# PEGASUS: El Spyware que Vigila a Periodistas y Activistas

# ¿Qué es Pegasus?

Pegasus es un software espía desarrollado por la empresa israelí NSO Group (fundada en 2010 por Shalev Hulio, Omri Lavie y Niv Carmi). Surgió como una herramienta de vigilancia legal para gobiernos, pero su uso se ha extendido a objetivos políticos, periodistas y activistas.

Año de creación: 2011 (primeras versiones conocidas).

Empresa matriz: NSO Group, con sede en Herzliya, Israel.

Inversores: Berkeley Research Group (BRG), Novalpina Capital (adquirió NSO en 2019).

Relación con el gobierno israelí: Operaba bajo licencia del Ministerio de Defensa israelí (exportación controlada como "arma cibernética").

# Tecnología y Funcionamiento

- Pegasus es un malware de acceso remoto (RAT) que infecta dispositivos móviles (iOS y Android).
- Métodos de Infección
- Explotación de vulnerabilidades zero-click:
- iMessage (Apple): CVE-2021-30860 (ForcedEntry).
- WhatsApp (CVE-2019-3568): En 2019, se usó un bug en llamadas VoIP para infectar sin interacción.
- Phishing: Enlaces maliciosos enviados por SMS o correo.
- Wi-Fi y Bluetooth: Ataques a redes vulnerables.

# Capacidades

Extracción de datos: Mensajes, correos, fotos, ubicación GPS.

Grabación de audio y video: Activación remota de micrófono y cámara.

Keylogging: Registro de pulsaciones de teclado.

Persistencia: Reinfección tras reinicio del dispositivo.

# Evolución Técnica

Versión 2016: Requería clics en enlaces.

Versión 2019-2021: Zero-click (sin interacción del usuario).

Modo "Network Injector": Intercepta tráfico en redes móviles (3G/4G).

# Empleabilidad y Clientes

NSO Group vende Pegasus exclusivamente a gobiernos y agencias de seguridad, pero investigaciones revelan abusos.

Clientes Confirmados o Sospechosos:

- México: Gobierno de Peña Nieto (2016-2017) espió a periodistas, políticos opositores y activistas. ASÍ FUE COMO EL GOBIERNO DE PEÑA NIETO ESPIÓ A PERIODISTAS CON PEGASUS.
- Arabia Saudita: Usado contra Jamal Khashoggi (asesinado en 2018) y familiares.
- Hungría: Viktor Orbán espió a opositores (2021, Citizen Lab).
- India: Gobierno atacó a políticos de oposición y periodistas (The Wire, 2021).
- España: Caso Cataluña (espionaje a independentistas, 2020).
- Emiratos Árabes Unidos: Diana, esposa del jeque Mohammed bin Rashid, hackeada (2020).

# Números Clave

Resumen de Vigilancia de Pegasus

120

**Números Vigilados**

Más de 50,000 números monitoreados

**Presencia Global**

Operaciones en 45 países

**Costo de Licencia**

$650,000 por 10 dispositivos

# Eficacia de Infección y Detecciones:

Pegasus es extremadamente efectivo, con una tasa de éxito superior al 90% en dispositivos no parcheados, según Citizen Lab.

Los ataques "zero-click" permiten la infección en menos de 2 minutos, sin necesidad de interacción del usuario.

Google Project Zero identificó 14 vulnerabilidades críticas explotadas por Pegasus entre 2014 y 2021. Estas vulnerabilidades permitieron ataques sofisticados y difíciles de detectar.

Amnistía Internacional descubrió que el 67% de los dispositivos analizados mostraban rastros de Pegasus, destacando su uso generalizado para espiar a periodistas, activistas y figuras políticas.

Una gran vulnerabilidad /

# Una amenaza terrorífica, así ha descrito Google al malware Pegasus de los iPhone

Project Zero ha analizado el malware, y comprobado su peligrosidad

¿Hasta cuándo se actualizará el iPhone 7? | Tecnoexplora

Jorge Sanz Fernández
Madrid
Publicado: 17 de diciembre de 2021, 15:16

Las más vistas | Lo último

- https://www.lasexta.com/tecnologia-tecnoxplora/moviles/amenaza-terrorifica-asi-descrito-google-malware-pegasus-iphone_2021121761bc9bc397e21a00014dfef7.html

# Actividades maliciosas: EE.UU. incluye en la lista negra a las empresas de software espía israelí NSO Group y Candiru

El Departamento de Comercio dice que las empresas israelíes sospechosas de estar vinculadas a "actividades contrarias a la seguridad nacional o a los intereses de la política exterior de Estados Unidos"

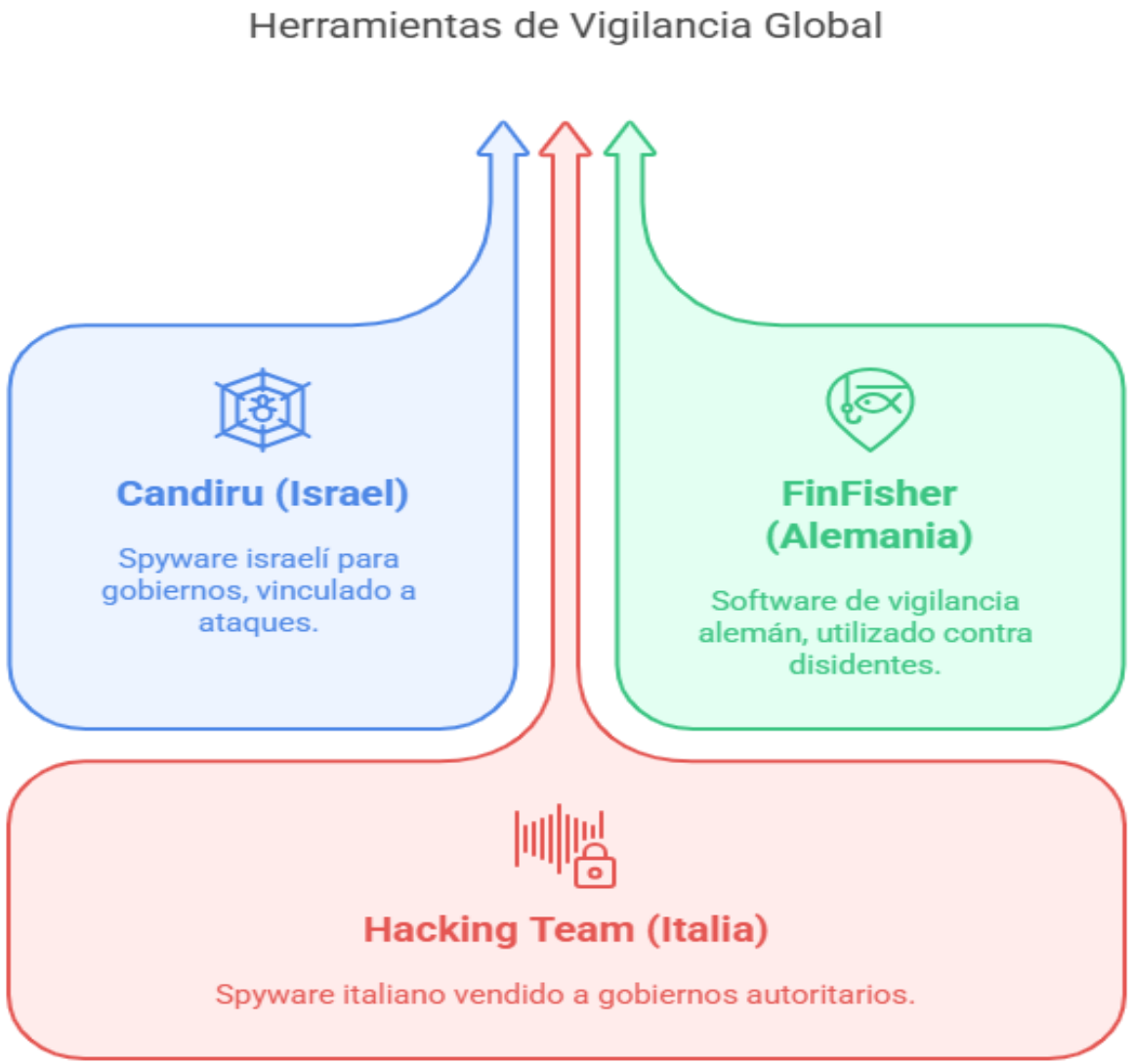
Por **PERSONAL DE TOI** y **JACOB MAGID** SEGUIR

3 de noviembre de 2021, 17:05

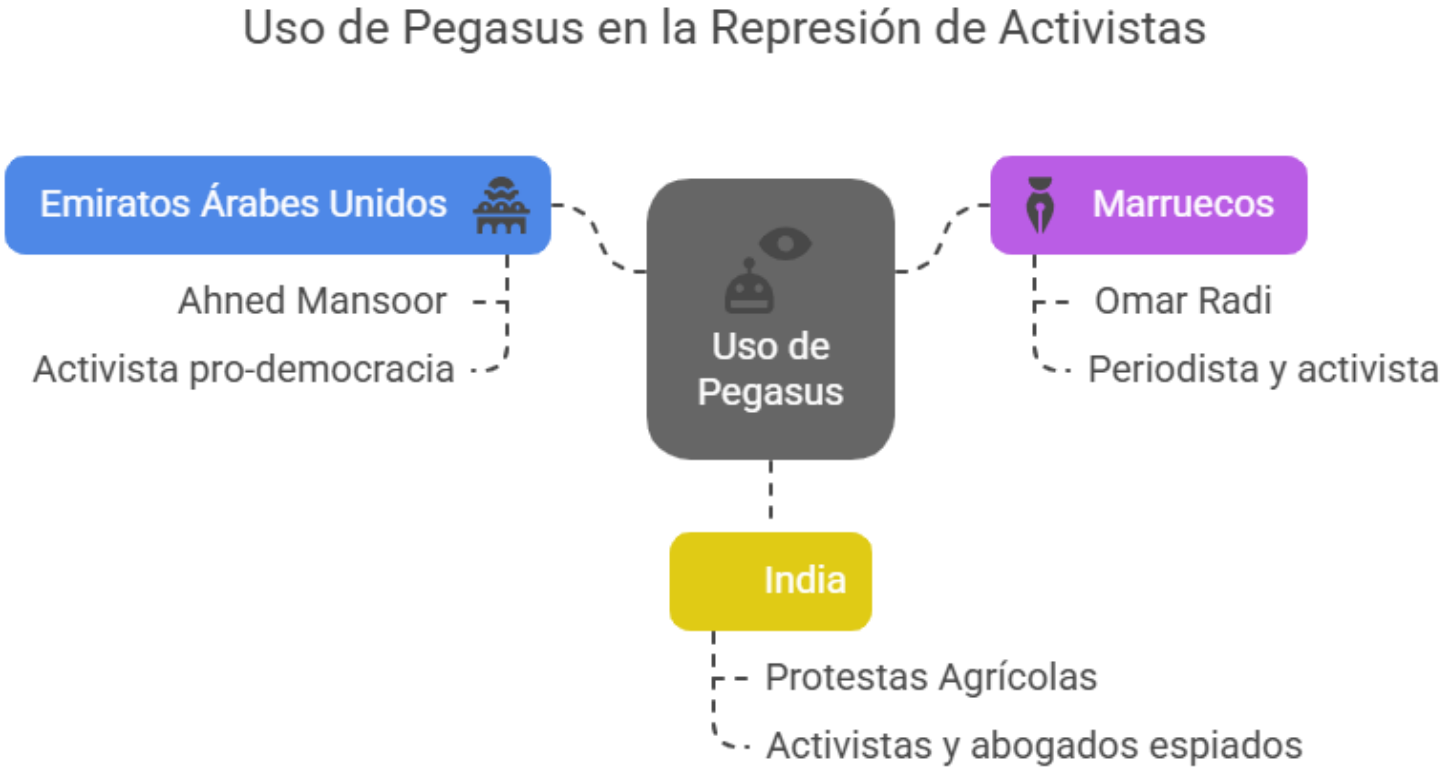
6

- https://www.timesofisrael.com/us-blacklists-israels-nso-group-and-candiru-spyware-firms/

# Alternativas y Competidores



# Activistas y Defensores de Derechos Humanos



# Consecuencias del Espionaje

Autocensura: Periodistas y activistas dejan de investigar por miedo.

Arrestos arbitrarios: Como en Marruecos y EAU.

Asesinatos: Casos como Khashoggi y Pineda Birto vinculados al spyware.

# Estadísticas de represión post-infección:

| País | Periodistas espiados | Activistas arrestados | Muertes vinculadas |
|---|---|---|---|
| México | 25+ | 12+ | 3+ |
| India | 40+ | 300+ (protestas) | 1+ |
| Arabia Saudita | 15+ | 50+ | 1 (Khashoggi) |
| Hungría | 5+ | 0 (pero intimidación) | 0 |

# ¿Cómo se Descubrieron Estos Casos?

The Pegasus Project (2021): Investigación de 17 medios internacionales.

Citizen Lab (Universidad de Toronto): Análisis forense de dispositivos.

Amnistía Internacional: Técnicas de detección en teléfonos iPhone y Android.

# Resumen:

Pegasus ha sido un arma de represión masiva, con un impacto demostrable en:

- ✅ Periodistas (silenciamiento de investigaciones).
- ✅ Activistas (encarcelamientos y vigilancia constante).
- ✅ Políticos (manipulación de procesos democráticos).

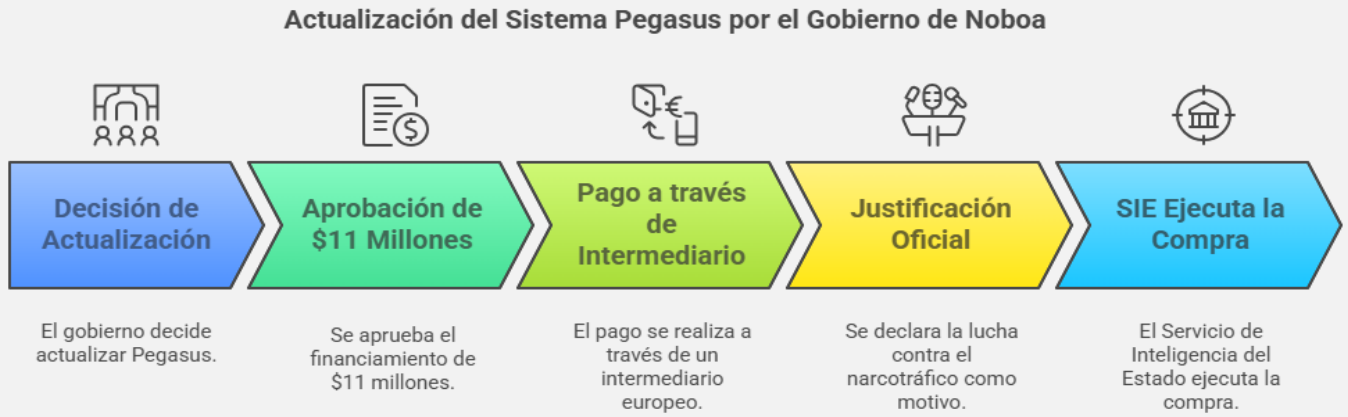
El 60% de las víctimas nunca supo que estaba siendo espiada hasta que organizaciones como Citizen Lab lo revelaron.

# El Uso de Pegasus en Ecuador

Ecuador ha estado vinculado a la adquisición y uso del spyware Pegasus, con compras confirmadas durante el gobierno de Rafael Correa (2007-2017) y una controvertida actualización en 2023 bajo el gobierno de Daniel Noboa, por un costo de $11 millones de dólares.

- Adquisición Original en el Gobierno de Correa (2014-2015)
- Fecha de compra: Entre 2014 y 2015, a través de la empresa israelí NSO Group.
- Costo inicial: Alrededor de $6 millones de dólares (según investigaciones de La Posta y Citizen Lab).
- Entidad compradora: Dirección Nacional de Inteligencia (DNI), bajo el mando de Pablo Romero, secretario de Inteligencia de Correa.
- Objetivo declarado: "Lucha contra el crimen organizado y el terrorismo".

En noviembre de 2023, el gobierno de Daniel Noboa aprobó una actualización del sistema Pegasus por $11 millones de dólares.



# Comparación con Otros Países de la Región

Ecuador es uno de los pocos países sudamericanos con compras confirmadas de Pegasus (junto con México y Panamá).

| PAÍS | AÑO DE COMPRA | COSTO ESTIMADO | USO CONFIRMADO CONTRA |
|---|---|---|---|
| **Ecuador** | 2014-2015 (actualizado en 2023) | **$17M (total)** | Periodistas, opositores |
| **México** | 2016 | **$32M+** | Periodistas, activistas |
| **Panamá** | 2019 | **$8M** | Políticos rivales |
| **El Salvador** | 2020 | **$12M** | Medios críticos a Bukele |

# Cifras Relevantes de Ecuador:

- Total de activistas y defensores espiados: Al menos 15 (confirmados por Citizen Lab).
- Período crítico: 2014-2017 (gobierno de Correa) y reactivación en 2023 (gobierno de Noboa).

El spyware Pegasus fue una herramienta de represión sistemática en Ecuador, dirigida a:

- Silenciar protestas ambientales.
- Obstruir la labor de defensores de DDHH.
- Intimidar a movimientos sociales críticos.

# Guía de Protección contra Pegasus para Activistas y Periodistas

- Para Dispositivos Móviles (iPhone y Android)
- ✅ Actualizaciones constantes:
- Instala todas las actualizaciones de iOS/Android (Pegasus explota vulnerabilidades parcheadas en versiones recientes).
- Ejemplo: iOS 16.6+ y Android 12+ tienen protecciones mejoradas.
- ✅ Usa un dispositivo separado para trabajo sensible:
- Un teléfono "limpio" (sin apps personales) solo para comunicaciones críticas.
- Ideal: iPhone sin jailbreak (Apple tiene protecciones más fuertes contra spyware).
- ✅ Protege tu número de teléfono:
- Usa un número secundario (Google Voice, Burner) para contactos de riesgo.
- Evita publicar tu número real en redes.
- ✅ Configuración de seguridad avanzada:
- iPhone: Activa Bloqueo de Modo (Settings → Face ID & Passcode → "Stolen Device Protection").
- Android: Usa Google Advanced Protection Program (requiere llaves físicas de seguridad).

**¿Cómo asegurar las comunicaciones digitales?**

### Usar Signal

La opción más segura para mensajes y llamadas.

### Usar WhatsApp

Seguro si está actualizado, pero evita archivos adjuntos.

### Verificar enlaces

Verifica URLs con herramientas como VirusTotal.

### Usar ProtonMail

Proporciona correo electrónico seguro con E2EE. Habilita autenticación de dos factores (2FA)

¿Cómo protegerse contra el espionaje digital?

## Implementar contraseñas fuertes

Usar contraseñas largas y autenticación biométrica para la seguridad de la cuenta

## Elegir aplicaciones de mensajería seguras

Evitar aplicaciones de mensajería no verificadas para la comunicación privada

## Instalar aplicaciones de fuentes oficiales

Asegurarse de que las aplicaciones provengan de tiendas oficiales para evitar malware

## Usar almacenamiento en la nube seguro

Utilizar discos duros cifrados offline para backups sensibles

# Herramienta para verificar infección:

MVT (Mobile Verification Toolkit):

Analiza tu iPhone/Android en busca de rastros de Pegasus.

Kit de herramientas de verificación móvil

# Resumen de Herramientas Clave

| Categoría | Herramienta Recomendada | Alternativa |
|---|---|---|
| **Mensajería** | Signal | WhatsApp (actualizado) |
| **Correo** | ProtonMail | Tutanota |
| **Videollamadas** | Jitsi Meet | Signal |
| **Almacenamiento** | Cryptomator | Tresorit |
| **Navegación** | Tor Browser | Brave + Tor |

# Plan de Contingencia si Eres Objetivo

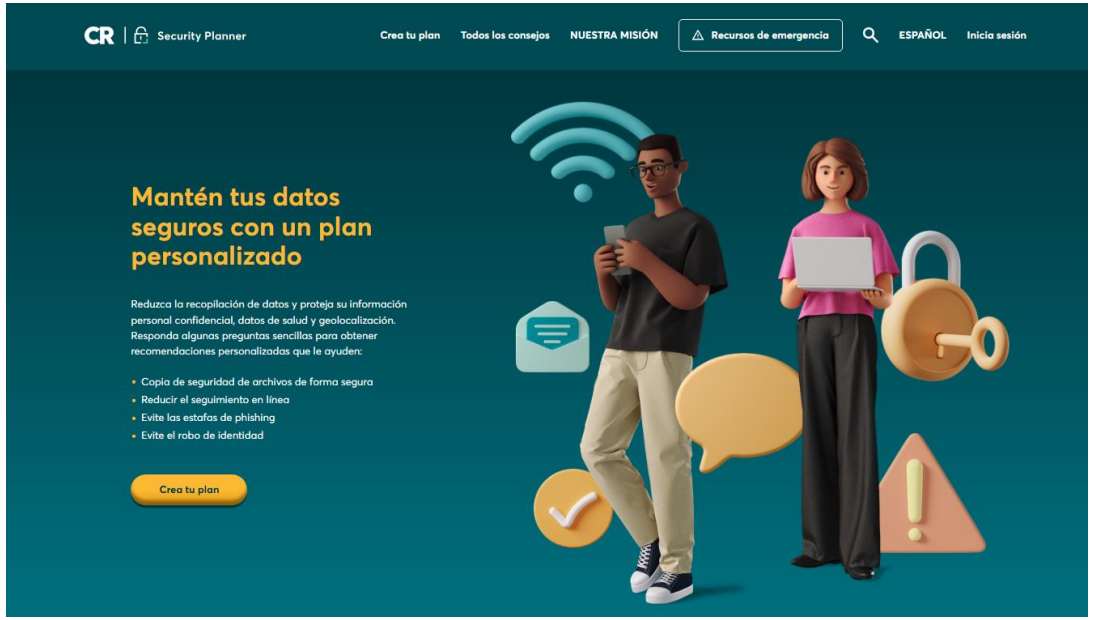
Pasos inmediatos:

- Aísla el dispositivo: Apágalo y desconéctalo de Internet.
- Cambia todas tus contraseñas desde otro dispositivo seguro.
- Notifica a tu organización o red de apoyo.

Denuncia:

- Internacional: CIDH, Access Now.
- Local: Fundaciones de DDHH.

# Recursos Adicionales




- Guía de seguridad de Citizen Lab: [Security Planner]
- Talleres de ciberseguridad para activistas.
- Asesoría legal.

Recuerda: Ningún sistema es 100% seguro, pero estas medidas reducen drásticamente el riesgo de espionaje.

¡Gracias por su atención!