# Proyecto 2 Seguridad Informática
# Desarrollo de Software para Seguridad

Ricardo Pérez - Rodrigo Paredes
riperez@utalca.cl

## Introducción

Los *keyloggers* son un tipo de herramienta que registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario. Un keylogger puede estar basado en hardware o software, y se puede usar como herramienta lícita de control TI. Sin embargo, los keyloggers también se pueden utilizar con fines delictivos. Por regla general, los keyloggers son un spyware malicioso que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos.
El objetivo de este proyecto es desarrollar un *keylogger* de acuerdo a nuestras necesidades, que no sea detectado por nuestra víctima y que nos permita capturar toda la información ingresada por el teclado. Para su desarrollo deberán cumplir los siguientes requisitos:

## Ejercicio 1 (35 puntos)

Utilizando el lenguaje de programación de su preferencia, desarrolle un keylogger que permita capturar toda la información ingresada por teclado en el dispositivo de la víctima. Puede asumir que la víctima utiliza cualquier sistema operativo (Andriod, Linux, macOS o Windows).
Se recomienda no re-utilizar fragmentos de código de otros equipos, ya que se utilizarán herramientas para comprobar la originalidad de lo implementado.

- Documente detalladamente el código.
- Muestre evidencias de funcionamiento.

## Ejercicio 2 (35 puntos)

Una vez capturada la información del teclado, esta debe cifrarse utilizando un mecanismo de cifrado seguro.

- Justifique la elección del algoritmo de cifrado. (Por ejemplo, si cifra con MD5, deberá justificar por qué su elección.)

- Envíe los datos cifrados a su dispositivo de forma periódica. Es decir, cada cierto tiempo deberá recibir los datos del keylogger en su dispositivo y estos deberán ser almacenados para su posterior análisis.
- Una vez recibida la información, obtenga (descifre) todo lo que la víctima ha escrito hasta el momento.
- Muestre evidencias en cada caso.

### Ejercicio 3 (30 puntos)

Lleve a cabo un ataque MITM que tenga como objetivo el dispositivo de la víctima y demuestre que a pesar de capturar la información enviada, la comunicación del keylogger no puede ser descifrada.

- Haga que su malware no sea detectado por los sistemas de detección de intrusos o el antivirus.
- Justifique las alternativas que tienen los usuarios, o los especialistas de TI, para mitigar este tipo de amenaza.

## Requisitos

- Deberán conformar equipos de 2 estudiantes como máximo.
- El proyecto debe ser defendido en la semana del 5 al 10 de julio. (Fecha a coordinar con el profesor).

### Evidencias

Deberán subir a alguna plataforma un video demostrativo donde todos los integrantes tengan la cámara encendida y expliquen el procedimiento utilizado. Este video debe ser subido un día antes de la defensa del proyecto.