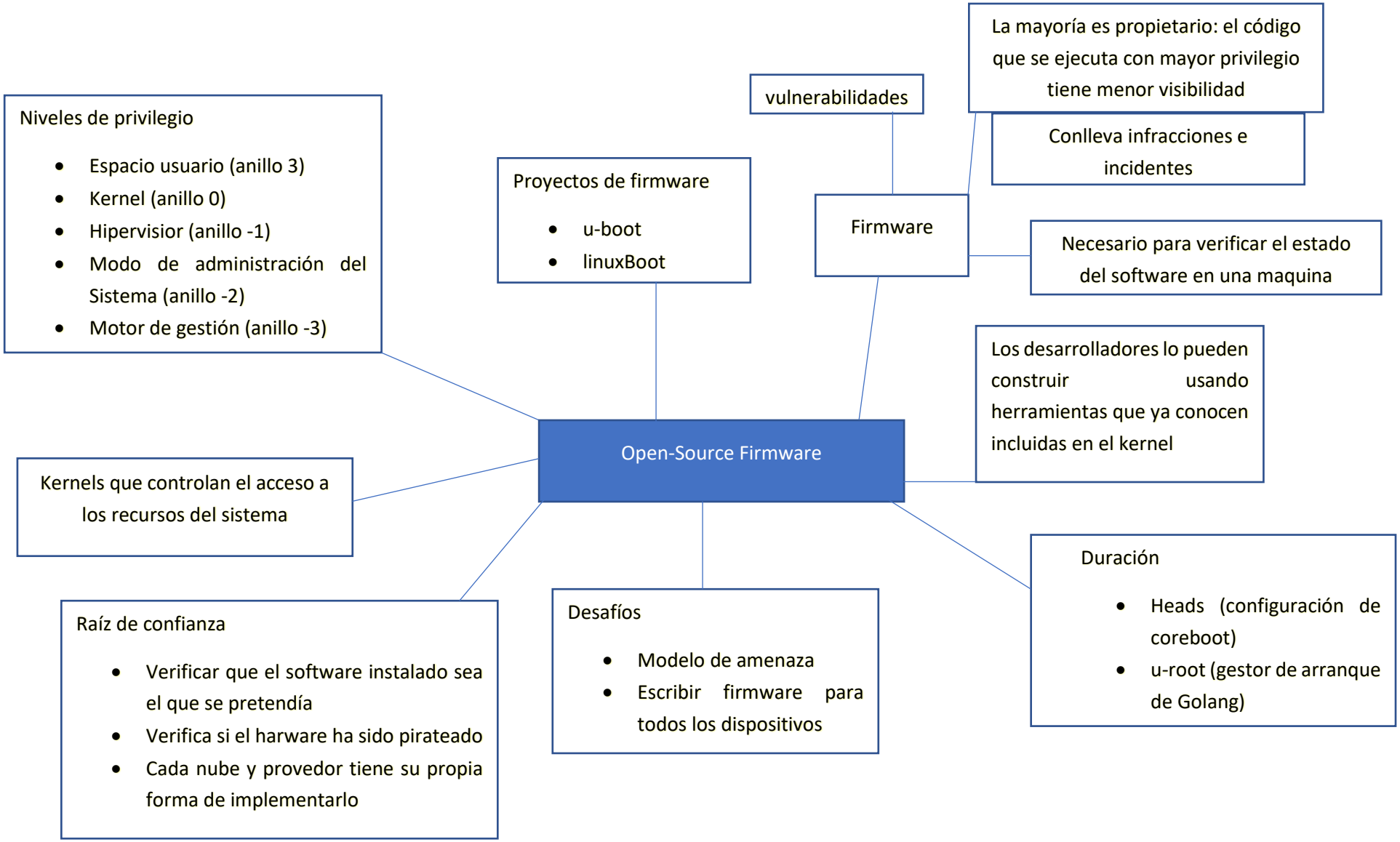
Niveles de privilegio
Espacio usuario (anillo 3)
Kernel (anillo 0)
Hipervisior (anillo -1)
Modo de administración del Sistema (anillo -2)
Motor de gestión (anillo -3)
vulnerabilidades
La mayoría es propietario: el código que se ejecuta con mayor privilegio tiene menor visibilidad
Conlleva infracciones e incidentes
Proyectos de firmware
u-boot
linuxBoot
Firmware
Necesario para verificar el estado del software en una maquina
Los desarrolladores lo pueden construir usando herramientas que ya conocen incluidas en el kernel
Open-Source Firmware
Kernels que controlan el acceso a los recursos del sistema
Raíz de confianza
Verificar que el software instalado sea el que se pretendía
Verifica si el harware ha sido pirateado
Cada nube y provedor tiene su propia forma de implementarlo
Desafíos
Modelo de amenaza
Escribir firmware para todos los dispositivos
Duración
Heads (configuración de coreboot)
u-root (gestor de arranque de Golang)