

**TÍTULO DEL PROYECTO:** Ciber Laberinto

**DATOS PERSONALES :**

**Centro:** IES María Casares

**Profesor:** Lucía Rodríguez Ríos

**Alumnas/os:** Javier Iglesias Diaz-Saúl González Sánchez

## **RESUMEN DEL PROYECTO**

Este proyecto es una experiencia física y digital que usa un laberinto para representar la memoria de un dispositivo. En este juego, el azar no sirve para avanzar; cada pasillo bloqueado funciona como un firewall que el jugador debe superar resolviendo un criptograma. Es una simulación interactiva sobre el viaje de los datos: si no descifras la clave, el acceso queda restringido. El objetivo es que el usuario joven deje de ser el eslabón más débil frente al spyware silencioso y aprenda que proteger sus permisos (cámara o GPS) es la única forma de no perder su identidad digital.

## **INTRODUCCIÓN**

Este proyecto nace por la necesidad de concienciar a nuestros adolescentes de que su intimidad puede ser vulnerada con gran facilidad a través de sus dispositivos digitales.

Por esta razón Javier y Saúl decidieron crear este ciber laberinto.

Argumento:

- “Un falso amigo” script malicioso, se ha colado en el laberinto, memoria del cualquier dispositivo móvil, e intenta llegar a tus fotos, conversaciones etc. Para ello tiene que sortear distintas claves de seguridad que el usuario ha colocado en los nodos del laberinto, en un tiempo limitado, si lo logra vuestra intimidad está expuesta a todo el mundo.

Versión digital

- Para crear la versión digital utilizamos Python. Esto nos permite que el laberinto sea visual, que el "script malicioso" se mueva y que aparezcan ventanas para resolver los códigos.

## **PROPÓSITO DEL PROYECTO**

Muchos jóvenes comparten información sin filtros. El laberinto visualiza que cada foto, ubicación o 'like' es un rastro que un script malicioso sigue para vulnerar tu intimidad. Aprenderás que si no puedes descifrar la identidad real de quien te contacta, es mejor no dejarlo entrar a tu zona segura. Tu móvil es una extensión de tu identidad: si no controlas quién recorre sus pasillos (permisos de cámara o GPS), pierdes el control de tu vida privada. El laberinto te enseña a que hay que protegerse a ser invisible: si no te ve, no puede atacarte.

## **ESTUDIO DEL ESTADO DEL ARTE**

Antiguamente, un virus bloqueaba tu PC y el daño era evidente. Hoy domina el spyware silencioso: software diseñado para infiltrarse en tu dispositivo digital, espiar y robar datos sin dejar rastro. En este proyecto, el laberinto representa la memoria del dispositivo, donde programas maliciosos intentan vulnerar nodos de seguridad, desactivar códigos y acceder a información privada.

El peligro actual no es un fallo técnico, sino el engaño psicológico. Los jóvenes son el eslabón más débil ante la manipulación digital. Por ello, este juego utiliza criptogramas para que el usuario aprenda jugando.

Según el Ministerio del Interior, la cibercriminalidad en España supera los 464.000 delitos anuales, siendo los menores un blanco principal.

## **HIPÓTESIS**

El nivel de exposición de un joven en redes sociales es directamente proporcional a la facilidad con la que un script malicioso puede navegar por su 'laberinto personal' y vulnerar su intimidad

Comprender la criptografía mediante el juego del laberinto permite a los jóvenes detectar engaños y scripts ocultos, reduciendo drásticamente la vulnerabilidad de su intimidad. Datos de Save the Children alertan que casi el 20% de las jóvenes ha sufrido violencia digital en España.

Al jugar, el usuario experimenta que bloquear códigos y restringir datos son sus mejores armas: si no te ven, no pueden atacarte. Quien controla sus permisos (cámara o GPS), tiene su intimidad más protegida.

## **MATERIAL Y MÉTODOS:**

### **Materiales:**

- Construcción: Cartón pluma, piezas Lego e impresión 3D.
- Criptografía: Tarjetas, discos de cifrado manual y reloj de arena.
- Digital: Python (Pygame) y códigos QR para hibridar el entorno físico y virtual.

### **Metodología:**

Fase 1: Diseño de trazado con nodos donde el script intenta vulnerar la intimidad.

Fase 2 (Defensa):

- Nivel 1 (Firewall): El "falso amigo" llega a la puerta 1. Debe descifrar el QR1/Sobre 1 para avanzar.
- Nivel 2 (Filtro Apps): Bifurcación triple. El QR2/Sobre 2 contiene un enigma; el error penaliza al atacante.
- Nivel 3 (Sello Final): Última barrera antes de comprometer el núcleo de privacidad.

## Resultados

- Acceso Denegado: Códigos robustos agotan el tiempo del intruso; la prevención funciona.
- Sistema Comprometido: El intruso entra. Alerta: urge reforzar permisos y claves.

## RESULTADOS

1. Al jugar, el usuario visualiza procesos invisibles. Deja de ver los dispositivos digitales, sobre todo el móvil como un juguete y empieza a verlo como una extensión de su identidad que debe proteger.
2. Se demuestra que la mejor defensa no es borrar un virus, sino no abrir la puerta al intruso. Los jugadores que usan códigos robustos logran el estado de "Acceso Denegado", agotando el tiempo del atacante.
3. El proyecto revela que el desconocimiento técnico es nuestra mayor vulnerabilidad. Al aprender a gestionar permisos (cámara, GPS) y descifrar códigos, el joven reduce drásticamente las probabilidades de que su intimidad sea vulnerada.

## CONCLUSIÓN:

Una vez que el script llega al final del laberinto —ya sea físico o digital— y accede a nuestra información, el daño es irreversible. La mejor defensa no es reparar el sistema, sino no abrirle la puerta al intruso y proteger nuestra privacidad desde el inicio. Entender el código criptográfico nos permite intuir peligros y estar alerta ante las trampas ocultas. El laberinto nos enseña que el móvil es hoy una extensión de nuestra identidad: si no controlas quién recorre sus pasillos (permisos de cámara, micrófono o GPS), pierdes el control de tu propia vida privada. Terminamos con esta frase que describe todo el proyecto: **“El laberinto es tu memoria; el código es tu escudo.”**

## BIBLIOGRAFÍA:

- **UNICEF España (2021):** *Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades.* (Datos sobre la vulnerabilidad y el acoso en entornos digitales).
- **Save the Children (2022):** *Violencia viral: la violencia contra la infancia en la red.* (Estudio clave sobre el 20% de víctimas de violencia digital).