UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

AUDITORÍAS DE SISTEMAS OPERATIVOS Y BASES DE DATOS

AGENDA

- Conceptos generales
- Sistemas operativos
- Ejecución de Auditoria al sistema operativo
- Bases de datos
- Ejecución de Auditoria a las bases de datos
- Referencias

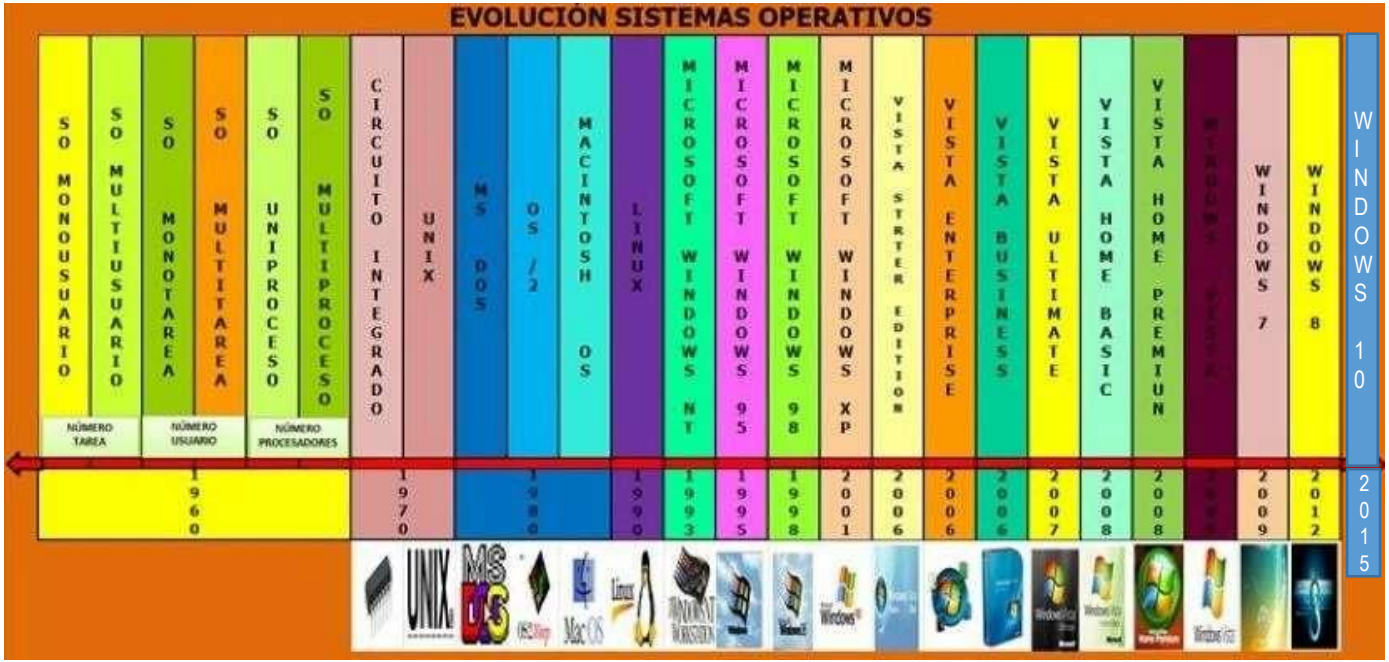
UNIVERSIDAD DE LIMA

60 años

CONCEPTOS GENERALES

Sistemas Operativos

Un **sistema operativo** (**SO** o, frecuentemente, **OS** —del inglés ***o****perating* ***s****ystem*—) es el software principal o conjunto de programas de un sistema informático, que **gestiona los recursos de hardware y provee servicios a los programas de aplicación de *software***, ejecutándose en modo privilegiado respecto de los restantes.



Gestión de los Sistemas Operativos

Gestión de procesos

Un proceso es simplemente, un programa en ejecución que necesita recursos para realizar su tarea: tiempo de CPU, memoria, archivos y dispositivos de E/S. El SO es el responsable de lo siguiente:

- ✓ Crear y destruir procesos.
- ✓ Parar y reanudar procesos.
- ✓ Ofrecer mecanismos para que los procesos puedan comunicarse y se sincronicen.

Gestión de la memoria principal

- ✓ Conocer qué partes de la memoria están siendo utilizadas y por quién.
- ✓ Decidir qué procesos se cargarán en memoria cuando haya espacio disponible.
- ✓ Asignar y reclamar espacio de memoria cuando sea necesario.

Gestión del almacenamiento secundario

- ✓ Planificar los discos.
- ✓ Gestionar el espacio libre.
- ✓ Asignar el almacenamiento.
- ✓ Verificar que los datos se guarden en orden.

Sistema de entrada y salida

Consiste en un sistema de almacenamiento temporal (caché), una interfaz de manejadores de dispositivos y otra para dispositivos concretos.

Sistema de archivos

- ✓ Construir, eliminar archivos y directorios.
- ✓ Ofrecer funciones para manipular archivos y directorios.
- ✓ Establecer la correspondencia entre archivos y unidades de almacenamiento.
- ✓ Realizar copias de seguridad de archivos.

Sistemas de protección

- ✓ Distinguir entre uso autorizado y no autorizado.
- ✓ Especificar los controles de seguridad a realizar.
- ✓ Forzar el uso de estos mecanismos de protección.

Sistema de comunicaciones

Para mantener las comunicaciones con otros sistemas es necesario poder controlar el envío y recepción de información a través de las interfaces de red.

Programas de sistema

- ✓ Manipulación y modificación de archivos.
- ✓ Información del estado del sistema.
- ✓ Soporte a lenguajes de programación.
- ✓ Comunicaciones.

Sistemas Operativos de Red

Un sistema operativo de red es aquel que mantiene a dos o más computadores unidos a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder **compartir los diferentes recursos y la información del sistema.**

En este entorno, cada computador mantiene su propio sistema operativo y su propio sistema de archivos local.

Figura. Representación esquemática de una red.

UNIVERSIDAD DE LIMA

60 años

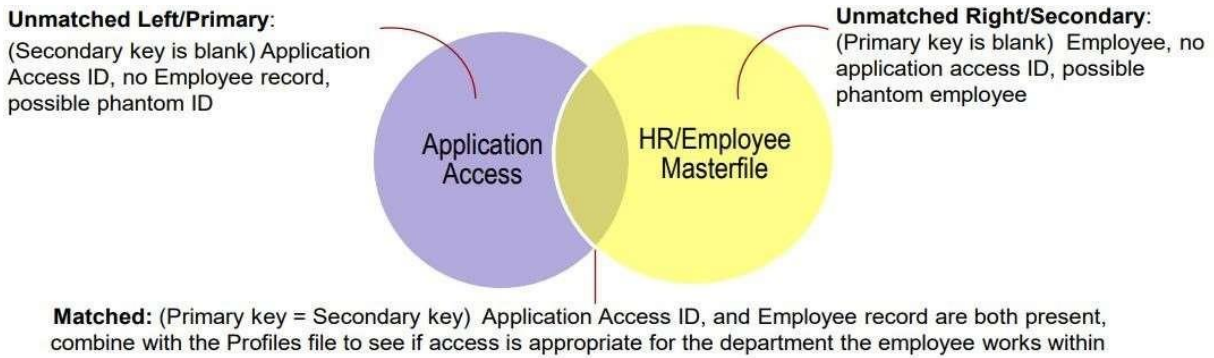
EJECUCIÓN DE AUDITORÍAS A LOS SISTEMAS OPERATIVOS

Alcance

- **Sistemas operativos de red**
  - Gestión de los usuarios: grupo de personas que tendrán posibilidad de acceder a los recursos de red.
    - ✓ Crear, borrar o modificar usuarios y grupos de usuarios.
    - ✓ Otorgar o quitar permisos de usuario a los recursos de la red controlados por el sistema operativo de red.
    - ✓ Asignar o denegar derechos de usuario en la red.
  - Políticas de contraseñas: ciclo de vida de la contraseña desde que se emite hasta que el usuario poseedor se le da de baja
  - Gestión de accesos: por lo general, se necesitan múltiples piezas de datos adicionales para aclarar **si empleados legítimos (Employee Master), con acceso (User Listing), tiene el acceso correcto (Roles / Derechos)**

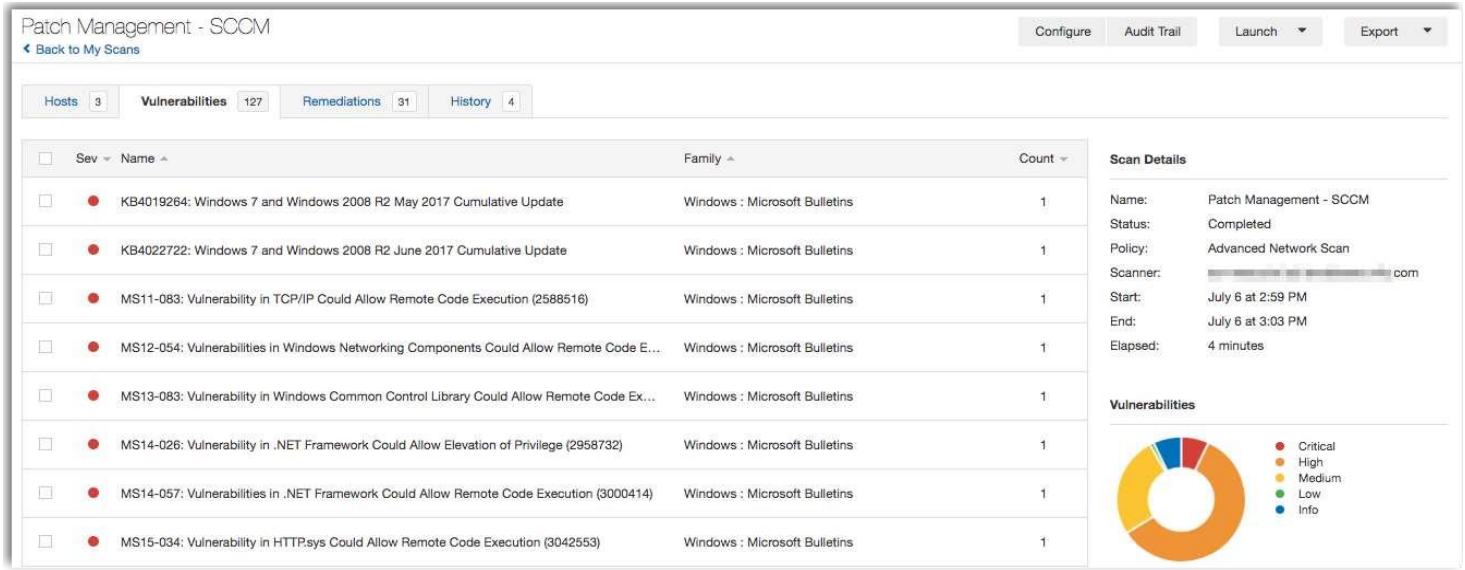
Alcance

- **Sistemas operativos de red**
  - Gestión de accesos: altas y bajas de usuarios; permisos razonables.
  - Segregación de funciones
    - ✓ Examinar a través de la tabla de roles para ver qué roles coexisten.
    - ✓ Correlacionar la roles y funciones versus la de conflictos para identificar las observaciones



Alcance

- **Sistemas operativos de red**
  - Gestión operativa de la red:
    - ✓ Aplicación de parches.



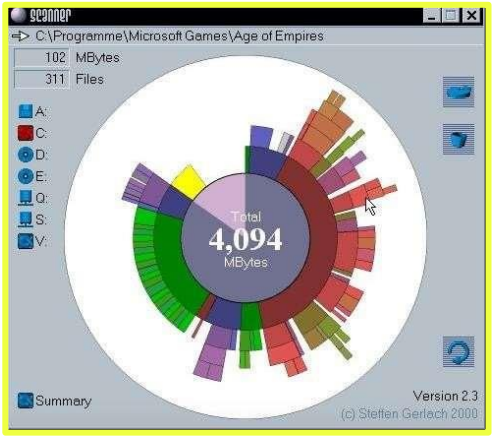
Alcance

- **Sistemas operativos de red**
  - Gestión operativa de la red: *Análisis del log de eventos*.
    - ✓ Nuevos eventos desde la última auditoria
    - ✓ Eventos perdidos
    - ✓ Clasificar eventos
    - ✓ Búsqueda por palabra clave
    - ✓ Correlacionarlos con tickets de Mesa de Ayuda
    - ✓ Correlacionarlos con la gestión de cambios.

Task_Category	Count	Percent of Count
Audit Policy Change	567	2.03%
Authentication Policy Change	7	0.03%
Event processing	1	0%
Logoff	1,585	5.67%
Logon	8,705	31.12%
Other System Events	5,360	19.16%
Security Group Management	43	0.15%
Security State Change	338	1.21%
Service shutdown	293	1.05%
Special Logon	5,323	19.03%
System Integrity	5,062	18.1%
User Account Management	684	2.45%
Totals	27,968	100%

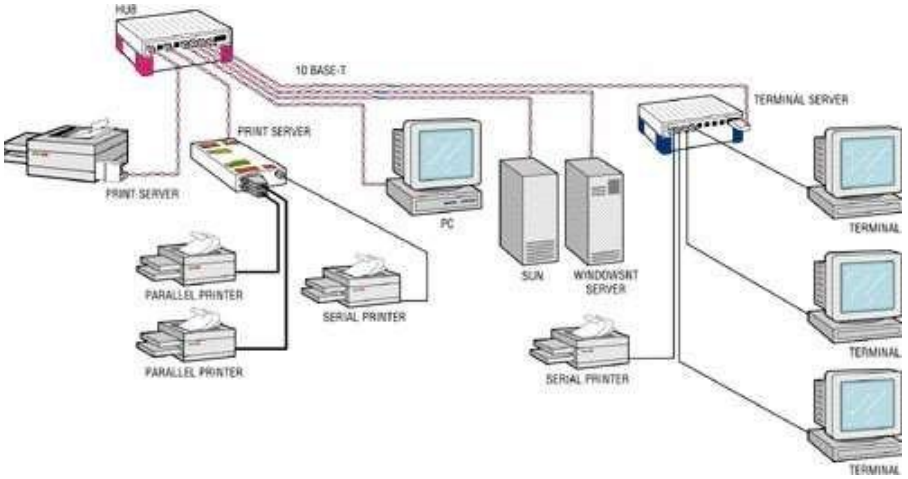
Alcance

- **Sistemas operativos de red**
  - Gestión operativa de la red:
    - ✓ Cambios en archivos críticos
    - ✓ Bloqueo de archivos y registros
      - ➢ Un mismo archivo o un registro de un archivo puede ser usado por más de un usuario y, por tanto, es necesario establecer un mecanismo para que dos usuarios no efectúen una modificación en el registro o en el archivo al mismo tiempo.
    - ✓ Distribución de espacio en discos duros



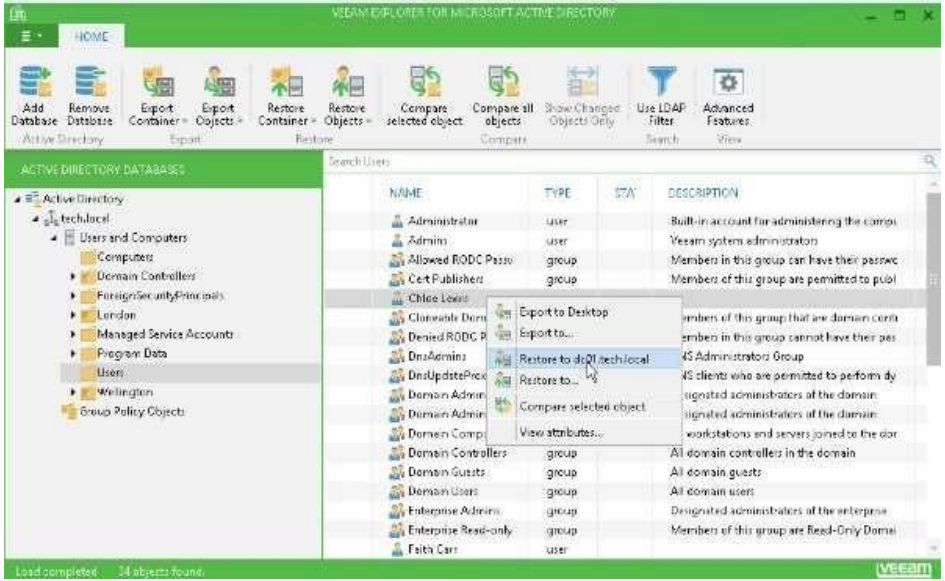
Alcance

- **Sistemas operativos de red**
  - Gestión operativa de la red: *Compartición de recursos*
    - ✓ Dentro de las ventajas de una red se encuentra la posibilidad de compartir los recursos que se encuentran en ella y, en especial, las impresoras.
    - ✓ El servidor de impresión y/o el servidor de archivos disponen de un programa que controla los trabajos de impresión mandados por los usuarios.



Alcance

- **Sistemas operativos de red**
  - Gestión operativa de la red: *Directorio activo*
    - ✓ Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.
    - ✓ De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.



EJERCICIO

Base de Datos

Un sistema gestor de bases de datos (SGBD) consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a dichos datos.

La colección de datos, normalmente denominada base de datos, contiene información relevante para una empresa.

El objetivo principal de un SGBD es proporcionar una forma de almacenar y recuperar la información de una base de datos de manera que sea tanto práctica como eficiente

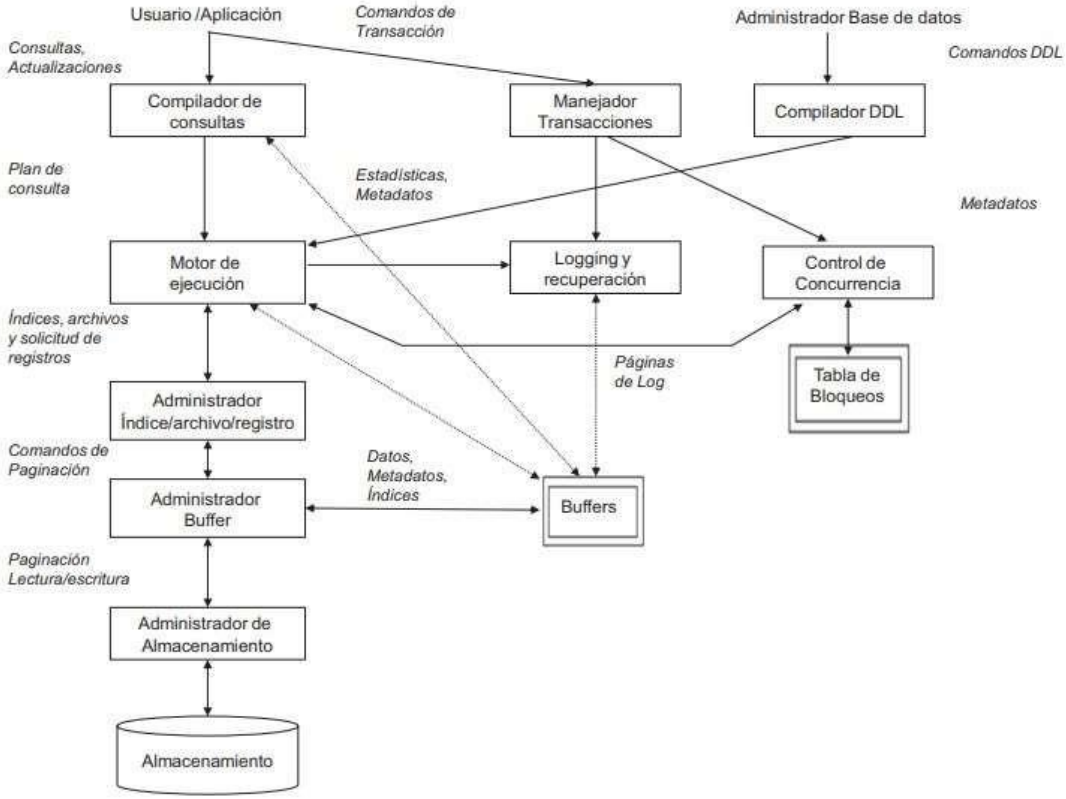


Figura 1.3 Componentes de un SGBD

UNIVERSIDAD DE LIMA

60 años

EJECUCIÓN DE AUDITORÍAS DE LAS BASES DE DATOS

Auditoria de Base de Datos

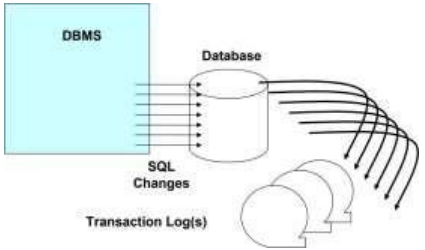
- Se define como el proceso de verificar y evaluar las bases de datos, su estructura y los objetos que contiene.
- Revisión y recuperación de todas las actividades que se hicieron en las bases de datos.

Alcance

- De Idoneidad:
  - ✓ Estructura física y lógica de la base de datos
- De Autorización:
  - ✓ "¿Quién puede hacer qué?”
- Auditoria de Acceso
  - ✓ "¿Quién hizo qué?
  - ✓ Modificaciones: INSERTAR, ACTUALIZAR, BORRAR
  - ✓ Lecturas: SELECCIONAR
  - ✓ Otro: DDL (CREAR / DESACTIVAR / ALTERAR), DCL (OTORGAMIENTO/ REVOCACIÓN),
  - ✓ Utilidades, errores de SQL, inicios de sesión fallidos, etc.
- Auditoria de replicación
  - ✓ ¿Quién copió qué datos y dónde?
- Auditoria de seguridad física
  - ¿Cómo se protege los servidores y otros que tienen almacenado la BD?

Métodos de Auditoría a Base de Datos

- Auditoría dentro del DBMS (trazas)
  - ✓ Debe iniciar el seguimiento de rendimiento
  - ✓ Overhead como registros de seguimiento son escritos por el DBMS
  - ✓ ¿Se requieren cambios de DDL a las tablas rastreadas?
- Auditoría con base a los archivos LOG
  - ✓ Las modificaciones están en el registro
- Auditoría a través de la red
  - ✓ Captura las solicitudes de SQL a medida que se envían a través de la red.
  - ✓ ¿Qué pasa con las solicitudes que no son de la red? (por ejemplo, CICS con DB2)
- Auditar directamente contra el servidor DBMS



¿Consultas?

UNIVERSIDAD DE LIMA

60 años

AUDITORÍAS DE SISTEMAS OPERATIVOS Y BASES DE DATOS