

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández	13/12/2025
GRUPO 7		

## Actividad grupal. Vectores de ataque

Con esta práctica conseguiremos documentar un ciberdelito, analizándolo al máximo en su funcionamiento, bien a través de código, vídeos, artículos científicos, prensa, etc.

Un vector de ataque es el camino que usa un ciberdelincuente para acceder al activo objetivo del ataque.

## Sobre la práctica

El objetivo es documentar un **ataque de phishing en redes inalámbricas usando WiFi Pineapple con portal cautivo**. En el proyecto, se detallan los conceptos básicos que más relevantes, se realiza una prueba de concepto, analizado posibles variaciones y documentado cómo protegerse de este tipo de ataques.

Toda la información recopilada está disponible en esta página web:  
<https://ciberunir.github.io/practica-grupal/>

La web está alojada en Github. Junto a este documento se incluye el ZIP del proyecto, con toda la documentación, que también es accesible a través del repositorio (<https://github.com/ciberunir/practica-grupal>). Ejecutando el index.html podemos visualizar la página web de forma local.

No obstante, en el presente documento, se adjuntan imágenes del trabajo realizado:

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández  GRUPO 7	13/12/2025



The screenshot shows a web-based educational platform for learning about WiFi phishing attacks. The main navigation bar includes links for 'Conceptos básicos', 'Prueba de concepto', 'Variaciones', 'Protocolos', 'Enlaces de interés', and 'Autosíntesis'.

## Conceptos básicos

**¿Qué es el phishing?**

El phishing es una técnica de ingeniería social utilizada por ataques para engañar a las víctimas y obtener información confidencial como credenciales de acceso, datos bancarios o información personal. Los ataques se basan justo por ventajas legítimas para ganar la confianza de sus víctimas.

Existen diferentes variantes de phishing:

- Correo electrónico falso: mensajes que imitan a bancos, empresas de pago o plataformas conocidas.
- Sociofísico: phishing a través del MMS con señales visuales.
- Vishing: llamadas telefónicas en las que el atacante冒充a una entidad legítima.
- Pharming: manipulación de DNS para redirigir a sitios fraudulentos.

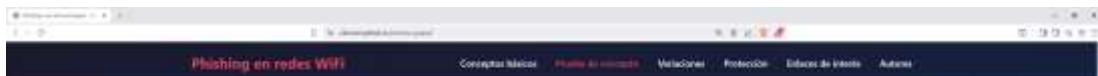
Las consecuencias incluyen robos de credenciales, fraude financiero y suplantación de identidad. Recomendada para revisar la conferencia sobre la IREA, incluyendo el tema suplantación, así como autenticación multifactor (MFA) y mantener actualizada la barra de seguridad. De la sección [Glossario](#) se accede a más detalles.

**¿Qué es WiFi Pineapple?**

WiFi Pineapple es un dispositivo de análisis de redes destinado a detectar ataques. Aunque su uso legal es para pruebas de penetración y formación en ciberseguridad, también puede ser explotado por ataques.

Los principales componentes incluyen:

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández  GRUPO 7	13/12/2025

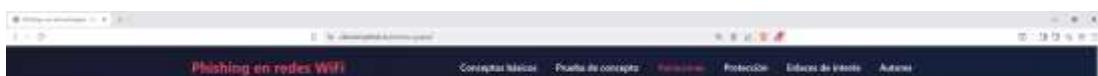


#### Material empleado

Para llevar a cabo este proyecto del conocimiento se necesitó el siguiente material:

- Dispositivo [WiFi Pineapple](#) (Placa de red inalámbrica "WIFI").
- Ordenador para la configuración (no requiere ninguna prestación específica).
- Conexión a Internet.
- Dispositivo o dispositivo móvil (smartphone, tablet, laptop) para activar modo captivo. Algunos que tienen conectividad WiFi.

WiFi Pineapple es un dispositivo no apto para todos los dispositivos. Deben instalar en el mercado. [www.wifipineapple.com](http://www.wifipineapple.com) (No) con memoria de flash para enviar al que tiene WiFi Pineapple por lo que se puede cargar el firmware oficial que WiFi Pineapple ofrece o tienen abierto en su [portal de descargas](#). Hay muchísima documentación en internet sobre el proyecto de convertir uno de estos routers en una pista. Un le recomienda que WiFi Pineapple no dejen objetos peligros de intento por si se cae por agua volviendo que no tiene partes de la PlC.



## Variaciones del ataque

### 1. Ataque con deautentificación

Este variante consiste en engañar al router para que el envío de tráfico de datos entre cliente y el autoridad IEEE 802.11. El objetivo es forzar a los dispositivos a desasociarse de su punto de acceso legal para que, en la ocasión, interactúen únicamente con el punto de acceso falso ofrecido por el atacante WiFi Pineapple.

- **Riesgo del ataque:** Si se logra identificar el MAC del punto de acceso real y los clientes conectados, y empieza a enviar tráfico de datos incorrecto y falsificado dirigido al cliente y al AP.
- Al recibir múltiples tramas de deautentificación, el dispositivo intentará que ha perdido la conexión y comienza a buscar redes disponibles.
- En ese momento, el Pineapple envía un AP con el nombre D02 que le es original, normalmente con mayor potencia o en un canal menos saturado.
- El dispositivo se reconecta automáticamente al AP falso, ya que la interfaz con la nueva red conectada.

**Qué es el ataque:** en resumen como el usuario lo permite una falsa red pirateada. Discretamente WiFi o ningún sistema visible. La conexión puede ser transparente.

**Qué es el ataque:** en la interfaz del Pineapple aparecen nuevas rutas asociadas al AP falso, solicitudes DHCP de nuevos hosts y URLs HTTP, almacenando el dispositivo.

**Límite:** Este ataque es más efectivo en redes con protocolos IEEE 802.11a (PMP) o universo WiFi 6/6E. Los sistemas de cliente AP que pueden detectar o limitar el ataque. Algunas dispositivas pueden priorizar la red real si sigue siendo estable y estable.

Asignatura	Datos de los alumnos	Fecha
Seguridad en los Sistemas de Información	Ignacio Delgado Torrejón José Carlos Gallego Cano Juan Antonio Aguado Gallego Silvia Rodríguez Fernández  GRUPO 7	13/12/2025



## Cómo protegerse

**User VPN**

- Verificar la conexión HTTPS
- Desactivar WiFi automático
- Activación de modo furto
- Descargar de redes públicas
- Eliminar redes guardadas
- Activar el software actualizado
- Usar protocolos de cifrado

**User VPN**

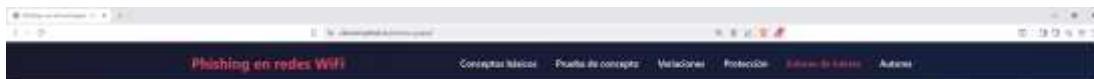
Usar una VPN (Red Privada Virtual) permite cifrar todo el tráfico de red de manera segura, impidiendo que un atacante pueda leer la información interceptada.

**Amenaza sin VPN**

- Interceptar (SePhingo o WiFiPwn) todo lo que entra y salirte al mundo protegido por HTTPS (correo electrónico, contraseñas, imágenes privadas, etc.).
- Realizar ataques Man in the Middle (MitM). Hacelos los datos en tránsito e obligarlos a pasarse cada tránsito (phishing) para robar su información.

**La solución con VPN**

- Instalar una VPN en tu dispositivo móvil y conexión segura y cifrada directamente con los servidores de la VPN (el tráfico de sus búsquedas).
- El atacante solo se atreve (MitM). Tú no vas a ser capaz de leer los datos cifrados y desencriptados.
- La intercepción es imposible. Aunque el atacante intercepta los paquetes de datos, no puede desencriptarlos ni leer su contenido, ya que la clave de cifrado solo la tienen la dispositivo y el servidor VPN.
- Tu actividad permanece privada. El atacante no puede ver a qué sitio web te conectas, qué palabras clave utilizas ni qué búsquedas realizas.



## Enlaces de interés

### Recursos oficiales de WiFi Pineapple

#### Hak5 - WiFi Pineapple

Wiki oficial del dispositivo WiFi Pineapple

#### Wiki de WiFi Pineapple

Documentación oficial, guías de uso y configuraciones del dispositivo

#### Portal de descargas de Hak5

Portal oficial de descargas de recursos de WiFi Pineapple

### Artículos académicos

#### Phishing attacks: A comprehensive study

Último compromiso sobre técnicas de phishing

## Autores del proyecto

Este proyecto ha sido desarrollado como parte de la asignatura de Seguridad de Sistemas de la Información

<b>Silvia Rodríguez Fernández</b> Investigación y desarrollo de la estrategia de investigación de sistemas de información y desarrollo del proyecto	<b>José Carlos Gallego Cano</b> Desarrollo del la Prueba de concepto	<b>Ignacio Delgado Torrejón</b> Análisis de vulnerabilidades	<b>Juan Antonio Aguado Gallego</b> Investigación de diferentes vulnerabilidades y desarrollo de la estrategia