Seguridad informática

Antonio Postigo Palacios

Paraninfo
ciclos formativos

FE DE ERRATAS

Noviembre 2021

Unidad 1

Página 2
Se corrige el nombre de la organización resaltado.

1.1. Planificación de la seguridad informática

La organización CCN-Cert definía la *seguridad informática* en su método Magerit como «la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles».

Página 16
Se corrige el comando resaltado.

Actividad propuesta 1.5

Gestión de usuarios en Linux mediante el uso de comandos

Usando las técnicas desarrolladas en este apartado, procede a generar diferentes usuarios y grupos, y a asignarles privilegios sobre diversos directorios y ficheros. Procede de la siguiente manera:

- Crea cuatro cuentas de usuarios con contraseñas cifradas (usuario01, usuario02, usuario03 y usuario04). Usa el comando `useradd` y cifra las contraseñas a través de alguna herramienta que genere contraseñas cifradas.
- Crea dos grupos de usuarios, llamados *ventas* y *jefeventas*. Los dos primeros usuarios estarán en el primer grupo (ventas), y los otros dos, en el segundo.
- Crea dos directorios (llamados *general* y *exclusivo*) e incluye cuatro ficheros en él.
- Asigna a los usuarios *usuario01* y *usuario03* los siguientes privilegios con el comando `setfacl`, según la información expuesta a continuación:

Página 17
Se corrige el término resaltado.

Actividad propuesta 1.6

La gestión de contraseñas con PAM

PAM (Pluggable Authentication Modules) es un mecanismo para la autenticación centralizada de usuarios que deja gestionar las políticas de seguridad de las diferentes aplicaciones que hagan uso de él.

Instala los paquetes slapd y ldap-utils en tu máquina Linux. Modifica el contenido del archivo /etc/hosts con el fin de almacenar la relación de la dirección IP estática del servidor con los nombres lógicos previstos.

A continuación, instala la librería libnss-ldap. Sigue los pasos de configuración.

Después, configura cómo autenticar usuarios. Para ello, usa el script auth-cliente-config para modificar los archivos de configuración de PAM y NSS.

Actualiza la configuración de las políticas de autenticación predeterminadas de PAM.

Página 21
Se corrige el código resaltado.

```
tcpdump -i eth1 tcp port 80
```

Página 35
Se corrige la opción de respuesta resaltada en la actividad de comprobación 1.10.

1.10. Con respecto al comando `passwd`, ¿cuál de las siguientes afirmaciones no es correcta?

a) Se puede indicar el número de días antes de un aviso.
b) Se puede indicar la duración mínima en días de la contraseña.
c) Se puede indicar la duración máxima de la contraseña.
d) No se puede cifrar la contraseña.

Unidad 2

Página 62
Se modifica el nombre de la máquina virtual.

Actividad propuesta 2.10

Creación de un sistema raid nivel 1 en Windows

Configura un sistema RAID 1 en tu máquina Windows. Crea, usando la aplicación de gestión de máquinas virtuales (VMWare, VirtualBox, XEN, o cualquier otra), diferentes discos, que luego usarás para acoplarlos al sistema RAID.

Recuerda que los volúmenes que tengas creados en tu sistema deben ser eliminados para que se pueda configurar un sistema RAID en Windows (Administración de discos).

Página 64
Se corrige el término resaltado.

Recuerda

El **firmware** es un programa generalmente almacenado en memorias ROM o PROM, que gestiona físicamente el funcionamiento de los dispositivos. La BIOS es un ejemplo de firmware.

Página 65
Se corrige el nombre del archivo.

Si se consulta el archivo /proc/mdstat, se podrá comprobar que aún no existe ningún raid configurado.

Unidad 3

Página 103
Se corrige el término resaltado.

Actividad propuesta 3.8

Despliegue de un servidor SAN en Windows Server

Usando un sistema operativo Windows Server, ofrece un servicio de almacenamiento por red usando iSCSI en red ethernet.

En Windows Server, la consola de administrador del servidor y los cmdlets de Windows Powershell para el administrador del servidor permiten la instalación de roles y características en servidores remotos o locales, o en discos duros virtuales (VHD) sin conexión. Despliega un servidor SAN en tu servidor haciendo uso de estas herramientas.

Página 108
Se corrigen los términos resaltados.

3.6.6. Despliegue de un servidor NAS usando FreeNAS/TrueNAS

TrueNAS, o su versión anterior FreeNAS, es un sistema operativo basado en FreeBSD que proporciona servicios de almacenamiento en red y que permite convertir un equipo en un soporte de almacenamiento accesible desde la red.

Página 109
Se corrige el texto resaltado.

Las funciones principales de FreeNAS y de TrueNAS son:

- **Réplica:** se usa el sistema de ficheros ZFS que permite el uso de instantáneas y replicación en otros sistemas. Estas instantáneas del mismo sistema de ficheros se pueden enviar de forma incremental, lo que reduce el tamaño de cada copia. Las instantáneas permitirán recuperar los datos en caso de catástrofe.

Unidad 4

Página 142
Se elimina el texto resaltado.

Se establece como una metodología de conexión alternativa a otros programas que permiten la conexión a equipos remotos, pero no usan metodologías seguras en la conexión, como pueden ser Telnet, SSH, FTP, etcétera.

Página 144
Se modifica el texto resaltado

4.5.2. El protocolo Secure Socket Layer (SSL)

El principal objetivo de este protocolo es establecer una conexión segura entre un cliente y un servidor, independientemente de los sistemas operativos que se estén usando en dichas máquinas. Trabaja en el nivel de transporte y está compuesto por una serie de niveles con funciones claramente definidas en cada uno de ellos. Estos niveles son SSL Record Protocol, SSL Handshake Protocol, SSL Assert Protocol y Change Cipher Spec Protocol. En la Figura 4.18, se detalla la función de cada uno de ellos:

Página 150
Se pasa a minúscula.

```
airodump-ng --write cap210901.cap wlan0
```

donde --write permite indicar que se desea registrar todos los paquetes, cap210901.cap es el nombre del fichero donde se almacenará todos estos registros y *wlan0,* el nombre de la interfaz de red.

Se puede indicar a través de `airodump` qué dirección MAC es la que se quiere escuchar a través de su identificación con el parámetro --bssid, e, incluso, indicar por qué canal

Página 151
Se añade la siguiente línea resaltada.

El siguiente comando generaría una falsa autenticación (tipo 1):

```
aireplay-ng -1 0 -a 0f:1c:f7:ba:78:9c -h 63:40:50:1f:2c:01 wlan
```

El siguiente generaría un ataque tipo inyección (tipo 3) de paquetes ARP-resquest:

Se corrige el texto de la línea resaltada.

```
aircrack-ng cap210901.cap
```

con el fin de que localice la clave. Si no es capaz, necesita más tramas capturadas.

Página 153
Se corrigen los textos resaltados.

```
gedit /etc/freeradius/3.0/clients.conf
```

desde el servidor maquinalinux, se usaría el comando `radtest Antonio 9fhn!39f 192.168.1.44 0 k8f.md521`.

Unidad 5

Página 164
Se corrigen los textos resaltados.

```
password_pbkdf2 antonio grub.pbkdf2.sha512.10000.BC902847CD29
F10385FF3938467393870A038C38745D378624BD7654F87642C387262…
password_pbkdf2 paco grub.pbkdf2.sha512.10000.93758ABC37DE
7AC2B38A10948C372D372A2383E3F36724C2373B4674652C302947F40…
EOF
```

Página 167
Se corrige el texto resaltado.

Para mandar una clave pública a un servidor de claves, se usa el comando gpg --send-keys --keyserver dirección-servidor ID-Clave. Por tanto, el comando podría ser

Unidad 6

Página 215
Se corrige el texto resaltado.

Solución

Si el paquete UFW no está instalado en el sistema, se ejecutará la orden `apt install UFW` para proceder a su instalación. Luego, se validará el estado actual del cortafuegos escribiendo `UFW status verbose`. Tras activar el cortafuegos con `UFW enable` y comprobar con `UFW status verbose` el nuevo estado, se comprueban las reglas por defecto de UFW. Las reglas definidas se almacenan en */etc/ufw*.

Si se quisieran permitir conexiones SSH a través del cortafuegos, se escribiría el comando `UFW allow ssh`. Si se usase un puerto personalizado, se debería usar la orden `UFW allow 2543/tcp`, donde se indica que el puerto tcp abierto es el 2543. Para denegar una conexión http usando protocolo udp, se usa el comando `UFW deny http/udp`.

Para indicar una interfaz de red específica de todas las que tiene el cortafuegos, se usa `UFW allow in on eth2 to any port 443`. Con 'in on' se indica la tarjeta de red.

Página 216
Se añade la aclaración resaltada.

A través del comando `IPTables` (escríbese en la terminal Linux con el texto iptables), se pueden llevar a cabo funciones como bloquear el acceso no permitido desde una red externa, restringir o limitar las conexiones de la red local con el exterior, etcétera.

Página 221
Se corrigen los términos resaltados.

Tabla 6.5. Parámetros del comando IPTables para añadir y borrar reglas

-j accion (--jump)	Se usará para indicar la acción de una regla, ya sea una ya creada o el nombre de la cadena definida por el usuario, que ha sido creada usando la opción –N.

Si se quisiera eliminar la regla que se acaba de agregar, se escribiría

```
IPTables -D INPUT -p icmp -j DROP
```

Este comando elimina la primera regla de la cadena INPUT que cumple con la especificación '–p icmp –j DROP'. Si hubiera varias reglas que coincidieran con la especificación,

Página 223
Se modifica la ubicación de los textos resaltados.

Para incluir en esta máquina el seguimiento de la conexión, las reglas deberían haber sido:

```
IPTables -A FORWARD -p udp --sport 1024:65536 --dport 53 -i eth1
  -o eth0 -s 192.168.143.0/24 -m state --state NEW,ESTABLISHED
                              -j ACCEPT
IPTables -A FORWARD -p udp --dport 1024:65536 --sport 53 -o eth1
    -i eth0 -d 192.168.143.0/24 -m state --state ESTABLISHED
                              -j ACCEPT
```

Página 228
Se corrigen los textos resaltados.

Se eliminan todas las reglas de la tabla Filter y se ponen los contadores a cero:

```
IPTables -F
IPTables -Z
IPTables -t nat -F
```

Se establece la política por defecto: se aceptan todas las cadenas de entrada, de salida y de enrutamiento de la tabla Filter (INPUT, OUTPUT Y FORWARD):

```
IPTables -P INPUT ACCEPT
IPTables -P OUTPUT ACCEPT
IPTables -P FORWARD ACCEPT
```

Página 229
Se corrigen los términos resaltados.

```
IPTables -t nat -p PREROUTING ACCEPT
IPTables -t nat -p POSTROUTING ACCEPT
```

Página 231
Se corrigen los textos resaltados.

```
IPTables -P FORWARD DROP
IPTables -t nat -P PREROUTING DROP
IPTables -t nat -P POSTROUTING DROP
```

Se aceptan todas las conexiones locales (interfaz localhost):

```
IPTables -A INPUT -i lo -j ACCEPT
```

Se permiten todas las conexiones desde la red local al cortafuegos. La red local se conecta al cortafuegos por la interfaz eht1 que pertenece a la red 192.168.1.0/24. Para aceptar todos los paquetes provenientes de dicha red, se aceptan (acción aceptar, -j ACCEPT) todos los paquetes de datos que entren en la cadena INPUT de la tabla Filter (recuerda, tabla por defecto, por lo que no es necesario indicar la tabla con –t Filter), cuya IP de origen (parámetro –s) sea 192.168.1.0/24 y la interfaz eth1 (parámetro –i):

No se debe olvidar que, para permitir hacer FORWARD de paquetes en el cortafuegos, se debe tener el valor ipforward puesto a 1 (en el archivo /proc/sys/net/ipv4/ip_forward).

Página 233
Se corrigen los textos resaltados.

```
IPTables -A FORWARD -s 192.168.2.43 -d 192.168.3.143
         -p tcp --sport 1521 -j ACCEPT
IPTables -A FORWARD -s 192.168.3.143 -d 192.168.2.43
         -p tcp --dport 1521 -j ACCEPT

IPTables -A INPUT -s 192.168.3.0/24 -i eth2 -j DROP
```

Por último, se cierran el resto de conexiones por los puertos tcp y udp bien conocidos (rango 1:1024). Se utiliza la dirección de red 0.0.0.0 para indicar cualquier red. Las reglas que se deben aplicar son:

```
IPTables -A INPUT -s 0.0.0.0 -p tcp --dport 1:1024 -j DROP
IPTables -A INPUT -s 0.0.0.0 -p udp --dport 1:1024 -j DROP
```

Página 236
Se corrigen los textos resaltados.

Por ejemplo,

```
nft list table ip FiltrosIP
```

6.4.2. Gestión de las cadenas

Igual que en IPTables, las reglas que interesa ir creando se deben almacenar en las cadenas. En NFTables, las tablas no tienen cadenas y deben ser definidas. Estas cadenas se denominan *cadenas base* y suelen ser añadidas antes de incluir cualquier regla. Para añadir una cadena a una tabla se usa el siguiente comando:

```
nft add chain tipo nombre-tabla nombre-cadena{
type tipocadena hook gancho priority valor \;}
```

Unidad 7

Página 255
Se corrige el texto resaltado.

```
sudo apt-get install Squid squidclient
```

Página 256
Se elimina el número 3 tras Squid en los textos resaltados.

Este paquete instala el fichero ejecutable de Squid en el directorio `/usr/sbin/Squid.` Los módulos o plugins se instalan en el directorio `/usr/lib/Squid.` La instalación de Squid crea un usuario y grupo llamados *proxy*. Es este usuario el que tiene los privilegios necesarios sobre los ficheros de configuración, los ficheros log y la caché del proxy. Por consiguiente, es este el usuario que se empleará para realizar cualquier configuración del servidor proxy.

Los objetos descargados se almacenan por defecto en el directorio /var/spool/Squid, por lo tanto, el usuario y grupo proxy deben tener los permisos suficientes para acceder a este. Para comprobar los permisos, se usa el comando `ls -ld /var/spool/Squid`. El usuario proxy requiere de acceso de lectura y escritura, y el grupo proxy, de acceso solo lectura. Una correcta salida sería, por ejemplo, drwxr-xr-x. También se puede comprobar que el usuario y grupo propietarios de dicho fichero son proxy:proxy (usuario:grupo). En caso de que no lo sean, se tiene que cambiar. Para ello, se usa el comando `chown`, escribiendo

```
chown proxy:proxy /var/spool/Squid
```

```
sudo chmod 755 /var/spool/Squid
```

Los ficheros log se almacenan en /var/log/Squid, por lo tanto, el usuario y grupo proxy también deben tener acceso a este directorio. De nuevo, se hará uso del comando `ls -ld /var/log/Squid` para comprobar sus permisos (drwxr-xr-x sería correcto), y el comando `chmod` para modificar los mismos.

Página 257
Se elimina el número 3 tras Squid en el texto resaltado.

El fichero de configuración de Squid está localizado en el directorio /etc/Squid con el nombre Squid.conf. Este fichero es un fichero plano, por lo tanto, es editable con cualquier editor de texto. La mayoría de su contenido son comentarios que comienzan con el carácter #, y diferentes parámetros, que son configurables, denominados *directivas de*

Página 258
Se corrige el texto resaltado.

donde htto_port es el nombre de la directiva y 3128 su valor, separados por un solo espacio. De esta manera, el programa Squid abrirá el puerto TCP 3128 en todas las direcciones IP.

Página 260
Se corrigen los textos resaltados.

El directorio por defecto para la caché en disco es */var/spool/squid*, pero también se puede indicar otro u otros si se desea. El tamaño indica el tamaño de dicho directorio expresado en megabytes, y su valor por defecto es 100MB. Se indicará otro valor si se necesita especificar un tamaño diferente. Los valores nivel1 y nivel2 se refieren al número de subdirectorios que se pueden crear en primer nivel (dentro del primero) y en segundo nivel (la suma de todos los subdirectorios dentro de cada directorio), y sus valores por defecto son 16 y 256, respectivamente. El siguiente ejemplo

```
cache_dir ufs /var/spool/Squid 16000 32 256
```

Actividad resuelta 7.2

Configuración de la caché de un proxy

Se desea activar la caché de un servidor proxy con la siguiente configuración:

- El usuario con el que programa Squid operará en la caché es Squid.
- El directorio de la caché será /var/spool/Squid/cache.

Página 261
Se corrigen los textos resaltados.

- El correo electrónico del administrador es admistrador@paraninfo.es.
- El tamaño de la memoria asignada para caché en RAM será de 32 megabytes.
- No se almacenará ningún objeto mayor de 2 megabytes.
- El sistema de archivos es ufs, y el número máximo de subdirectorios será de 16 a primer nivel y de 64 a segundo nivel.

Indica las directivas que editar y el valor de cada una de ellas.

Para indicar el sistema de archivos y el número de directorios a nivel1 y a nivel2, se usa cache_dir:

```
cache_dir ufs /var/spool/Squid/cache 16 64
```

Página 262
Se corrigen los textos resaltados.

```
logformat infEspecial %>a %<A %lp %wl %ru
```

nde se va a encontrar el fichero log se hace con el parámetro acce

Se elimina el número 3 tras Squid.

pretende indicar que el directorio donde se almacena el fichero log es /var/log/Squid, que su nombre es accesos.log, y que el formato es el declarado con anterioridad en el uso de logformat, denominado *infEspecial*, se escribiría

```
access_log /var/log/Squid/accesos.log infEspecial
```

Si no se requiere registrar actividad de los clientes, se especifica el valor none en dicho parámetro.

```
access_log none
```

Cuando se inicia Squid, almacena información log en el fichero parametrizado con la directiva cache_log. Por ejemplo,

```
cache_log /var/log/Squid/cache.log
```

Cada vez que el proxy almacena un objeto en la caché, este guarda información log en el fichero parametrizado con la directiva *cache_store_log*. Por ejemplo,

```
cache_store_log /var/log/Squid/objetoscache.log
```

Página 263

Se elimina el número 3 tras Squid.

talado.

- El formato de los registros log será el de por defecto denominado *Squid*.
- La ruta con la actividad de los clientes se hará en /var/log/Squid/actividad.
- El nombre del archivo será accesos.log.
- La ruta de la caché será /var/log/Squid/cache.
- El nombre del archivo log de la caché será cache.log.

Indica las directivas que editar y el valor de cada una de las mismas, así como algún pro-

Para indicar la ruta del archivo de log con la actividad de los clientes, se emplea la directiva Access_log y el formato ya creado Squid:

```
access_log /var/log/Squid/actividad/accesos.log Squid
```

Para definir la ruta del log de la caché, se emplea la directiva cache_store:

```
access_log /var/log/Squid/cache/cache.log
```

```
/etc/init.d/Squid start
```

En el fichero squid.conf se puede localizar una variable denominada SQUID_ARGS. Esta variable permite configurar el modo en que el programa se ejecuta en segundo plano. Sus valores por defecto son –D –sYC, que deshabilitan los chequeos DNS iniciales, habilitan el registro de eventos y no atrapan las señales fatales.

Con el objetivo de detener Squid, se emplearán los scripts rc ejecutando

```
/etc/init.d/Squid stop
```

Página 264
Se elimina el número 3 tras Squid.

Cuando se van a realizar cambios en el fichero de configuración, y estos son significativos, se tiene que parar el servicio y arrancarlo de nuevo. Para ello, se usa el comando `/etc /init.d/Squid stop`.

Se añade la aclaración resaltada.

Lo primero que se tiene que hacer es identificar las diferentes listas de valores e indicar de qué tipo son, es decir, si una lista de valores se trata de direcciones IP, de puertos, de nombres de usuarios, de nombre de grupos de usuarios, de nombres de dominios, de direcciones URL, etc. Para especificar estos valores y darles un nombre se emplea la directiva ACL en la forma (escribir acl en minúsculas en la consola de comandos)

Página 266
Se corrigen los textos resaltados.

– Definiendo un rango de direcciones IP usando nomenclatura CIDR: `ACL equipos Ventas 192.168.143.1/24-192.168.143.30/24`.

Para los tres equipos de los jefes de la sala de ventas (dirección de red 192.168.2.0/24) se va a usar un rango de direcciones y la máscara de subred 255.255.255.0:

```
ACL jefesVentas src 192.168.2.73/24-192.168.2.75/24
```

Página 267
Se corrige el texto resaltado.

Elementos de ACL de tipo destino

- **Tipos dst y dstdomain:** dst permite indicar direcciones IP de destino, y dstdomain define dominios destino solicitas por el cliente. Ejemplo:

Página 268
Se corrigen los textos resaltados.

```
ACL direccionesIP src "/etc/Squid/direccionesIP.ACL"
```

Si una línea de valores ocupa más de una línea, se continúa en la siguiente sin necesidad de usar ningún indicador especial.

Para que la lista no discrimine entre mayúsculas y minúsculas, se usa el parámetro –i en la directiva ACL. Por ejemplo,

```
ACL metodosHTTP method -i POST CONNECT GET
```

Cuando existen dos listas ACL o más con el mismo nombre, no da como resultado un error, sino una lista resultante con dicho nombre y la unión de los valores de dichas listas. Por ejemplo, con la declaración de estas tres listas ACL,

```
ACL IP_aulaPrincipal src 192.168.143.64.64/26 192.168.144.143
ACL IP_aulaPrincipal src 192.168.143.64.129-145/26
ACL IP_aulaPrincipal src 192.168.143.64.200-233/26
```

el efecto resultante es el mismo que si se hubiera declarado la siguiente lista:

```
ACL IP_aulaPrincipal src 192.168.143.64.64/26 192.168.144.143
 192.168.143.64.129-145/26 192.168.143.64.200-233/26
```

Página 271
Se corrigen los textos resaltados.

Solución

Para el requerimiento uno, en el que solo los equipos de la sala de formación (192.168.1.0/24 y 192.168.2.0/24), informática (192.168.3.0/24) y dirección (192.168.8.0/24) pueden usar los protocolos ftp y telnet, se crea una lista con las tres subredes y otra con los puertos 21 y 23 (para los protocolos ftp y telnet). De esta manera, se obtienen las listas ACL siguientes:

```
ACL Req1Maq src 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24
                192.168.8.0/24
ACL Req1Puertos port 21 23
```

Las reglas de acceso serán permitir accesos desde esas máquinas si usan esos puertos. Las reglas que se obtienen son:

```
http_access allow Req1Maq Req1Puertos
```

Para el requisito dos, en las que las direcciones físicas de las tarjetas de red de los equipos que usan los jefes del departamento de informática, formación y dirección son 90:E1:7B:09:4C:DE, 90:E1:7B:3C:2A:2E y 90:E1:7B:BB:40:19, y estos pueden usar los métodos http get, post y connect, se creará una lista con las direcciones MAC y otra lista con los métodos que pueden usar. Las listas ACL que se obtienen son estas:

```
ACL req2MAC arp 90:E1:7B:09:4C:DE 90:E1:7B:3C:2A:2E 90:E1:7B:
                BB:40:19
ACL req2metodos methods GET POST CONNECT
```

Página 272
Se corrigen los textos resaltados.

```
ACL req4maquinas src 192.168.5.0/24 102.168.6.0/24 192.168.7.0/24
                     ACL puertohttps port 443
```

La regla http_access que se define para tal rango de IP, con dicho número de puerto y que permite el acceso, es

```
http_access allow req4maquinas puertohttps
```

Finalmente, se deniega todo el resto de conexiones. Para ello, se añade:

```
http_access deny all
```

El conjunto de listas de acceso de control (ACL) y reglas de accesos (http_access) se añade al final del fichero Squid.conf, teniendo especial cuidado con las listas y reglas que ya están definidas. El resultado final es el siguiente:

```
ACL Req1Maq src 192.168.1.0/24 192.168.2.0/24 192.18.3.0/24
192.168.8.0/24
ACL Req1Puertos port 21 23
ACL req2MAC arp 90:E1:7B:09:4C:DE 90:E1:7B:3C:2A:2E 90:E1:7B:
BB:40:19
ACL req2metodos methods GET POST CONNECT
ACL req3maquinas src 192.168.3.0/24
```

Unidad 8

Página 303
Se corrige el nombre de la herramienta.

Actividad propuesta 8.5

El uso de big data

Investiga sobre el tratamiento de Facebook y de Instagram en su almacenamiento de datos masivos, el uso de Hadoop como herramienta para la gestión de big data y los mecanismos para ofrecer seguridad a estos sistemas.

Crea una cuenta en Facebook y evalúa en el proceso de alta cómo te informa del tratamiento de tus datos personales y de los contenidos que subas a la plataforma.

Página 318
Se corrige el texto resaltado.

8.18. ¿Qué es un big data?