DAM / DAW Año 1

Lenguaje de marcas y sistemas de gestión de información

Temporalización

📘 Tema 1: Conceptos básicos y virtualización (3 sesiones)

Sesión 1 – Conceptos de sistema operativo, kernel, llamadas al sistema. Licencias de software.
Sesión 2 – Modelos de virtualización (bare-metal, hosted, contenedores). Herramientas: VirtualBox, VMware, Hyper-V, Docker.
Sesión 3 – Creación de una máquina virtual paso a paso. Configuración de red y recursos.

📘 Tema 2: Arranque e instalación de sistemas operativos (5 sesiones

Sesión 4 – BIOS vs UEFI. Bootloaders: GRUB, LILO, BOOTMGR. Tipos de arranque (legacy, seguro, múltiple).
Sesión 5 – Instalación de Windows paso a paso (creación de medios, configuración inicial, licencias).
Sesión 6 – Instalación de Linux (Ubuntu/Debian). Configuración de particiones e instalación de software adicional.
Sesión 7 – Dual Boot: instalación de dos SO en paralelo. Gestión con GRUB.
Sesión 8 – MBR, GPT y registro de arranque. Resolución de problemas de inicio.

📘 Tema 3: Administración de usuarios y grupos (3 sesiones)

Sesión 9 – Estrategias de organización: cuentas locales, de dominio y de equipo. Contraseñas y bloqueo.
Sesión 10 – Perfiles móviles, obligatorios y carpetas personales. Scripts de inicio de sesión.
Sesión 11 – OUs y grupos en Active Directory. Delegación de tareas y políticas.

📘 Tema 4: Gestión de sistemas de archivos y almacenamiento (5 sesiones)

Sesión 12 – Sistemas de archivos: NTFS, EXT4, ZFS. Estructura de directorios en Windows y Linux.
Sesión 13 – Particiones, volúmenes lógicos (LVM). Extensión de volúmenes.
Sesión 14 – RAID 0, 1, 5, 6: conceptos, ventajas y limitaciones. Implementación en Linux.
Sesión 15 – Estrategias de backup: completas, incrementales, diferenciales, híbridas. Herramientas (rsync, Veeam, Bacula).
Sesión 16 – Planes de recuperación ante desastres, copias en la nube, alta disponibilidad.

📘 Tema 5: Seguridad y auditoría en sistemas operativos (4 sesiones)

Sesión 17 – Principios de la seguridad informática (CIA: confidencialidad, integridad, disponibilidad). Normativas ISO 27001, RGPD.
Sesión 18 – Políticas de contraseñas, autenticación multifactor, protección contra malware.
Sesión 19 – Configuración segura de equipos y redes locales (firewalls, cifrado, segmentación).
Sesión 20 – Auditoría de procesos, logs, SIEM y planes de continuidad.

📘 Tema 6: Supervisión y rendimiento del sistema (3 sesiones)

Sesión 21 – Monitorización en tiempo real (htop, Task Manager, Nagios, Grafana).
Sesión 22 – Monitorización continuada y análisis de rendimiento: CPU, RAM, disco, red.
Sesión 23 – Registro y análisis de sucesos. Herramientas (Event Viewer, journalctl, Splunk).

📘 Tema 7: Resolución de incidencias y administración avanzada (2 sesiones)

Sesión 24 – Instalaciones desatendidas, ficheros de respuesta, WSUS y actualizaciones centralizadas.
Sesión 25 – Protocolos de actuación, administración remota (RDP, SSH, VNC), resolución telemática de incidencias.