Temas que entran para el examen del día 24

Índice

[Tema 5 – Aplicaciones de criptografía 4](#_Toc93777559)

[Firma digital o firma electrónica: 4](#_Toc93777560)

[Firma digital con árbitro: 4](#_Toc93777561)

[Firma digital ordinaria: 4](#_Toc93777562)

[Clases de firma digital: 4](#_Toc93777563)

[ Firma electrónica: 4](#_Toc93777564)

[ Firma electrónica avanzada: 4](#_Toc93777565)

[ Firma electrónica reconocida: 4](#_Toc93777566)

[ Firma electrónica avanzada reconocida: 4](#_Toc93777567)

[Tema 6 – Software Malicioso 5](#_Toc93777568)

[Utiliza dos vulnerabilidades: 5](#_Toc93777569)

[ Vulnerabilidades del software: 5](#_Toc93777570)

[ Vulnerabilidades asociadas a las personas: 5](#_Toc93777571)

[CLASIFICACIÓN DEL MALWARE 5](#_Toc93777572)

[Según su forma de propagación: 5](#_Toc93777573)

[ Virus 5](#_Toc93777574)

[ Gusanos 5](#_Toc93777575)

[ Troyanos 5](#_Toc93777576)

[Hay dos tipos de conexiones: 6](#_Toc93777577)

[ Conexión directa: 6](#_Toc93777578)

[ Conexión inversa: 6](#_Toc93777579)

[Los más Habituales son: 6](#_Toc93777580)

[Backdoor: 6](#_Toc93777581)

[Keylogger: 6](#_Toc93777582)

[Downloader: 6](#_Toc93777583)

[Proxy: 6](#_Toc93777584)

[Software malicioso no dañino: 6](#_Toc93777585)

[Spyware: 6](#_Toc93777586)

[Adware: 6](#_Toc93777587)

[Hijacking: 6](#_Toc93777588)

[Jokes: 6](#_Toc93777589)

[Bulos: 6](#_Toc93777590)

[Software malicioso DAÑINO 6](#_Toc93777591)

[Ransomware: 6](#_Toc93777592)

[Rogueware: 6](#_Toc93777593)

[Password stealer: 6](#_Toc93777594)

[Bombas lógicas: 6](#_Toc93777595)

[Denegación de servicio o DOS: 6](#_Toc93777596)

[Ataques de denegación de servicio: 6](#_Toc93777597)

[Ingeniería social. Fraudes informáticos 7](#_Toc93777598)

[ Suplantación de la identidad: 7](#_Toc93777599)

[ Cadenas de correos: 7](#_Toc93777600)

[ Correos millonarios: 7](#_Toc93777601)

[Tema 7 – Medidas de protección contra el malware 8](#_Toc93777602)

[Medidas preventivas contra el malware: 8](#_Toc93777603)

[ Suites de seguridad (preventiva y paliativa): 8](#_Toc93777604)

[Combaten el malware de dos maneras: 8](#_Toc93777605)

[Las técnicas que utilizan son: 8](#_Toc93777606)

[ Comparación con firmas: 8](#_Toc93777607)

[ Métodos heurísticos: 8](#_Toc93777608)

[ Cortafuegos: 8](#_Toc93777609)

[Iptables 9](#_Toc93777610)

[Medidas paliativas contra el malware: 9](#_Toc93777611)

[Copias de seguridad 9](#_Toc93777612)

[ Copias de seguridad del sistema: 9](#_Toc93777613)

[ Copias de seguridad de datos: 9](#_Toc93777614)

[ Software congelador: 9](#_Toc93777615)

[Centros de protección y respuesta frente a amenazas: 9](#_Toc93777616)

[ Preventivos 9](#_Toc93777617)

[ Reactivos 9](#_Toc93777618)

[Buenas prácticas para protegerse del malware: 10](#_Toc93777619)

[Tema 8 - Gestión del Almacenamiento 11](#_Toc93777620)

[Seguridad física 11](#_Toc93777621)

[Seguridad lógica 11](#_Toc93777622)

[Políticas de almacenamiento 11](#_Toc93777623)

[Dispositivos de almacenamiento 11](#_Toc93777624)

[Clasificación: 11](#_Toc93777625)

[Otra clasificación: 11](#_Toc93777626)

[Dispositivos locales/internos: 11](#_Toc93777627)

[Dispositivos externos: 11](#_Toc93777628)

[Tecnologías de almacenamiento redundante y distribuido 12](#_Toc93777629)

[RAID 0: 12](#_Toc93777630)

[RAID 1: 12](#_Toc93777631)

[RAID 5: 12](#_Toc93777632)

[RAID 10: 12](#_Toc93777633)

[Copias de seguridad 12](#_Toc93777634)

[Clases de copias de seguridad: 13](#_Toc93777635)

[ Normales o completas: 13](#_Toc93777636)

[ Diferenciales: 13](#_Toc93777637)

[ Incrementales: 13](#_Toc93777638)

[Realización de copias de seguridad: 13](#_Toc93777639)

[Parte práctica tema 8 – Debian 14](#_Toc93777640)

[Parte práctica tema 8 – Windows 15](#_Toc93777641)

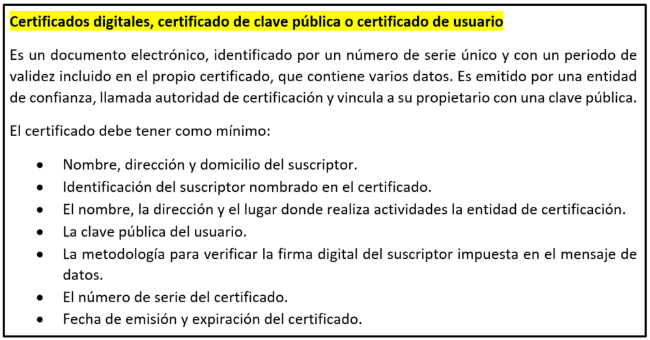
# Tema 5 – Aplicaciones de criptografía

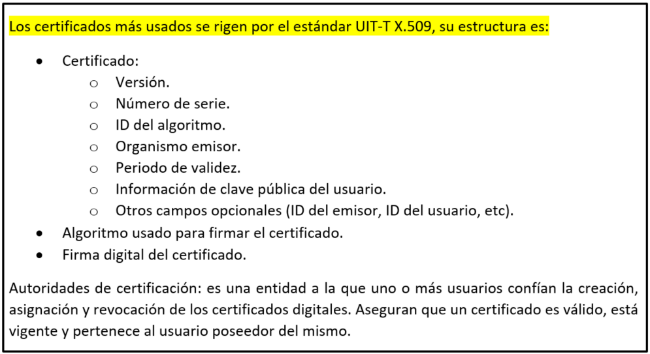
Firma digital o firma electrónica: la firma se encarga de uno de los principios de la seguridad informática, la autenticación, es decir, verifica que el mensaje recibido es exactamente igual al original y que proviene del mismo emisor.

Firma digital con árbitro: se utiliza en sistemas de clave simétrica. Se escoge a una tercera persona para que compruebe la veracidad tanto del mensaje como del emisor.

Firma digital ordinaria: se basa en funciones hash y cifrado público. El emisor aplica una función hash sobre el documento a firmar, cifra el resultado con su clave privada y adjunta la firma digital en el documento que se va a enviar.

## Clases de firma digital:

* Firma electrónica: conjunto de datos de forma electrónica que se utilizan para identificar al firmante.
* Firma electrónica avanzada: permite identificar al firmante, verificar que el contenido del mensaje no se ha modificado, que está vinculada al firmante de manera única y a los datos que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
* Firma electrónica reconocida: se basa en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma, como el DNI electrónico.
* Firma electrónica avanzada reconocida: se genera un hash del archivo y dicho hash se cifra con la propia clave privada. Para verificar la autenticidad del archivo y del emisor, el receptor descifra, con la clave pública del emisor, el hash del archivo enviado.



# Tema 6 – Software Malicioso

Malware: Malicious software

El software malicioso puede modificar el funcionamiento de un equipo informático o alterar la información que procesa, ya sea borrándola, modificándola o enviándola sin nuestro conocimiento a terceras personas.

## Utiliza dos vulnerabilidades:

* Vulnerabilidades del software: explota debilidades del sistema operativo o de algún programa. Algunos se pueden copiarse a sí mismos y enviarse automáticamente a través de la red.
* Vulnerabilidades asociadas a las personas: desde el desconocimiento o del exceso de confianza de los usuarios, contribuyen a la propagación del software malicioso

## CLASIFICACIÓN DEL MALWARE

Según el impacto producido sobre la víctima: hay 3 niveles de peligrosidad, bajo, medio, elevado. Para evaluar el grado de peligrosidad, se estudia la gravedad de las acciones que produce sobre un equipo infectado, su velocidad y facilidad de propagación y la cantidad de infecciones producidas recientemente.

## Según su forma de propagación:

* + Virus es un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático, corrompiendo o destruyendo archivos.

Una vez que se ejecuta, se propaga infectando a otros ficheros y se almacena en ficheros ejecutables para ejecutarse.

* + Gusanos es un tipo de malware que se propaga automáticamente, ya que puede duplicarse a sí mismo. Su finalidad no es destruir archivos o equipos, sino que están pensados para consumir recursos de un sistema o una red de comunicaciones hasta saturarlo y provocar su caída.

La desinfección de un gusano es más sencilla que la de un virus porque los gusanos no modifican archivos, solo cambian algunos parámetros.

* + Troyanos es un software malicioso y es un programa inofensivo, pero su finalidad es permitir a un usuario no autorizado tomar el control de una máquina infectada. Las infecciones se pueden producir cuando un usuario ejecuta un programa infectado, el programa funciona correctamente, pero el troyano se instala en segundo plano.

## Hay dos tipos de conexiones:

* + Conexión directa: el cliente se conecta al servidor para enviarle órdenes.
  + Conexión inversa: es el servidor el que envía directamente la información al cliente. Es más efectiva ya que los firewalls no suelen analizar la información saliente del ordenador.

## Los más Habituales son:

Backdoor: permite el acceso remoto a un atacante al sistema

Keylogger: captura las pulsaciones de las teclas realizadas en el equipo de la víctima

Downloader: su misión es descargar archivos maliciosos y ejecutarlos en el equipo infectado.

Proxy: el intruso utiliza la red infectada como un servidor proxy

## Software malicioso no dañino:

Spyware: su función es conseguir información del usuario

Adware: muestra publicidad de forma intrusiva y suele camuflar las acciones de otros malware y se suele combinar con spyware.

Hijacking: cambian la configuración del navegador y también puede modificar los enlaces de la carpeta “Favoritos” o añadir nuevas barras de herramientas.

Jokes: no realiza ninguna acción dañina sobre el equipo infectado, se limita a hacer creer al usuario que se va a borrar el contenido del disco, pero no lo hace

Bulos: suele propagarse por correo electrónico y alerta a los usuarios de alguna amenaza no real

## Software malicioso DAÑINO

Ransomware: cifra el disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.

Rogueware: Hace que el usuario crea que su equipo está infectado por un virus y para solucionarlo es descargar un archivo dando control total al equipo

Password stealer: se aprovechan de las herramientas que tienen los navegadores para crear cuentas de correo o redes sociales y modifican el navegador para que capture la contraseña de la victima

Bombas lógicas: se pone en marcha cuando se cumple alguna condición, como un dia en concreto

Denegación de servicio o DOS: se define como la imposibilidad de acceder temporalmente a un servicio

## Ataques de denegación de servicio:

* Ataques internos: provocados por usuarios legítimos de la organización que, ya sea por desconocimiento o de forma intencionada, provocan la degradación de un recurso o servicio, impidiendo su acceso a otros usuarios y a ellos mismos.
* Ataques externos: en este caso, el atacante es una entidad ajena a la organización, es decir, lo provocan usuarios ilegítimos. Se aprovechan las vulnerabilidades del sistema para acceder a él.

Publicidad y correo no deseado: es todo correo no esperado por el usuario que lo recibe.

## Ingeniería social. Fraudes informáticos

La ingeniería social es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.

* + Suplantación de la identidad: es un tipo de fraude que consiste en hacerse pasar por otra persona. Hay varias categorías:
* Phising: el atacante suele crear una página web falsa aparentemente idéntica a la de una empresa que requiere autenticación y el cliente, al introducir sus datos, le revela esa información al atacante. Una de las técnicas del phishing es el pharming, que es fraude informático que suplanta el sistema de resolución de nombres de dominio (DNS).
* Vishing: es parecida al phishing, pero utiliza como vehículo el protocolo de voz sobre IP (VoIP). La víctima recibe una llamada en la que se le indica que debe teclear en su terminal un determinado dato para realizar alguna acción.
* SMShing: se engaña a las víctimas a través del envío de mensajes SMS a tus teléfonos móviles para conseguir sus contraseñas. Se les pide que accedan a una determinada página web para, por ejemplo, desbloquear su tarjeta de crédito.
* Grooming: consiste en el acoso a menores por parte de un adulto que trata de ganarse su confianza o la coacciona de alguna forma para que realice alguna acción de tipo sexual.
  + Cadenas de correos: son mensajes en los que se incita a su destinatario a difundirlos al mayor número de personas posible bajo promesas o amenazas, con el ánimo de conseguir direcciones de correo.
  + Correos millonarios: es el envío de correos prometiendo a los usuarios que pueden hacerse ricos fácilmente.

# Tema 7 – Medidas de protección contra el malware

## Medidas preventivas contra el malware:

* Suites de seguridad (preventiva y paliativa): es un conjunto de varios programas de seguridad como antivirus, antispyware, antirootkit, antiphishing, antispam, cortafuegos, herramientas de control y protección al navegar como filtros de contenido o control parental, etc.

## Combaten el malware de dos maneras:

* Protegiendo el equipo, en tiempo real, contra la instalación de malware, escaneando todos los datos procedentes de la red en busca de malware y bloqueando todo lo que suponga una amenaza.
* Detectando y eliminando malware que ya ha sido instalado en el equipo escaneando el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en el ordenador.

## Las técnicas que utilizan son:

* Comparación con firmas: se comparan los archivos sospechosos con una base de datos con las firmas de todo el malware conocido hasta la fecha.
* Métodos heurísticos: también se deduce si el equipo está infectado utilizando técnicas para detectar malware sin tener su firma en la base de datos. Los motores antimalware utilizan:
  + Firmas genéricas: no buscan una coincidencia al 100% pero sí una similitud con una firma, para detectar mutaciones de virus.
  + Desensamblado: se obtiene el código en lenguaje ensamblador del malware y se estudia el código con técnicas conocidas.
  + Desempaquetado: algunos virus han sido empaquetados y comprimidos para evitar que sean detectados. Los antivirus los desempaquetan y analizan.
* Cortafuegos: es un dispositivo software o hardware diseñado para proteger dicho sistema bloqueando accesos no autorizados.
  + Políticas permisivas: se deniega explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones.
  + Políticas restrictivas: prohíbe el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso.

Las reglas son un conjunto de condiciones que deben cumplir los mensajes para que el Firewall permita o rechace su paso. Las reglas suelen tener información como:

* Equipo o red que ha enviado el mensaje
* Dirección IP del equipo o red que recibirá el mensaje
* Protocolo utilizado (TCP, UDP, ICMP)
* Puerto del equipo destinatario o emisor del mensaje
* Acción a realizar sobre el paquete (aceptar, rechazar informando al emisor del motivo por el que se rechazó el mensaje, rechazar sin informar al origen, etc…)

Iptables es el cortafuego por defecto de los sistemas Linux.

## Medidas paliativas contra el malware:

Constituyen todo el conjunto de acciones que los usuarios realizan para eliminar malware que ha conseguido infectar al equipo.

Las mejores medidas paliativas son las copias de seguridad, el software congelador, los sistemas RAID o las herramientas de recuperación de datos de borrado.

## Copias de seguridad

* + Copias de seguridad del sistema: permiten restaurar un equipo a un estao operacional después de un desastre.
  + Copias de seguridad de datos: permiten restaurar algunos ficheros después de que hayan sido borrados o dañados accidentalmente.
  + Software congelador: permite congelar el estado del equipo en el momento determinado, con la configuración y contenidos exactos que el equipo tenía en ese momento determinado. Esto proporciona varios beneficios:
  + Se contribuye al anonimato de los usuarios, ya que un usuario malintencionado no puede acceder a información previa a la sesión actual, al borrarse el historial, las cookies y las contraseñas que hayan podido quedar almacenadas por algún descuido.
  + Se protege a los equipos frente a infecciones por software malicioso, ya que durante el proceso de restauración se elimina cualquier malware que haya infectado al equipo.

## Centros de protección y respuesta frente a amenazas:

Dos tipos de servicios:

* Preventivos:
  + Avisos de seguridad
  + Búsqueda de vulnerabilidades
  + Auditorías o evaluaciones de seguridad
  + Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras
  + Desarrollo de herramientas de seguridad
  + Propagación de información relacionada con la seguridad
* Reactivos:
  + Gestión de incidentes de seguridad (análisis, respuesta, soporte y coordinación de incidentes de seguridad)
  + Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas).

## Buenas prácticas para protegerse del malware:

* Actualizar el sistema operativo y aplicaciones: actualizar periódicamente el sistema operativo y todas las aplicaciones.
* Protección antimalware: se debe instalar una suite antimalware, así como un cortafuegos y mantenerlos actualizados.
* Cuentas de usuario: usar cuentas de usuario con privilegios limitados para el uso diario del equipo y solo utilizar la cuenta de usuario cuando sea necesario.
* Políticas de seguridad: diseñar políticas que incluyan la definición de contraseñas complejas.
* Datos personales y claves: no facilitar datos personales, ni claves, ni códigos PIN solicitados por correo electrónico u otro medio.
* Precaución al navegar: no navegar por páginas web sospechosas, no confiables o que ofrezcan regalos o promociones dudosas.
* Correo electrónico: se deben observar las recomendaciones expuestas a esta unidad, en el apartado dedicado al correo electrónico.
* Instalación de aplicaciones: se debe tener precaución al instalar o ejecutar programas procedentes de Internet, así como evitar la descarga de software de redes P2P y tener un antivirus.
* Reciclaje constante: los administradores de sistemas deben mantenerse actualizados, suscribiéndose a boletines de seguridad, consultando periódicamente web de información.
* Copias de seguridad: se deben hacer regularmente copias de respaldo a medios extraíbles de los documentos importantes para poderlos recuperar en caso de infección.
* Otras medidas: una realización periódica de auditorías de seguridad y la concienciación de los usuarios en cuestiones de seguridad informática.

# Tema 8 - Gestión del Almacenamiento

## Seguridad física

Control de acceso al medio con sistemas biométricos, utilización de dispositivos NAS, utilización de una red de área de almacenamiento (SAN), etc…

## Seguridad lógica

Cifrado de datos, bloqueo de dispositivo, etc.

*La Ley Orgánica de Protección de Datos Carácter Personal (LOPD) tiene por objeto proteger el derecho a la intimidad personal y familiar de los ciudadanos y el adecuado tratamiento de la información referente a las personas físicas.*

## Políticas de almacenamiento

* Normas de almacenamiento en los equipos de trabajo
* Normas de uso de dispositivos externos de memoria
* Normas de almacenamiento en la red de la empresa
* Normativa de realización de copias de seguridad

## Dispositivos de almacenamiento

### Clasificación:

* Medios magnéticos: discos duros, disquetes y cintas magnéticas.
* Medios ópticos: CD, DVD, HD-DVD o Blu-ray
* Electrónicos o memorias de estado sólido: memorias flash, tarjetas de memoria y discos duros SSD
* Otros: memorias híbridas magneto-ópticas, memoria holográfica, memoria molecular, patterned media, etc.

## Otra clasificación:

Dispositivos locales/internos: se conectan directamente al equipo y son gestionados por el mismo.

Dispositivos externos: gestionados por un sistema externo al equipo:

* Dispositivos remotos: dispositivos externos a la organización donde se almacena información
* Dispositivos de almacenamiento externo:
* NAS (Network Attached Storage): es una tecnología de almacenamiento accesible desde la red. Se accede a ellos a través de protocolos de red, como TCP/IP. Ofrecen, entre otras funciones, realizar backups, tener tolerancia de fallos, balanceo de carga, compartir archivos y capacidad de expansión al poder agregar otros dispositivos. FreeNAS es un tipo de software que crea sistemas NAS.
* SAN (Storage Area Network): es una red de área de almacenamiento. Esta tecnología crea una red especializada y normalmente complementaria a la red de datos de configuración, para conectar los servidores, los discos de almacenamiento y demás elementos necesarios. Generalmente utilizan fibra óptica para poder garantizar una conexión rápida y fiable.

## Tecnologías de almacenamiento redundante y distribuido

RAID (Redundant Array of Independent Disks) es la utilización de varios discos sobre los cuales se distribuyen los datos y alguna información adicional.

RAID 0: se necesitan, como mínimo dos discos. La información se distribuye en stripes o bandas entre los dos discos con el objetivo de poder acceder más rápidamente a los datos. Se pueden acceder simultáneamente a los dos discos.

RAID 1: se necesitan, como mínimo, dos discos y la información se duplica de un disco al otro (disk mirroring o discos en espejo).

RAID 5: como mínimo se pueden utilizar tres discos, pero lo recomendable es utilizar cinco. La información se reparte igual que en el RAID 0 entre los 4 discos y, en la banda correspondiente del 5, en vez de datos, hay información de paridad. La paridad está repartida en bandas por los cinco discos, de esta manera, se reduce la posible pérdida de almacenamiento.

Este no entra

RAID 10: es el conjunto de un RAID 1 y un RAID 0, se junta la velocidad de lectura del RAID 0 y la redundancia del RAID 1 y se necesitan, como mínimo, cuatro discos.

**Inconvenientes de los RAID:**

El coste y la complejidad de su configuración pueden llegar a ser altos, dependiendo del tipo de configuración elegidos.

## Copias de seguridad

Es una copia de la información que se realiza como medida preventiva para el caso de que la información original se pierda o se dañe.

## Clases de copias de seguridad:

* Normales o completas: se copian todos los archivos que indiquemos.
* Diferenciales: se copian únicamente los archivos modificados después de la última copia completa.
* Incrementales: se copian únicamente los archivos que se hayan modificado después de la última copia completa o diferencial.

## Realización de copias de seguridad:

* Datos a incluir en la copia de seguridad: discos completos, directorios, ficheros, base de datos, etc.
* Frecuencia de modificación de los datos: no es lo mismo hacer copia de ficheros que varían mensualmente que diariamente.
* Frecuencia de las copias de seguridad: cada cuanto tiempo se va a realizar un backup y de qué tipo. Para recuperar una copia de seguridad necesitaremos la última copia completa y todas las incrementales o diferenciales a partir de ésta.
* Tipo de datos: no es lo mismo hacer una copia de registros de bases de datos o de bases de datos completas que de ficheros ordinarios.
* Uso de los datos durante la realización de la copia: hay veces que se necesitan para realizar copias de seguridad de ficheros en uso. Se suelen hacer durante la noche, ya que la actividad de los servidores es más baja.
* Tiempo requerido para la recuperación de datos: hay información crítica que, en caso de fallo, necesita ser accesible al instante.
* Política de retención: cuánto tiempo se va a conservar cada backup. La retención influye en las versiones que queremos conservar de los datos. Así si se hace un backup diario con una retención de quince días, podríamos devolver un fichero al estado que tuvo hace quince días.

Para un correcto soporte o dispositivo en el que se va a hacer la copia de seguridad hay que tener en cuenta:

* Capacidad o cantidad de información que puede almacenar.
* Velocidad a la que se realizará la copia y el tiempo de acceso a los datos.
* Tiempo de vida.
* La relación de coste por byte.

Gestión de imágenes del sistema:

Es la clonación o realización de una copia exacta de un disco o partición. Existen varios tipos:

* Disco a disco: se copia todo el contenido de un disco a otro compatible, que puede ser interno o externo.
* Partición a partición: se copia una partición en otra, creada anteriormente, que pueda estar guardada en el mismo disco o en otro.
* Archivo de imagen: se copia el disco o una partición en un archivo. Este archivo puede guardarse en cualquier medio.

Recuperación de datos eliminados

En el caso de que las circunstancias nos lleven a no utilizar los métodos anteriores, se pueden utilizar los puntos de restauración, que es un estado anterior al sistema.

El modo a prueba de fallos es el intento de iniciar el sistema utilizando la última configuración que funcionó correctamente.

# Parte práctica tema 8 – Debian

Apt update ; apt install mdadm –y

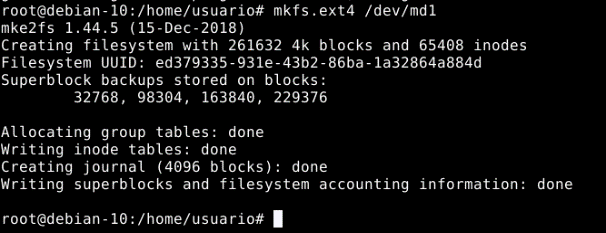
lsblk -fm ---> Para ver la cantidad de discos que hay

fdisk /dev/(disco) ---> Para ver la información del disco

Mdadm --create /dev/md1 --level=1 -- raid-device=2 /dev/sdc /dev/sdb Forma Jose Antonio

mdadm -C /dev/md1 -l raid5 -n 6 /dev/sd[b-g] (b-g depende de los discos que sean) Forma Paco

mdadm --detail /dev/md1 ---> Para ver los detalles del RAID que hemos hecho

mkfs.ext4 /dev/md1 ---> Para dar formato al disco

mkdir espejo ---> Carpeta donde vamos a poner el mount del RAID

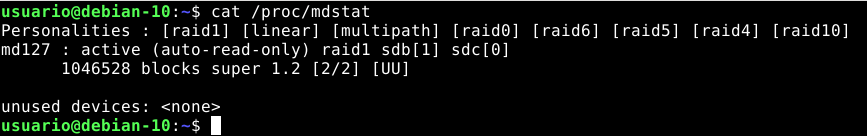
mount /dev/md1 espejo/ ---> Para montar el disco que hemos creado en ese directorio

mdadm /dev/md1 --fail /dev/sdb ---> Para deshabilitar un disco al raid

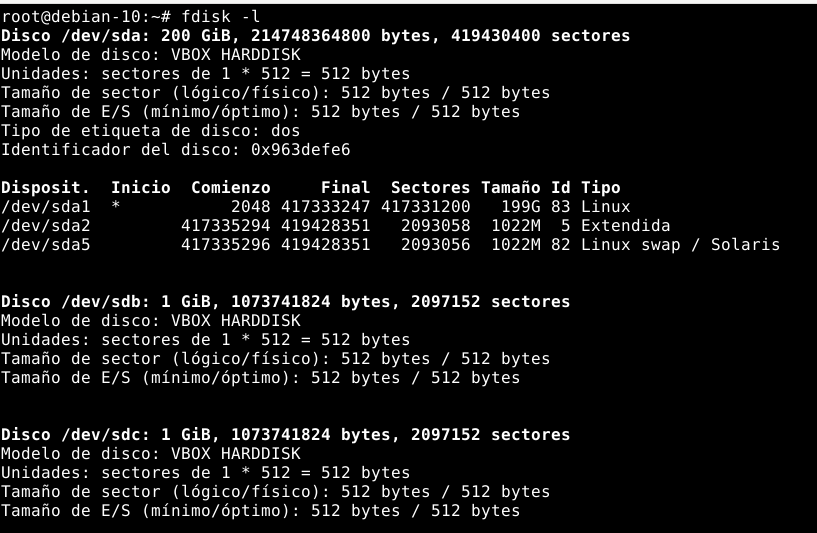
mdadm /dev/md1 --remove /dev/sdb ---> Para quitar un disco al raid

mdadm /dev/md1 --add /dev/sdb ---> Para agregar un disco al raid

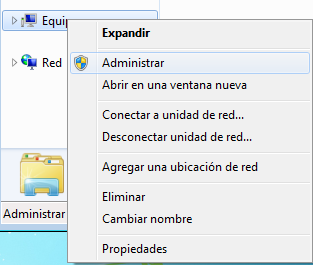
cat /proc/mdstat ---> Para ver los tipos de raid que hay



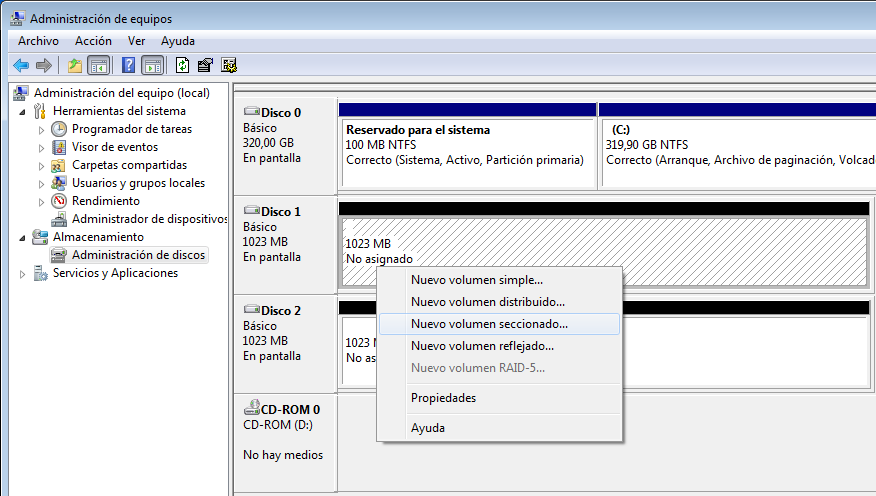
Fdisk -l ---> Para ver los discos que hay en nuestro sistema



# Parte práctica tema 8 – Windows



Raid 0



Raid 1

