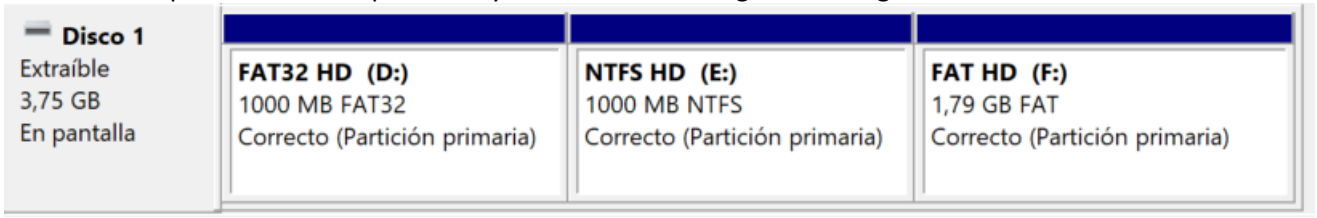
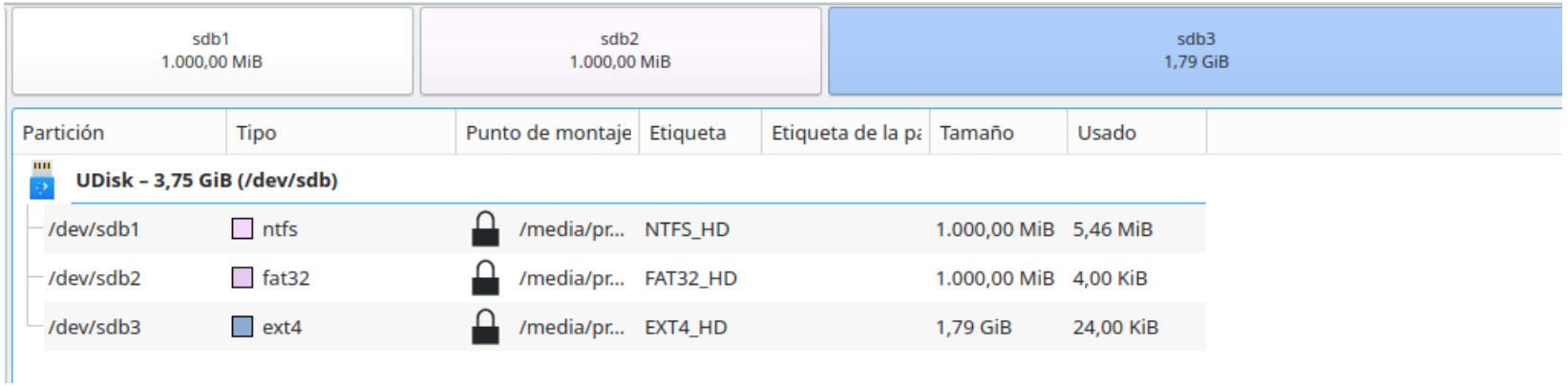
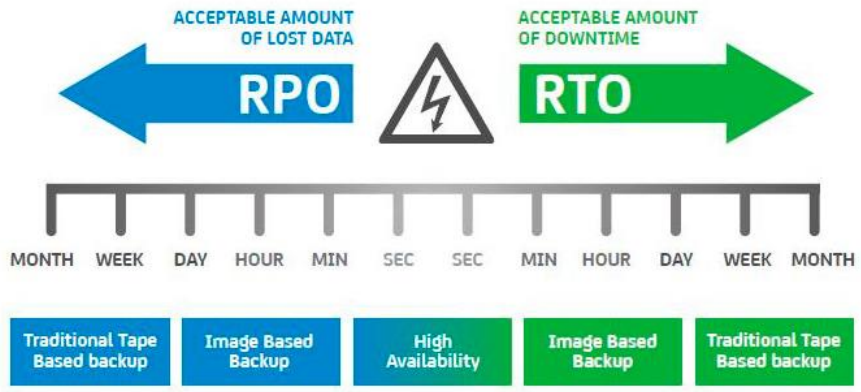
Planificación UF1466 - Sistemas de almacenamiento

Dr. Juan Pedro Cerro

Día 1	• Presentar esta unidad formativa sobre sistemas de almacenamiento repasando las ventajas e inconvenientes que presentan A NIVEL FÍSICO los diferentes sistemas de memoria secundaria: Cintas magnéticas, CD/DVD (ópticos), discos duros electro-mecánicos, memorias en estado sólido (flash), sistemas de almacenaje distribuido (NAS) (Usar la presentación "*10.- Sistemas de almacenamiento (Vol. físicos).pptx*") Comprobar algunos de estos medios en Internet viendo cómo algunos de ellos todavía se venden. • Explicar el concepto de volumen LÓGICO y los conceptos relacionados: MBR, GPT, Partición primaria, extendida y lógica. (Usar la presentación "*11.- Sistemas de almacenamiento (Vol. lógicos).pptx*") • Particionar el pendrive en tres partes tal y como muestra la siguiente imagen usan do el "Administrador de discos" en Windows:  • Crear un archivo en la partición NTFS y en FAT32 y ver como la ventana de propiedades del fichero no es la misma (Pestaña *Seguridad*). • Ahora en el Linux virtualizado eliminar todas las particiones del disco extraíble y crear una tabla de particiones GPT nueva usando la aplicación GParted. • Crear un sistema de particiones como el de la imagen inferior usando GParted:  • Abrir el pendrive en Windows y ver como la partición EXT4 no la lee el *Explorador de archivos*, pero sí que la muestra el *Administrador de discos*.

Día 2	• Formatear la unidad FAT32 del Pendrive a NTFS.
	• Usar la aplicación *Minitool Partition Wizard* para hacer lo que el resto de las herramientas no permite. (Usar los discos duros extraíbles de la escuela)
	• Explicar el sistema de acceso paralelo a disco RAID. (Usar la presentación "*12.- Sistemas RAID.pptx*")
	• Explicar los conceptos RPO y RTO:
	  ○ RPO (Recovery Point Objective): Es el punto hasta el cual una organización está dispuesta a aceptar la pérdida de datos en caso de un desastre o interrupción. En otras palabras, el RPO determina la frecuencia con la que se realizan copias de seguridad o se replican los datos. Por ejemplo, si el RPO de una empresa es de una hora y ocurre un desastre, la empresa puede perder hasta una hora de datos, dependiendo de cuándo se haya realizado la última copia de seguridad.
	  ○ RTO (Recovery Time Objective): Es el tiempo máximo que una organización está dispuesta a tolerar para recuperarse de un desastre o una interrupción y restaurar sus operaciones a un estado funcional. Esencialmente, el RTO establece el tiempo que una empresa puede estar sin acceso a sus sistemas o datos antes de que comiencen a sufrir consecuencias significativas. Por ejemplo, si el RTO de una empresa es de 4 horas, significa que la empresa debe ser capaz de restaurar sus sistemas y datos críticos dentro de las 4 horas posteriores a un incidente.
	 
	
	 
	
	• Explicar seguridad y protección de los datos usando la presentación "*13.- Seguridad de la información (Conceptos clave).pptx*".

<table>
<tr><td>Día 3</td><td>

Explicar los sistemas de protección de la información hasta la certificación digital usando la presentación “14.- Seguridad de la información (Sistemas de protección).pptx”.

PRÁCTICA 1:

Cifrar un archivo en Windows 10/11 (Home no incluido)
Luego usar un servicio para encriptar y desencriptar archivos https://ciberprotector.com/encriptar-desencriptar-ficheros-online/

PRÁCTICA 2:

Cambiar la extensión de los archivos como técnica para ocultar información sensible. (Ofuscación)

PRÁCTICA 3:

Usar la técnica de esteganografía (OPENSTEGO) para ocultar un texto (*.txt) dentro de una imagen.

PRÁCTICA 4:

Explicar brevemente las opciones más comunes del antivirus instalado en los equipos (AVAST).
Explorar ejemplos de phishing.

PRÁCTICA 5:

Abrir un PDF creado y explicar la Firma electrónica (escrita o dibujada)
Descargar el set de certificados de la DGP
Ir al administrador de certificados (certmgr) y explicar la estructura del almacén
Instalar el certificado_autenticación_activo.cer

</td></tr>
<tr><td>Día 4</td><td>

Abrir el Chrome y ver si el certificado está instalado en este navegador accediendo a la sede electrónica de la Seguridad Social y comprobar que no es posible acceder con el certificado .CER por ser la clave pública.
Intentar firmar digitalmente el PDF creado antes, ver como tampoco es posible.
Borrar el certificado .CER e instalar el .P12, tanto el activo como el revocado.
Ver en certmgr como está en la carpeta Personal
Autenticarase en la Sede Electrónica de la Seguridad Social con los dos certificados y ver cómo los mensajes son diferentes.
Firmar digitalmente el PDF con el certificado activo.
Ahora exportar un certificado .P12 sin la clave privada.

Abrir el navegador y acceder a la Sede Electrónica de la Seguridad Social parar ver cómo se usa.
Continuar con la presentación “14.- Seguridad de la información (Sistemas de protección).pptx” explicando el cifrado con clave asimétrica.

PRÁCTICA 6:

Instalar GnuPG (GNU Privacy Guard) para Windows (Gestor de llaves Kleopatra + Asistente GPA)
Crear un nuevo par de claves con Kleopatra
Ir a las propiedades del certificado. Pulsar sobre Editar para cambiar la contraseña o la fecha de caducidad.
En Kleopatra importar el certificado de la DGP y ver cómo se han añadido dos claves
Cifrar y descifrar un documento con el certificado GPG creado. También usando el botón derecho del ratón encima del icono (Shell)
Crear la firma de comprobación a través del Shell de un archivo de texto nuevo. Luego cambiar el contenido y volver a generar la firma de comprobación y verificar que no coinciden.

</td></tr>
</table>

	▪ Cifrar y descifrar también el Bloc de notas integrado. ▪ **Exportar** la clave pública del certificado generado con GPG usando **Kleopatra**. ▪ **Hacer una copia de seguridad** de la clave secreta de ese mismo certificado usando **Kleopatra**. ▪ **Eliminar** todos los certificados y crear un nuevo certificado con el par de claves, pero con otro nombre. ▪ **Importar** el que hemos exportado como si perteneciera a otra persona ya que sólo contiene la clave pública. Ver como en el GPA aparecen los dos, pero sólo uno muestra que tiene la clave secreta y pública. ▪ Intentar **descifrar el archivo** que antes ciframos con el certificado que tenía la clave secreta y que ahora ya no tenemos. Veremos como no es posible. ▪ A continuación, **instalar el certificado inicial usando la copia de seguridad**. Ver como en **Kleopatra** aparecen los dos certificados completos. ▪ **Descifrar** el archivo que ciframos inicialmente. • Empezar a realizar el **ejercicio de evaluación continua 1**.
Día 5	• Continuar el **ejercicio de evaluación continua 1**. • Continuar con la presentación "*14.- Seguridad de la información (Sistemas de protección).pptx*" realizar: o PRÁCTICA 7: ▪ Explicar la **Copia de Seguridad** del Panel de Configuración de Windows 11. ▪ Instalar y explicar COBIAN BACKUP 11 GRAVITY. • Explicar el control de acceso y la autenticación usando la presentación "*15.- Seguridad de la información (Control de acceso).pptx*". o PRÁCTICA 8: ▪ Crear un archivo e inspeccionar los permisos de acceso. Crear un usuario nuevo y asignarle permisos a ese objeto. o PRÁCTICA 9: ▪ Usar un servicio en línea (hipdf.com o ilovepdf.com) para proteger el acceso a un archivo PDF, bloqueándolo y después desbloqueándolo. o PRÁCTICA 10: Explicar el uso de un gestor de contraseñas y sus ventajas.
Día 6	• CIBERPROTECTOR: Darse de alta en https://dashboard.ciberprotector.com/ e instalar el plug-in de Google Chrome. • Explicar la diferencia en la organización de los archivos en Windows y en Linux (virtualizado anteriormente). • Presentar las propiedades genéricas de los archivos en Linux (en Windows ya fue tratado en la UF anterior): o Crear un archivo de texto en el escritorio desde la interfaz gráfica y añadirle algo de contenido. o Ir a la consola, dentro del escritorio y explicar la diferencia entre `DIR` y `LS`. Usar `LS -L` ▪ `-rw-r--r-- 1 usuario grupo 1024 Feb 10 12:30 archivo.txt` - archivo regular | l enlace simbólico | d directorio permisos del propietario, grupo y otros número de enlaces duros propietario y luego grupo al que pertenece tamaño, fecha de modificación y nombre o Usar el comando `CP` para copiar archivos y el `CD` para movernos. o Comandos `MKDIR` y `RMDIR` o Crear un enlace simbólico al archivo creado llamado "enlace" (desde consola sería `LN -S fichero enlace`)

	○ Explicar la diferencia entre un enlace simbólico y un enlace duro ○ Crear un enlace duro mediante el comando `LN fichero enlace` • Hacer una introducción a las **redes de computadores** con la presentación "*16.- Redes de computadores para BBDD*" explicando los orígenes y su evolución • Explicar las características de una red por medio su arquitectura. Usar la presentación "*17.- Arquitectura de redes de computadores*".
Día 7	• Continuar con la presentación "*17.- Arquitectura de redes de computadores*". • Darse de alta en Cisco Packet Tracer e instalar el programa. • Explicar el funcionamiento básico de Packer Tracer usado como guía el documento "*18.- Guia packet tracer*". • Explicar el modelo OSI y el protocolo TCP/IP usando la presentación "*19.- El modelo de capas OSI y el protocolo TCP-IP.pptx*". • Realizar el **ejercicio de evaluación continua 2**.
Día 8	• Continuar con el **ejercicio de evaluación continua 2**. • Explicar el direccionamiento lógico por IP usando la presentación "*20.- Direccionamiento IP*". • Explicar cómo configurar una red IP usando la presentación "*21.- Configuración y enrutamiento IP*". • Explicar el funcionamiento de un router conectando con Cisco Packet Tracer dos redes. •
Día 9	• Explicar los conceptos MTU, MSS y ARP usando la presentación "*22.- MTU_MSS_ARP*" y también la guía "*22b.- Simulaciones MTU_ARP*". • Explicar los conceptos VLAN e ICMP usando la presentación "*23.- VLAN_ICMP*" y también la guía "*23b.- Simulaciones VLAN_ICMP*" • Hacer el "**24.- Ejercicio de repaso**" • Revisar los documentos relativos a **legislación** publicados en el espacio compartido. • Comenzar a explicar PYTHON…
Día 10	PYTHON…
Día 11	• REPASO GLOBAL DEL MÓDULO FORMATIVO
Día 12	• EXAMEN FINAL DE MÓDULO