Proyectos de firmware

u-boot
core-boot

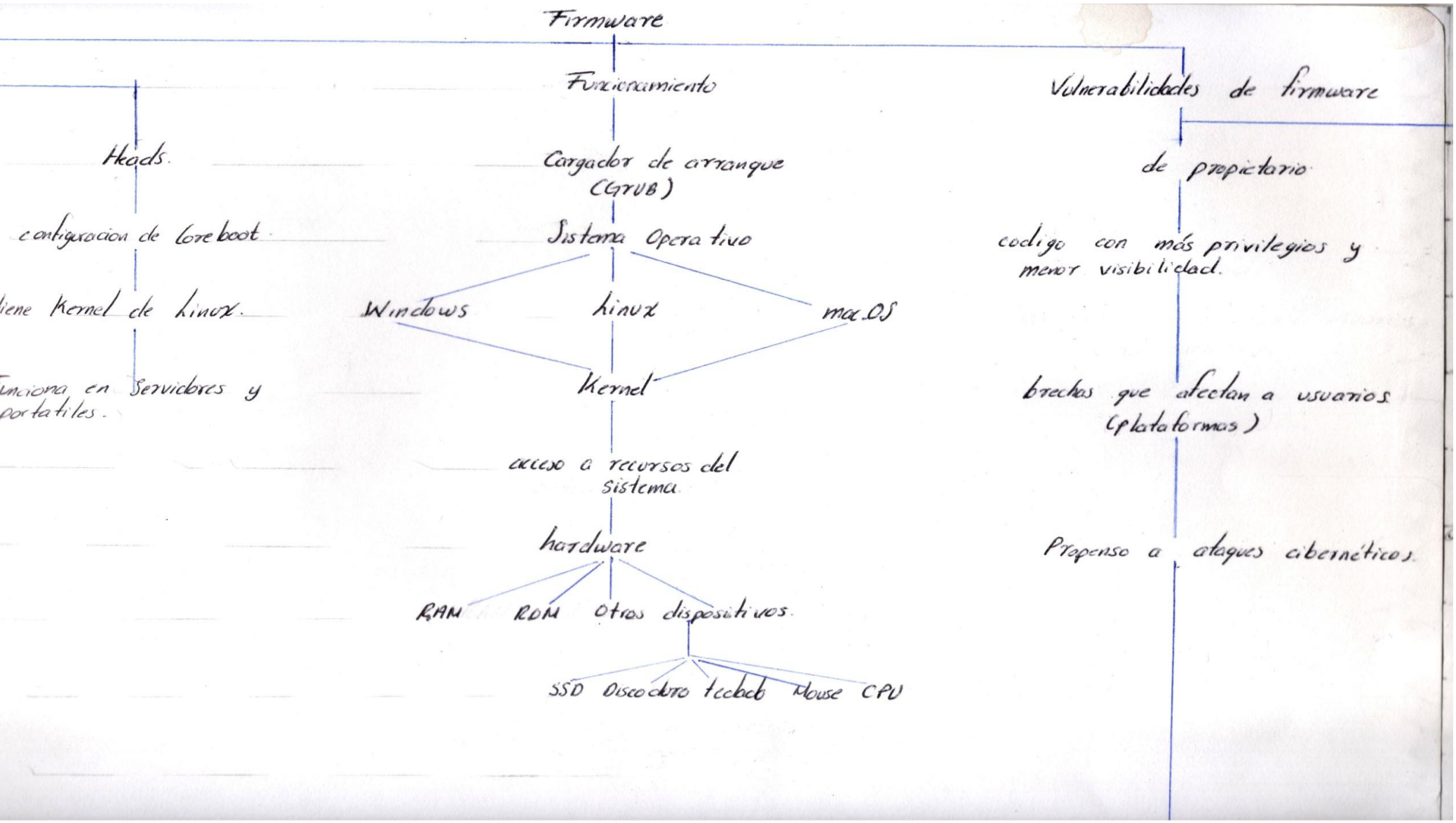
- codigo abierto
- inicialización del silicio y DRAM
- usado por Google para verificar arranque
- reduce el riesgo de malware
- actualizaciones seguras.

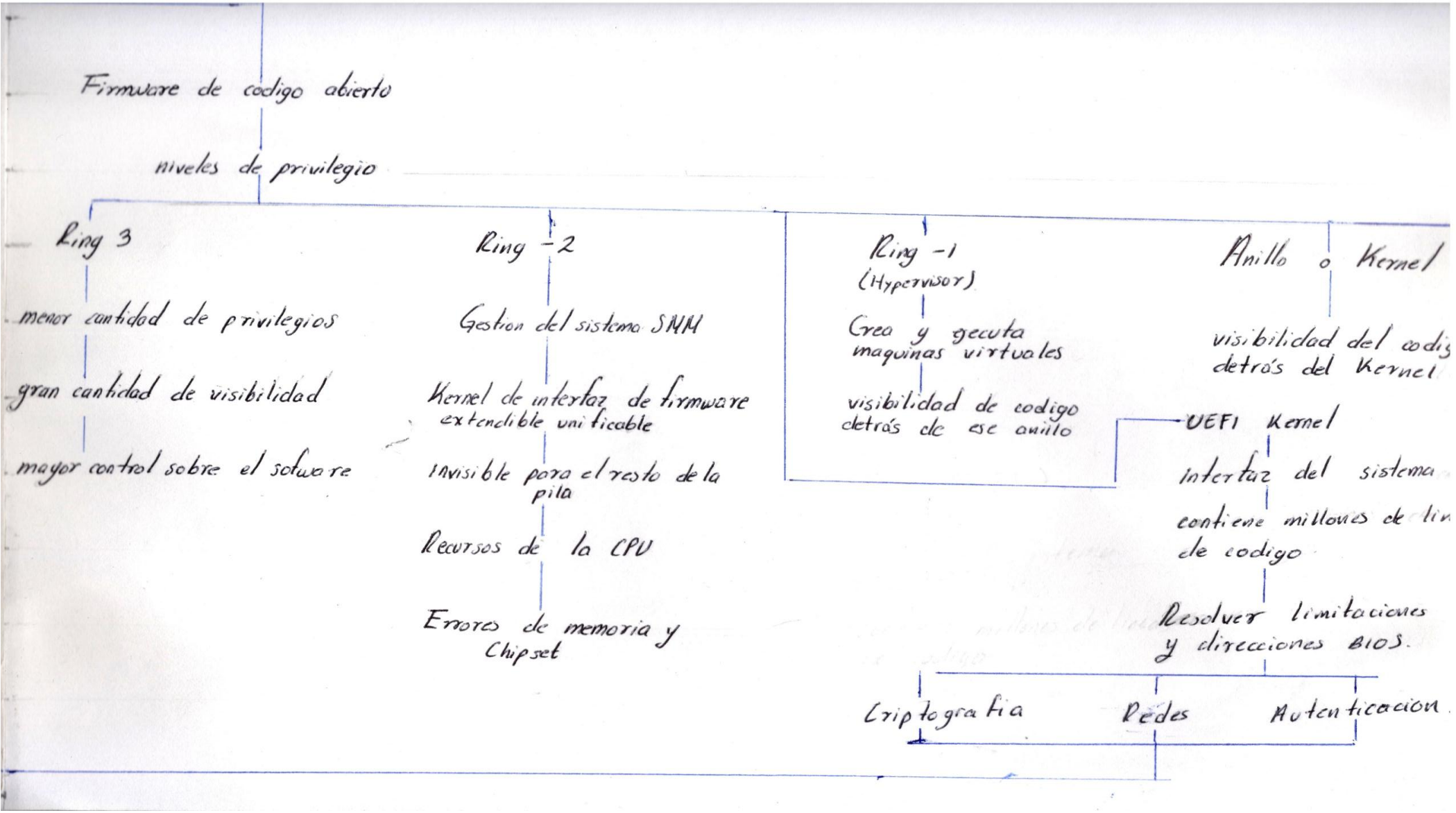
Tiempo de ejecución

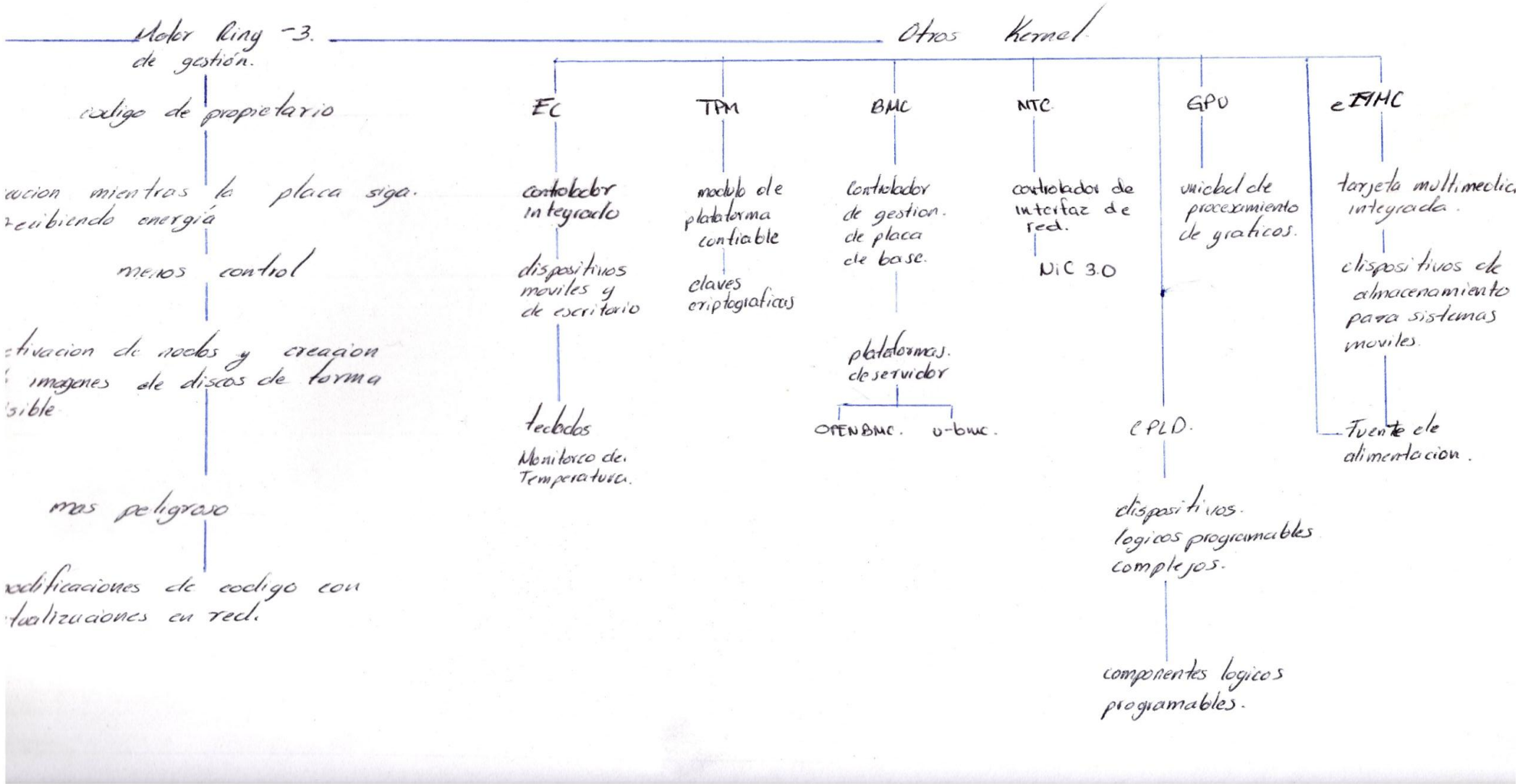
- conjunto de herramientas de espacio de usuario y cargador de arranque Golang
- Se utiliza ipitramfs para Kernel de linux
- codigo abierto
- la pila ayuda a mejorar la visibilidad de componentes de tipo propietarios.
- El uso de linux-Boot mejora 20 veces más los tiempos

Linux-Boot

- Reducido no extensible.
- controladores de dispositivo
- administra la pila de red y proporciona un multiusuario
- un solo nucleo para varias placas
- disminuyendo superficie de ataque al tener menos variaciones de codigo.


Firmware
Funcionamiento
Vulnerabilidades de firmware
Heads
configuracion de coreboot
tiene Kernel de Linux.
funciona en Servidores y portatiles.
Cargador de arranque (GRUB)
Sistema Operativo
Windows
Linux
mac OS
Kernel
acceso a recursos del sistema
hardware
RAM
ROM
Otros dispositivos
SSD
Disco duro
Teclado
Mouse
CPU
de propietario
codigo con más privilegios y menor visibilidad.
brechas que afectan a usuarios (plataformas)
Propenso a ataques cibernéticos.


Firmware de codigo abierto
niveles de privilegio
Ring 3
menor cantidad de privilegios
gran cantidad de visibilidad
mayor control sobre el sotware
Ring -2
Gestion del sistema SMM
Kernel de interfaz de firmware extendible unificable
Invisible para el resto de la pila
Recursos de la CPU
Errores de memoria y Chipset
Ring -1 (Hypervisor)
Crea y gecuta maquinas virtuales
visibilidad de codigo detrás de ese anillo
Anillo 0 Kernel
visibilidad del codig detrás del Kernel
UEFI Kernel
Interfaz del sistema
contiene millones de lin de codigo
Resolver limitaciones y direcciones BIOS.
Criptografia
Redes
Autenticacion


Motor Ring -3.
de gestión.
codigo de propietario
cacion mientras la placa siga.
recibiendo energía
menos control
ctivacion de nodos y creacion
imagenes de discos de forma
sible
mas peligroso
odificaciones de codigo con
tualizaciones en red.
Otros Kernel
EC
TPM
BMC
NTC
GPU
eMMC
controlador integrado
dispositivos moviles y de escritorio
teclados
Monitoreo de Temperatura.
modulo de plataforma confiable
claves criptograficas
Controlador de gestion. de placa de base.
plataformas. de servidor
OPENBMC.
u-bmc.
controlador de interfaz de red.
NIC 3.0
unidad de procesamiento de graficos.
CPLD.
dispositivos. logicos programables complejos.
componentes logicos programables.
tarjeta multimedia integrada.
dispositivos de almacenamiento para sistemas moviles.
Fuente de alimentacion.