Temas que entran para el examen del día 24

Índice

[Tema 5 – Aplicaciones de criptografía 4](#_Toc93077792)

[Firma digital o firma electrónica: 4](#_Toc93077793)

[Firma digital con árbitro: 4](#_Toc93077794)

[Firma digital ordinaria: 4](#_Toc93077795)

[Clases de firma digital: 4](#_Toc93077796)

[ Firma electrónica: 4](#_Toc93077797)

[ Firma electrónica avanzada: 4](#_Toc93077798)

[ Firma electrónica reconocida: 4](#_Toc93077799)

[ Firma electrónica avanzada reconocida: 4](#_Toc93077800)

[Tema 6 – Software Malicioso 5](#_Toc93077801)

[Tema 8 - Gestión del Almacenamiento 6](#_Toc93077802)

[Seguridad física 6](#_Toc93077803)

[Seguridad lógica 6](#_Toc93077804)

[Políticas de almacenamiento 6](#_Toc93077805)

[Dispositivos de almacenamiento 6](#_Toc93077806)

[Clasificación: 6](#_Toc93077807)

[ Medios magnéticos: 6](#_Toc93077808)

[ Medios ópticos: 6](#_Toc93077809)

[ Electrónicos o memorias de estado sólido: 6](#_Toc93077810)

[ Otros: 6](#_Toc93077811)

[Otra clasificación: 6](#_Toc93077812)

[Dispositivos locales/internos: 6](#_Toc93077813)

[Dispositivos externos: 6](#_Toc93077814)

[Tecnologías de almacenamiento redundante y distribuido 7](#_Toc93077815)

[RAID 0: 7](#_Toc93077816)

[RAID 1: 7](#_Toc93077817)

[RAID 5: 7](#_Toc93077818)

[RAID 10: 7](#_Toc93077819)

[Copias de seguridad 7](#_Toc93077820)

[Clases de copias de seguridad: 7](#_Toc93077821)

[ Normales o completas: 7](#_Toc93077822)

[ Diferenciales: 7](#_Toc93077823)

[ Incrementales: 7](#_Toc93077824)

[Realización de copias de seguridad: 8](#_Toc93077825)

[Parte práctica tema 8 – Debian 9](#_Toc93077826)

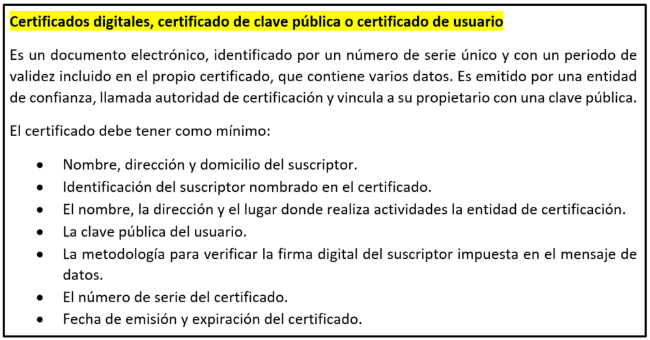
# Tema 5 – Aplicaciones de criptografía

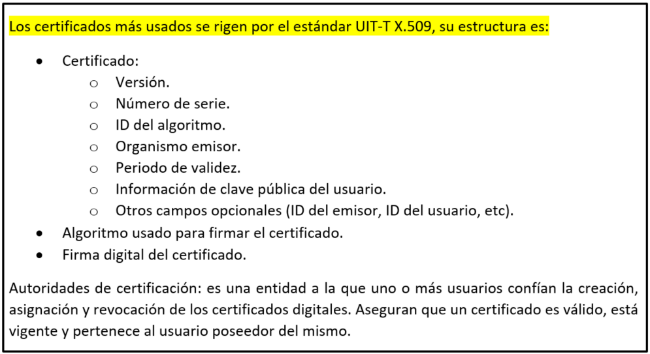
Firma digital o firma electrónica: la firma se encarga de uno de los principios de la seguridad informática, la autenticación, es decir, verifica que el mensaje recibido es exactamente igual al original y que proviene del mismo emisor.

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: hay virus, gusanos y troyanos:
  + **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.

# 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

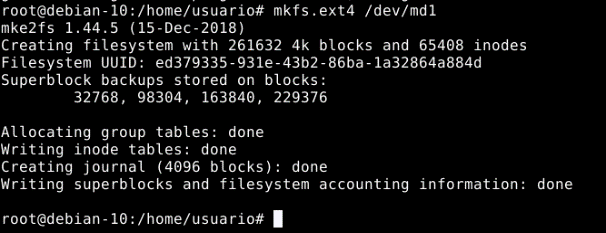
lsblk -fm ---> Para ver la cantidad de discos que hay

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

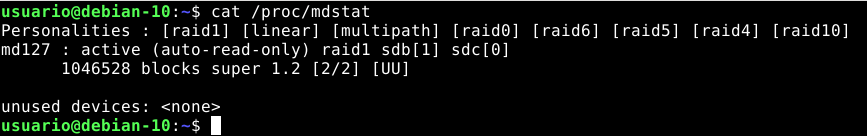
mount /dev/md1 espejo/ ---> Para montar el disco que hemos creado en ese directorio

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

