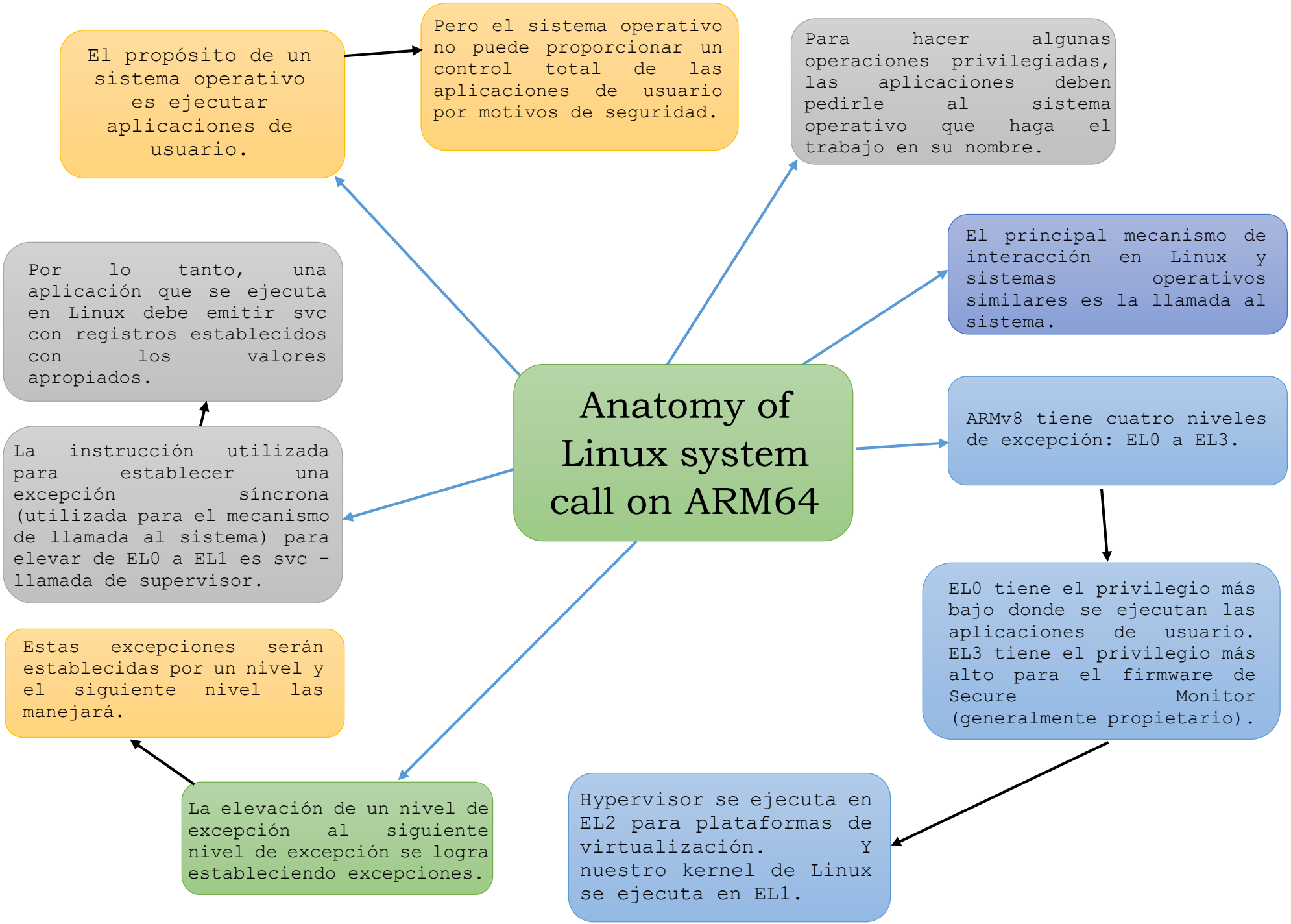
Anatomy of Linux system call on ARM64
El propósito de un sistema operativo es ejecutar aplicaciones de usuario.
Pero el sistema operativo no puede proporcionar un control total de las aplicaciones de usuario por motivos de seguridad.
Para hacer algunas operaciones privilegiadas, las aplicaciones deben pedirle al sistema operativo que haga el trabajo en su nombre.
El principal mecanismo de interacción en Linux y sistemas operativos similares es la llamada al sistema.
ARMv8 tiene cuatro niveles de excepción: EL0 a EL3.
EL0 tiene el privilegio más bajo donde se ejecutan las aplicaciones de usuario. EL3 tiene el privilegio más alto para el firmware de Secure Monitor (generalmente propietario).
Hypervisor se ejecuta en EL2 para plataformas de virtualización. Y nuestro kernel de Linux se ejecuta en EL1.
La elevación de un nivel de excepción al siguiente nivel de excepción se logra estableciendo excepciones.
Estas excepciones serán establecidas por un nivel y el siguiente nivel las manejará.
La instrucción utilizada para establecer una excepción síncrona (utilizada para el mecanismo de llamada al sistema) para elevar de EL0 a EL1 es svc - llamada de supervisor.
Por lo tanto, una aplicación que se ejecuta en Linux debe emitir svc con registros establecidos con los valores apropiados.