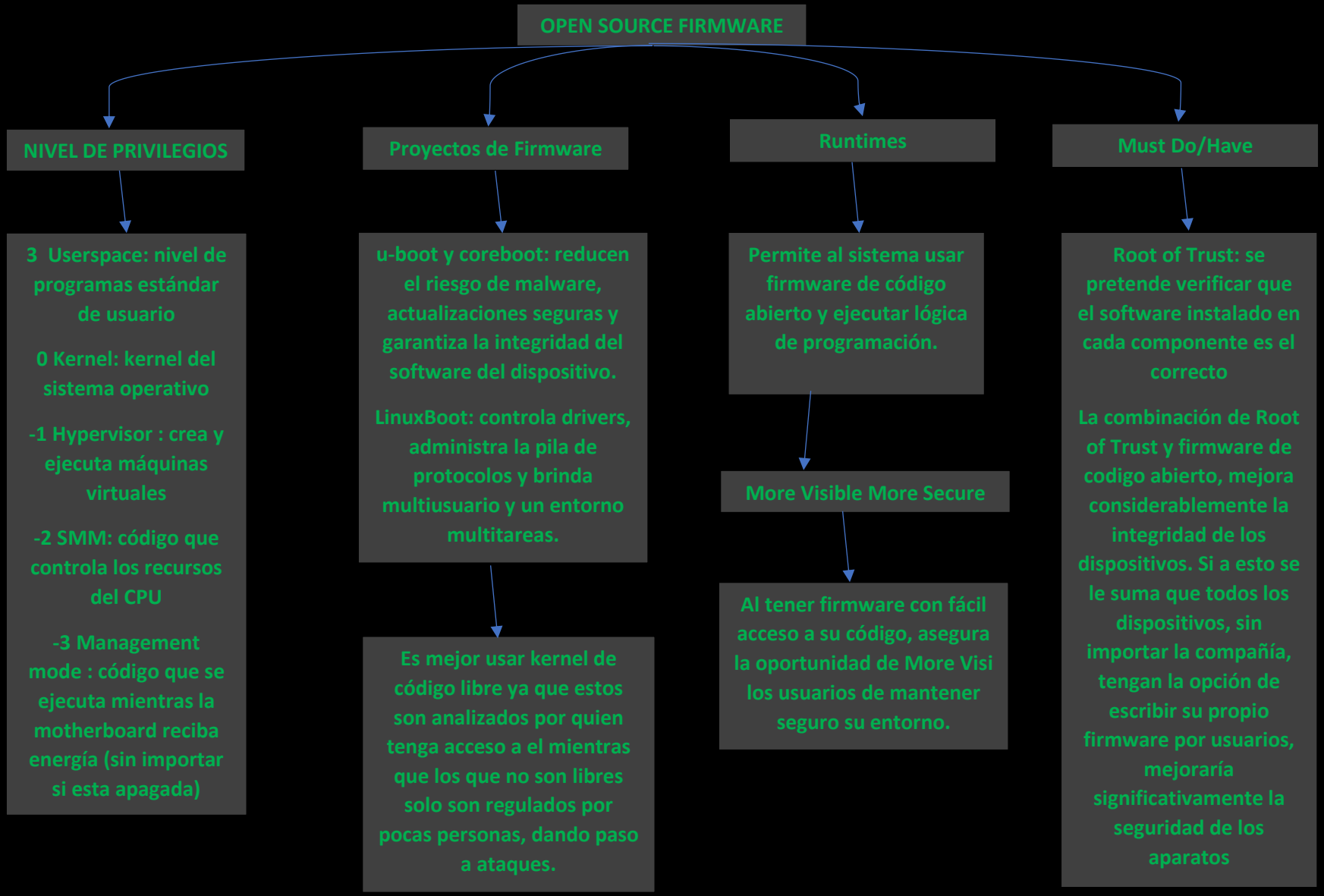
OPEN SOURCE FIRMWARE
NIVEL DE PRIVILEGIOS
3 Userspace: nivel de programas estándar de usuario
0 Kernel: kernel del sistema operativo
-1 Hypervisor : crea y ejecuta máquinas virtuales
-2 SMM: código que controla los recursos del CPU
-3 Management mode : código que se ejecuta mientras la motherboard reciba energía (sin importar si esta apagada)
Proyectos de Firmware
u-boot y coreboot: reducen el riesgo de malware, actualizaciones seguras y garantiza la integridad del software del dispositivo.
LinuxBoot: controla drivers, administra la pila de protocolos y brinda multiusuario y un entorno multitareas.
Es mejor usar kernel de código libre ya que estos son analizados por quien tenga acceso a el mientras que los que no son libres solo son regulados por pocas personas, dando paso a ataques.
Runtimes
Permite al sistema usar firmware de código abierto y ejecutar lógica de programación.
More Visible More Secure
Al tener firmware con fácil acceso a su código, asegura la oportunidad de More Visi los usuarios de mantener seguro su entorno.
Must Do/Have
Root of Trust: se pretende verificar que el software instalado en cada componente es el correcto
La combinación de Root of Trust y firmware de codigo abierto, mejora considerablemente la integridad de los dispositivos. Si a esto se le suma que todos los dispositivos, sin importar la compañía, tengan la opción de escribir su propio firmware por usuarios, mejoraría significativamente la seguridad de los aparatos