

# Programas

# Daniel Valero

## IDES

*VsCode*

Instalado.

*IntelliJ IDEA*

Faltante, basta con instalar la versión gratuita de comunidad.

*Eclipse*

Faltante.

*Apache NetBeans*

Faltante.

*PHP Storm*

Faltante.

*Warp*

Faltante. Programa similar a IDES modernos destinado a trabajar con Bash u otros shells, uso muy limitado sin ser Root.

## **IMPORTANTE**

La actualización de estos programas así como la instalación de extensiones o librerías es constante y variado, según el ejercicio o proyecto a realizar.

- Plugins
- Extensiones
- SDKs
- Librerías específicas según el proyecto

Todo esto exige permisos administrativos.

# Lenguajes / Runtimes

<i>JDK</i>	Faltante. Java Development Kit. Es un conjunto de herramientas destinadas a todas las fases y procesos del desarrollo en Java.
<i>Node.js</i>	Faltante.
<i>NPM</i>	Faltante. Gestor de paquetes instalable desde Node.js
<i>TypeScript</i>	Faltante. Paquete de Node.js, es JS potenciado.
<i>Python</i>	Instalado.
<i>Bash</i>	Instalado por defecto en linux.
<i>Powershell</i>	Faltante. No instalado por defecto en Linux Mint.

# BBDD

<i>MySQL</i>	<i>PostgreSQL</i>	<i>DBeaver</i>
Faltante.  No solo necesito el Workbench, sino levantar un servidor en una versión superior a la 8.4 y configurar el Workbench. Siendo operable desde consola y desde el Workbench	Faltante.  Necesito el servidor de PostgreSQL y también instalar una versión superior a la 16 de pgAdmin. El servidor debe poder operarse tanto desde la consola como desde la interfaz de pgAdmin.	Faltante.  GUI destinada a las bases de datos, orientado a múltiples de ellas.

## IMPORTANTE

Desconozco si se puede operar una base de datos sin ser root en la máquina que la aloja, además hasta donde sé habilitar estos permisos desde cualquier consola me permitiría ser root de la máquina. Y por cierto se precisa ser root para modificar e instalar plugins así como operar con los motores de almacenamiento.

(Root es como se llama en linux al administrador, esto quiere decir que de darme capacidad de modificar y trabajar con una base de datos, lo que es una asignatura entera e imprescindible, también me haría administrador del ordenador completo).

Instalar y ejecutar servidores de bases de datos requiere permisos administrativos para:

- Crear servicios del sistema
- Configurar puertos
- Gestionar motores de almacenamiento
- Ejecutar demonios (mysqld, postgres, etc.)

Sin estos permisos **no es posible aprender administración de bases de datos**, parte esencial del ciclo.

# Control de Versiones

*Git*

Faltante.

*Github Desktop*

Faltante.

*GitKraken*

Faltante.

## **IMPORTANTE**

Sin permisos de root, no puedo configurar el entorno para crear repositorios locales completos, usar ciertas extensiones ni gestionar ramas o hooks de manera operativa. Los permisos de root son esenciales para instalar plugins y poder desarrollar correctamente los proyectos que debo realizar:

- Configurar claves SSH
- Inicializar repositorios
- Instalar hooks y extensiones
- Modificar directorios protegidos en ciertos entornos

Sin ello, el trabajo con repositorios se vuelve limitado o inviable.

---

# Entornos de Desarrollo

*XAMPP / WAMP*

Faltante.

*TOMCAT*

Faltante.

*Apache*

Faltante.

*Docker*

Faltante.

## IMPORTANTE

Sin permisos de root en la máquina del centro, no puedo instalar ni configurar correctamente varias herramientas necesarias para el desarrollo de proyectos:

- **XAMPP/WAMP:** No es posible instalar servidores locales de Apache, MySQL y PHP completos ni configurarlos para ejecutar mis proyectos web de manera operativa.
- **Tomcat:** No puedo levantar servidores Java ni desplegar aplicaciones web que dependen de este contenedor de servlets.
- **Apache:** La configuración de servidores web y la gestión de módulos esenciales requieren permisos de administrador para modificar archivos de configuración y servicios del sistema.
- **Docker:** No puedo instalar ni ejecutar contenedores, lo que limita la posibilidad de usar entornos aislados y reproducibles para pruebas y desarrollo.

# Otras

---

<i>Brave Browser</i>	Faltante.
<i>VirtualBox</i>	Instalado. Para ejecutar Kali Linux o entornos de prueba. Requiere permisos para instalar extensiones, controladores y máquinas virtuales.
<i>HyperV</i>	Faltante. Alternativa de virtualización, solo disponible en Windows.
<i>Microsoft Visual C++</i>	Faltante. Dependencias necesarias para muchos programas.
<i>V14 Y 2017</i>	
<i>DBnginx</i>	Faltante. Prescindible pero hace más comoda el arranque y parada de BBDD.

# Además

Actualmente tengo limitado el acceso a permisos de administrador (root) en el equipo principal que se me ha entregado. Sin embargo, dentro de este mismo ordenador estoy obligado a operar una máquina virtual de **Kali Linux**, —que sí cuenta con privilegios completos y está conectada por cable a la red del centro— porque forma parte de mi formación y de la especialización que estoy cursando.

Esto genera una situación contradictoria:

- Se restringen permisos en el sistema anfitrión (el ordenador del centro).
- Pero se me exige trabajar dentro de un entorno (Kali Linux) que, por su naturaleza educativa, necesita privilegios elevados y herramientas que requieren administrar el sistema.

El resultado es que **las limitaciones del equipo principal no aportan seguridad real**, ya que la propia máquina virtual necesita operar con privilegios completos.

En cambio, **sí suponen una barrera para mis tareas legítimas**, como instalar servidores, runtimes, IDEs y bases de datos necesarios para el ciclo.

## Sobre seguridad

Además, esta restricción aplicada al usuario no está acompañada de ninguna medida de seguridad adicional que refuerce realmente el sistema. El equipo no cuenta con:

- Hardening básico del sistema
- Políticas de seguridad activas
- Monitorización de actividad
- Firewall configurado adecuadamente
- Filtrado de conexiones

Sin estas medidas, limitar permisos no constituye una estrategia de seguridad efectiva. Uno de muchos ejemplos, haciendo una breve comprobación en consola se visualiza que todas las *capabilities* de binarios están activadas, en términos sencillos sirven para limitar qué puede hacer cada programa, incluso aunque el usuario tenga pocos privilegios.

En un equipo configurado para mayor seguridad, algunas de estas *capabilities* se desactivan o se restringen para evitar que ciertos programas tengan más funciones de las necesarias. Mientras que en este ordenador:

- No se ha desactivado ninguna de esas capacidades internas
- No existe reducción de funciones sensibles
- No se ha aplicado ninguna medida de endurecimiento (hardening)

En términos sencillos significa que el ordenador no tiene ninguna protección adicional por dentro, aunque el usuario normal tenga restricciones.

Por tanto:

- La seguridad del equipo **no depende de medidas técnicas**, solo de limitar al usuario
- La restricción aplicada **no refuerza realmente el sistema**
- Y, en cambio, **sí dificulta mi trabajo académico** al no poder instalar herramientas necesarias

## En conjunto

- La limitación del usuario principal **no mejora la seguridad del centro**, porque no está respaldada por medidas adicionales ni por un endurecimiento real del sistema.
- Pero sí **impide el correcto desarrollo de mi formación académica**, al bloquear herramientas, instalaciones y configuraciones que forman parte del currículo oficial.
- Todo esto mientras estoy obligado a usar una máquina virtual con permisos completos, lo que hace que la restricción aplicada al equipo principal sea incoherente y contraproducente.
- Además el equipo que se me ha dado es mucho más lento, y aunque se actualice el sistema operativo tarda demasiado en cargar, lo que sin duda supondrá un problema al usar herramientas más complejas en la máquina virtual.
- Y todo esto ha sido obviando la cantidad de configuraciones y plugins que tendría que volver a instalar, cuya migración a un nuevo equipo supondría un suplicio de varias jornadas. Sobre todo por la parte de las bases de datos, cuya migración sería una ardua tarea.

---

Por todo esto, y agradeciendo mucho los esfuerzos de la fundación por brindarnos un material adaptado, quisiera seguir trabajando con mi ordenador actual, ya que la seguridad es la misma. Le doy un uso estrictamente académico por lo que no voy sacarlo ni introducirlo del centro jamás en mis permisos, en casa tengo otro mejor. Con esto me ahorraría mucho trabajo y lío ya que el curso ha empezado y ya estoy funcionando a pleno rendimiento con este equipo. Habiendo demostrado en todos los sentidos que pretendo hacer las cosas bien y de buena fe.

---