INTEGRANTES:

- ALVAREZ SALGADO EDUARDO ANTONIO
- MORALES CASTILLO ARUMY LIZETH

SANDBOX

Aislamiento de aplicaciones y mecanismos de seguridad y control SO.

ÍNDICE

1. INTRODUCCIÓN

En la actualidad, el creciente número de amenazas informáticas y el incremento constante de vulnerabilidades en los sistemas modernos exigen nuevas formas de proteger los entornos digitales.

Una de las estrategias más efectivas para enfrentar este desafío es aislar las aplicaciones del resto del sistema operativo, evitando que un fallo o ataque en una aplicación comprometa la integridad del sistema completo.

En este contexto, surge una técnica preventiva clave: el sandboxing.

Mientras sandbox se refiere al entorno seguro donde se ejecuta el software, sandboxing se refiere al proceso o técnica de aislar y controlar la ejecución de ese software dentro del entorno, es la aplicación práctica del principio de aislamiento, un mecanismo que refuerza la seguridad y protege el sistema operativo."

2. FUNDAMENTOS TEÓRICOS

2.1 HISTORIA Y DEFINICIÓN DE SANDBOXING

ORIGEN

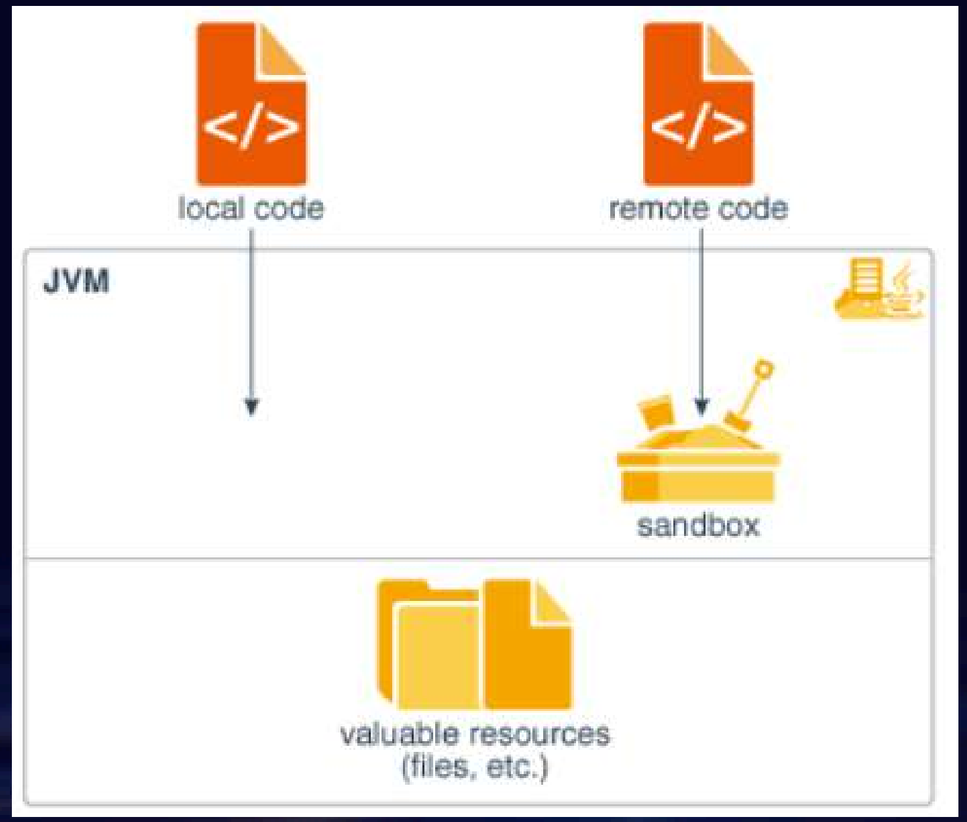
El término sandbox (“caja de arena”) proviene del ámbito infantil y representa un espacio seguro donde se puede experimentar sin riesgo.

EN INFORMÁTICA

Un sandbox es un entorno controlado que permite ejecutar software potencialmente inseguro sin afectar al sistema principal, actuando como un espacio confinado que evita que el código malicioso acceda a recursos, aplicaciones o datos sensibles.

2.1 HISTORIA Y DEFINICIÓN DE SANDBOXING

Primera adopción formal en informática: Java (1996).

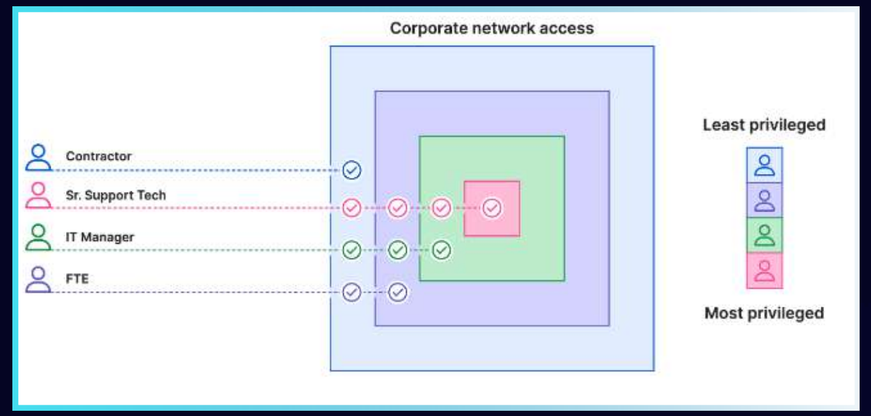


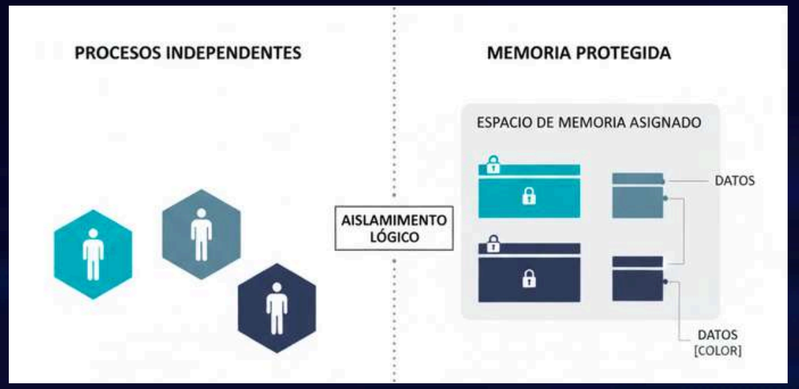
2.2 DEFINICIÓN Y PROPÓSITO DEL AISLAMIENTO DE APLICACIONES

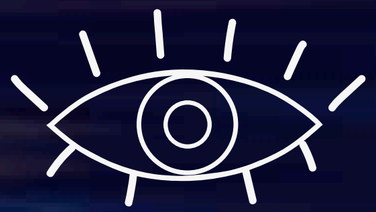
Reducir el riesgo de que una app comprometida ponga en peligro la integridad del sistema operativo o la información del usuario.

Para lograrlo, el aislamiento se basa en tres pilares fundamentales:

- Separación de procesos y memoria.
- Limitación de impacto en caso de vulneración.
- Supervisión del comportamiento.







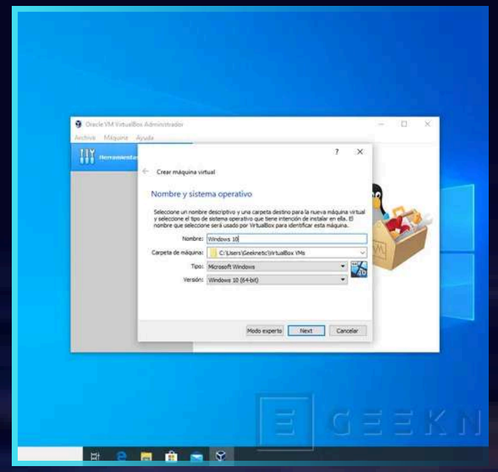
2.3 SEGURIDAD POR DISEÑO

SEGURIDAD POR DISEÑO

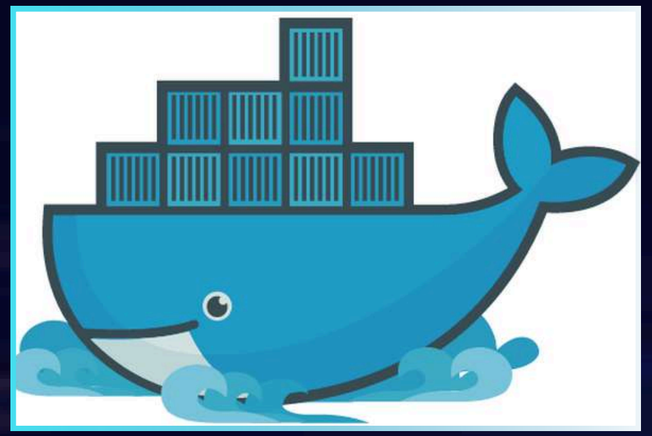
- La seguridad como parte fundamental del diseño.
- Restricción inherente de privilegios.
- Políticas de acceso predefinidas e inflexibles.
- Prevención > Corrección.
- Ejemplos: SELinux, AppArmor, macOS Sandbox, permisos de Android.
- Protección contra técnicas modernas de explotación.

2.4 TIPOS DE SANDBOX Y ENFOQUES DE AISLAMIENTO

Virtualización / microVMs (Windows Sandbox, Firecracker).



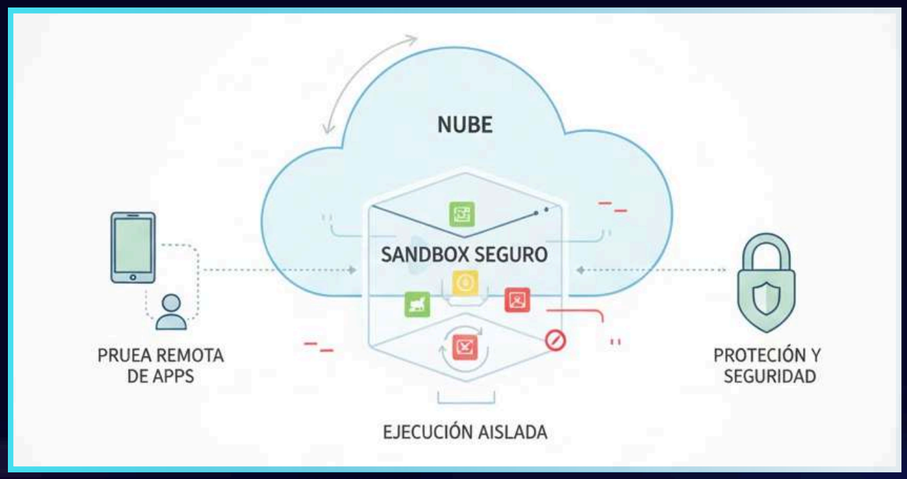
Contenedores (Docker, LXC).



2.4 TIPOS DE SANDBOX Y ENFOQUES DE AISLAMIENTO

Filtrado de syscalls (seccomp, WASM sandboxing).

Sandbox en la nube



La elección depende de: nivel de seguridad, rendimiento y flexibilidad.

3. ARQUITECTURA Y FUNCIONAMIENTO DEL SANDBOX EN LOS SISTEMAS OPERATIVOS

3.1 . CONCEPTOS ESENCIALES

Kernel

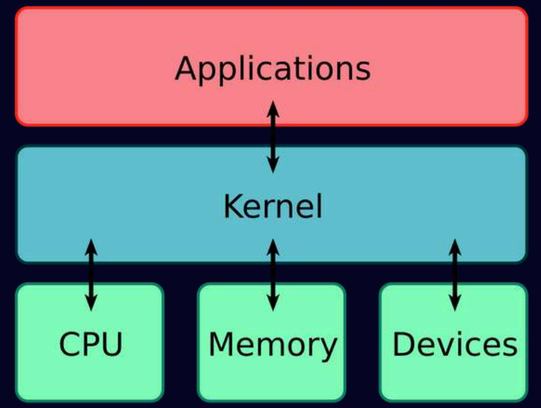
- Gestiona las llamadas al sistema.
- Controla acceso a CPU, memoria y periféricos.

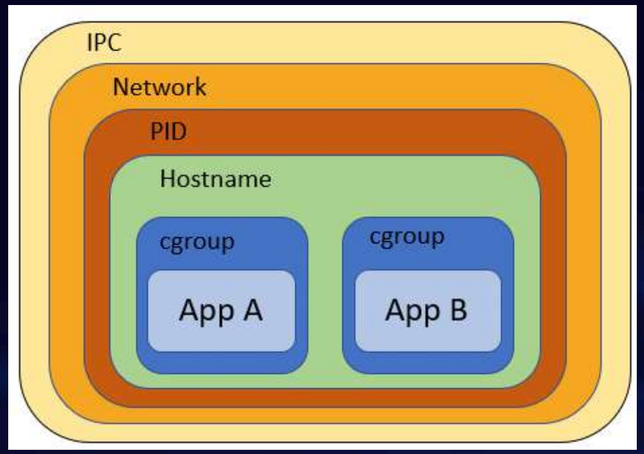
Namespaces

- Vista “privada” del sistema para cada proceso.
- Aíslan procesos, red, montajes, usuarios, etc.

cgroups

- Regulan uso de CPU, RAM y E/S.
- Evitan que un proceso consuma recursos en exceso.

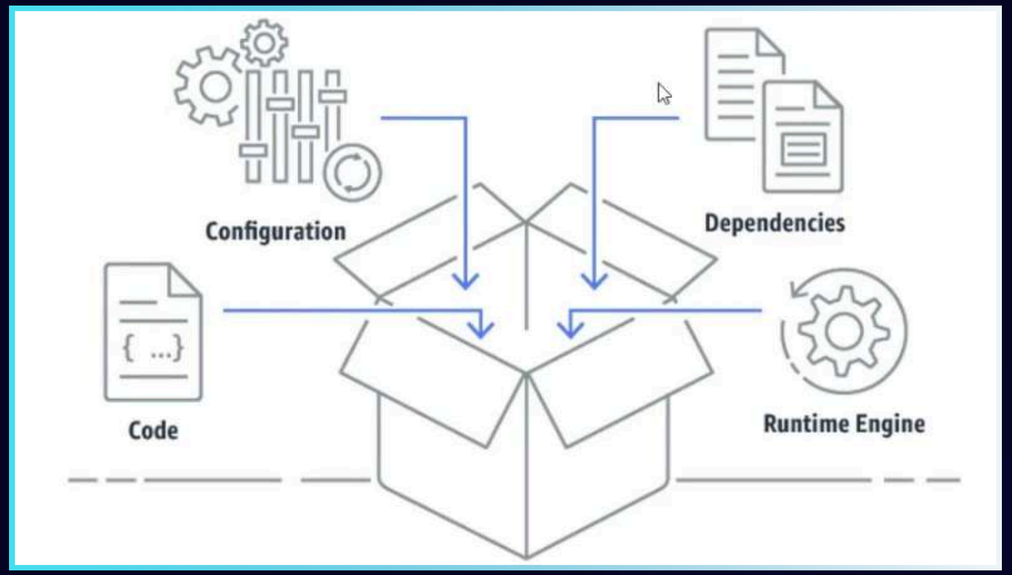




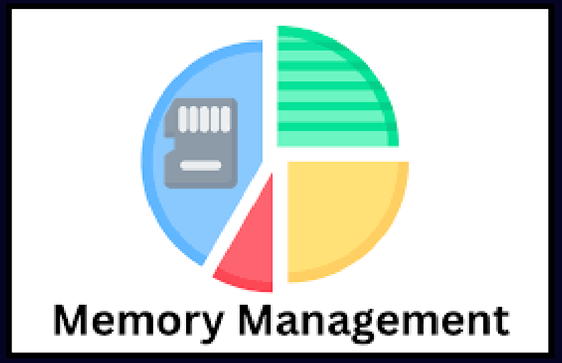
3.2 ARQUITECTURA GENERAL DEL SANDBOX

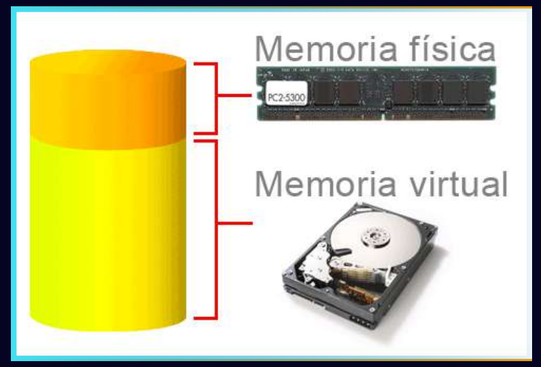
ARQUITECTURA GENERAL DEL SANDBOX

- **Entorno aislado (contenedores, máquinas virtuales ligeras o espacios restringidos)**
- **Monitor:** Verifica las acciones del proceso.
- **Mecanismo de control:** intercepta las llamadas al sistema y las compara con las políticas definidas.
- **Políticas definidas:** especifican los recursos accesibles.
- **Interfaz Kernel:** Verifica el cumplimiento de estas reglas.



3.3 AISLAMIENTO DE MEMORIA Y RECURSOS





1. **Memoria virtual protegida y espacios de direcciones independientes.**

2. **MMU**

   Evita lecturas/modificaciones no autorizadas.

2. **Namespaces**

   Procesos, red, archivos, montajes aislados.

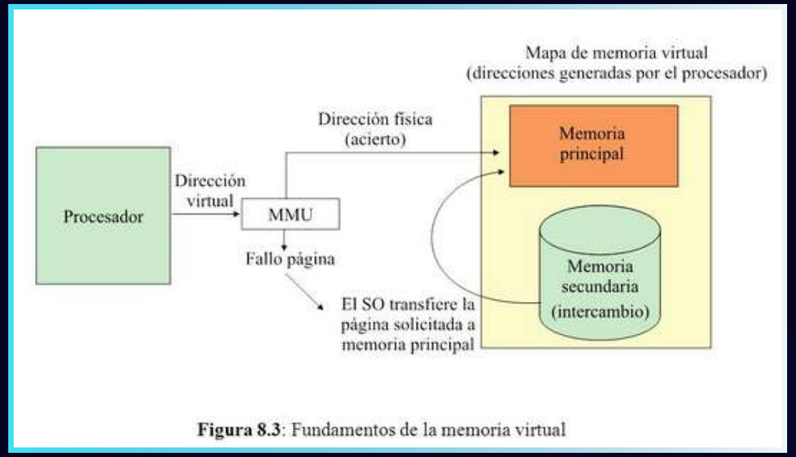
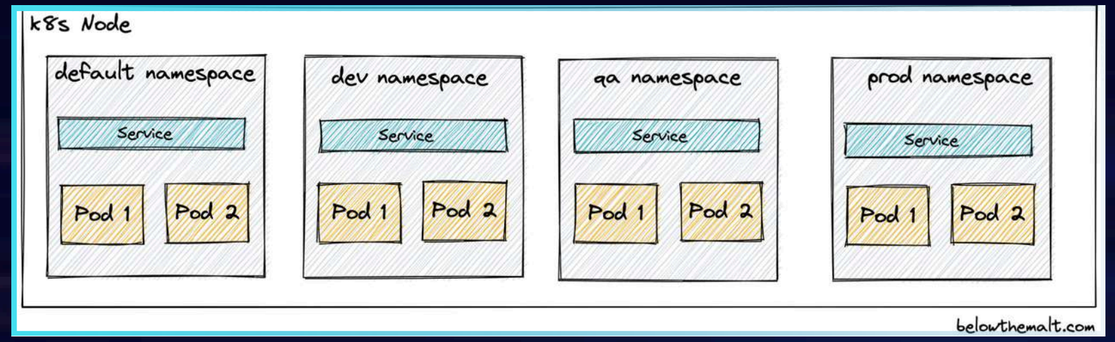


Figura 8.3: Fundamentos de la memoria virtual

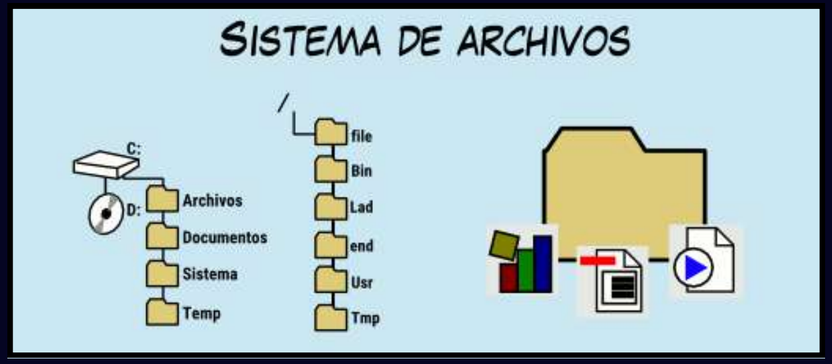


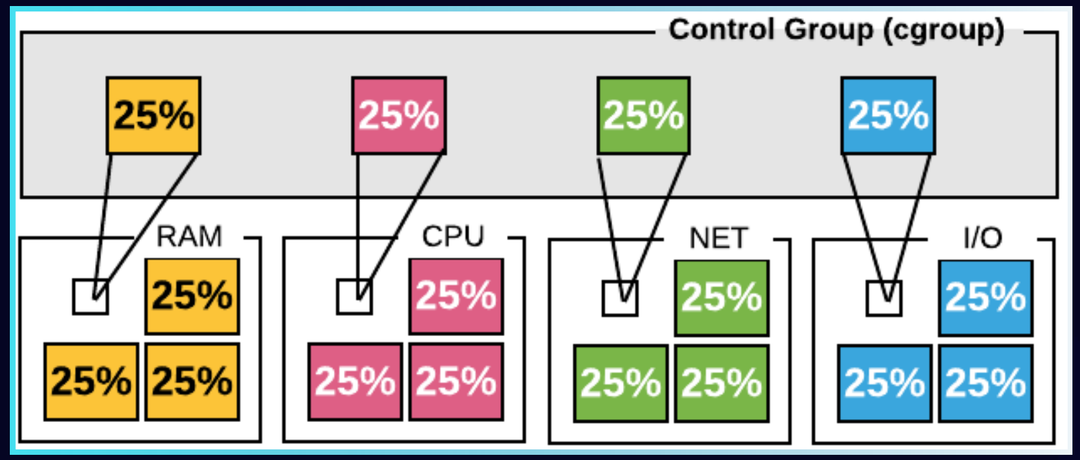
3.3 AISLAMIENTO DE MEMORIA Y RECURSOS

4 **Restricción del sistema de archivos mediante rutas controladas.**

5 **Cgroups**
Límites de CPU, memoria y almacenamiento.

6 **Reduce la superficie de ataque y evita fugas de información.**





3.4 CONTROL DE PERMISOS Y POLÍTICAS DE ACCESO

- Regulan lo que la aplicación puede hacer dentro del sandbox.
- Políticas detalladas: archivos, red, hardware, procesos.
- Tecnologías:
  a. AppArmor, SELinux (Linux)
  b. Entitlements (macOS)
  c. AppContainer (Windows)
- Intercepción y validación de llamadas al sistema.
- Bloqueo de acciones no autorizadas.
- Refuerza la seguridad y el aislamiento.

4. CASOS REALES E IMPLEMENTACIONES DESTACADAS DE SANDBOXING EN SISTEMAS OPERATIVOS

4.1 WINDOWS SANDBOX Y APPCONTAINER

- AppContainer: Introducido en Windows 8.
  - Entorno restringido para apps modernas.
  - Permisos declarativos.
  - Limitación de acceso a archivos, red y configuraciones sensibles.
- Windows Sandbox: Virtualización ligera basada en Hyper-V.
  - Entorno temporal y completamente aislado.
  - Ideal para ejecutar software desconocido.
  - Todo se descarta al cerrarlo.

4.2 MACOS Y IOS SANDBOX

- Modelo obligatorio en iOS; opcional pero ampliamente usado en macOS.
- Cada app se ejecuta en un contenedor aislado.
- **ENTITLEMENTS**: PERMISOS MÍNIMOS POR RECURSO.
- Complementado con firma de código y revisión de la App Store.
- Previene abuso, manipulación o acceso indebido.

4.3 LINUX: SELINUX, APPARMOR Y SECCOMP

LSELINUX

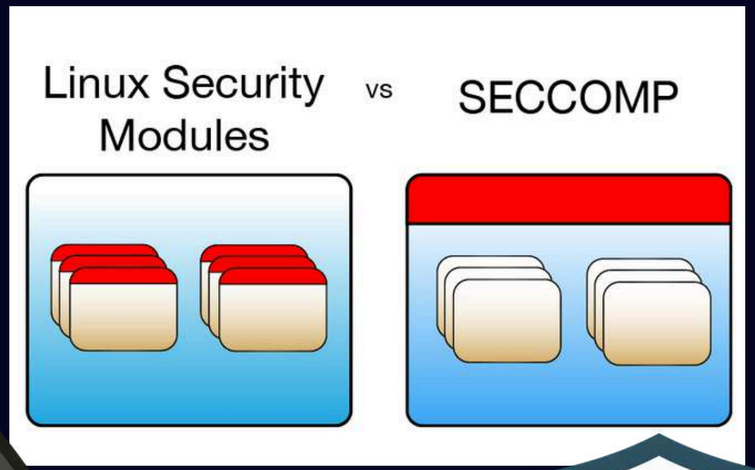
- Control de acceso obligatorio (MAC).
- Reglas detalladas por proceso y recurso.

APPARMOR

- Perfiles simples y flexibles.
- Más fácil de configurar.

SECCOMP

- Restricción de llamadas al sistema.
- Reduce la superficie de ataque.



Amplio uso en servidores, contenedores y entornos empresariales.

4.4 NAVEGADORES WEB: CHROME SANDBOX Y FIREFOX CONTENT PROCESS

1 **CHROME**

Arquitectura multiproceso: Pestañas, extensiones y plugins en sandboxes separados.

2 **FIREFOX**

Content processes: Separación entre interfaz, renderizado y red. Contención de daños ante vulnerabilidades en páginas web.

4.5 ANDROID: SANDBOX POR USUARIO Y UID

- Cada app tiene un UID único asignado por el kernel.
- Impide acceso a datos de otras apps.
- Permisos declarativos aprobados por el usuario.
- Firma de aplicaciones y ejecución en ART.
- Aislamiento fuerte y controlado.

5. REFERENCIAS

Sysarmy. (s. f.). [Docker thumbnail]. https://sysarmy.com/blog/assets/docker-thumbnail.png
Geeknetic. (2020). [Entorno seguro – tutorial]. https://acf.geeknetic.es/imgw/imagenes/tutoriales/2020/1758-como-crear-un-entorno-seguro/4.jpg?f=webp
PhoenixNAP. (2023). [Mac control example]. https://phoenixnap.com/glossary/wp-content/uploads/2023/08/mac-control-example.jpg
El Androide Libre. (2019). [Imagen de Android]. https://s1.elespanol.com/2019/04/26/elandroidelibre/el_androide_libre_393974250_179686759_1200x600.jpg
HeadSpin. (s. f.). [Browser sandboxing].
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.headspin.io%2Fblog%2Fbrowser-sandboxing-what-is-it-and-why-do-we-need-it
SRE DevOps. (s. f.). [WebAssembly – WASM]. https://www.sredevops.org/es/que-es-web-assembly-wasm-y-para-que-sirve/
José7331. (2016). [GIF de proceso]. https://jose7331.wordpress.com/wp-content/uploads/2016/08/f010.gif
CHSOS. (2015). [Captura de pantalla]. https://chsos20152906538.wordpress.com/wp-content/uploads/2015/10/captura10.png
Espacios.net.mx. (2022). [Robo de información en internet]. https://www.espacios.net.mx/wp-content/uploads/2022/09/robo-de-informacion-internet.jpg
NimbusTech. (2025). [Fuga de información en una empresa]. https://nimbustech.es/wp-content/uploads/2025/01/Como-gestionar-una-fuga-de-informacion-en-una-empresa.jpg.webp
Blogger. (s. f.). [Sistema de archivos – imagen destacada].
https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjHDVBv0f6FUmVXkmgZw2ZjH_L4ZZudGmUo3yqWQFSsdoWpzsf7fA22eEHE6BOlh_f2aEOCs9HxRFa8pbvKQXkLmZVGEX707wtZhTDF6IUlXenIjAR3TBkWoAzoS4JLq91fVEB7rafYnh-5/s1600/MBS-post-05-sistema_de_archivos-destacada-520x245.png
NinjaOne. (2024). [Habilitar Hyper-V – imagen].
https://mlfk3cv5yvnx.i.optimole.com/cb:HA53.300ea/w:800/h:418/q:mauto/f:best/https://www.ninjaone.com/wp-content/uploads/2024/04/N1-0921-How-to-Install-and-Enable-Hyper-V-blog-image-2-2.png
StarWind Software. (2021). [Word image 29]. https://www.starwindsoftware.com/blog/wp-content/uploads/2021/05/word-image-29.png
10Duke. (2023). [Software entitlement]. https://www.10duke.com/wp-content/uploads/2023/03/software-entitlement.png
Wikimedia Commons. (s. f.). [SELinux logo]. https://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/SELinux_logo.svg/1200px-SELinux_logo.svg.png
Wikipedia. (s. f.). [AppArmor].
https://www.google.com/url?sa=i&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FAppArmor
CNET. (2022). [Google Chrome logo].
https://www.cnet.com/a/img/resize/7ae96b5c2d76caa81d1b4141b31582da9c60d760/hub/2022/03/30/64f1f0c6-4a75-477e-b536-7ef2e105e0be/google-chrome-logo.jpg

GRACIAS POR SU ATENCIÓN