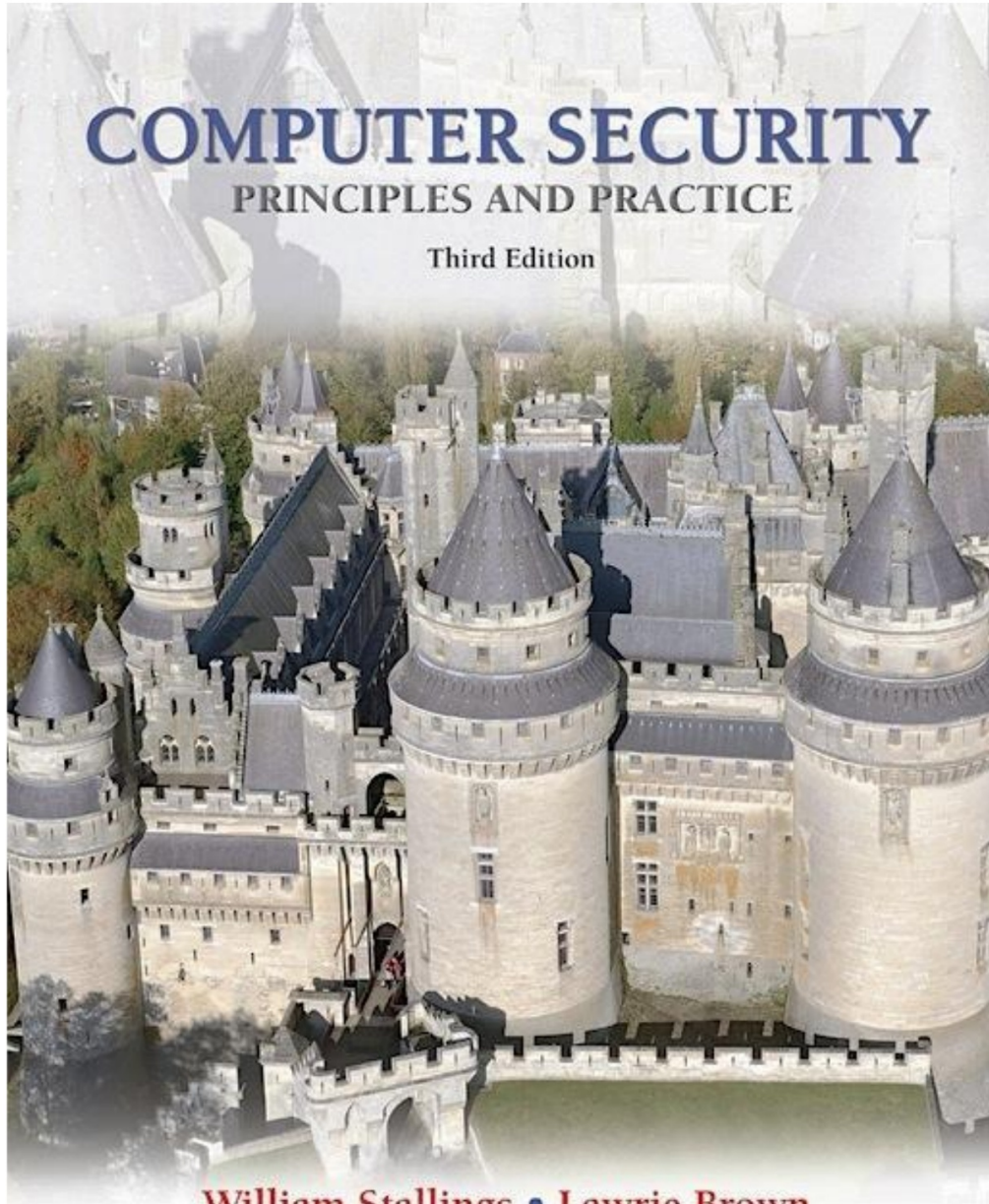


COMPUTER SECURITY

PRINCIPLES AND PRACTICE

Third Edition



William Stallings • Lawrie Brown



Capítulo 12

Seguridad del sistema operativo

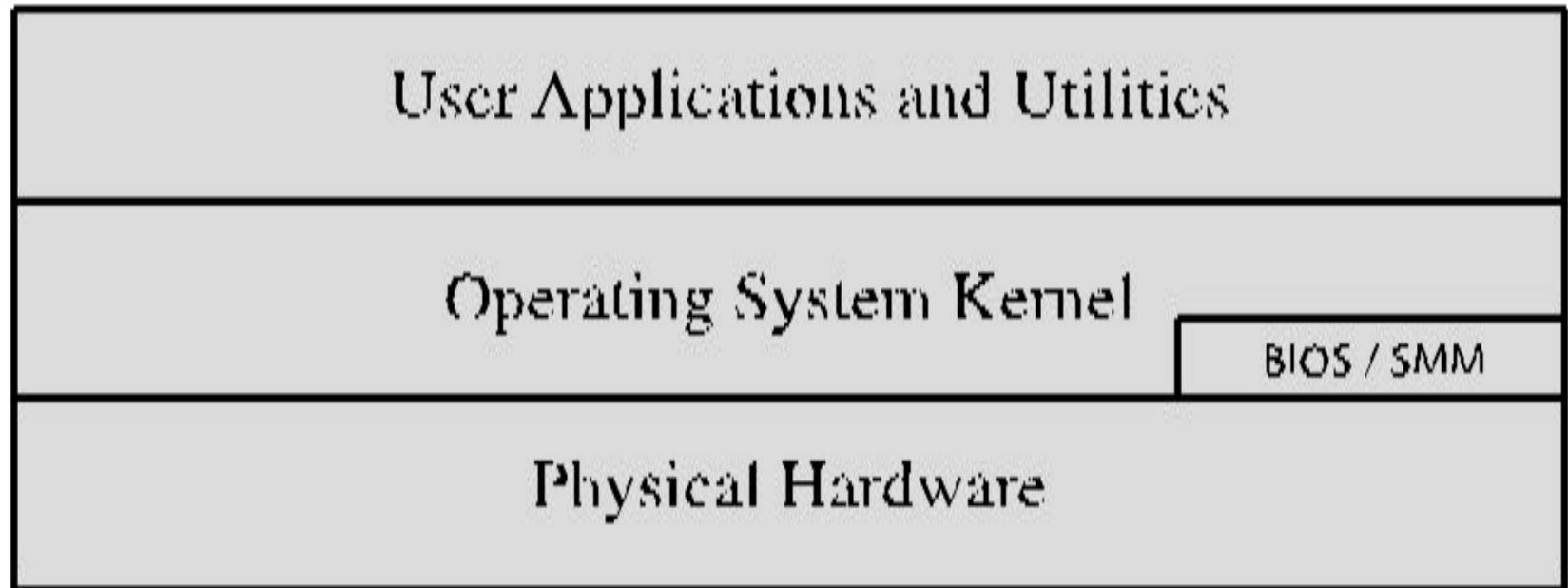


Figure 12.1 Operating System Security Layers

Estrategias

- La Dirección de Señales de Australia (ASD) de 2010 enumera las “Las 35 principales estrategias de mitigación”
- Más del 85% de las intrusiones cibernéticas dirigidas
Los hechos investigados por la ASD en 2009 podrían haberse evitado
- Las cuatro principales estrategias de prevención son:
 - Aplicaciones aprobadas en lista blanca
 - Parchear aplicaciones de terceros y vulnerabilidades del sistema operativo
 - Restringir privilegios administrativos
 - Crear un sistema de defensa en profundidad
- Estas estrategias se alinean en gran medida con las del “20
“Controles críticos” desarrollados por el DHS, la NSA y la
Departamento de Energía, SANS y otros en el
Estados Unidos

Sistema operativo

Seguridad

- Es posible que un sistema se vea comprometido durante el proceso de instalación antes de que pueda instalar los parches más recientes.
- Construir e implementar un sistema debe ser un proceso planificado diseñado para contrarrestar esta amenaza
- El proceso debe:
 - Evaluar los riesgos y planificar la implementación del sistema
 - Proteja el sistema operativo subyacente y luego las aplicaciones clave
 - Asegúrese de que todo el contenido crítico esté protegido
 - Asegúrese de que se utilicen mecanismos de protección de red adecuados
 - Garantizar que se utilicen procesos adecuados para mantener la seguridad.

Planificación de la seguridad del sistema

El plan debe identificar el personal y la capacitación adecuados para instalar y administrar el sistema.

El proceso de planificación debe determinar los requisitos de seguridad para el sistema, las aplicaciones, los datos y los usuarios.

El primer paso para implementar un nuevo sistema es la planificación

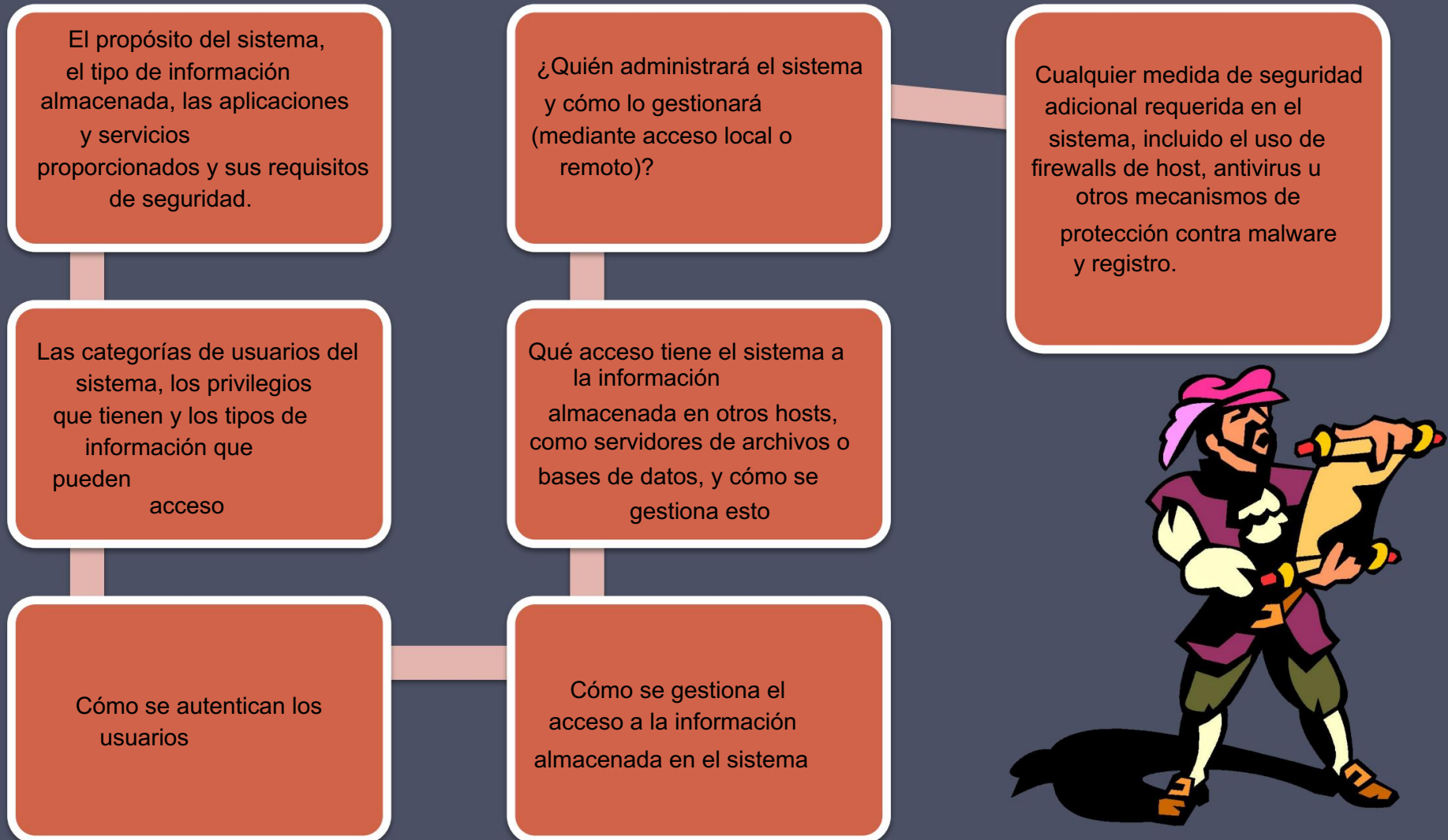


La planificación debe incluir una amplia evaluación de seguridad de la organización.

El objetivo es maximizar la seguridad y minimizar los costos.

Planificación de la seguridad del sistema

Proceso

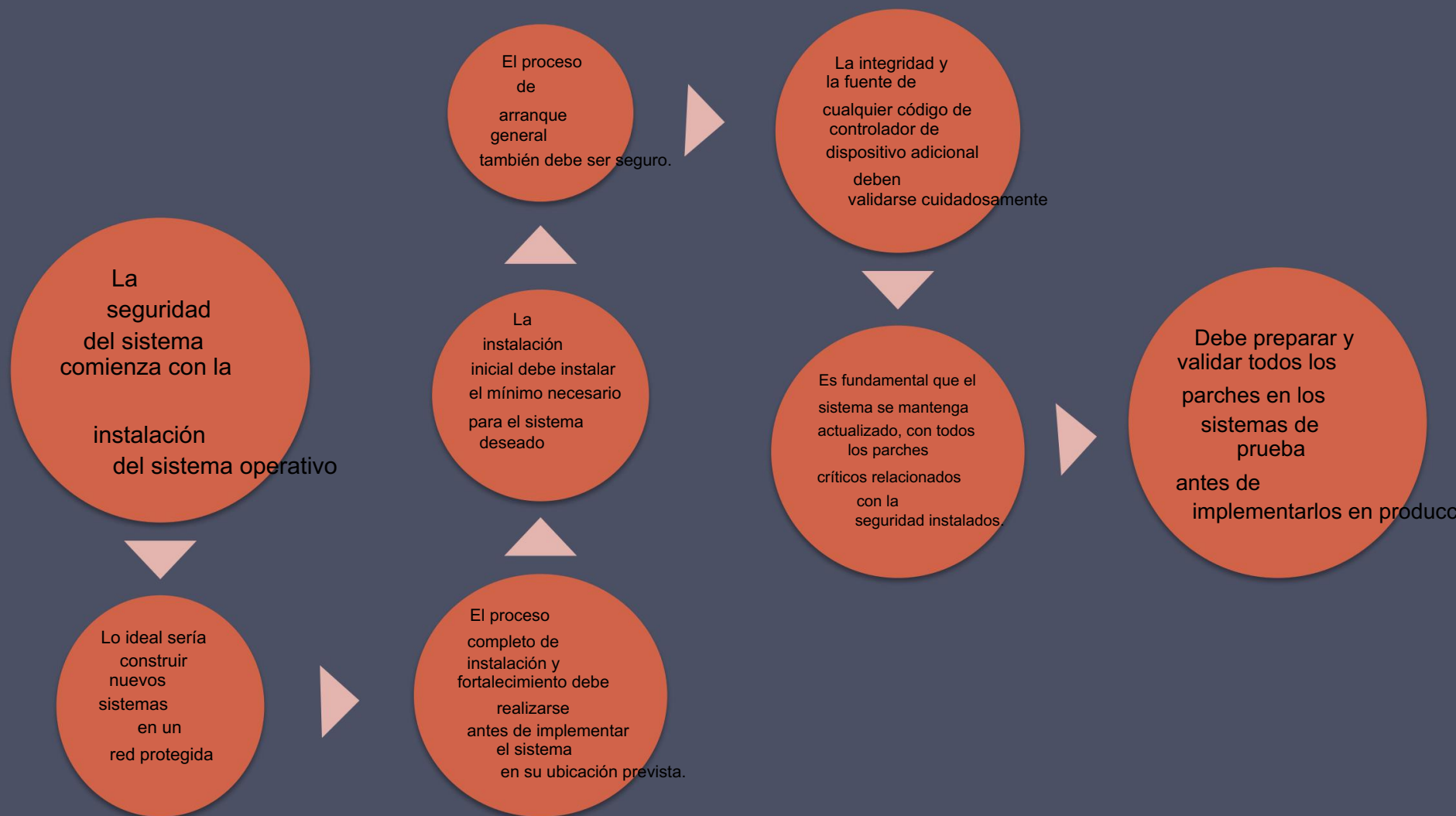



Sistemas operativos

Endurecimiento

- El primer paso crítico para proteger un sistema es proteger el sistema operativo base.
- Pasos básicos
 - o Instalar y parchear el sistema operativo
 - o Fortalecer y configurar el sistema operativo para abordar adecuadamente las necesidades de seguridad identificadas del sistema mediante:
 - Eliminar servicios, aplicaciones y protocolos innecesarios
 - Configuración de usuarios, grupos y permisos
 - Configuración de controles de recursos
 - o Instalar y configurar controles de seguridad adicionales, como antivirus, firewalls basados en host y sistemas de detección de intrusiones (IDS)
 - o Probar la seguridad del sistema operativo básico para garantizar que las medidas adoptadas aborden adecuadamente sus necesidades de seguridad

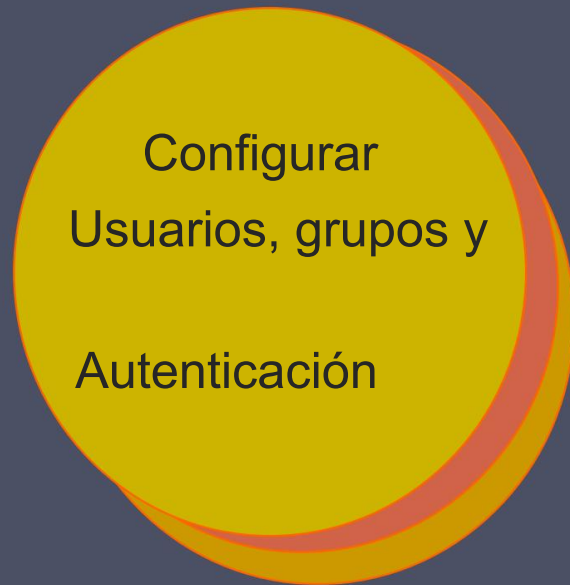
Configuración inicial y aplicación de parches





Eliminar
Innecesario
Servicios,
Aplicaciones,
Protocolos

- Si hay menos paquetes de software disponibles para ejecutar, el riesgo se reduce.
 - El proceso de planificación del sistema debe identificar lo que realmente se requiere para un sistema determinado.
- Al realizar la instalación inicial no se deben utilizar los valores predeterminados proporcionados
 - La configuración predeterminada está configurada para maximizar la facilidad de uso y la funcionalidad en lugar de la seguridad.
 - Si más adelante se necesitan paquetes adicionales, se pueden instalar cuando sean necesarios.



- No todos los usuarios con acceso a un sistema tendrán el mismo acceso a todos los datos y recursos de ese sistema.
- Los privilegios elevados deben restringirse únicamente a aquellos usuarios que los requieran, y solo cuando sean necesarios para realizar una tarea.

- El proceso de planificación del sistema debe considerar:
 - Categorías de usuarios en el sistema
 - Privilegios que tienen
 - Tipos de información que pueden acceso
 - Cómo y dónde están definido y autenticado
- Las cuentas predeterminadas incluidas como parte de la instalación del sistema deben estar protegidas.
 - Aquellos que no son obligatorios Debería eliminarse o deshabilitarse
 - Políticas que se aplican a las credenciales de autenticación configuradas

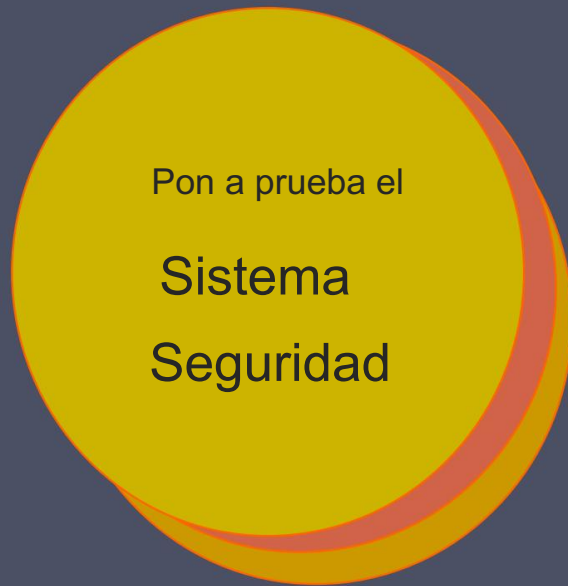
Configurar
Recurso
Controles



Instalar
Adicional
Seguridad
Controles

- Una vez definidos los usuarios y grupos, se pueden establecer los permisos adecuados sobre los datos y recursos.
- Muchas de las guías de fortalecimiento de la seguridad proporcionan listas de cambios recomendados para la configuración de acceso predeterminada.

- Mayor seguridad posible mediante la instalación y configuración de herramientas de seguridad adicionales:
 - Software antivirus
 - Cortafuegos basados en host
 - software IDS o IPS
 - Lista blanca de aplicaciones



- El paso final en el proceso de protección inicial del sistema operativo base es la prueba de seguridad.
- Meta:
 - Asegúrese de que los pasos de configuración de seguridad anteriores se implementen correctamente
 - Identificar posibles vulnerabilidades

- Las listas de verificación se incluyen en las guías de fortalecimiento de la seguridad.
- Existen programas diseñados específicamente para:
 - Revisar un sistema para garantizar que cumpla con los requisitos básicos de seguridad.
 - Analizar en busca de vulnerabilidades conocidas y malas prácticas de configuración.
- Debería hacerse tras el endurecimiento inicial del s
- Se repite periódicamente como parte del proceso de mantenimiento de seguridad.

Configuración de la aplicación

- Puede incluir:
 - Crear y especificar áreas de almacenamiento de datos apropiadas para la aplicación
 - Realizar los cambios apropiados en los detalles de configuración predeterminados de la aplicación o el servicio
- Algunas aplicaciones o servicios pueden incluir:
 - Datos predeterminados
 - Guiones
 - Cuentas de usuario
- De particular preocupación con servicios a los que se accede de forma remota, como servicios web y de transferencia de archivos.
 - El riesgo de esta forma de ataque se reduce al garantizar que la mayoría de los archivos solo puedan ser leídos, pero no escritos, por el servidor.

Tecnología de encriptación

Es una tecnología habilitadora clave que puede utilizarse para proteger los datos tanto en tránsito como cuando están almacenados.

Se deben configurar y crear claves criptográficas apropiadas, firmadas y protegidas.

Si se proporcionan servicios de red seguros mediante TLS o IPsec, se deben generar claves públicas y privadas adecuadas para cada uno de ellos.

Si se proporcionan servicios de red seguros utilizando SSH, se deben crear claves de servidor y cliente adecuadas.

Los sistemas de archivos criptográficos son otro uso del cifrado.



Mantenimiento de seguridad

- El proceso de mantenimiento de la seguridad es continuo.
- El mantenimiento de seguridad incluye:
 - Monitorear y analizar la información de registro
 - Realizar copias de seguridad periódicas
 - Recuperarse de los problemas de seguridad
 - Probar periódicamente la seguridad del sistema
 - Utilizar procesos de mantenimiento de software adecuados para
Aplicar parches y actualizar todo el software crítico, y supervisar y revisar la configuración según sea necesario

Explotación florestal

Sólo puedo informarle sobre cosas malas que ya han sucedido.

En caso de una violación o falla del sistema, los administradores del sistema pueden identificar más rápidamente lo que sucedió.

La clave es asegurarse de capturar los datos correctos y luego monitorearlos y analizarlos adecuadamente.

La información puede ser generada por el sistema, la red y las aplicaciones.

El rango de datos adquiridos debe determinarse durante la etapa de planificación del sistema.

Genera volúmenes importantes de información y es importante que se les asigne suficiente espacio.

Se prefiere el análisis automatizado

Copia de seguridad y archivo de datos

Realizar copias de seguridad periódicas de los datos es un control fundamental que ayuda a mantener la integridad del sistema y los datos del usuario.

Pueden existir requisitos legales u operativos para la conservación de datos.

Respaldo

El proceso de realizar copias de datos a intervalos regulares.

Archivo

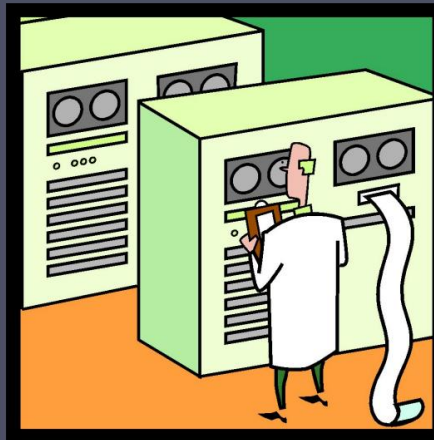
El proceso de conservar copias de datos durante períodos prolongados de tiempo para cumplir con los requisitos legales y operativos para acceder a datos pasados.

Las necesidades y políticas relacionadas con la copia de seguridad y el archivo deben determinarse durante la etapa de planificación del sistema.

Mantenido en línea o fuera de línea

Almacenado localmente o transportado a un sitio remoto

- Las compensaciones incluyen la facilidad de implementación y el costo versus una mayor seguridad y solidez contra diferentes amenazas.



Seguridad de Linux/Unix

- Gestión de parches

- Mantener los parches de seguridad actualizados es una cuestión ampliamente reconocida y crítica.
control para mantener la seguridad

- Configuración de aplicaciones y servicios

- Lo más común es implementarlo utilizando archivos de texto separados para cada aplicación y servicio
 - Generalmente se encuentra en el directorio /etc o en el árbol de instalación de una aplicación específica
 - Las configuraciones de usuario individuales que pueden anular los valores predeterminados del sistema se encuentran en archivos "dot" ocultos en el directorio de inicio de cada usuario.
 - Los cambios más importantes necesarios para mejorar la seguridad del sistema son deshabilitar los servicios y aplicaciones que no son necesarios.

Seguridad de Linux/Unix

- Usuarios, grupos y permisos
 - El acceso se especifica otorgando permisos de lectura, escritura y ejecución a cada propietario, grupo y otros para cada recurso
 - Las guías recomiendan cambiar los permisos de acceso para directorios y archivos críticos
 - Exploit local
 - Vulnerabilidad de software que puede ser explotada por un atacante para obtener privilegios elevados.
 - Explotación remota
 - Vulnerabilidad de software en un servidor de red que podría ser activada por un atacante remoto

Seguridad de Linux/Unix

Controles de acceso remoto

- Varios firewalls de host
Se pueden utilizar programas
- La mayoría de los sistemas proporcionan una
Utilidad administrativa para seleccionar
qué servicios tendrán
permitido acceder al sistema

Registro y rotación de registros

- No debe asumirse que el
La configuración predeterminada es
necesariamente apropiada



Seguridad de Linux/Unix

- cárcel chroot
 - Restringe la vista del servidor del sistema de archivos a solo una parte específica
 - Utiliza la llamada al sistema chroot para confinar un proceso asignando la raíz del sistema de archivos a algún otro directorio
 - Los directorios de archivos fuera de la cárcel chroot no son visibles o accesible
 - La principal desventaja es la complejidad añadida.



Seguridad de Windows

Gestión de parches

- “Actualización de Windows” y “Actualización de Windows Server”
El servicio “ayuda con el mantenimiento regular y debe utilizarse
- Las aplicaciones de terceros también brindan soporte de actualización automática.



Administración de usuarios y controles de acceso

- Los sistemas implementan controles de acceso discrecionales recursos
- Los sistemas Vista y posteriores incluyen controles de integridad obligatorios
- Los objetos se etiquetan como de nivel de integridad bajo, medio, alto o del sistema. • El sistema garantiza que la integridad del sujeto sea igual o superior al nivel del objeto.
- Implementa una forma de la Modelo de integridad de Biba

Seguridad de Windows

Administración de usuarios y controles de acceso

Los sistemas Windows también definen privilegios

- Para todo el sistema y concedido a cuentas de usuario

Combinación de acciones y

Los permisos NTFS se pueden utilizar para proporcionar seguridad y granularidad adicionales al acceder a archivos en un recurso compartido.

Control de cuentas de usuario (UAC)

- Proporcionado en Vista y sistemas posteriores
- Ayuda a garantizar que los usuarios con derechos administrativos solo los utilicen cuando sea necesario; de lo contrario, acceden al sistema de forma normal. usuario

Servicio de bajo privilegio Cuentas

- Se utiliza para procesos de servicio de larga duración, como archivo, impresión y Servicios DNS

Seguridad de Windows

Configuración de aplicaciones y servicios

- Gran parte de la información de configuración está centralizada en el Registro
 - Forma una base de datos de claves y valores que pueden ser consultados e interpretados por las aplicaciones.
- Las claves de registro se pueden modificar directamente utilizando el “Editor de registro”
 - Más útil para realizar cambios masivos

Seguridad de Windows

Otros controles de seguridad

- Es esencial que los antivirus, antispyware, firewall personal y otros
Se instalan y configuran paquetes de software de detección y manejo de malware y ataques.
- Los sistemas Windows de la generación actual incluyen un firewall básico y
Capacidades de contramedidas contra malware
- Es importante garantizar que el conjunto de productos en uso sea compatible.

Los sistemas Windows también admiten una variedad de funciones criptográficas:

- Cifrado de archivos y directorios mediante el Sistema de cifrado de archivos (EFS)
- Cifrado de disco completo con AES mediante BitLocker

“Analizador de seguridad de línea base de Microsoft”

- Herramienta gratuita y fácil de usar que verifica el cumplimiento de las normas de Microsoft.
recomendaciones de seguridad

Virtualización

- Una tecnología que proporciona una abstracción de los recursos utilizados por algún software que se ejecuta en un entorno simulado llamado máquina virtual.

(M.V.)

- Los beneficios incluyen una mejor eficiencia en el uso de la recursos del sistema físico
- Proporciona soporte para múltiples sistemas operativos distintos y aplicaciones asociadas en un sistema físico
- Plantea problemas de seguridad adicionales

Alternativas de virtualización

Virtualización de aplicaciones

Permite
que las
aplicaciones
escritas para un
entorno se ejecuten
en otro sistema
operativo.

Virtualización completa

Varias
instancias
de
sistema
operativo
completo se ejecutan en paralelo

Monitor de máquina virtual (VMM)

Hipervisor

Coordina el acceso entre
cada uno de los invitados y
el hardware físico real

recursos

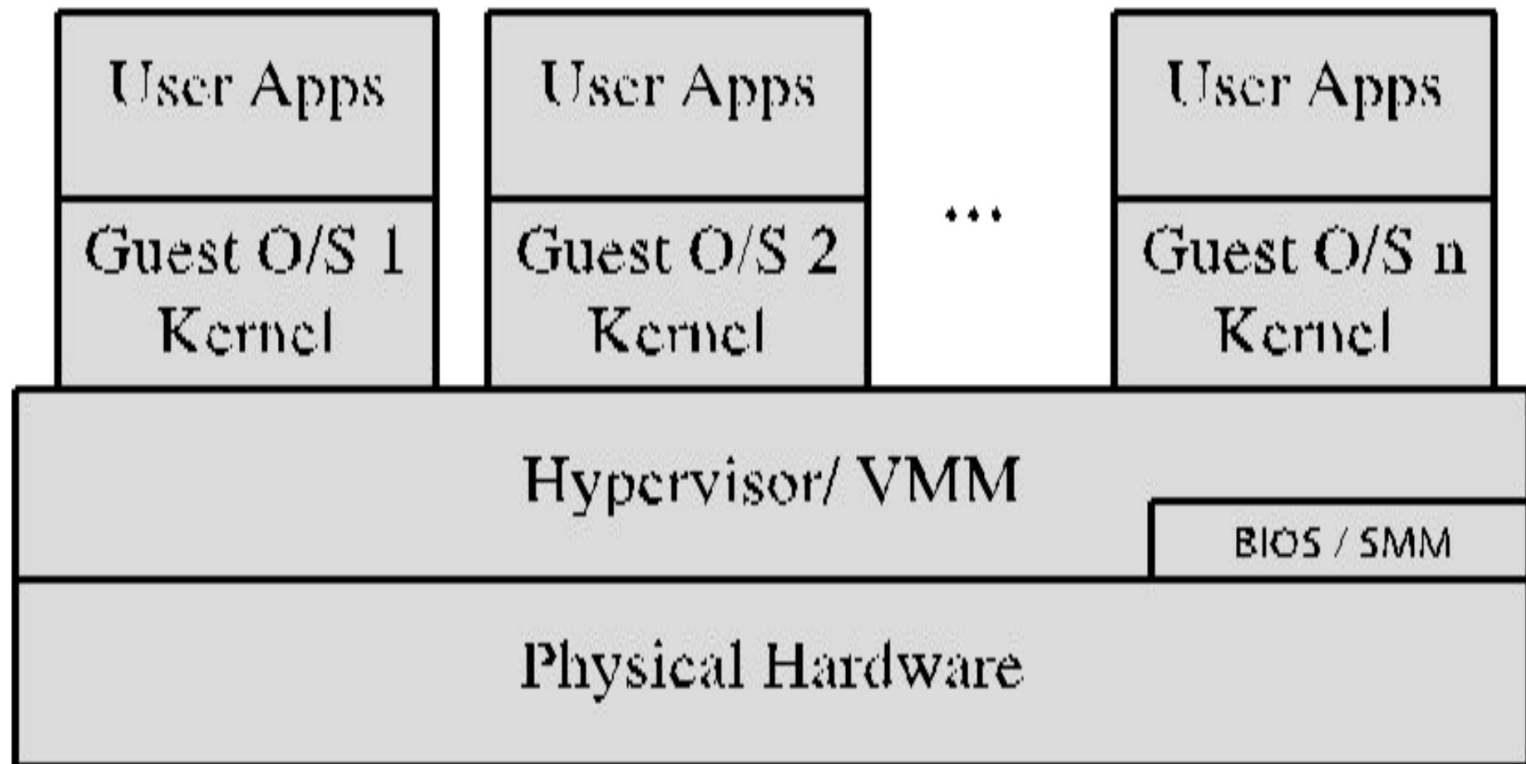


Figure 12.2 Native Virtualization Security Layers

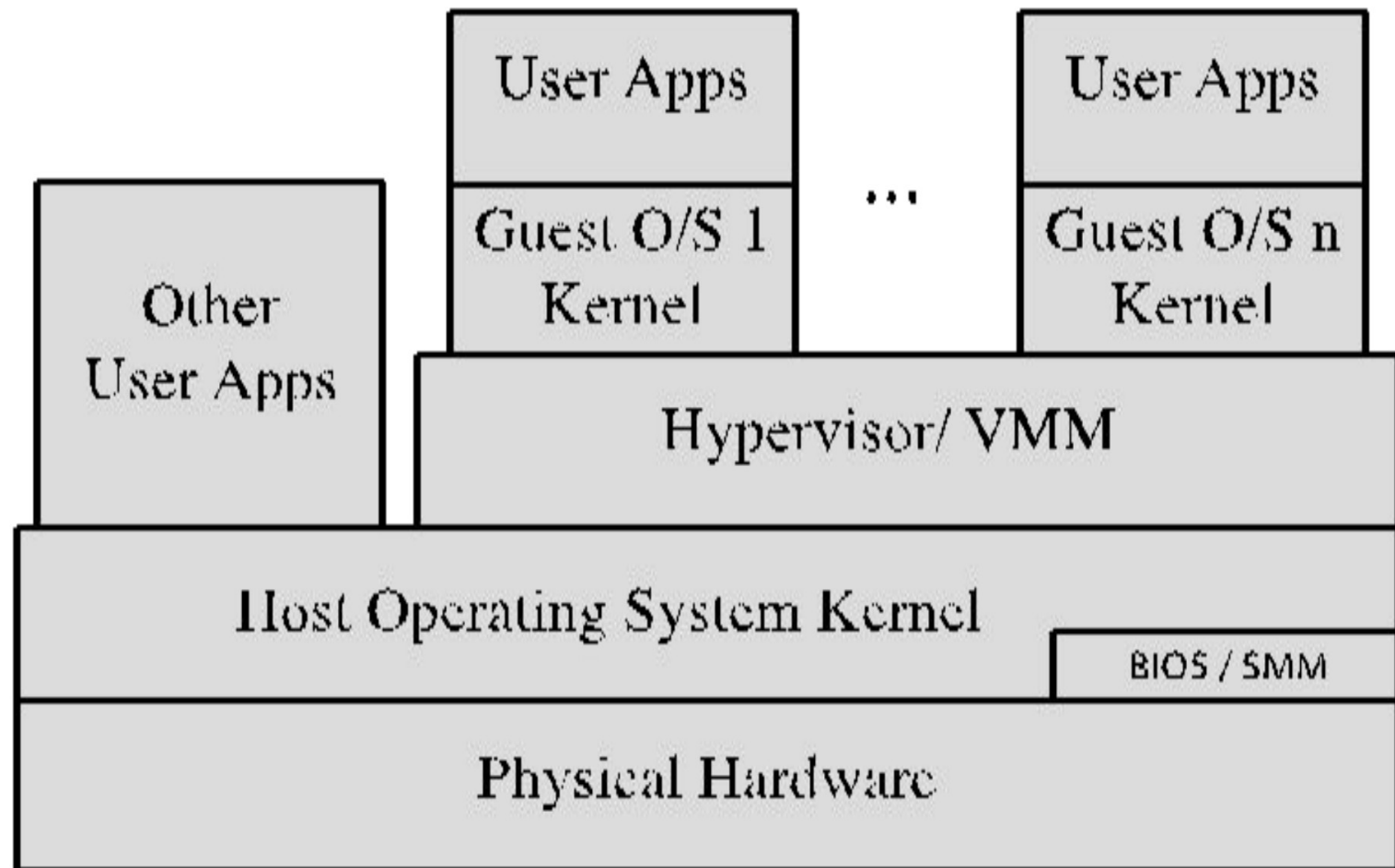


Figure 12.3 Hosted Virtualization Security Layers

Seguridad de la virtualización

Asuntos

- Las preocupaciones de seguridad incluyen:
 - Aislamiento del sistema operativo invitado
 - Garantizar que los programas que se ejecutan dentro de un sistema operativo invitado
Sólo podrá acceder y utilizar los recursos que le sean asignados.
 - Monitoreo del sistema operativo invitado por parte del hipervisor
 - Que tiene acceso privilegiado a los programas y datos de cada sistema operativo invitado
 - Seguridad del entorno virtualizado
 - En particular, la gestión de imágenes e instantáneas que los atacantes pueden intentar ver o modificar.

Asegurar la virtualización Sistemas

**Organizaciones
que
utilizan la virtualización
debería:**

- Planifique cuidadosamente la seguridad del sistema virtualizado
- Asegurar todos los elementos de una solución de virtualización completa y mantener su seguridad
- Asegúrese de que el hipervisor esté correctamente protegido.
- Restringir y proteger el acceso del administrador a la solución de virtualización.

Seguridad del hipervisor

- Debería ser
 - o Protegido mediante un proceso similar al de proteger un sistema operativo
 - o Instalado en un entorno aislado
 - o Configurado para que se actualice automáticamente
 - o Se monitorea para detectar cualquier signo de compromiso.
 - o Accedido únicamente por la administración autorizada
- Puede admitir tanto la administración local como la remota, por lo que debe ser configurado apropiadamente
- Se debe considerar y proteger el acceso a la administración remota.
 - en el diseño de cualquier firewall de red y capacidad IDS en uso
- Lo ideal sería que el tráfico administrativo utilizara una red separada con Acceso muy limitado proporcionado desde fuera de la organización.

Virtualización

Infraestructura

Seguridad



Resumen

- Introducción a seguridad del sistema operativo
- Planificación de la seguridad del sistema
- Fortalecimiento de los sistemas operativos
 - o Instalación del sistema operativo: configuración inicial y parches
 - o Eliminar servicios, aplicaciones y protocolos innecesarios
 - o Configurar usuarios, grupos y autenticaciones
 - o Configurar controles de recursos
 - o Instalar controles de seguridad adicionales
 - o Probar la seguridad del sistema
- Seguridad de la aplicación
 - o Configuración de la aplicación
 - o Tecnología de cifrado
- Mantenimiento de seguridad
 - o Registro
 - o Copia de seguridad y archivo de datos



- Seguridad de Linux/Unix
 - o Gestión de parches
 - o Configuración de aplicaciones y servicios
 - o Usuarios, grupos y permisos
 - o Controles de acceso remoto
 - o Registro y rotación de registros
 - o Seguridad de la aplicación mediante una cárcel chroot
 - o Pruebas de seguridad
- Seguridad de Windows
 - o Gestión de parches
 - o Administración de usuarios y controles de acceso
 - o Configuración de aplicaciones y servicios
 - o Otros controles de seguridad
 - o Pruebas de seguridad
- Seguridad de virtualización
 - o Seguridad de virtualización