



Seguridad

Equipo 7

-Chávez Rodríguez Héctor

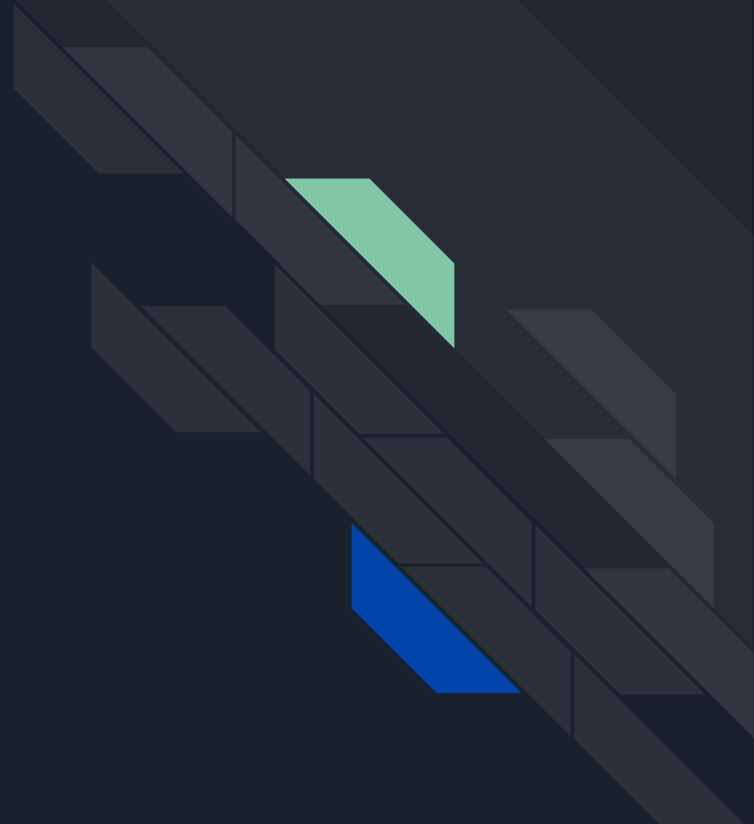
-Delgado Mendoza María Fernanda

-Gómez Marban Jonathan Said

-Ramírez Farías Luis Antonio

¿Qué es la seguridad?


Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.



¿Por qué es importante la seguridad?

Previene el robo de datos tales como números de cuentas bancarias, información de tarjetas de crédito, contraseñas, documentos relacionados con el trabajo, hojas de cálculo, etc.





Las violaciones de seguridad se clasifican en dos tipos:

a) Intencionadas (maliciosas)

b) Accidentales

Algunas formas de violaciones de seguridad accidentales o intencionadas

01

Ruptura de Confidencialidad

Se refiere a la lectura no autorizada de determinados datos, o el robo de información



02

Ruptura de Integridad

Modificación no autorizada de datos o información



Algunas formas de violaciones de seguridad accidentales o intencionadas

03

Ruptura de la Disponibilidad

Se refiere a la destrucción no autorizada de determinados datos, o información



04

Robo de servicio

Uso no autorizado de recursos



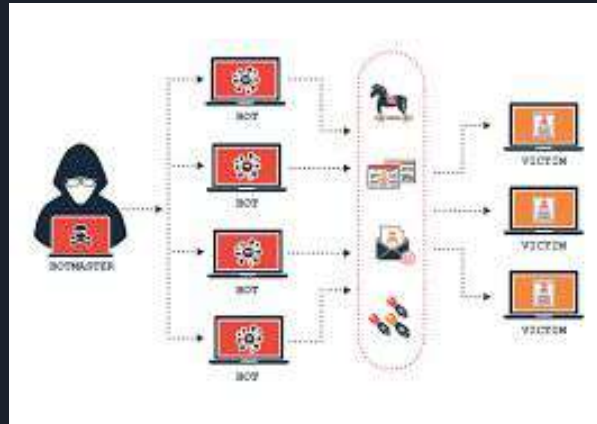
Algunas formas de violaciones de seguridad accidentales o intencionadas

05

Denegación de Servicio

Impide el uso legítimo del sistema.

Ejemplo: El ataque de denegación del servicio DOS






Algunos de los ataques más utilizados son:

Mascarada:

Un participante en una comunicación pretende ser otra persona, así rompe la autenticación, es decir la corrección de la identificación así pueden obtener tipos de acceso que normalmente no les estarían permitidos o escalar sus privilegios.





Algunos de los ataques más utilizados son:

Ataques de reproducción:

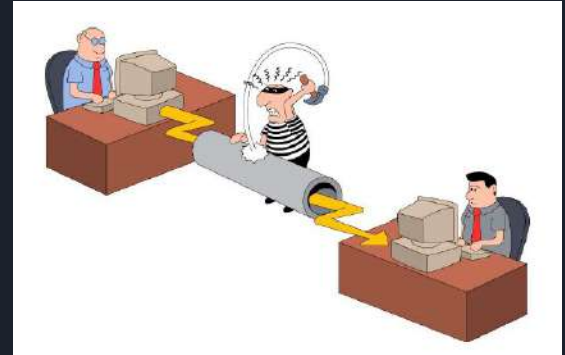
Repetición fraudulenta de una transmisión de datos válida.



Algunos de los ataques más utilizados son:

Ataque por interposición:

Un atacante se introduce dentro del flujo de datos de una comunicación por red, es decir intercepta una sesión de comunicación abierta



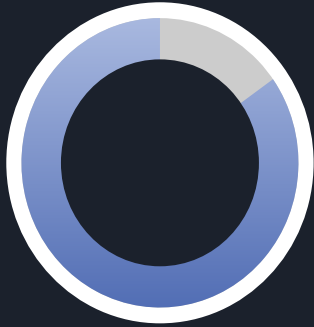


Resulta imposible garantizar la protección absoluta de un sistema frente a posibles ataques maliciosos, sin embargo se puede optar ciertas medida para que la mayoría de los intrusos quiera disuadir de estos ataques.

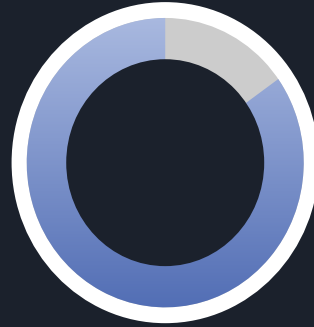
Para proteger un sistema se debe de adoptar la necesarias medidas de seguridad en cuatro niveles distintos



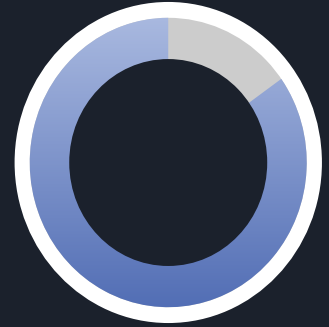
Físico



Humano



Sistema Operativo



Red

Para poder mantener la seguridad se debe de contemplar todos estos aspectos



Amenazas relacionadas con los programas

Los procesos, junto con el kernel, son el único medio de realizar un trabajo útil en la computadora, por lo tanto, un objetivo común de los “piratas informáticos” consiste en escribir un programa que cree una brecha para vulnerar la seguridad.

Estos son algunos métodos comunes mediante programas que pueden provocar un ataque en la seguridad de un sistema

A) Caballo de Troya

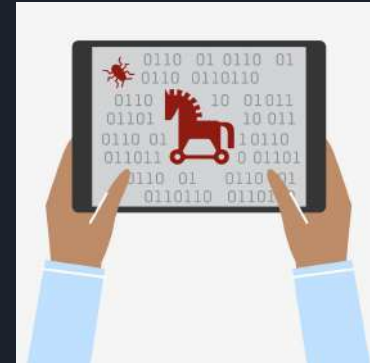
Los atacantes implementan un troyano para dañar o tomar el control de tu computadora. Su nombre proviene del método por el cual infecta la computadora: se disfraza de algo que quieres para engañarte y dejarlo pasar por tus defensas.

un troyano se asemeja a una aplicación o archivo confiable que convence al usuario de que es seguro descargarlo en computadoras o portátiles. Cuando el usuario descarga y ejecuta el software malicioso en un dispositivo, se activa el malware que contiene.

Una vez que el malware troyano se descarga y se activa, los ciberdelincuentes pueden tomar el control del dispositivo en sí, bloquear al usuario con ataques o realizar cualquier amenaza maliciosa que tenga en mente.

Algunas características:

- Pueden actuar como Puerta Trasera
- Contienen exploits





B) Puerta Trasera

Es una secuencia especial o un término dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autenticación) para acceder al sistema.

Las puertas traseras pueden “actuar” solas o bien ser parte de un troyano. Es decir, pueden ser fragmentos de código que simplemente nos permitirán saltarnos los sistemas de autenticación, o bien **pueden funcionar en combinación con un troyano** para, una vez abierto el “pasadizo”, realizar alguna acción ilícita.



C) Bomba Lógica

Del término en inglés LogicBomb.

Una bomba lógica es un programa informático que se instala en una computadora y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola.

Ejemplos de condiciones predeterminadas: día de la semana, hora, pulsación de una tecla o una secuencia de teclas, levantamiento de un interfaz de red, etc.

Ejemplos de acciones: borrar la información del disco duro, mostrar un mensaje, reproducir una canción, enviar un correo electrónico.



D) Desbordamiento de Pila y de Búfer

Es una situación en la que un programa en ejecución intenta escribir datos fuera del buffer de memoria que no está destinado a almacenar estos datos. Cuando esto sucede, estamos hablando de un desbordamiento del buffer.

Un buffer de memoria es un área en la memoria de la computadora (RAM) destinada a almacenar datos temporalmente. Este tipo de buffers se puede encontrar en todos los programas y se utilizan para almacenar datos para entrada, salida y procesamiento.

Un ejemplo de datos almacenados en buffers son las credenciales de inicio de sesión o el nombre de host para un servidor FTP. Además, otros datos almacenados temporalmente antes del procesamiento pueden almacenarse en buffers. Esto literalmente podría ser cualquier cosa, desde campos de entrada del usuario, como los campos de nombre de usuario y contraseña, hasta los archivos de entrada utilizados para importar ciertos archivos de configuración.



E) Virus

Un virus informático es un programa o código malicioso y autorreplicante que se cuela en su dispositivo sin su conocimiento ni permiso.

En cuanto a su funcionamiento exacto, los virus informáticos pueden dividirse en dos categorías: los que empiezan a infectar y replicarse en cuanto llegan al equipo y los que permanecen inactivos, a la espera de que una persona los active (es decir, a la espera de que ejecute el código de forma inadvertida).

Una vez instalado el virus puede hacer varias cosas, y se les puede clasificar de la siguiente forma:

- | | | | |
|-----------|----------------|-------------|-------------|
| -Archivo | -Código Fuente | -Encubierto | -Encorazado |
| -Arranque | -Polimórfico | -Túnel | |
| -Macro | -Cifrado | -Multiparte | |



Amenazas del Sistema y de la Red

Las amenazas del sistema y de la red implican el abuso de los servicios y de las conexiones de red, estas amenazas crean una situación en la que se usan inapropiadamente los recursos del Sistema Operativo y los archivos del usuario

Algunos ejemplos son:



Gusano

Un gusano informático es un tipo engañoso de malware, diseñado para propagarse a través de varios dispositivos mientras permanece activo en todos ellos.

Los gusanos informáticos son peligrosos a causa de su capacidad. Tan pronto como un gusano se afianza en una máquina , puede extenderse a través de una red **sin necesidad de ayuda o de acciones externas**. Como malware autónomo, los gusanos no necesitan engañarle para que se active, como sucede con los troyanos.

Los gusanos **explotan vulnerabilidades ocultas** en el sistema operativo (S.O.) de su equipo. Los hackers crean gusanos que pueden penetrar en el S.O. de destino y hacer distintos movimientos o procesos sin su conocimiento.



Escaneo de Puertos

El escaneo de puertos es un proceso mediante el cual, a través de herramientas especializadas, se analizan los puertos de un sistema informático.

Al escanear puertos se puede obtener información como los puertos que están abiertos, los que están cerrados o aquellos que están protegidos con cortafuegos.

Este procedimiento se puede usar con distintas finalidades.

Muchos atacantes emplean este tipo de técnicas para aprovecharse de esos fallos de seguridad. Al final, los puertos abiertos pueden funcionar como una puerta de entrada a un equipo, para luego realizar otras actividades maliciosas, como ataques de denegación de servicio.



Denegación de Servicio

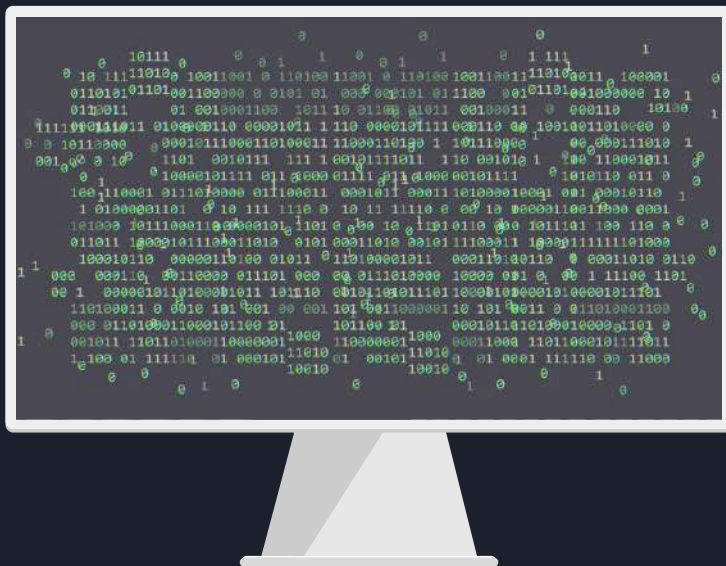
un **ataque de denegación de servicio**, llamado también ataque **DoS** (por sus siglas en inglés, *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos

Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio.

Criptografía como herramienta de seguridad

La criptografía se encarga de que el intercambio de información y de datos se produzca de forma segura. Se centra en el desarrollo de sistemas basados en algoritmos que aumentan su complejidad a medida que la tecnología avanza.²





Existen 3 tipos de
criptografía



- Criptografía de Clave Secreta
- Criptología de Clave Pública
- Funciones Hash



Cifrado

El cifrado en ciberseguridad es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados sólo se pueden leer o procesar luego de descifrarlos.

El cifrado es la base principal de la seguridad de datos. Es la forma más sencilla e importante para garantizar que la información de un sistema de computadora no pueda robarla ni leerla alguien que desee utilizarla con fines maliciosos.

El algoritmo de cifrado consta de los siguientes componentes:

- Un conjunto K de claves
- Un conjunto M de mensajes
- Un conjunto C de mensajes de texto cifrados
- Una función $E: K \rightarrow (M \rightarrow C)$

Una función $D: K \rightarrow (C \rightarrow M)$

Cifrado simétrico

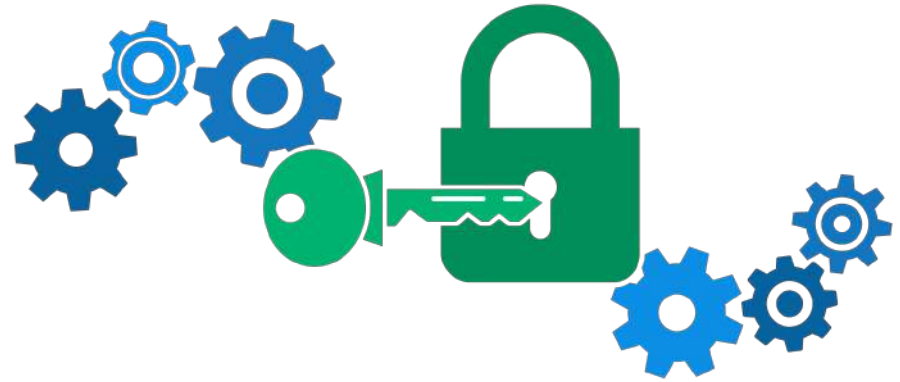
- DES (data-encryption standard)
- Cajas negras
- Cifrado de bloques
- AES (advanced-encryption standard)
- Flujo de clave





Cifrado asimétrico

- RSA (Rivest, Shamir, Adleman)
- Algoritmo RSA





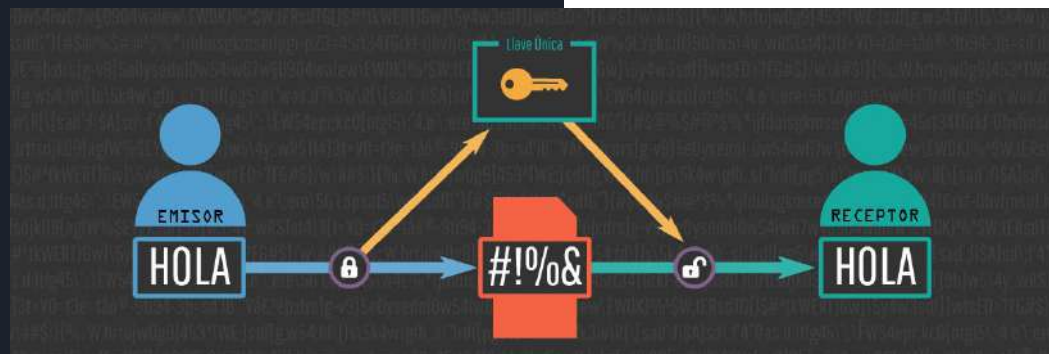
Autenticación

- Función hash
- MAC (message-authentication code)
- No repudio

Componentes de un algoritmo de autenticación:

- Un conjunto K de claves
- Un conjunto M de mensajes
- Un conjunto A de autenticadores
- Una función S
- Una función V

Implementación de mecanismos criptográficos





Autenticación del usuario





Vulnerabilidad de las contraseñas

- Adivinar una contraseña
- Método de enumeración
- cifrado de flujo de datos
- Tipos de amenaza





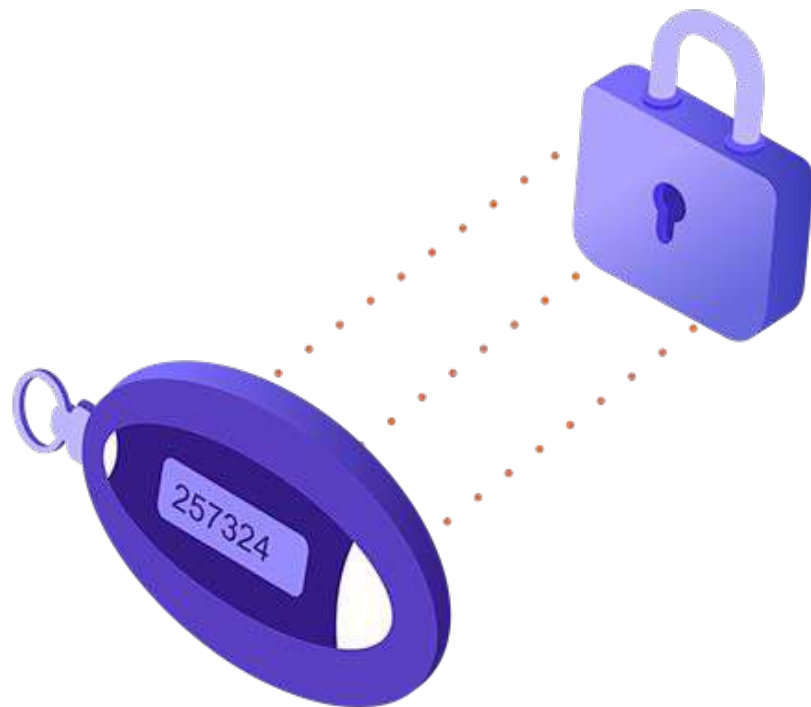
Contraseñas cifradas

¿Como puede
almacenar una
contraseña de
forma segura?



Contraseñas en un solo uso

- contraseñas emparejadas
- no son susceptibles
- semilla
- diferente en varios casos

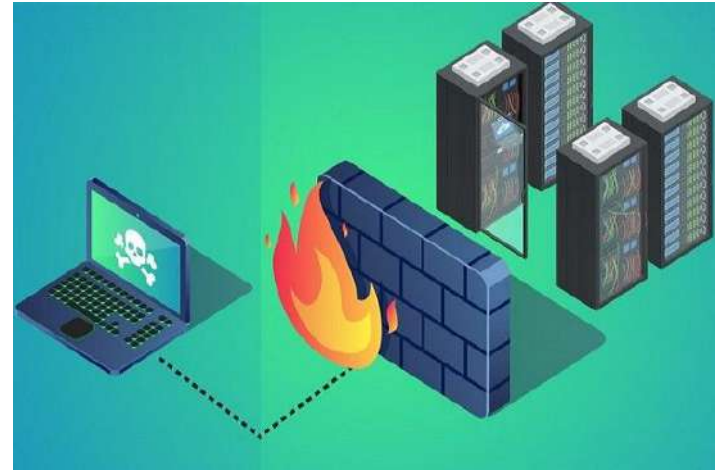


Biométrica



Implementación de defensas de seguridad

- Soluciones de seguridad
- Teoría de defensa en profundidad



Virtualización

Permite que una sola computadora contenga varias máquinas virtuales, cada una de las cuales puede llegar a ejecutar un sistema operativo distinto.

El software llamado "hipervisor" se conecta directamente con el hardware y permite dividir un sistema en entornos separados, distintos y seguros, conocidos como "máquinas virtuales" (VM)



Ejemplo de la aplicación de virtualización

En una empresa que tiene un servidor de correo electrónico, un servidor Web, un servidor FTP, algunos servidores de comercio electrónico, y entre otros servidores más. Todos estos servidores se ejecutan en distintas computadoras, mientras están conectadas por una red de alta velocidad. A veces, dichos servicios se ejecutan en máquinas separadas debido a que una sola máquina no puede manejar la carga, sin embargo, en mucho de los casos la razón para no ejecutar todo en una misma computadora es la **confiabilidad**



Desventaja



Consolidar los servidores en una sola computadora es riesgoso, ya que, si falla el servidor que ejecuta todas las máquinas virtuales, todos los servidores dejarán de ejecutarse.

Pérdida de rendimiento

Ventajas



Costo mucho menor (al tener menos máquinas físicas hay un ahorro en hardware y electricidad) y con una administración más sencilla

- Un sólido aislamiento entre servicios.
- Cada aplicación puede tener su propio entorno
- Facilidad que proporcionan para usar puntos de comprobación y migrar datos entre una máquina virtual y otra. Dicha facilidad se debe a que, Al migrar una máquina virtual, todo lo que hay que mover es la imagen de memoria, ya que todas las tablas del sistema operativo se mueven también.

Ejecutar aplicaciones heredadas o versiones de los sistemas operativos que ya no tienen soporte o que no funcionan en el hardware actual.

El desarrollo de software.



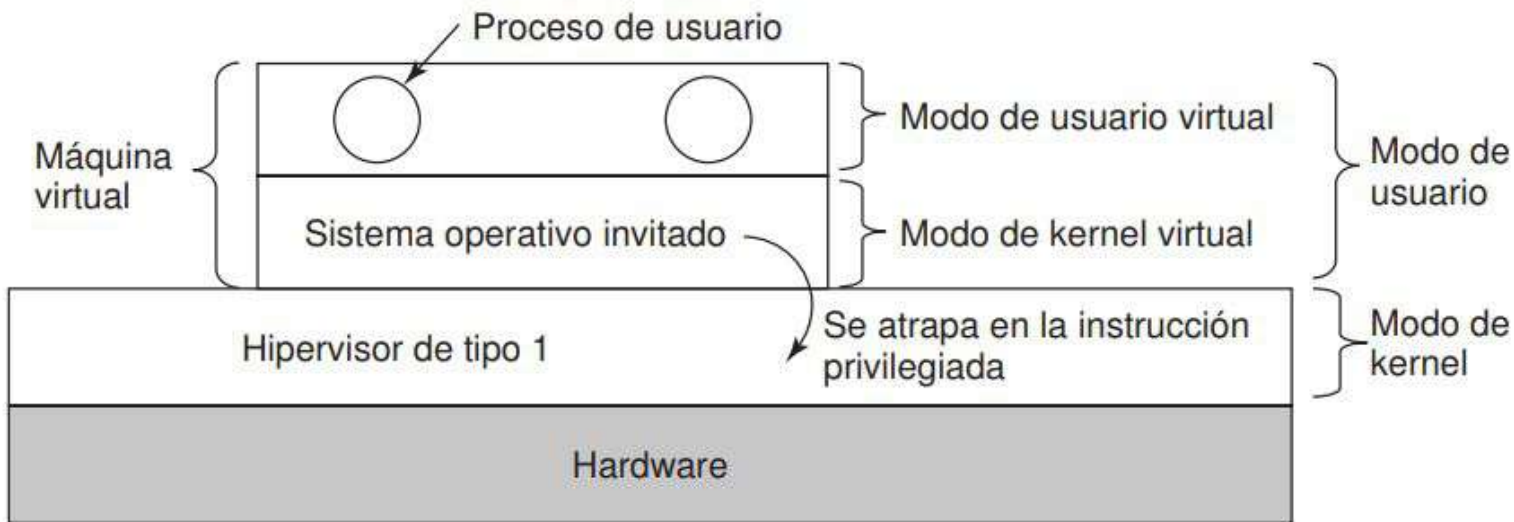
Requerimientos para la virtualización

Tecnología de virtualización presente en las CPU. Estas se integraron en el 2005 por lo que a partir de los Intel Core 2 y AMD pacific y sus sucesores, todas las computadoras son capaces de tener un ambiente de virtualización.

Esta tecnología de virtualización se introdujo debido a errores que tenían anteriormente los sistemas operativos con las instrucciones sensibles (instrucciones que realizan operaciones de E/S, las que modifican las opciones de la MMU) e instrucciones privilegiadas (instrucciones que producen una interrupción)

Hipervisor tipo 1

El hipervisor de tipo 1, también conocido como hipervisor nativo o sin sistema operativo, se ejecuta directamente en el hardware del host y gestiona los sistemas operativos guest. Ocupa el lugar de un sistema operativo host y programa los recursos de las máquinas virtuales directamente en el hardware.





Hipervisor tipo 2

El hipervisor de tipo 2 también se conoce como hipervisor alojado, y se ejecuta en un sistema operativo convencional como una capa de software o una aplicación.

Funciona extrayendo los sistemas operativos guest del sistema operativo host. Los recursos de la máquina virtual se programan en un sistema operativo host, que después se ejecuta en el sistema de hardware.

El hipervisor de tipo 2 es mejor para los usuarios individuales que buscan ejecutar varios sistemas operativos en una computadora personal.

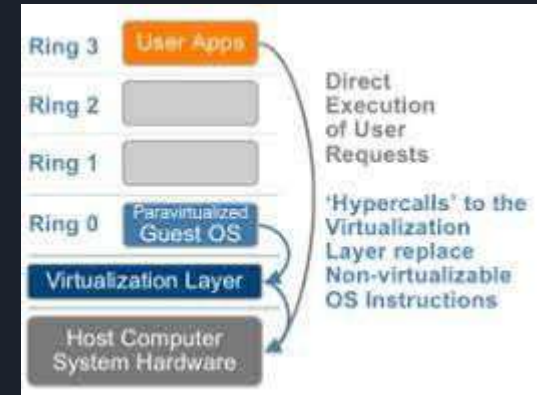
VMware Workstation y Oracle VirtualBox son ejemplos de hipervisores de tipo 2.

Paravirtualización

La paravirtualización es un método que permite que el software que se ejecuta en un sistema virtual omita la interfaz virtual y ejecute operaciones en el hardware real del sistema.

En un sistema virtual estándar, el único programa que utiliza el hardware real del sistema es la interfaz virtual. El resto del software se ejecuta totalmente dentro del entorno virtual.

Con la paravirtualización, hay formas en que el software incluido puede acceder a recursos reales en lugar de virtuales. Esto acelera ciertas funciones sin sacrificar la potencia informática.





Virtualización de la memoria

La virtualización de memoria surge como una solución a las limitaciones que impone la memoria física, al ser uno de los elementos que constituyen un cuello de botella en el desarrollo y el desempeño de aplicaciones.

Es el proceso mediante el cual los recursos de memoria RAM de sistemas computacionales individuales son agrupados y presentados como un único recurso (pool), disponible para cualquiera de ellos. Este conjunto de memorias distribuidas puede ser utilizado como una caché de alta velocidad o como un gran recurso de memoria compartida.



Dispositivos de virtualización

El problema es que muchas aplicaciones dependen de otras tantas aplicaciones y bibliotecas, que a su vez dependen de muchos otros paquetes de software, y así en lo sucesivo.

Este método implica que sólo el desarrollador de software tiene que conocer todas las dependencias. Los clientes reciben un paquete completo que funciona de verdad, sin importar qué sistema operativo estén ejecutando ni qué otro software, paquetes y bibliotecas tengan instalados. A estas máquinas virtuales «empaquetadas y listas para usarse» se les conoce comúnmente como dispositivos virtuales.



Gracias

Inserta tu texto aquí Inserta tu texto
aquí Inserta tu texto aquí Inserta tu
texto aquí Inserta tu texto aquí.

