UAI Universidad Abierta Interamericana

SISTEMAS OPERATIVOS

Mg. Leandro Ezequiel Mascarello

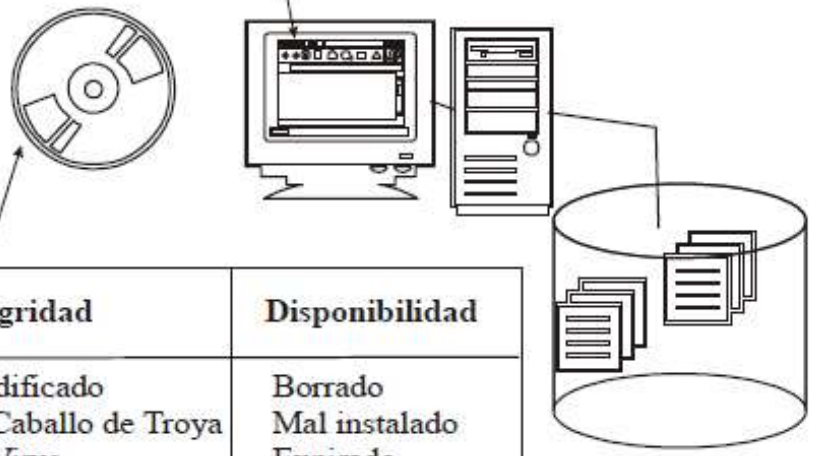
<leandro.mascarello@uai.edu.ar>

UAIOnline ultra

- La **seguridad** de un sistema tiene múltiples facetas:
  - Protección ante posibles daños físicos de los datos (fuegos, terremotos, etc.).
  - Acceso indebido a los mismos (intrusos, fallos de privacidad, etc.).
  - ...
- La **protección** consiste en evitar que se haga un uso indebido de los recursos cuando se está dentro del ámbito del sistema operativo.
  - Deben existir mecanismos y políticas que aseguren que los usuarios sólo acceden a sus propios recursos (archivos, zonas de memoria, etc.).

Posibles Problemas de Seguridad

Elemento	Privacidad	Integridad	Disponibilidad
Hardware	Robado Copiado	Destruido Sobrecargado Pinchado Falsificado	Fallido No disponible Robado Destruido



Elemento	Privacidad	Integridad	Disponibilidad
Software	Robado Copiado	Modificado Caballo de Troya Virus Falsificado	Borrado Mal instalado Expirado

Elemento	Privacidad	Integridad	Disponibilidad
Datos	Descubiertos Inferidos Interceptados	Dañados Error HW Error SW Error usuario	Borrados Mal instalados Destruídos

Aspecto de Seguridad de un S.O.

- Tres aspectos de diseño:

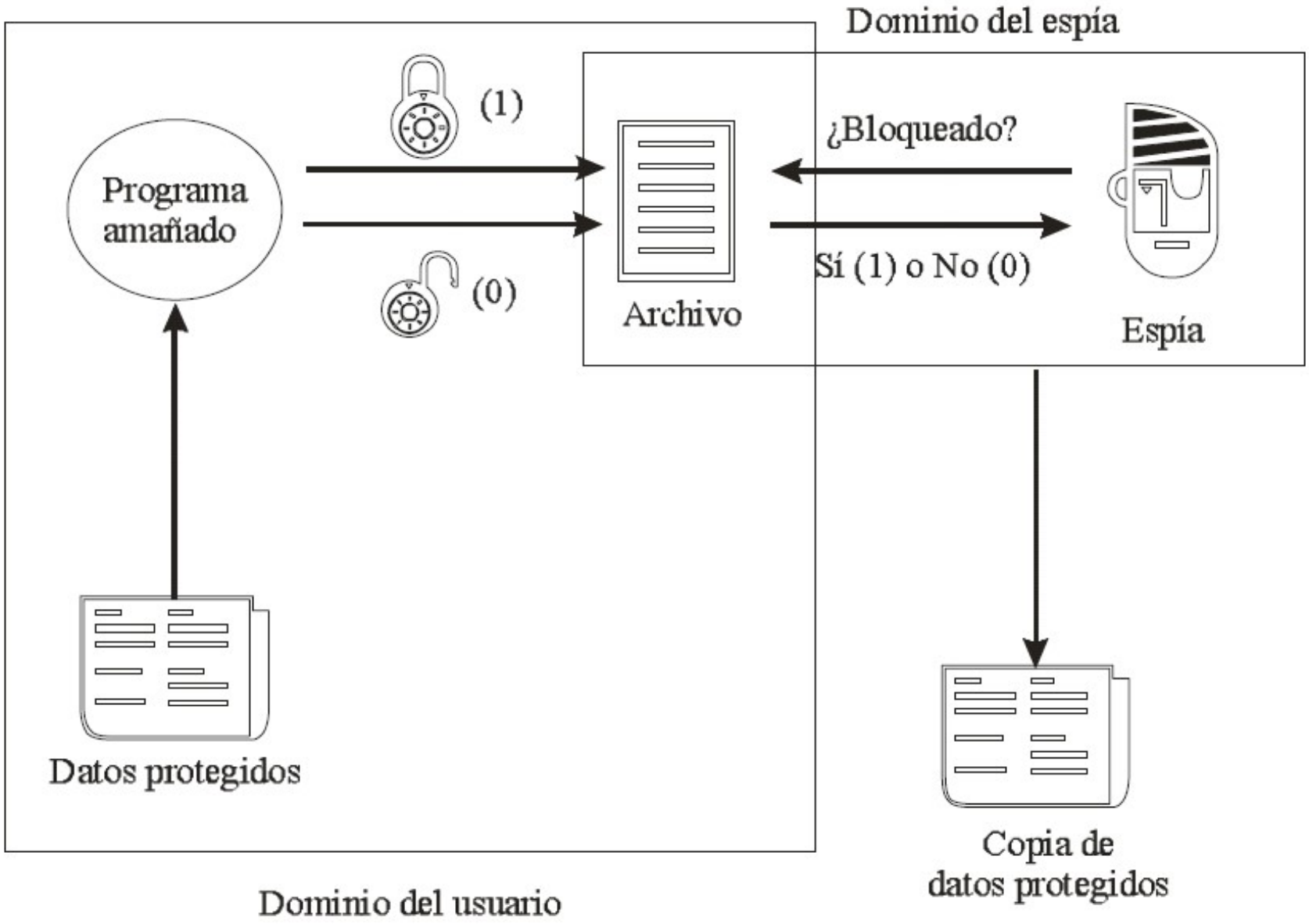
- Evitar la pérdida de datos.
  - Copias de seguridad, ...

- Controlar la privacidad de los datos.
  - Cifrado, ...

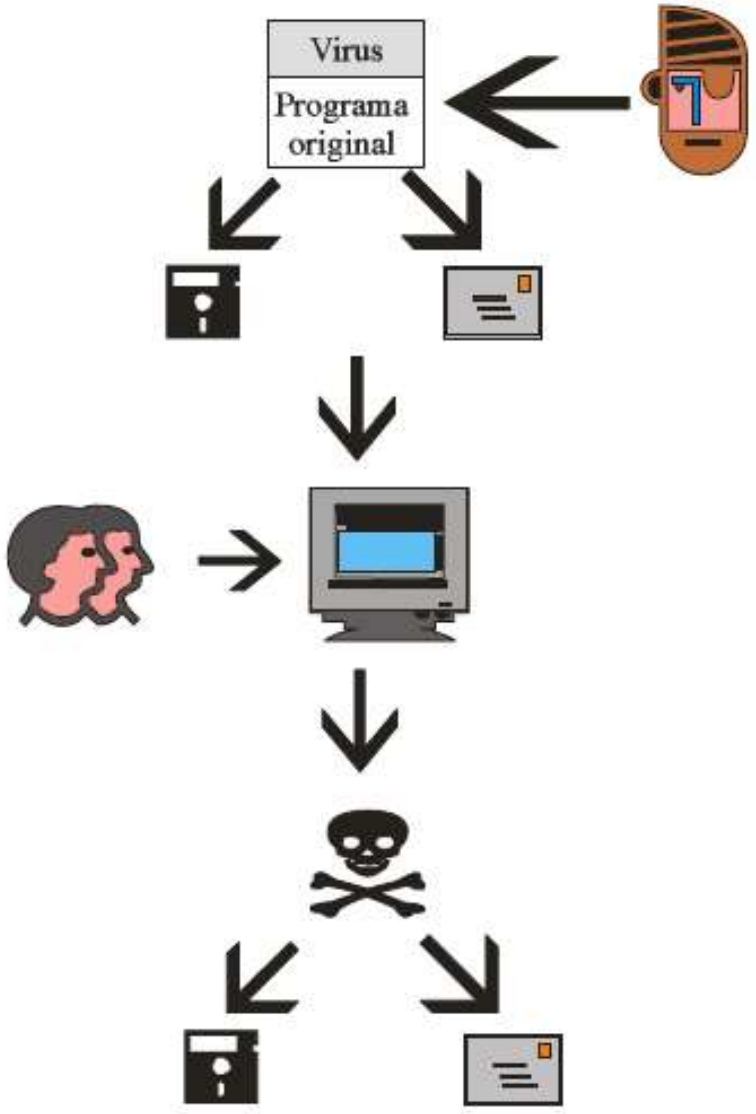
Problemas de Seguridad

- Uso indebido o malicioso de programas
  - Caballo de Troya
  - Puerta de atrás
  - Canales encubiertos
- Usuarios inexpertos o descuidados
- Usuarios no autorizados
  - Autenticación

Uso de un canal encubierto



Instalación y propagación de un Virus



Problemas de Seguridad

- Gusanos
  - Programas destructivos que se autopropagan
  - Con fines maliciosos
- Rompedores de sistemas de protección
  - Analizadores de contraseñas
- Bombardeos
  - Ataques por denegación de servicio

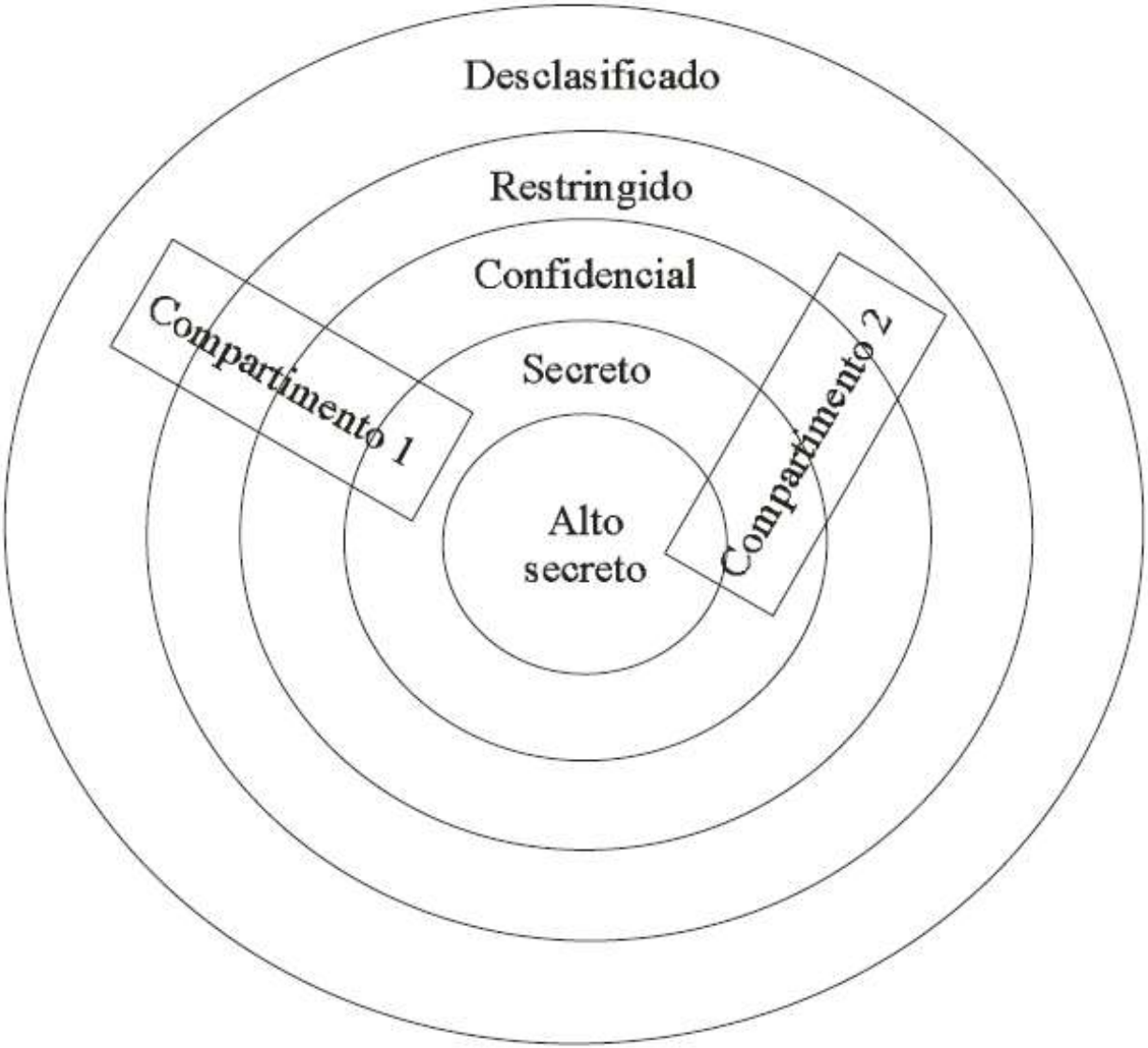
Políticas de Seguridad

- Cada organización tiene requisitos de seguridad distintos
- La política de seguridad dicta las normas a seguir para proporcionar protección y dotar de seguridad a los sistemas
- No implica mecanismos, sólo políticas
- Existen leyes que se deben cumplir cuando se usa información confidencial
- La política de seguridad debe dar confianza

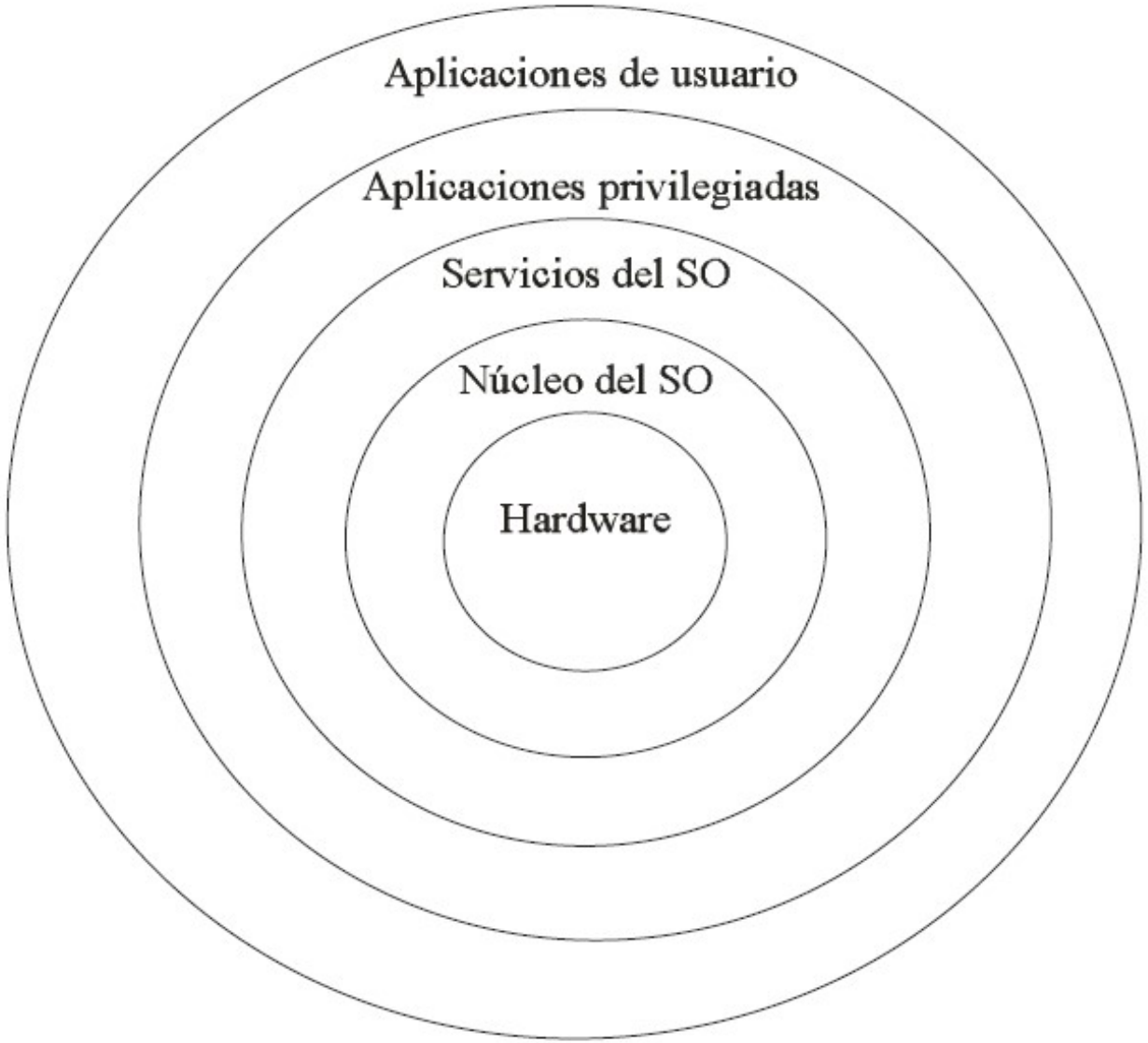
Política Militar

- Se basa en la clasificación de todos los objetos con requisitos de seguridad en uno de los siguientes cinco **niveles de seguridad**:
  - Desclasificado, Restringido, Confidencial, Secreto, Alto secreto.
- Los usuarios que tienen acceso a objetos de nivel `i` también lo tienen a los de `i+1`.
- Regla de **lo que se necesita saber**: sólo se permite el acceso a datos sensibles a quien los necesita para hacer su trabajo.
- De esta forma, se puede **compartimentar** a los usuarios, haciendo más estricta la regla general de acceso.
- Un **compartimento** se puede extender a varios niveles y dentro del mismo se aplica también la regla general de acceso.

Criterio de la Política Militar

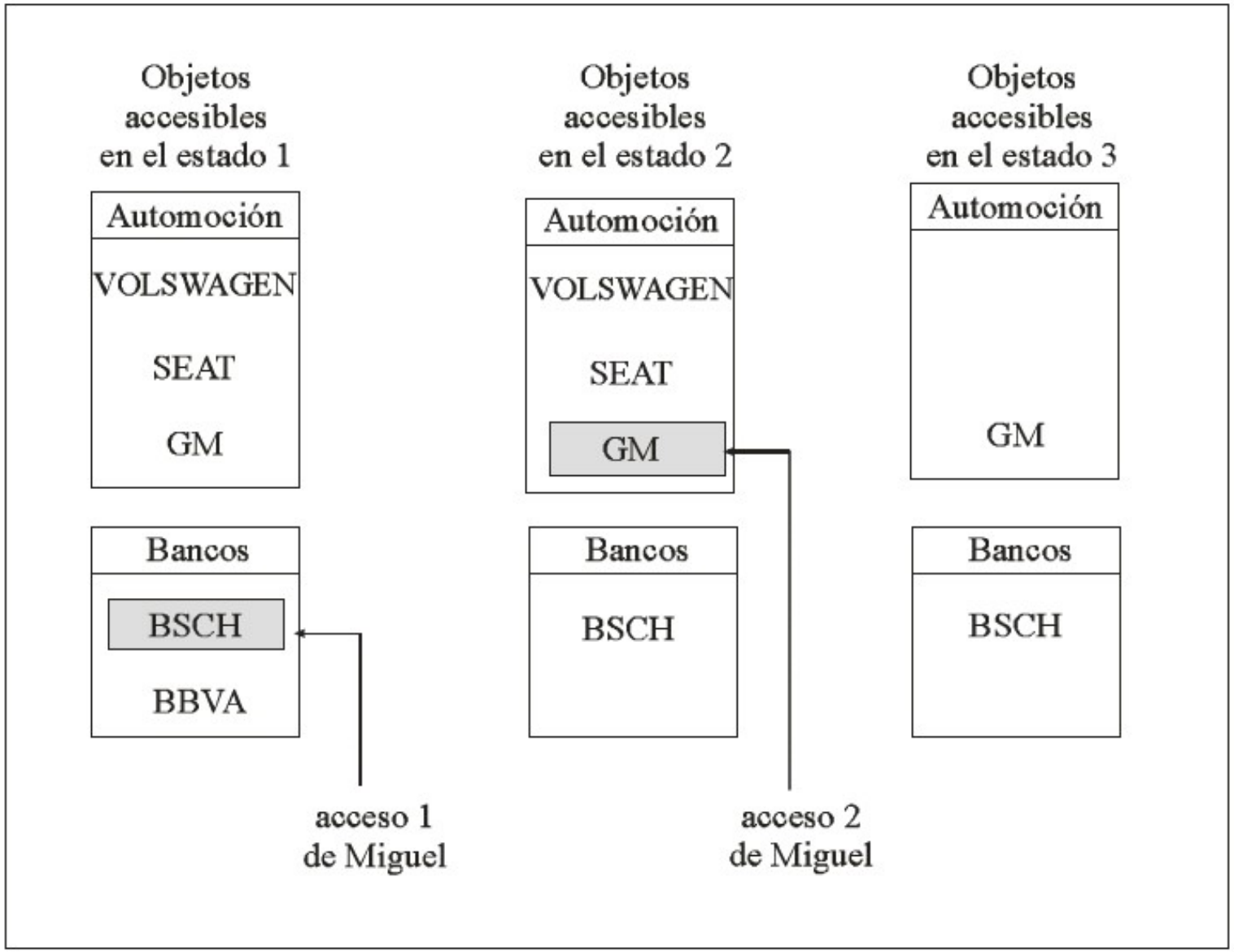


Política de Seguridad en VMS



- Se basan en la política militar, pero debilitan los requisitos.
- **Muralla china**: clasifica a objetos y usuarios en tres niveles de abstracción:
    - Objetos, Grupos y Clases de conflicto.
  - Cada objeto pertenece a un único grupo y cada grupo a una única clase de conflicto.
  - Una clase de conflicto, sin embargo, puede incluir a varios grupos.
- Política de control de acceso: Una persona puede acceder a la información siempre que antes no haya accedido a otro grupo de la clase de conflicto a la que pertenece la información a la que quiere acceder.

Ejemplo de la Muralla China



Modelos de Seguridad

- Un modelo es un mecanismo que permite hacer explícita una política de seguridad.
- **Modelos de seguridad multinivel:** rangos de sensibilidad y separación rigurosa entre sujetos y los objetos a los que no tienen acceso.
  - Suelen ser modelos abstractos y muy generales, lo que los convierte en muy complejos, difíciles de verificar y muy costosos de implementar.
- **Modelos de seguridad limitada:** responder formalmente a las propiedades que un sistema seguro debe satisfacer, pero introduciendo restricciones a los sistemas de seguridad multinivel. Todos ellos se basan en dos principios:
  - Usan la teoría general de la computación para definir un sistema formal de reglas de protección.
  - Usan una matriz de control de acceso, en cuyas filas están los sujetos y en cuyas columnas están los sujetos.
- Los derechos de acceso del sujeto `i` sobre el objeto `j` son los contenidos del elemento de la matriz `(i,j)`.
- Ejemplos: Graham-Denning, Harrison-Ruzzo-Hullman (HRU) y los de permiso de acceso.

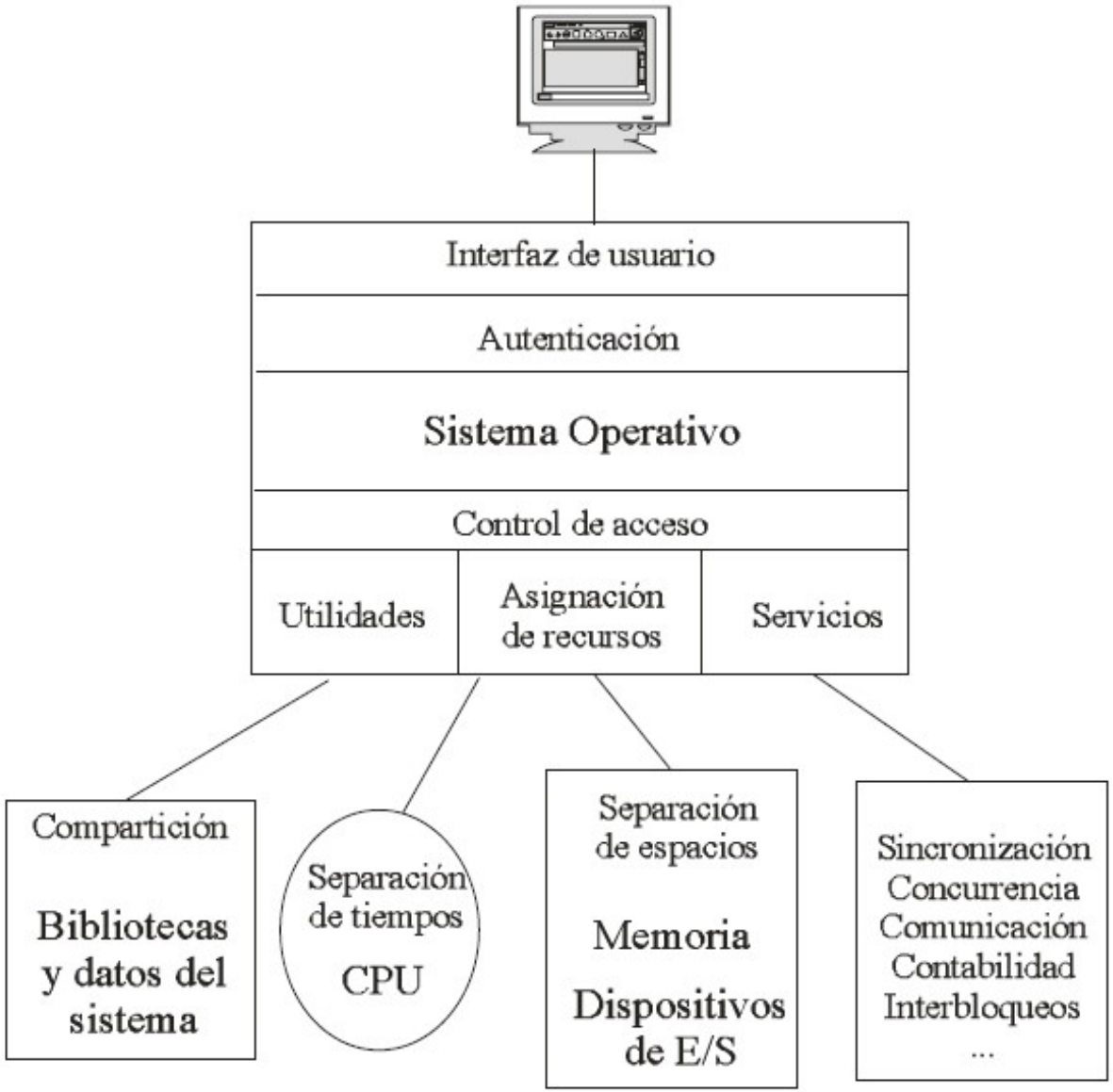
Principios de Seguridad

- Diseño abierto.
- Exigir permisos.
- Privilegio mínimos.
- Mecanismos económicos.
- Intermediación completa.
- Compartición mínima.
- Fáciles de usar y adaptar.
- Separación de privilegios.

Tareas de Seguridad

- Autenticación de recursos.
- Asignación de recursos.
- Control de acceso a los recursos.
- Control de comunicación y compartición entre procesos.
- Protección de datos.

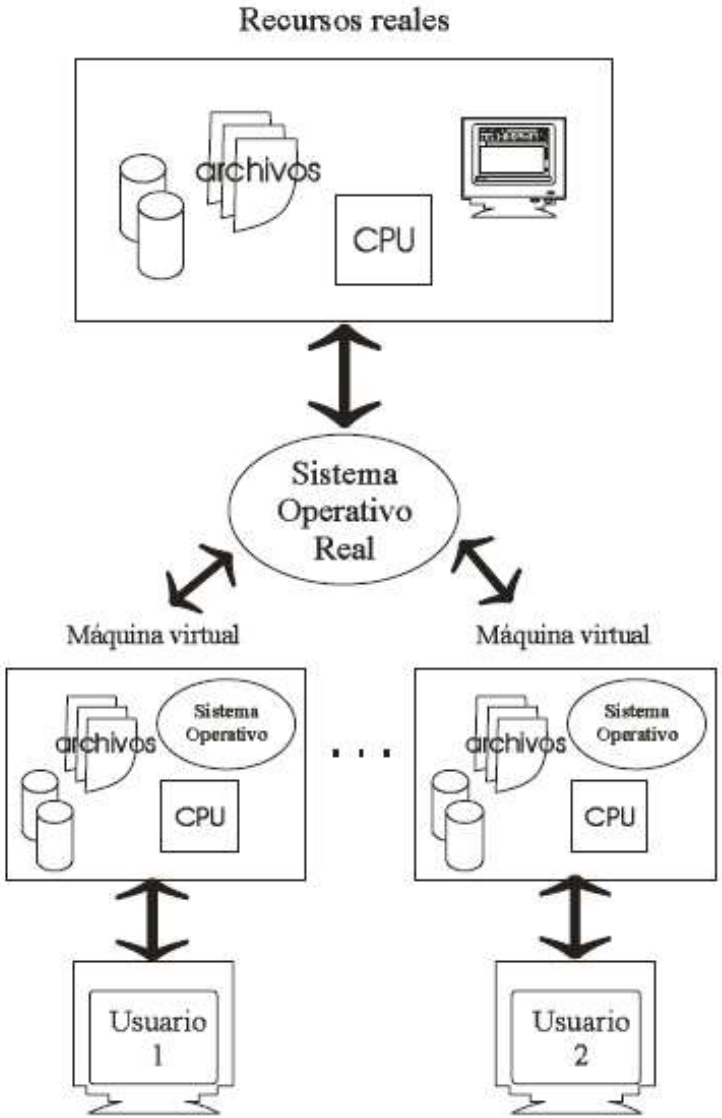
Tareas de Seguridad y componentes del S.O.



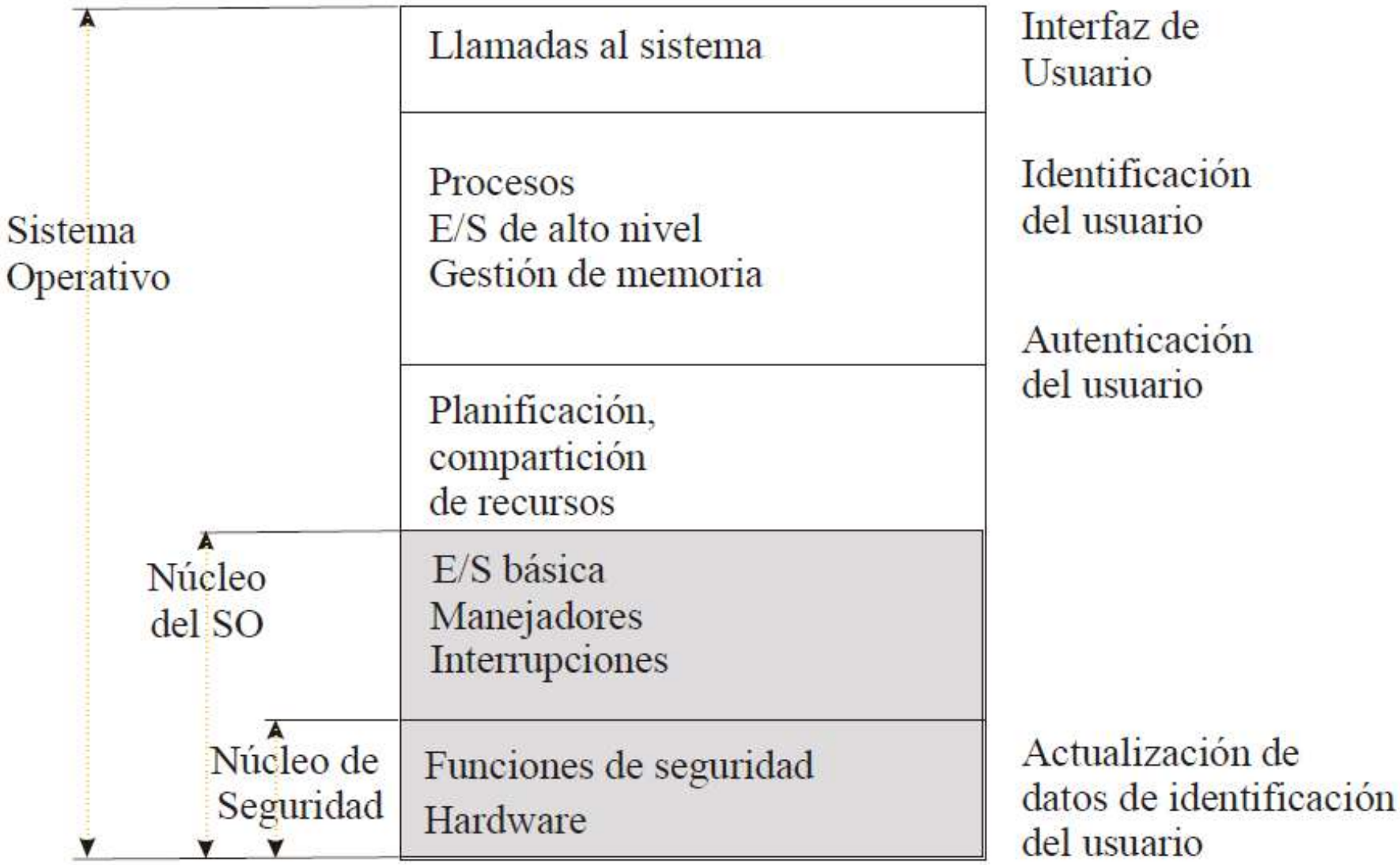
Técnicas de diseño de sistemas seguros

- Separación de recursos
  - Física
  - Temporal
  - Criptográfica
  - Lógica
- Uso de entornos virtuales
  - Espacios múltiples de memoria virtual
  - Máquinas virtuales
- Diseño por capas
  - Núcleos seguros
  - Monitores de seguridad
  - Capas de recubrimiento

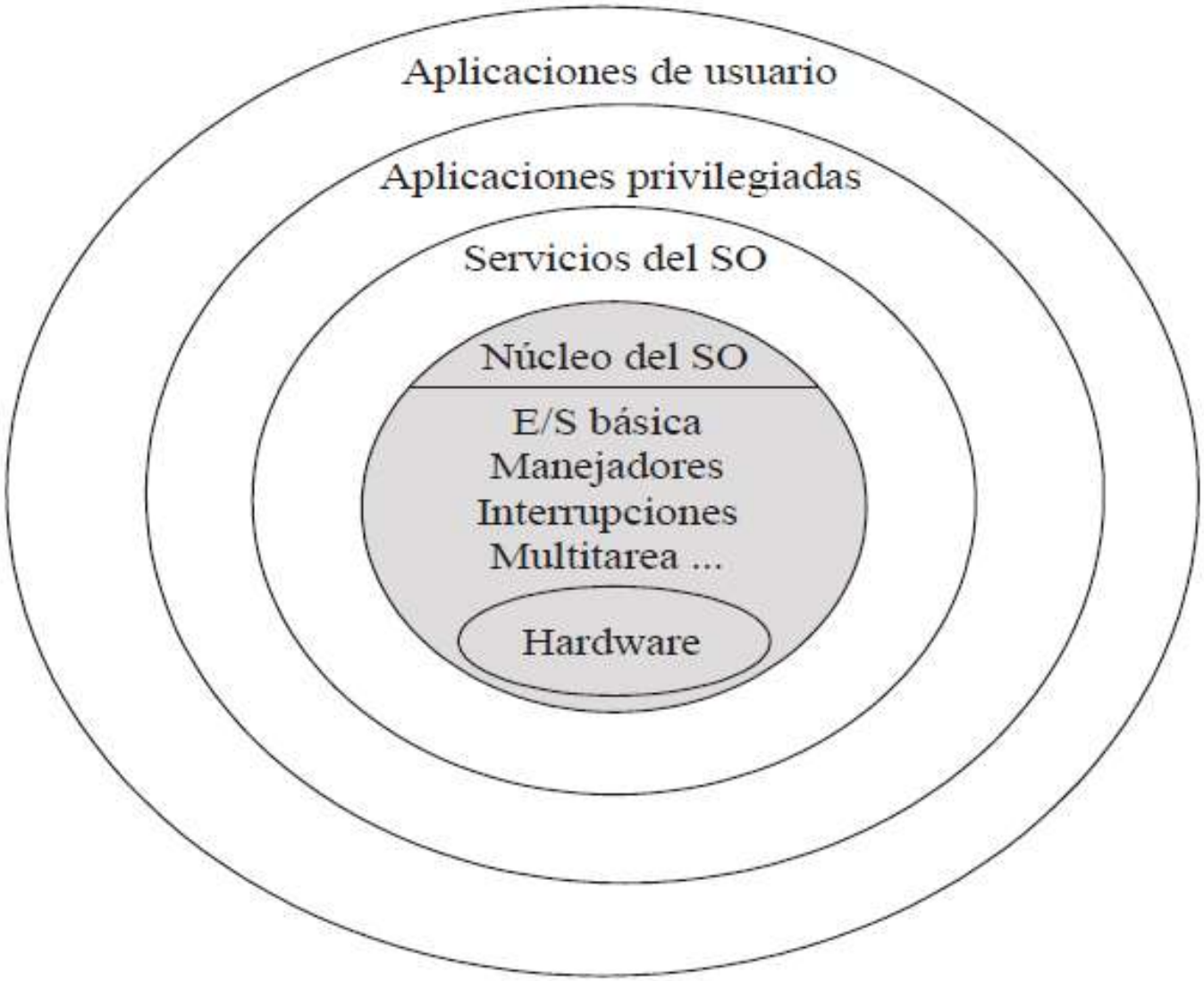
Maquinas Virtuales en MVS



Seguridad en capas de un S.O.



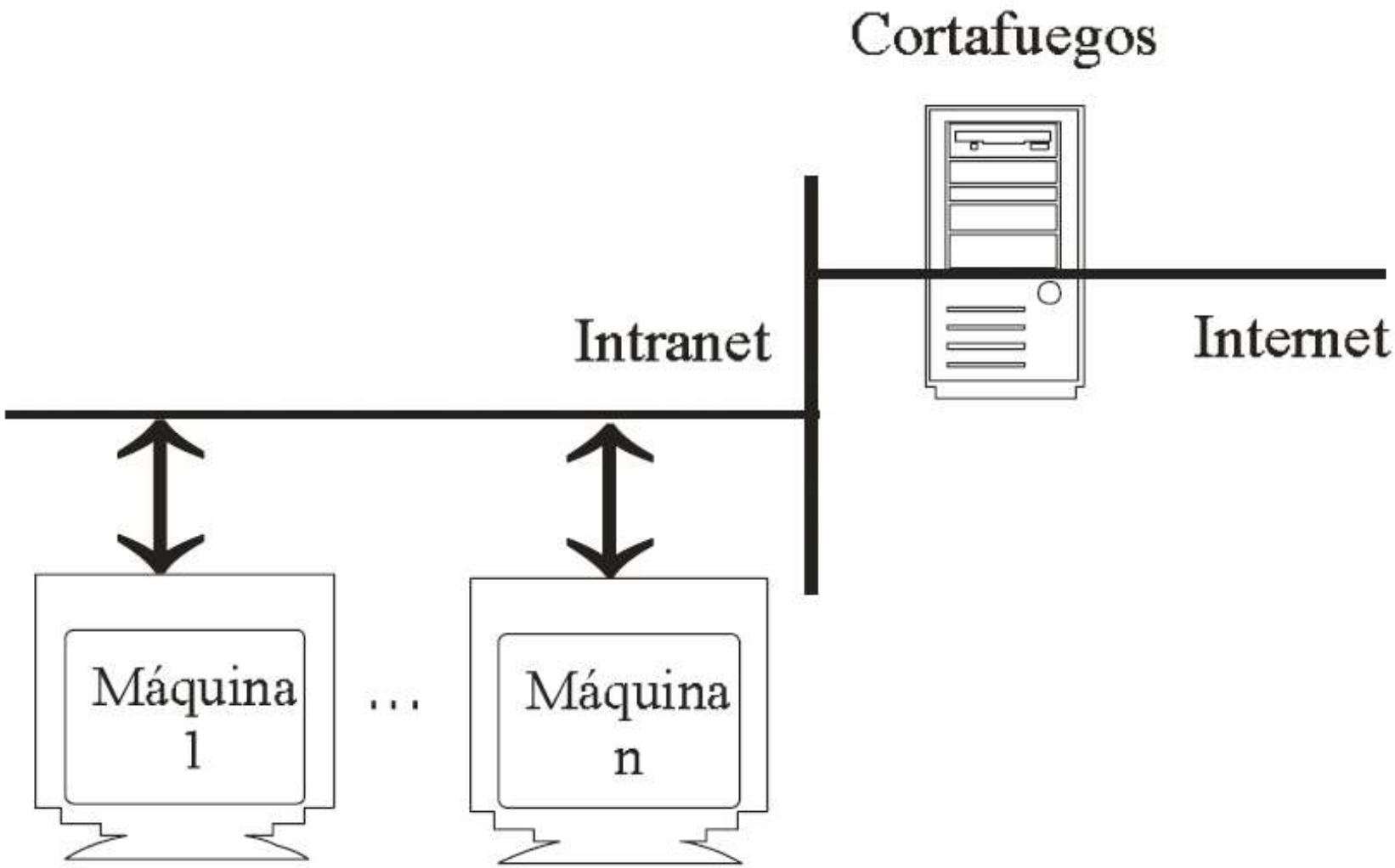
S.O. por núcleo Seguro



Controles Externos de Seguridad

- Equipos de penetración y limitación de acceso
  - Cortafuegos y redes internas
- Controles de programación
  - Diseño detallado y contrastado
  - Principio de aislamiento
  - Probadores independientes
  - Gestión de configuración
- Estándares para seguridad
  - DoD 2167A
  - SEE-CMM
  - ISO-9000

Seguridad con Cortafuegos (Firewalls)



Controles de Seguridad en el S.O.

- Ejecutar software fiable
  - No descargar de las redes software desconocido
- Sospechar de los procesos
  - Privilegios mínimos
- Ejecutar procesos con confinamiento
  - Máquinas aisladas si es necesario
- Registrar accesos
  - Activar los registros del sistema operativo
- Buscar periódicamente agujeros de seguridad
  - Estudiar los registros
  - Ver si hay flujos raros de información, ...

Criptografía

- La **criptografía** es la técnica que permite codificar un objeto de forma que su significado no sea obvio.

- Objeto original (O) se puede convertir en un objeto cifrado (C) aplicando una función de encriptado (E). Se descifra mediante otra función (D).

- Aspectos clave:
  - Algoritmos de cifra
  - Contraseñas

Cifrado y Descifrado

Algoritmo de Cifrado

- Procedimientos que permiten ocultar el contenido del objeto y ponerlo en su forma original, respectivamente.
- Sustitución: cambian un texto por otro
  - Monoalfabéticos
  - Polialfabéticos
- Transposición o permutación: reordenan el texto
  - Flujo caracteres
  - Bloques
- Actualmente: algoritmos exponenciales con claves muy largas
  - RSA
  - DES
  - Escrutinio de claves

Contraseñas

- La clave es el patrón que usan los algoritmos de cifrado y descifrado para manipular los mensajes en uno u otro sentido.
- Existen sistemas criptográficos que no usan clave.
- Sistemas de criptografía:
  - Simétricos
  - Asimétricos
- Ventajas de las contraseñas:
  - Algoritmos públicos
  - Es necesario conocer algoritmo y contraseña
  - Mismo algoritmo sirve con claves distintas
- Desventajas:
  - Propagación de claves -> algoritmos complejos
  - Debe resistir intentos de rotura

Claves Privadas y Publicas

- Claves privadas: conocidas sólo por cifrador y descifrador.
  - Ejemplo: DES.
  - Problema: propagación de claves.
- Claves públicas: la clave de cifrado es conocida, pero para descifrar hace falta otra que sólo tiene el descifrador.
  - Cualquiera puede enviar mensajes cifrados, pero sólo el destinatario legal puede descifrarlos.
  - No hay problema de propagación de claves
  - Ejemplo: RSA
- Firmas digitales: claves que identifican a un usuario o sistema de forma inequívoca.
  - Se aceptan a nivel legal
  - Hay autoridades que conceden firmas y certificados válidos.

Clasificaciones de Seguridad

- DoD.
  - Se basa en la política militar.
  - Mucho éxito.
  - Se usa para clasificar los sistemas operativos
- Criterio alemán
- Criterio canadiense
- ITSEC
- Criterio común.
  - Se ha estandarizado.
  - Es muy compleja y no tiene mucho éxito.

Niveles de Seguridad de DoD

A	Plan de seguridad acreditado	Ax	A1 + Desarrollo con instalaciones y personal fiables
		A1	B3 + Sistema de seguridad con verificación formal
B	Sistema de seguridad obligatorio	B3	B2 + ACL para denegar acceso + registro y auditoria de violaciones de seguridad
		B2	B1 + Protección obligatoria para todo recurso
		B1	C2 + Protección obligatoria para todo objeto de usuario
C	Capacidad discreccional de controlar Accesos	C2	C1 + Control de acceso individual
		C1	Control de acceso por dominio de seguridad
D	No existen medidas de seguridad		

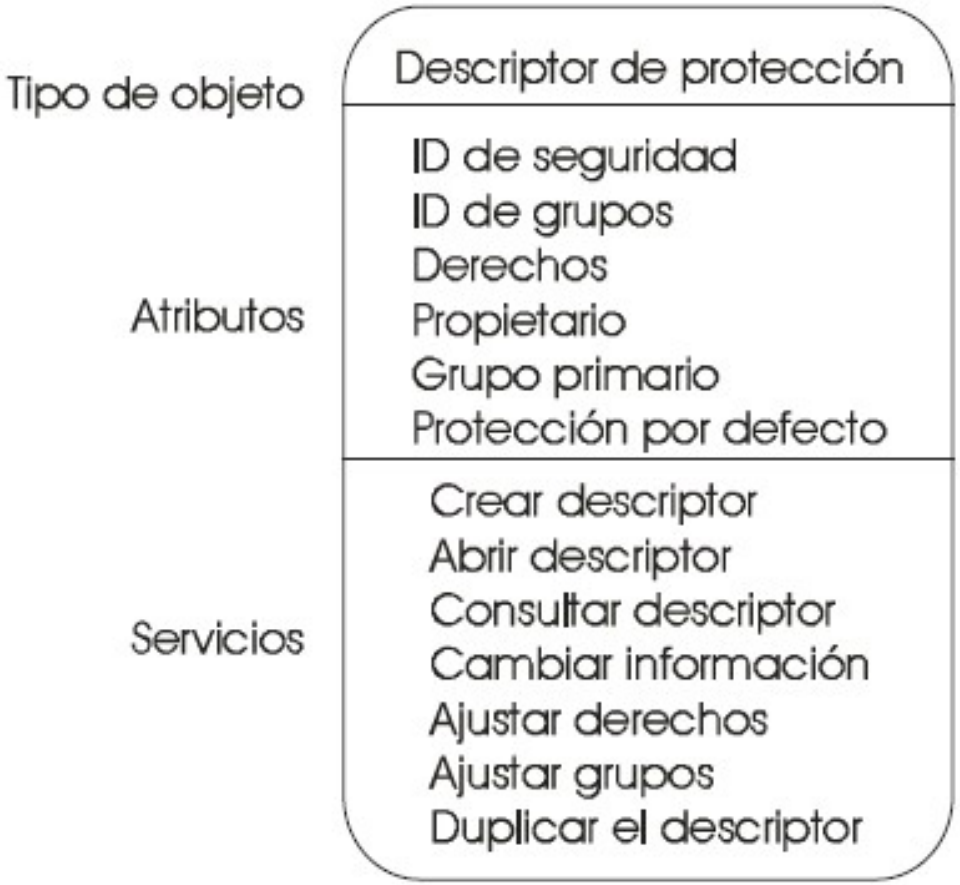
Protección

- Proteger del acceso inadecuado
- Distintos tipos de protección:
  - Lectura
  - Escritura
  - Ejecución
  - Eliminación
- Todos los sistemas operativos deben tener mecanismos de protección que permitan implementar distintas políticas de seguridad para los accesos al sistema.
- Compromiso seguridad-compartición

Autenticación de Usuarios

- Autenticación (¿quién?)
  - Claves (paswords)
  - Identificación física
    - Tarjetas inteligentes
    - Reconocimiento de voz
- Derechos de acceso (¿qué?)
  - Objeto => qué usuarios y qué derechos
  - Usuario => qué objetos y qué derechos
- Descriptor de seguridad por objeto que indica qué derechos de acceso tiene cada usuario a ese objeto

Descriptor de Seguridad en Windows



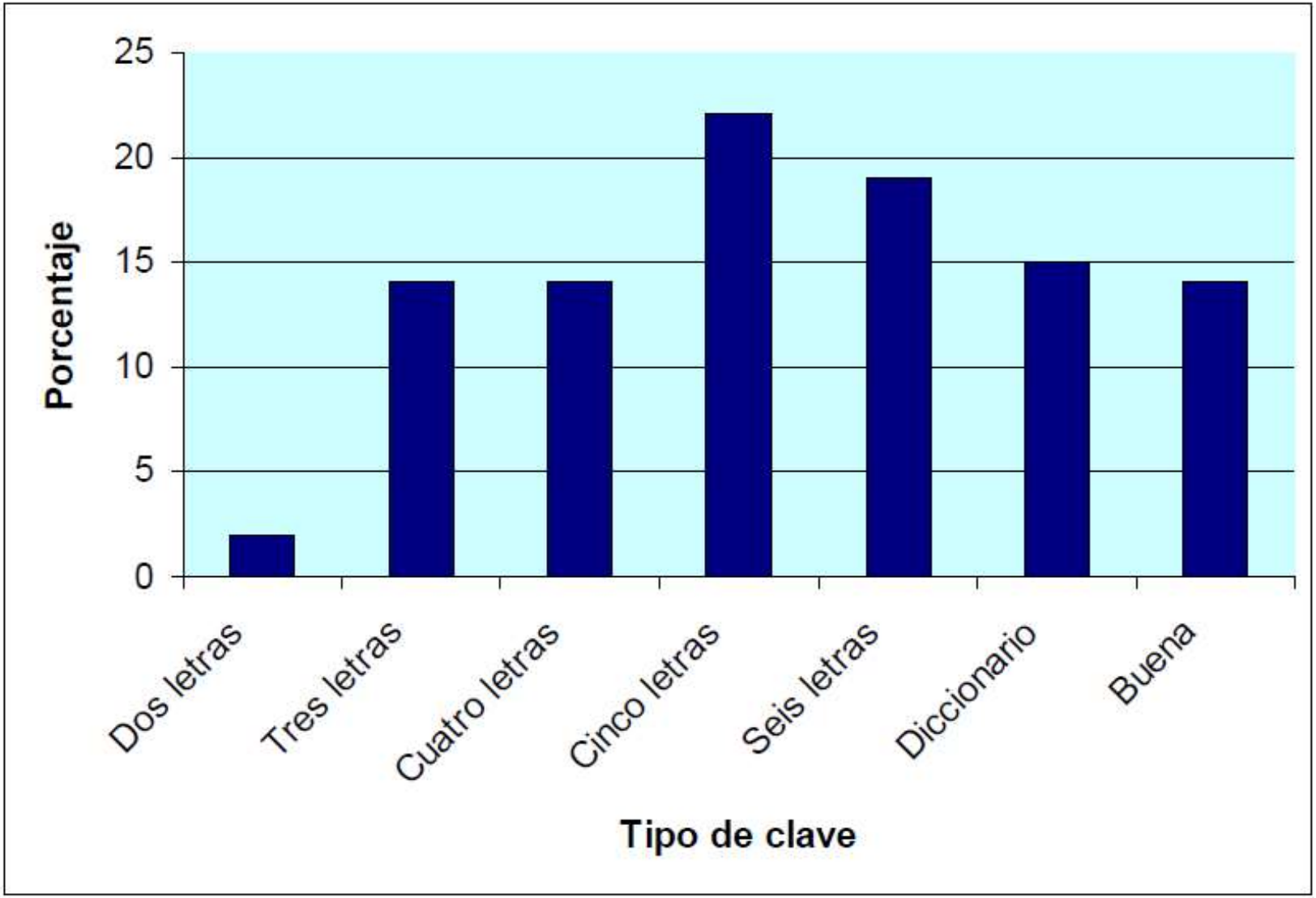
Proceso de Autenticación

- Cuando un usuario quiere acceder al sistema se le piden datos:
  - Identificación del usuario: nombre del usuario en el sistema.
  - Palabra clave o contraseña: espacio para teclear la clave (el eco muestra *).
  - Dominio de protección al que pertenece el usuario.
- Autenticación: comprobar que todos los datos son coherentes.
- Problemas:
  - Archivos de datos visibles (claves, usuarios, ...)
  - Proceso incompleto o por partes. Da pistas.
  - Suplantanción proceso de autenticación
- Principio básico: desconfianza

Contraseñas

- Una **contraseña** es un conjunto de caracteres alfanuméricos y especiales conocido únicamente por el usuario y por el sistema operativo sobre el que se ha llegado a un acuerdo para que sea usado como clave de acceso al sistema.
- La autenticación se basa en tuplas **<usuario, clave>**
- Decisiones:
  - ¿Quién asigna las palabras clave?
    - Administrador, usuario, ...
  - Longitud y formato de las palabras clave.
    - Longitud mínima, caracteres especiales, ...
  - ¿Dónde se almacenan las claves?
    - Archivos sombra
  - Duración de las claves.
    - Claves con caducidad

Distribución de claves



Dominios de Protección

- Dominio: un conjunto de pares (objeto, derechos), donde cada par especifica un objeto y las operaciones que se pueden ejecutar sobre el mismo.
- Identificación de usuarios y grupos
  - UID: identificador de usuario
  - GID: identificador de grupo
- Los procesos se ejecutan con
  - UID real
  - UID efectivo
  - GID real
  - GID efectivo

Protección en Unix

- Protección sobre un archivo
  - UID del propietario y GID del grupo
  - 9 bits de protección `rwx` para el propietario grupo y otros.

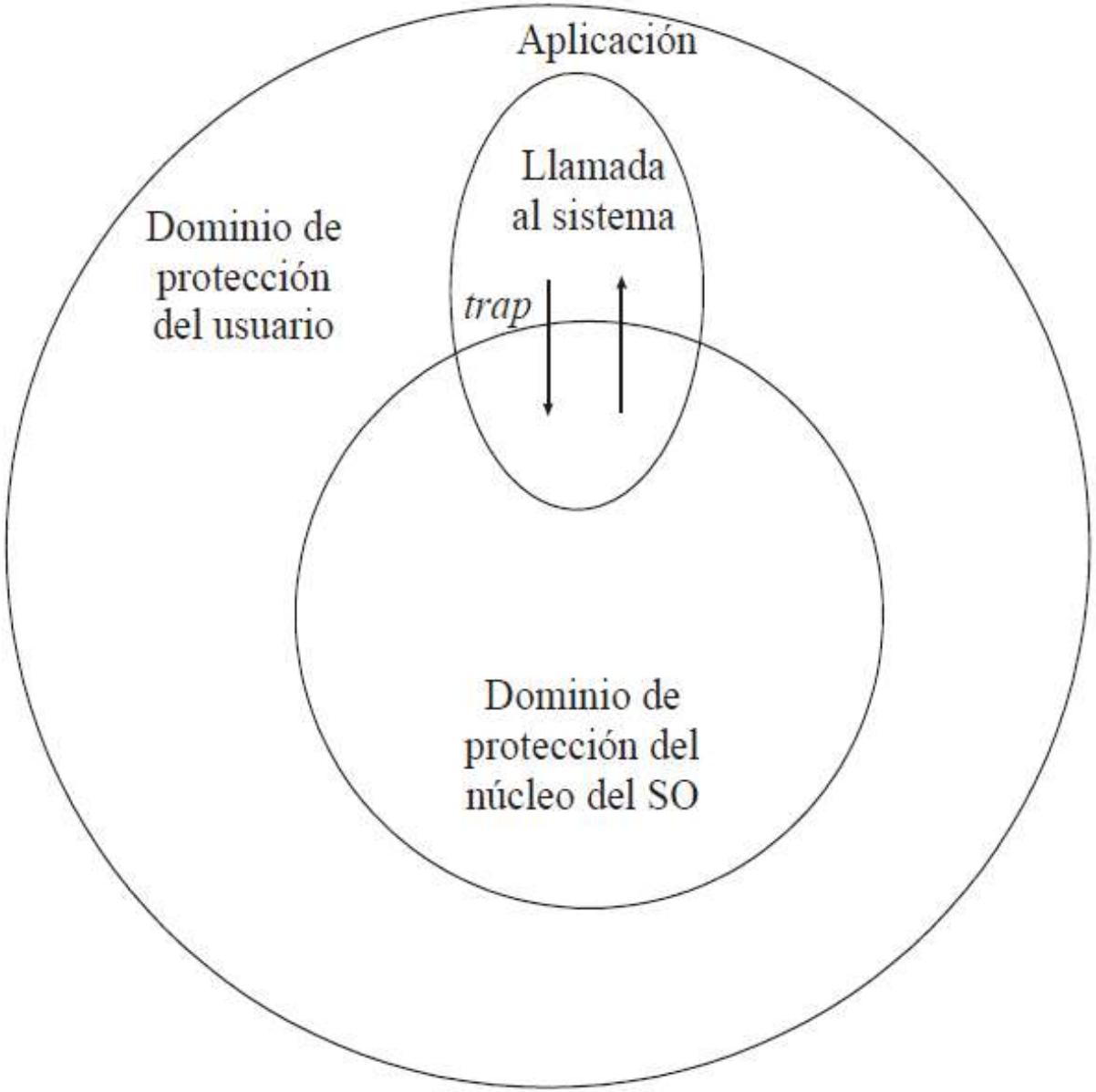
  - En archivos
    - `r` => leer
    - `w` => escribir
    - `x` => permiso de ejecución

  - En directorios
    - `r` => listar contenidos
    - `w` => crear o eliminar entradas
    - `x` => permiso de acceso

Protección en Unix

- Bits SETUID y GETUID
  - Si un proceso ejecuta un archivo con el SETUID activo UID efectivo = UID del propietario del archivo
  - Si un proceso ejecuta un archivo con el GETUID activo GID efectivo = GID del propietario del archivo
- Reglas de protección:
  - Si UID efectivo = 0 se concede el acceso
  - Si UID efectivo = UID del propietario se utiliza el primer grupo de bits; si no
  - Si GID efectivo = GID del propietario se utiliza el segundo grupos de bits; si no
  - Se utiliza el último grupo de bits.

Cambio de Dominio de Protección



Matriz de Protección

- Define la relación entre dominios y objetos del sistema.
- El elemento (i,j) indica las operaciones que el dominio i puede efectuar sobre el objeto j.
- Deriva del modelo HRU y es muy claro, pero hay problemas de implementación:
  - Puede ser muy grande y dispersa
  - Es una estructura estática -> número de dominios y objetos fijos -> ¿dimensionamiento?
- Soluciones:
  - Recorrerla por filas: capacidades
  - Recorrerla por columnas: listas de control de acceso (ACL)

Matriz de Protección: Ejemplo

Dominio \ Objeto	Fic_1	Fic_2	Modem	Printer	Dom_1	Dom_2
Dom_1	RWX	R	RW	W		Switch
Dom_2	R	R	RW			

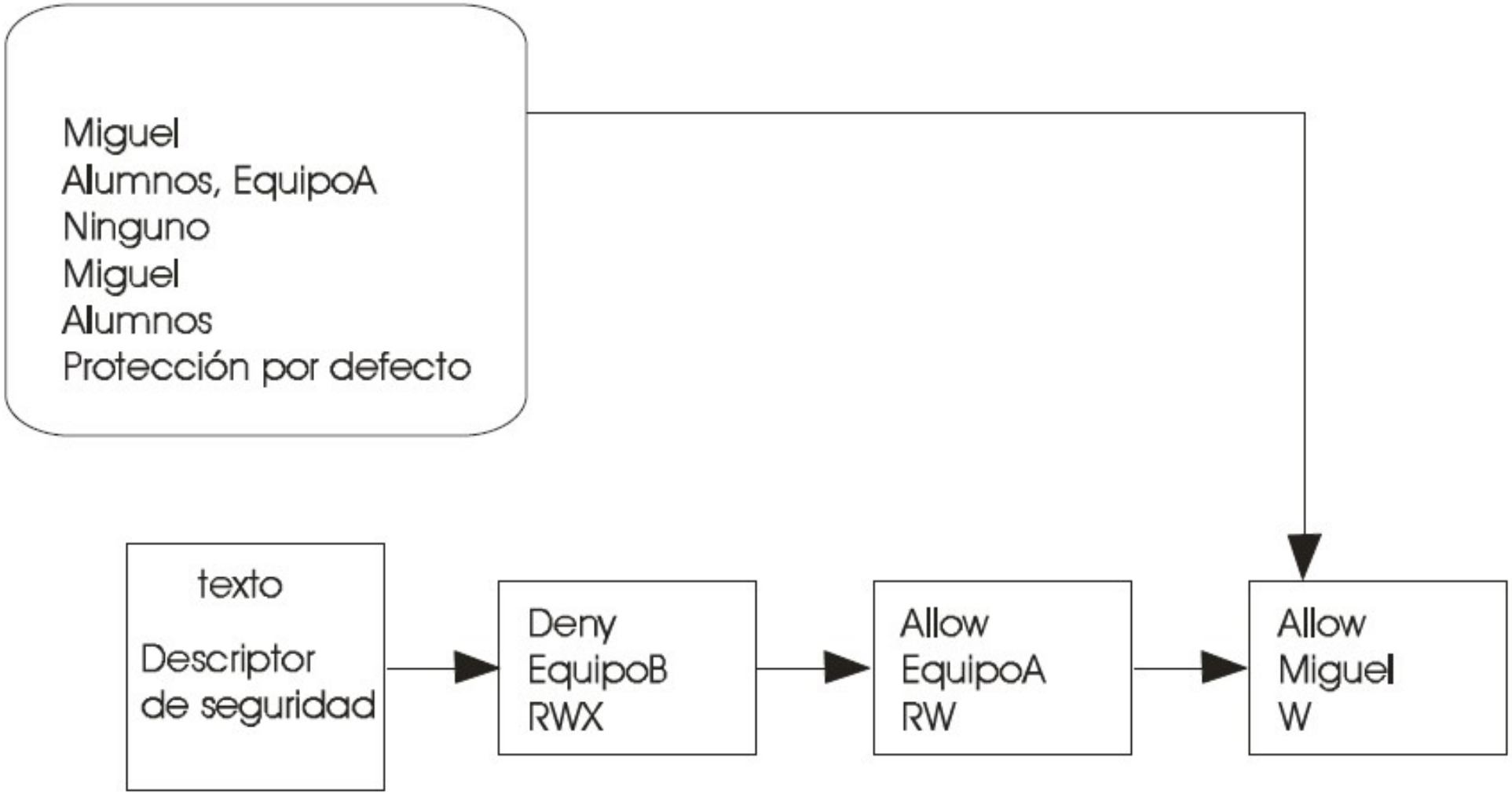
Listas de Control de Acceso (ACL)

- A cada objeto se le asigna una lista de pares (dominio, operación) que describe lo que el dominio puede hacer en el objeto. Ej.:

```
datos -> (juan,profesor,RW)(elvira,alumno,R)
```

- Concesiones y denegaciones de servicio
  - Denegaciones primero
  - Se puede especificar usuario y grupo.
- Son fáciles de crear y mantener.
- Están centralizadas con el objeto, lo que hace fácil revocar permisos.
- Pero no son buenas si el sistema es grande y está muy solicitado: las ACL se vuelven muy grandes y sus operaciones son lentas

ACL en Windows



Capacidades

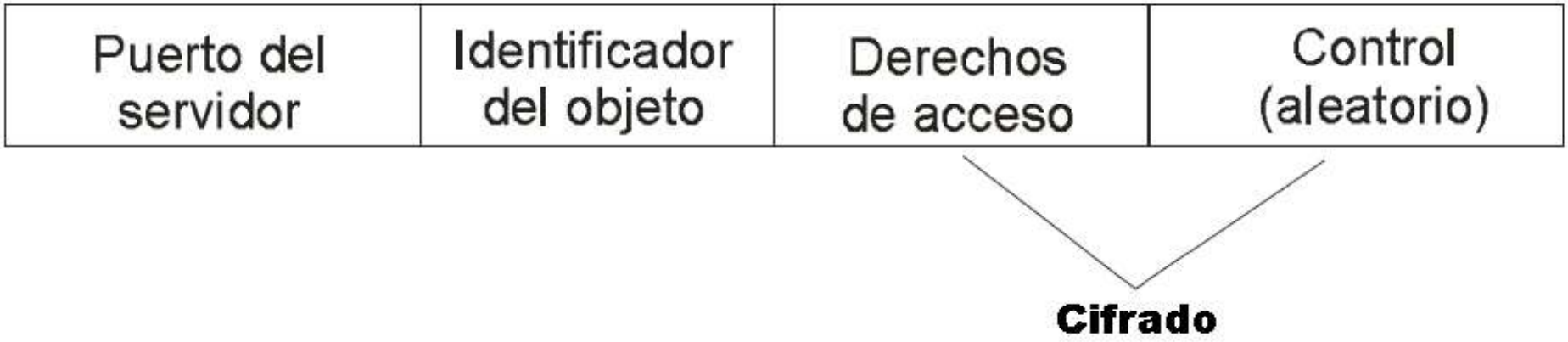
- Asocian a cada dominio un conjunto de descriptores que indiquen las operaciones que los componentes de ese dominio pueden efectuar sobre cada objeto del sistema. Ej.:

Cap-id	Tipo	Derechos	Objeto
0	archivo	rw-	datos

- Se piden explícitamente o se conceden para una sesión o conjunto de operaciones.
- Las posee su dueño, que las puede ceder a otros.
- Las listas de capacidades son capacidades.
- Problema: conceder derechos es fácil, pero revocarlos muy difícil si el sistema es grande.

Estructura de una Capacidad

Estructura de una capacidad en el sistema operativo distribuido Amoeba (Tanenbaum).



Las capacidades no se corresponden directamente con las necesidades de los usuarios y son menos intuitivas que las ACL.

Debido a ello, la mayoría de los sistemas operativos proporcionan ACL como mecanismo de protección.

Servicios Genéricos

- Crear descriptor de protección
- Abrir descriptor de protección
- Cerrar descriptor de protección
- Destruir descriptor de protección
- Obtener información de protección
- Definir información de protección
- Definir información de protección por defecto

Servicios POSIX

- POSIX ofrece servicios similares a los anteriores.
- Sin embargo, no existen servicios específicos para crear, destruir o abrir descriptores de protección.
- Los descriptores se asocian a los objetos y se crean y se destruyen con dichos objetos.
- Consultar ejemplo de uso.

Access – Comprueba la accesibilidad sobre un archivo

- Servicio:

```
#include <unistd.h>

int access(char *name, int amode);
```

- Argumentos:
  - `name` nombre del archivo
  - `amode` modo de acceso que se quiere comprobar. `amode` es el `OR` inclusivo de `R_OK`, `W_OK`, `X_OK` o `F_OK`.
- Devuelve:
  - 0 si el proceso tiene acceso al archivo (para lectura, escritura o ejecución) ó -1 en caso contrario
- Ejemplo:
  - `access("archivo", F_OK)` devuelve 0 si el archivo existe ó -1 si no existe.

chmod – Cambia los bits de permiso

- Servicio:

```
#include <sys/types.h>
#include <sys/stat.h>

int chmod(char *name, mode_t mode);
```

- Argumentos:
  - `name` nombre del archivo
  - `mode` nuevos bits de protección
- Devuelve:
  - Cero ó -1 si error.
- Descripción:
  - Modifica los bits de permiso y los bits SETUID y SETGID del archivo.
  - Sólo el propietario del archivo puede cambiar estos bits

chown – Cambia la propiedad de un archivo

- Servicio:

```
#include <sys/types.h>
#include <unistd.h>
int chown(char name, uid_t owner, gid_t group);
```

- Argumentos:
  - `name` nombre del archivo
  - `owner` nuevo propietario del archivo
  - `group` nuevo identificador de grupo del archivo
- Devuelve:
  - Cero ó -1 si error
- Descripción:
  - Modifica el identificador de usuario y de grupo del archivo
  - Los bits SETUID y SETGID son borrados

- Descripción:
  - Obtiene información sobre el identificador de un proceso o su grupo.

```
uid_t getuid  (void);
uid_t geteuid (void);
gid_t getgid  (void);
gid_t getegid (void);
```

  - Permiten cambiar el identificador de un proceso o de su grupo.

```
uid_t setuid  (uid_t uid);
gid_t setgid  (gid_t gid);
```

umask – Asigna la máscara de creación

- Servicio:

```
#include <sys/types.h>
#include <sys/stat.h>
mode_t umask(mode_t cmask);
```

- Argumentos:
  - `cmask` bits de permiso a desasignar en la creación de archivos.
- Devuelve:
  - Devuelve la máscara previa
- Descripción:
  - Asigna la máscara de creación de archivos del proceso que la invoca.
  - Los bits activos en la máscara son desactivados en la palabra de protección del archivo.
    - Si máscara =022 , y se crea un archivo con bits 0777 , los bits reales del archivo serán 0755 .

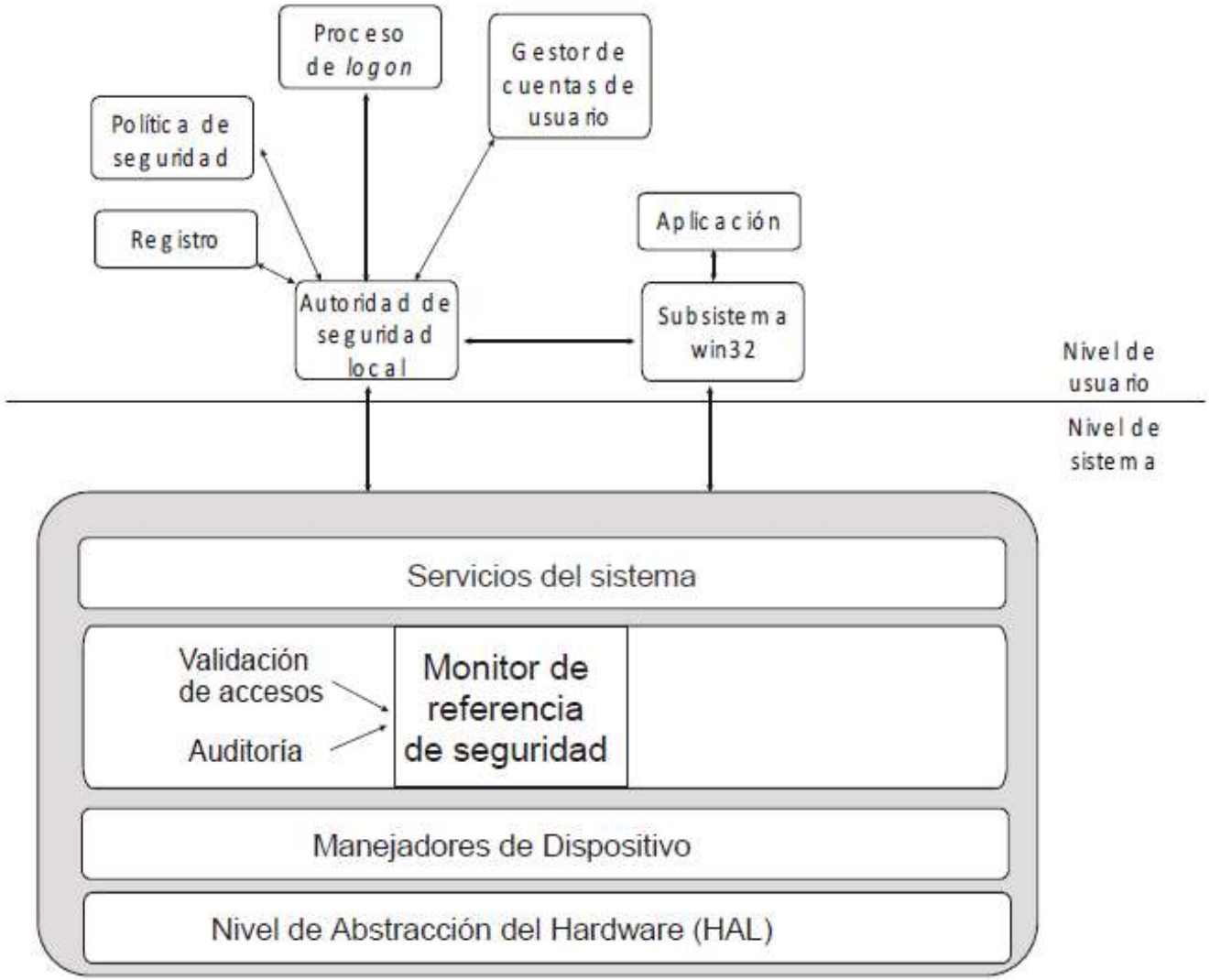
Servicios Windows

- Windows NT tiene un nivel de seguridad C2 según DoD.
- Existencia de control de acceso discrecional:
  - Posibilidad de permitir o denegar derechos de acceso para cualquier objeto partiendo de la identidad del usuario.
- Windows NT usa un descriptor de seguridad y listas de control de acceso (ACL), con entradas de control de acceso (ACE) para:
  - permisos y negaciones de accesos.
- Consultar ejemplo de uso.

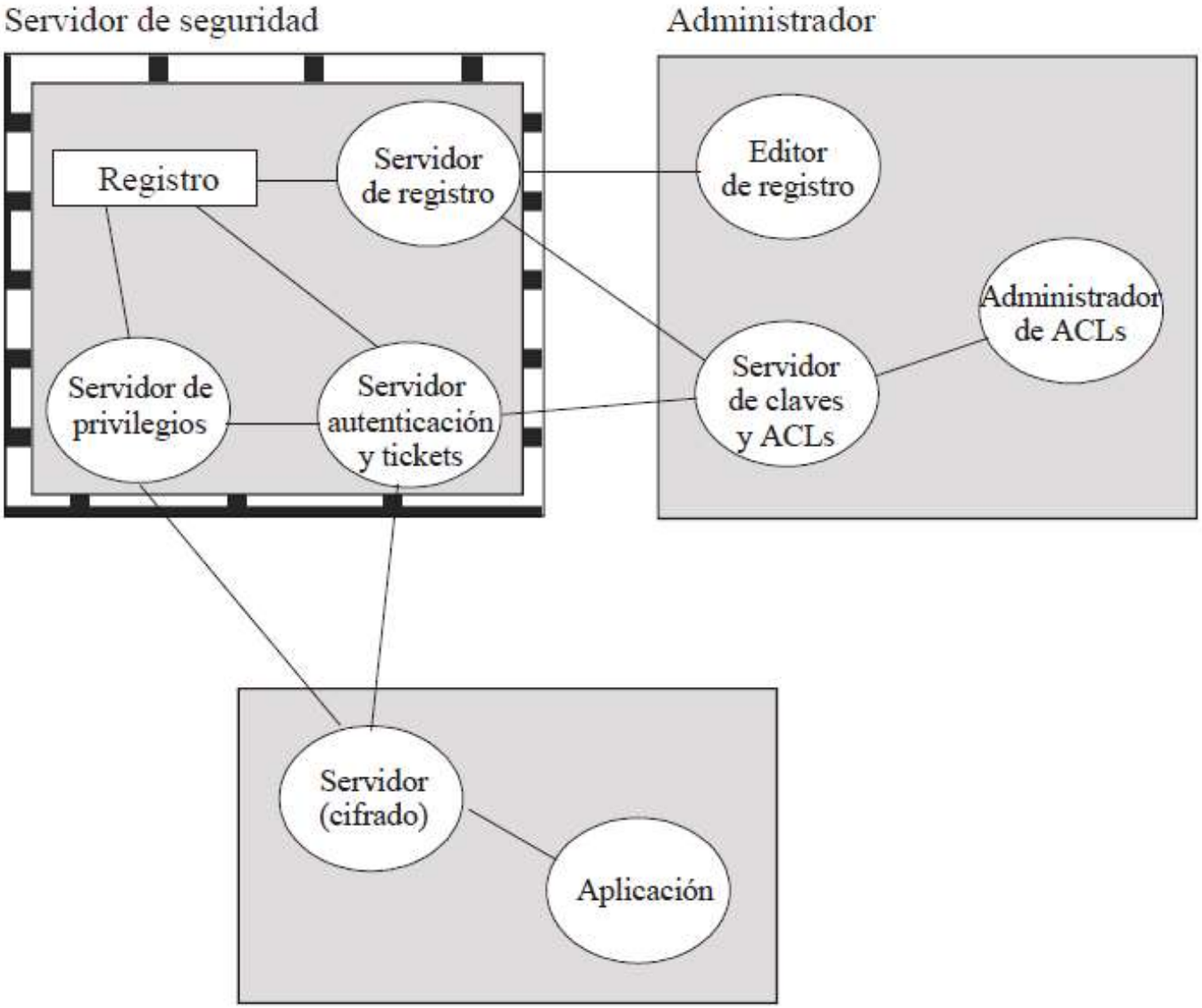
Subsistema de Seguridad

- *Subsistema de seguridad* específico Windows NT.
- • Procesos de *logon*, que muestran las ventanas de diálogo para que los usuarios puedan acceder al sistema, piden el identificador del usuario, su palabra clave y su dominio.
- • Autoridad de seguridad local, que controla que el usuario tenga permiso para acceder al sistema. Es el corazón del sistema porque gestiona la política local, los servicios de autenticación, política de auditoría y registro de eventos auditados.
- • Gestor de cuentas de usuario, que mantiene las base de datos de usuarios y grupos. Proporciona servicios de validación de usuarios.
- • Monitor de referencia de seguridad, que controla los accesos de los usuarios a los objetos para ver si tienen los permisos apropiados aplicando la política de seguridad y genera eventos para los registros de auditoría.

Estructura del Sistema de Seguridad



Estructura de Servidores: Kerberos



Kerberos: Intercambio de Ticketes