

Seguridad en TI (TICS413)

Laboratorio n°1

Matías García
matiasgarcia@alumnos.uai.cl

19 de Agosto 2025

1.- Conoce tu entorno

1.1.- ¿Qué es Linux?

Todos tienen un dispositivo inteligente, y para poder observar lo que sucede en él, necesitan un **sistema operativo**. Los más comunes son **Windows** o **macOS** en computadores personales, y **Android** o **iOS** en dispositivos móviles.

Linux es el **sistema operativo preferido por los informáticos**. Se trata de un sistema tipo **Unix**, de **código abierto** y altamente configurable.

Se utiliza en **servidores**, **computadores personales**, **dispositivos embebidos**, entre otros. Su núcleo (*kernel*) gestiona los recursos del hardware y permite la ejecución de software.

Una de sus grandes ventajas es la posibilidad de personalización, lo que ha dado origen a múltiples variaciones llamadas distribuciones. Existen más de 24 **distribuciones diferentes**, tales como **Ubuntu**, **Fedora**, **Arch Linux**, **Kali Linux**, entre muchas otras, cada una con un enfoque particular.

1.2.- ¿Cuál es nuestro enfoque?

La asignatura no se centra en sistemas operativos, por lo que no trabajaremos con una distribución de Linux genérica y configurable. Nuestro enfoque está en la **seguridad en entornos tecnológicos**, por lo que utilizaremos distribuciones creadas con ese propósito, como **Kali Linux**.

En los laboratorios de ciberseguridad de la universidad, esta distribución ya se encuentra instalada, por lo que no es necesario que los estudiantes la busquen o instalen por su cuenta.

1.3.- ¿En qué consiste Kali Linux?

Kali Linux es una distribución desarrollada y mantenida por **Offensive Security**, una empresa especializada en capacitación en seguridad informática. Fue creada como una **herramienta** para realizar pruebas de penetración y evaluar la seguridad de sistemas y redes.

2.- Comandos básicos

En sistemas Linux es común la utilización de **comandos** para explorar, administrar y trabajar con archivos y directorios. Además, muchas de las herramientas de seguridad requieren el uso de la línea de comandos.

Algunos comandos esenciales son:

- `ls` → Lista archivos y directorios.
- `pwd` → Muestra la ruta del directorio actual.
- `cd <directorio>` → Cambia de directorio.
- `cd ..` → Regresa al directorio anterior.
- `mkdir <nombre>` → Crea un nuevo directorio.
- `rm <archivo>` → Elimina un archivo.
- `rm -r <directorio>` → Elimina un directorio y su contenido.
- `cp <origen> <destino>` → Copia un archivo o directorio.
- `mv <origen> <destino>` → Mueve o renombra archivos o directorios.

Si deseas practicar, puedes hacerlo en un entorno Linux en línea: [Haz clic aquí para probar los comandos](#)

3.- Funcionamiento de los laboratorios

En cada laboratorio se presentará una herramienta utilizada en el mundo de la ****seguridad en TI**** o se buscará profundizar en los conocimientos adquiridos en la asignatura.

3.1.- Conoce un poco los CTF

Los **CTF (Capture The Flag)** son evaluaciones prácticas que se realizarán durante las clases. El objetivo será encontrar una ***bandera*** en el formato:

```
segti{--bandera--}
```

La bandera puede encontrarse dentro de un archivo, una dirección o tras realizar una acción específica.