Implantación de Sistemas Operativos (Ciclo ASIR)

Implantación de Sistemas Operativos do Ciclo ASIR

- **Curso:** 1º
- **Duración:** 213 horas
- **Profesorado:** Sistemas e Aplicacións Informáticas

Sumario

RA1. Instala sistemas operativos, logo de analizar as súas características e de interpretar a documentación técnica.

? CE1.1. Identifícáronse os elementos funcionais dun sistema informático.

- Estrutura dun sistema informático.

? CE1.2. Identifícáronse as características, as funcións e a arquitectura dun sistema operativo.
? CE1.3. Compáraronse sistemas operativos, así como as súas versións e as súas licenzas de uso, en función dos seus requisitos, das súas características e dos campos de aplicación.
? CE1.4. Instaláronse diferentes sistemas operativos.
? CE1.5. Prevíronse e aplicáronse técnicas de actualización e recuperación do sistema.
? CE1.6. Arranxáronse incidencias do sistema e do proceso de inicio.

- Actualización de sistemas operativos e aplicacións.
  - GNU/Linux

    - Configuración da rede. Comandos e ficheiros distribución GNU/Linux baseada en Debian
    - Actualizar o sistema. Instalar e desinstalar paquetes

- Recuperación do sistema
  - GNU/Linux

    - OBRIGADA LECTURA. ESCENARIO
    - Recuperación dun Sistema Operativo GNU/Linux mediante unha Xaula chroot

? CE1.7. Utilizáronse ferramentas para coñecer o software instalado no sistema e a súa orixe.
? CE1.8. Elaborouse documentación de soporte relativa ás instalacións efectuadas e ás incidencias detectadas.

◊ Licenzas e tipos de licenzas.
◊ Xestores de arranque.
◊ Consideracións previas á instalación de sistemas operativos libres e propietarios.
◊ Instalación de sistemas operativos: requisitos, versións e licenzas.
◊ Ficheiros de inicio de sistemas operativos.
◊ Rexistro do sistema.
◊ Tipos de aplicacións.
◊ Instalación e desinstalación de aplicacións: requisitos, versións e licenzas.
◊ Aplicacións de inventariado do software instalado nun sistema.
◊ Actualización e mantemento de controladores de dispositivos.

RA2. Configura o software de base, logo de analizar as necesidades de explotación do siste-ma informático.

? CE2.1. Planificáronse, creáronse e configuráronse contas de usuario, grupos, perfís e políti-cas de contrasinais locais.
? CE2.2. Asegurouse o acceso ao sistema mediante o uso de directivas de conta e directivas de contrasinais.
? CE2.3. Actuouse sobre os servizos e os procesos en función das necesidades do sistema.
? CE2.4. Instaláronse, configuráronse e verificáronse protocolos de rede.
? CE2.5. Analizáronse e configuráronse os métodos de resolución de nomes.
? CE2.6. Optimizouse o uso dos sistemas operativos para sistemas portátiles.
? CE2.7. Utilizáronse máquinas virtuais para realizar tarefas de configuración de sistemas operativos e analizar os seus resultados.
? CE2.8. Documentáronse as tarefas de configuración do software de base.

◊ Administración de usuarios e grupos locais.
◊ Usuarios e grupos predeterminados.
◊ Directivas de conta locais.
◊ Seguridade de contas de usuario.
◊ Seguridade de contrasinais.
◊ Administración de perfís locais de usuario.
◊ Configuración do protocolo TCP/IP en sistemas operativos cliente.
◊ Configuración da resolución de nomes.
◊ Ficheiros de configuración de rede. Configuracións múltiples. Configuracións de respaldo.
◊ Resolución de problemas de conectividade do sistema operativo.
◊ Optimización de sistemas para computadores portátiles.
◊ Acceso a ficheiros de rede sen conexión.
◊ Configuración das opcións de accesibilidade do sistema operativo.
◊ Máquinas virtuais.

RA3. Asegura a información do sistema utilizando copias de seguridade e sistemas tolerantes de fallos, e describe os procedementos.

? CE3.1. Comparáronse diversos sistemas de ficheiros e analizáronse as súas diferenzas e as súas vantaxes de implementación.
? CE3.2. Describiuse a estrutura de directorios do sistema operativo.
? CE3.3. Identificáronse os directorios contedores dos ficheiros de configuración do sistema (binarios, ordes e librarías).
? CE3.4. Utilizáronse ferramentas de administración de discos para crear particións, unidades lóxicas, volumes simples e volumes distribuídos.
? CE3.5. Implantáronse sistemas de almacenaxe redundante (RAID).
? CE3.6. Puxéronse en práctica e automatizáronse plans de copias de seguridade.
? CE3.7. Administráronse cotas de disco.
? CE3.8. Documentáronse as operacións realizadas e os métodos para a recuperación ante desastres.

◊ Sistemas de ficheiros. Características.
◊ Sistemas de ficheiros empregados na actualidade.
◊ Sistemas de ficheiros distribuidos, transaccionais, cifrados, comprimidos e virtuais.
◊ Xestión de sistemas de ficheiros mediante comandos e contornos gráficos.
◊ Xestión de enlaces.
◊ Estrutura de directorios de sistemas operativos libres e propietarios.
◊ Procura de información do sistema mediante comandos e ferramentas gráficas.
◊ Xestión da información do sistema: rendemento e estatísticas.
◊ Montaxe e desmontaxe de dispositivos en sistemas operativos: automatización.
◊ Ferramentas de administración de discos: particións e volumes; desfragmentación e recoñecemento.
◊ Extensión dun volume. Volumes distribuídos.
◊ Tolerancia a fallos de hardware.
◊ RAID0, RAID1 e RAID5 por software.
◊ Outros sistemas RAID. RAID aniñados.
◊ Sistemas NAS e SAN.
◊ Tolerancia dos datos a fallos de software.
◊ Tipos de copias de seguridade. Copias totais, incrementais, diferenciais e outras.
◊ Plans e programación de copias de seguridade.
◊ Recuperación en caso de fallo do sistema.

◊ Discos de arranque e discos de recuperación.
◊ Copias de seguridade do sistema. Recuperación do sistema mediante consola. Puntos de recuperación.
◊ Creación e recuperación de imaxes de servidores.
◊ Cotas de disco. Niveis de cota e niveis de advertencia.

RA4. Centraliza a información en servidores administrando estruturas de dominios, e analiza as súas vantaxes.

? CE4.1. Implementáronse dominios.
? CE4.2. Administráronse contas de usuario e contas de equipamento.
? CE4.3. Centralizouse a información persoal dos usuarios do dominio mediante o uso de per-fís móbiles e cartafoles persoais.
? CE4.4. Creáronse e administráronse grupos de seguridade.
? CE4.5. Creáronse patróns que faciliten a administración de usuarios con características si-milares.
? CE4.6. Organizáronse os obxectos do dominio para facilitar a súa administración.
? CE4.7. Utilizáronse máquinas virtuais para administrar dominios e verificar o seu funcio-namento.
? CE4.8. Documentouse a estrutura do dominio e as tarefas realizadas.

◊ Estrutura cliente servidor.
◊ Protocolo LDAP.
◊ Concepto de dominio. Subdominios. Requisitos necesarios para montar un dominio.
◊ Servidores de dominio. Estrutura e topoloxía. Xerarquía. Roles.
◊ Estacións e servidores membros dun dominio.
◊ Estratexias organizativas.
◊ Instalación dunha infraestrutura de dominio.
◊ Operacións sobre os servidores de dominio.
◊ Ferramentas gráficas e en liña de comandos para a administración de dominios.
◊ Distribución e replicación de dominios.
◊ Relacións de confianza entre dominios.
◊ Delegación das funcións de administración.
◊ Obxectos do dominio. Organización dos obxectos na estrutura do dominio.
◊ Tipos de contas. Contas de usuarios e equipamentos.
◊ Administración de contas. Contas predeterminadas.
◊ Contrasinais. Bloqueos de conta.
◊ Perfís móbiles e obrigatorios.
◊ Cartafoles persoais.
◊ Guións de inicio e peche de sesión.
◊ Patróns de usuario. Variables de contorno.
◊ Administración de grupos: tipos. Estratexias de aniñamento. Grupos predeterminados.

RA5. Administra o acceso a dominios respectando os requisitos de seguridade.

? CE5.1. Incorporáronselle equipamentos ao dominio.
? CE5.2. Prevíronse bloqueos de accesos non autorizados ao dominio.
? CE5.3. Administrouse o acceso a recursos locais e recursos de rede.
? CE5.4. Tivéronse en conta os requisitos de seguridade.
? CE5.5. Implementáronse e verificáronse directivas de grupo.
? CE5.6. Asignáronse directivas de grupo.
? CE5.7. Documentáronse as tarefas e as incidencias.

◊ Equipamentos do dominio.
◊ Permisos e dereitos.
◊ Administración do acceso a recursos. SAMBA. NFS.
◊ Permisos de rede. Permisos locais. Herdanza. Permisos efectivos.
◊ Delegación de permisos.
◊ Listas de control de acceso.
◊ Directivas de grupo. Creación, enlace e distribución.
◊ Directivas de seguridade. Dereitos de usuarios. Obxectos de directiva. Ámbito das directivas. Patróns.
◊ Tarefas de administración das directivas de grupo.
◊ Ferramentas de xestión das directivas de grupo.

RA6. Detecta problemas de rendemento monitorizando o sistema coas ferramentas adecua-das, e documenta o procedemento.

? CE6.1. Identificáronse os obxectos monitorizables nun sistema informático.
? CE6.2. Identificáronse os tipos de sucesos.
? CE6.3. Utilizáronse ferramentas de monitorización en tempo real.
? CE6.4. Monitorizouse o rendemento mediante rexistros de contador e de seguimento do sis-tema.
? CE6.5. Planificáronse e configuráronse alertas de rendemento.
? CE6.6. Interpretáronse os rexistros de rendemento almacenados.
? CE6.7. Analizouse o sistema mediante técnicas de simulación para mellorar o rendemento.
? CE6.8. Elaborouse documentación de soporte e de incidencias.

◊ Ferramentas de monitorización en tempo real e continuada.
◊ Ferramentas de análise do rendemento.
◊ Tipos de sucesos: do sistema, de seguridade, de aplicacións, etc.
◊ Rexistros de sucesos.
◊ Monitorización de sucesos.
◊ Xestión de aplicacións, servizos, procesos e subprocesos.
◊ Monitorización de aplicacións e procesos.
◊ Monitorización do sistema e do seu rendemento. Xeración de rexistros de funcionamento. Ferramentas de análise dos rexistros.

RA7. Audita o uso e o acceso a recursos, respectando as necesidades de seguridade do sistema.

? CE7.1. Administráronse dereitos de usuario e directivas de seguridade.
? CE7.2. Identificáronse os obxectos e os sucesos auditables.
? CE7.3. Elaborouse un plan de auditorías.
? CE7.4. Identificáronse as repercusións das auditorías no rendemento do sistema.
? CE7.5. Auditáronse sucesos correctos e erróneos.
? CE7.6. Auditáronse os intentos de acceso e os accesos a recursos do sistema.
? CE7.7. Xestionáronse os rexistros de auditoría.
? CE7.8. Documentouse o proceso de auditoría e os seus resultados.

◊ Requisitos de seguridade do sistema e dos datos.
◊ Obxectivos da auditoría.
◊ Ámbito da auditoría. Aspectos auditables.
◊ Mecanismos de auditoría. Alarmas e accións correctivas.
◊ Información do rexistro de auditoría.
◊ Técnicas e ferramentas de auditoría.
◊ Informes de auditoría.

RA8. Implanta software específico con estrutura cliente/servidor que dea resposta aos requi-sitos funcionais.

? CE8.1. Instalouse software específico segundo a documentación técnica.
? CE8.2. Realizáronse instalacións desatendidas.
? CE8.3. Configurouse e utilizouse un servidor de actualizacións.
? CE8.4. Planificáronse protocolos de actuación para resolver incidencias.
? CE8.5. Seguíronse os protocolos de actuación para resolver incidencias.
? CE8.6. Deuse asistencia técnica a través da rede, e documentáronse as incidencias.
? CE8.7. Elaboráronse guías visuais e manuais para instruír no uso de sistemas operativos ou aplicacións.
? CE8.8. Documentáronse as tarefas realizadas.

◊ Interpretación, análise e elaboración de documentación técnica.
◊ Interpretación, análise e elaboración de manuais de instalación e configuración de sistemas operativos e aplicacións.
◊ Licenzas de cliente e de servidor.
◊ Instalacións desatendidas.
◊ Implementación de ficheiros de respostas.
◊ Servidores de actualizacións automáticas.
◊ Partes de incidencias.

◊ Protocolos de actuación.
◊ Administración remota.