[Curso de Informática Forense](https://platzi.com/clases/forense/)

**ArtículoArranque y ejecución de procesos en Linux**

[**Juan Pablo Caro**](https://platzi.com/%40juanpcaro)

23 de Mayo de 2019

Para comprender la ejecución de procesos y la información que estos almacenan en un sistema Linux, es importante entender cómo es el proceso de inicio del Sistema Operativo, qué archivos se acceden durante este proceso y qué información se modifica.

**Primer paso: El BIOS**
El BIOS (Basic Input/Basic Output) es el primer sistema que carga el procesador cuando se enciende. El BIOS se encarga de detectar el hardware disponible y proporcionar un primer acceso a los dispositivos periféricos, así como de identificar un dispositivo desde el cual iniciar el sistema (regularmente, la primera partición de un disco local). Una vez el BIOS encuentra un dispositivo disponible para iniciar, le deja el control del sistema a éste.

**Segundo paso: El gestor de arranque**
En los sistemas Unix existen diferentes gestores de arranque. Éste se encarga de escoger un sistema operativo a partir de una lista de dispositivos y sectores de arranque disponibles. El gestor de arranque más común en Linux probablemente sea GRUB (GRand Unified Bootloader), pero existen otros y es común encontrarlos.

**Tercer paso: El kernel de Linux**
El kernel es el proceso principal que ejecuta el sistema operativo Unix y del que dependen todos los demás procesos. Se encarga de administrar los controladores necesarios para usar el hardware, inicializa el sistema de archivos y prepara la memoria.

**Cuarto paso: proceso /sbin/init**
Este proceso se encarga de configurar el entorno de usuario. Los archivos de configuración de este proceso se encuentran en la carpeta **/etc/inittab**, y el primer script que se ejecuta es **/etc/init.d/rcS**.

A nivel lógico, el proceso init es el proceso del que derivan todos los demás procesos automáticos del sistema. Éste ejecuta todos los procesos que se encuentran en la carpeta **/etc/rcS.d/** y en **/etc/rc.boot/**. Estas carpetas son una gran fuente de referencia para revisar los procesos que se ejecutan por defecto al iniciar el sistema.

El proceso de inicio de procesos descrito es el que ha sido utilizado tradicionalmente en la gran mayoría de distribuciones de Linux. Sin embargo, existen otras alternativas y otros sistemas desarrollados para cumplir el mismo propósito. Como siempre, es importante que sigas aprendiendo y te documentes en todas estas herramientas, porque cambian constantemente y debes estar preparado para entender lo que te encuentres en campo.