
0x00000190 B2 43 08 08 1C 43 21 53 30 41 0A 12 4A 4C 4C 93  
0x000001A0 0B 20 B2 40 50 CC 02 07 92 D3 00 07 B2 C0 00 02  
0x000001B0 00 07 A2 D2 00 07 02 3C 92 12 82 1C 32 D0 D8 00  
0x000001C0 E2 B3 C3 1C 09 28 E2 C3 C3 1C 4A 93 05 24 12 C3  
0x000001D0 12 10 A4 1C 12 11 A4 1C 3A 41 30 41 0A 12 0B 12  
0x000001E0 08 12 09 12 06 12 F2 90 07 00 06 08 68 20 B0 12  
0x000001F0 3A FB 61 20 92 12 78 1C 3A 40 FA F9 4C 43 8A 12  
0x00000200 3B 40 84 1C 26 4B 38 40 B0 F9 39 40 A4 1C B2 90  
0x00000210 00 20 A4 1C 09 2C 1F 43 B0 12 30 FB 3F 40 00 20  
0x00000220 2F 89 82 4F A4 1C 06 3C 0F 43 B0 12 30 FB B2 50  
0x00000230 00 E0 A4 1C 92 52 A4 1C A4 1C 2F 49 7E 42 0D 43

Footer

Patch code

&

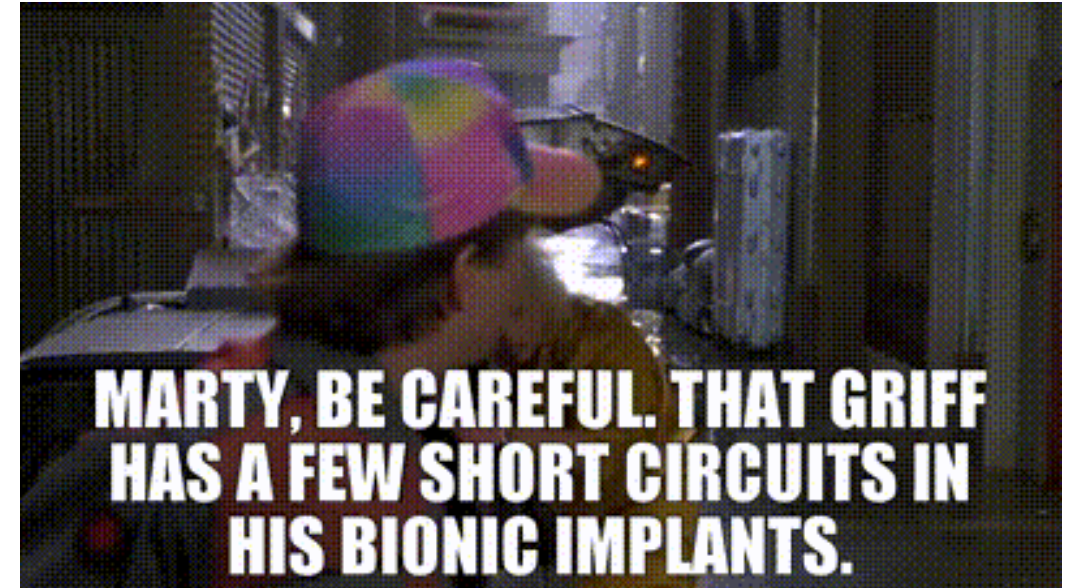
Proprietary  
NFC functions

...  
0x000006B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x000006C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x000006D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x000006E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x000006F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
0x00000720 00 00 00 00 00 00 00 00 FF FF 84 FD 25 00 9A FC  
0x00000730 14 00 50 FC 19 00 20 FC 03 00 5F F5 00 00 00 00  
0x00000740 00 00 00 00 00 00 00 00 00 00 00 00 AB AB 4A FB  
0x00000750 E2 00 3C FA E1 00 AE FB AB AB 2C 5A A4 00 CA FB  
0x00000760 A3 00 56 5A A2 00 BA F9 A1 00 24 57 A0 00 AB AB  
0x00000770 00 00 00 00 FF FF FF FF 20 00 71 62 00 00 00  
0x00000780 00 00 00 00 00 00 00 00 00 AE 5C 00 00 A8 57  
0x00000790 00 00 28 4E 68 45 00 00 DC 5F AE 5A 7A 5A DA 50

Interrupt vect.

# Implicaciones éticas y médicas

- Riesgos para pacientes:
  - Sobredosis de insulina por datos falsos.
  - Privacidad: Exposición de historiales médicos.
- Regulatorios: Sensores manipulados infringen certificaciones (FDA/CE).
- Éticos: Mercado negro de sensores pirateados.





# Estrategias de mitigación

## Mejoras técnicas

- Cifrado NFC (ej. AES) y códigos rodantes.
- Autenticación mutua sensor-lector.
- Actualizaciones periódicas de firmware.

## Ciberseguridad en dispositivos biomédicos

- Reforzamiento de normativas y estándares

## Concientización

- Educación de usuarios sobre riesgos.
- Aplicaciones móviles con anti manipulación.



# Conclusión

- Fortalezas:
  - Innovación en CGM.
  - Precisión clínica.
  - Portabilidad.
- Retos:
  - Las vulnerabilidades identificadas plantean riesgos significativos, especialmente en la manipulación de datos.
  - Se requieren medidas integrales de seguridad para salvaguardar la salud del paciente.
  - Retraso en mediciones.
  - Vulnerabilidades NFC.
- Futuro:
  - Equilibrar avances tecnológicos con robustos mecanismos de seguridad.
  - Integración de Bluetooth para alertas en tiempo real.
  - Sensores más seguros con IA y biosensores avanzados (parches de microagujas).