

## **EXAMEN 03/09/2024**

### ***DESCRIPCIÓN GENERAL DE LA PRÁCTICA:***

Esta actividad evaluable consiste en cuatro apartados.

- En el primero se solicita información de las máquinas Metasploitable2 y Metasploitable3 Linux y Windows.
- En el segundo utilizar la herramienta Wireshark para analizar el tráfico de red al arrancar las máquinas en la red.
- En la tercera se trata sobre riesgos y controles de seguridad.
- En la cuarta se trata sobre la normativa de protección de datos de carácter personal.

La actividad consta de 4 apartados:

1. Se pide que de la máquina Metasploitable muestres:
  - a. La información sobre la máquina (dirección IP, dirección MAC, etc.).
  - b. Los puertos y servicios abiertos.
  - c. Las vulnerabilidades.
2. Se pide:
  - a. Captura y guarda en un documento en texto plano ("ARP-DHCP") el tráfico de paquetes ARP y DHCP del proceso de arranque de todas las máquinas de tu laboratorio.
3. Se pide:
  - a. Describir 10 riesgos de seguridad.
  - b. Describir 10 controles de seguridad.
  - c. Determina el riesgo inherente y residual de cada uno de ellos.
  - d. Elabora matriz de riesgos inherente y residual.
  - e. Explica que riesgos son prioritarios de tratar.
4. Se pide:
  - a. Indicar la normativa aplicable para el tratamiento de datos de carácter personal.
  - b. Describir las figuras del delegado de Protección de Datos, responsable del Tratamiento y encargado del tratamiento. Elaborar un documento con la respuesta a los mismos.

## 1. METASPLOITABLE:

### a. La información sobre la máquina:

Con el siguiente comando “*ifconfig*”,

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c5:ab:27
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec5:ab27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5636 (5.5 KB)  TX bytes:6830 (6.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

observamos que nuestra **dirección IP (inet addr)** es la **10.0.2.4**, el **broadcast (Bcast)** es hasta la **10.0.2.255**, y la **máscara (Mask)** es la **255.255.255.0**

### b. Los puertos y servicios abiertos

Nos vamos a la máquina Kali Linux y ejecutamos el siguiente comando “*nmap -sV IP*”, en este caso nuestra IP es la 10.0.2.4.

```
jorgehallinux@jorgehallinux:~$ nmap -sV 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 11:12 WEST
Nmap scan report for 10.0.2.4
Host is up (0.001s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
35/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
112/tcp   open  rpcbind       2 (RPC #10000)
139/tcp   open  netbios-ssn   Samba smbd 3.0 - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.0 - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netatalk execd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-remote   GNU Classpath gmicregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2.4 (RPC #100003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3306/tcp  open  mysql         MySQL 5.0.51a-Subunto5
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6080/tcp  open  x11           (access denied)
6087/tcp  open  irc           UnrealIRCd
8080/tcp  open  ajp13         Apache Jserv (Protocol v2.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds
jorgehallinux@jorgehallinux:~$
```

### c. Las vulnerabilidades

Para detectar cuáles son las vulnerabilidades de la máquina, iniciamos Metasploit en Kali Linux con el comando “*msfconsole*”. Una vez entrado en Metasploit, realizamos un escaneo de ésta misma para detectar vulnerabilidades conocidas. Después del escaneo, se pueden usar módulos específicos de Metasploit para explotar o detectar vulnerabilidades en los servicios identificados.

Estos son los siguientes comandos para realizar el escaneo (“*use auxiliary/scanner/portscan/tcp*”, “*set RHOSTS IP*”, “*run*”):

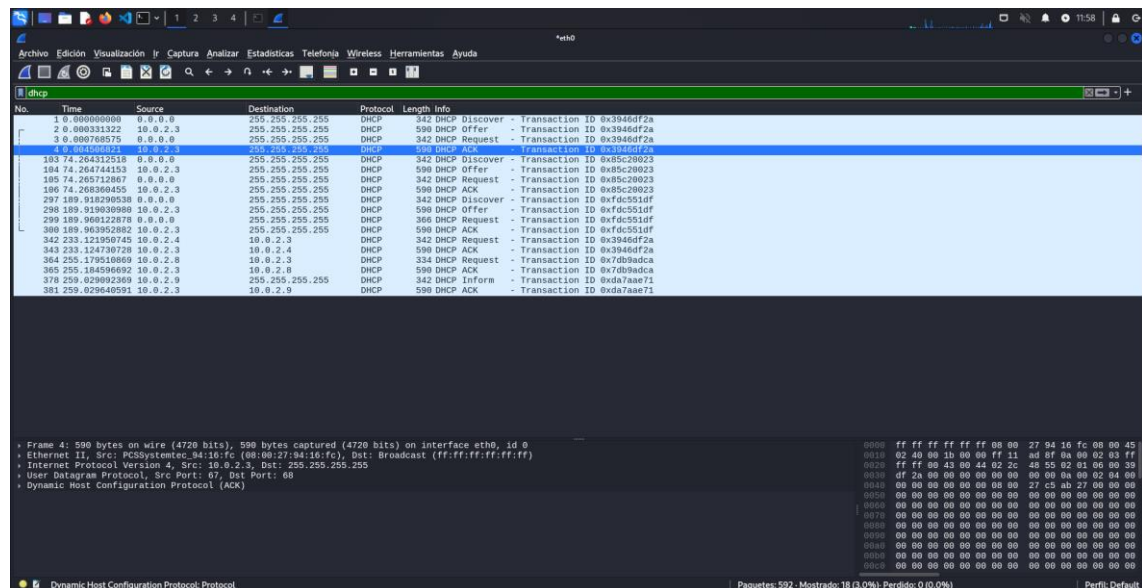
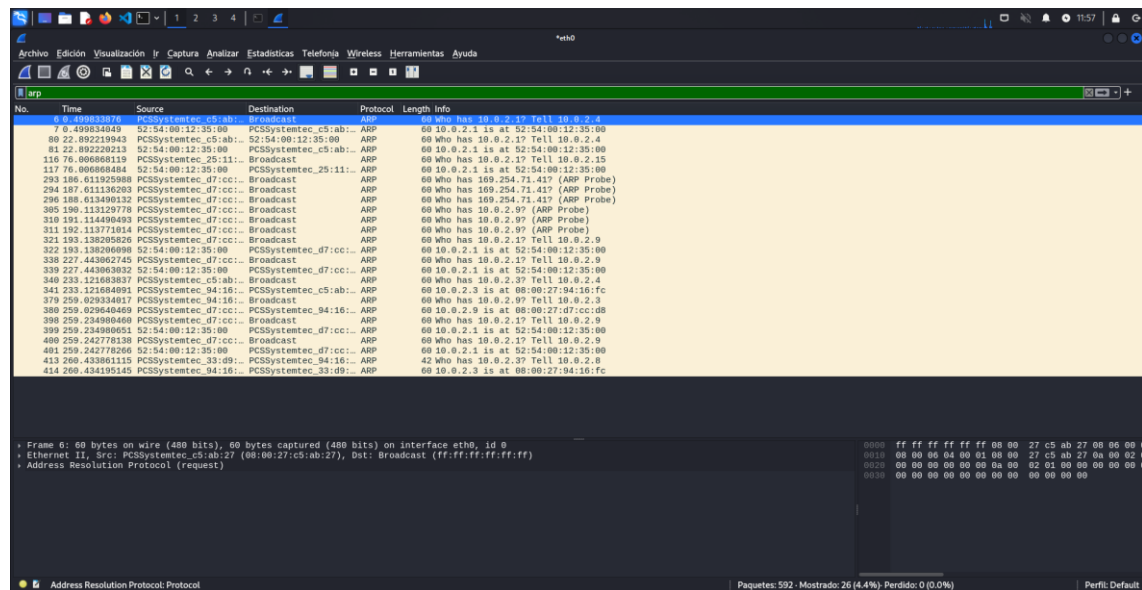
```
jorgehallinux@jorgehallinux:~$ msfconsole
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf5 auxiliary(scanner/portscan/tcp) > run

10.0.2.4: - 10.0.2.4:25 - TCP OPEN
10.0.2.4: - 10.0.2.4:23 - TCP OPEN
10.0.2.4: - 10.0.2.4:21 - TCP OPEN
10.0.2.4: - 10.0.2.4:22 - TCP OPEN
10.0.2.4: - 10.0.2.4:33 - TCP OPEN
10.0.2.4: - 10.0.2.4:80 - TCP OPEN
10.0.2.4: - 10.0.2.4:111 - TCP OPEN
10.0.2.4: - 10.0.2.4:139 - TCP OPEN
10.0.2.4: - 10.0.2.4:445 - TCP OPEN
10.0.2.4: - 10.0.2.4:513 - TCP OPEN
10.0.2.4: - 10.0.2.4:512 - TCP OPEN
10.0.2.4: - 10.0.2.4:514 - TCP OPEN
10.0.2.4: - 10.0.2.4:1099 - TCP OPEN
10.0.2.4: - 10.0.2.4:1524 - TCP OPEN
10.0.2.4: - 10.0.2.4:2049 - TCP OPEN
10.0.2.4: - 10.0.2.4:2121 - TCP OPEN
10.0.2.4: - 10.0.2.4:3306 - TCP OPEN
10.0.2.4: - 10.0.2.4:5432 - TCP OPEN
10.0.2.4: - 10.0.2.4:5900 - TCP OPEN
10.0.2.4: - 10.0.2.4:6080 - TCP OPEN
10.0.2.4: - 10.0.2.4:6087 - TCP OPEN
10.0.2.4: - 10.0.2.4:8080 - TCP OPEN
10.0.2.4: - 10.0.2.4:8087 - TCP OPEN
10.0.2.4: - 10.0.2.4:8180 - TCP OPEN
10.0.2.4: - 10.0.2.4:8187 - TCP OPEN
10.0.2.4: - Scanned 1 of 0 hosts (100% complete)
Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/tcp) >
```

## 2. WIRESHARK:

Para realizar este ejercicio, he encendido 3 máquinas: Kali Linux (para comprobar con Wireshark), Metasploitable2 de Linux y Metasploitable3 de Windows.

Ejecutamos Wireshark y vemos ARP y DHCP:



## 3. RIESGOS Y CONTROLES DE SEGURIDAD:

10 riesgos de seguridad:


10 controles de seguridad:

Riesgo inherente y residual de cada uno de ellos:

Matriz de riesgos inherente y residual:

=BUSCAR(BUSCARV(F11;Impacto!\$A\$3:\$B\$7;2;0)*BUSCARV(G11;Prioridad!\$A\$2:\$B\$6;2;0);Riesgo!\$A\$12:\$A\$15;Riesgo!\$B\$12:\$B\$15)										
Código	Activo	Tipos de activo	Amenaza	Tipos de amenaza	Impacto	Probabilidad	Riesgo potencial			
001	Personal de Dirección	Personal, Infraestructura de redes físicas	Ciberataque	Ataque, interceptación, Modificación, destrucción de la información	CRÍTICO	ALTA	18-18	CRÍTICA	ALTA	CRÍTICA
002	Personal de Dirección	Personal, Infraestructura de redes físicas	Fuga de información	Fuga de datos, interceptación, Detección de espionaje de información	CRÍTICO	MODERADA	17-17	CRÍTICA	MODERADA	CRÍTICA
003	Servidor web	Personal, Servidor web	Denegación de servicios	Ataque, interceptación, Denegación de servicios, Interrupción del sistema informático	CRÍTICO	MODERADA	10	CRÍTICA	MODERADA	CRÍTICA
004	CDP	Infraestructura, Centro	Acceso no autorizado	Fuga de datos, interceptación, Acceso no autorizado de la información	CRÍTICO	MODERADA	17-17	CRÍTICA	MODERADA	CRÍTICA
005	Aplicación web	Software, Aplicaciones informáticas, Sistema de gestión	Intervención	Ataque, interceptación, Denegación de servicios, Interrupción del sistema informático	CRÍTICO	MODERADA	10	CRÍTICA	MODERADA	CRÍTICA
006	Base de datos	Personal, Almacenamiento de ficheros	Intervención	Ataque, interceptación, Acceso no autorizado, Fuga de datos, Interceptación	CRÍTICO	ALTA	18-18	CRÍTICA	ALTA	CRÍTICA
007	Equipo de trabajo	Equipo personal, Personal, Gestión de recursos	Intervención	Fuga de datos, interceptación, Detección de espionaje de información	CRÍTICO	MODERADA	17-17	CRÍTICA	MODERADA	CRÍTICA
008	Red corporativa	Software, Información, Redes de gestión interna	Intervención de servicios	Ataque, interceptación, Denegación de servicios, Interrupción del sistema informático	CRÍTICO	ALTA	18-18	CRÍTICA	ALTA	CRÍTICA
009	Información de clientes	Software, Aplicaciones informáticas, Servicio de correo electrónico	Fuga de datos	Ataque, interceptación, Acceso no autorizado, Uso no autorizado del hardware	CRÍTICO	MODERADA	17-17	CRÍTICA	MODERADA	CRÍTICA
010	Servidor de archivos	Servicio, Almacenamiento de ficheros	Intervención de datos	Fuga de datos, interceptación, Alteración accidental de la información	CRÍTICO	MODERADA	17-17	CRÍTICA	MODERADA	CRÍTICA
011										
012										
013										
014										
015										
016										
017										
018										
019										
020										
021										
022										
023										
024										
025										
026										
027										
028										
029										
030										
031										
032										
033										
034										
035										
036										
037										
038										
039										
040										
041										
042										
043										
044										
045										
046										
047										
048										
049										
050										
051										
052										
053										
054										
055										
056										
057										
058										
059										
060										
061										
062										
063										
064										
065										
066										
067										
068										
069										
070										
071										
072										
073										
074										
075										
076										
077										
078										
079										
080										
081										
082										
083										
084										
085										
086										
087										
088										
089										
090										
091										
092										
093										
094										
095										
096										
097										
098										
099										
100										
101										
102										
103										
104										
105										
106										
107										
108										
109										
110										
111										
112										
113										
114										
115										
116										
117										
118										
119										
120										
121										
122										
123										
124										
125										
126										
127										
128										
129										
130										
131										
132										
133										
134										
135										
136										
137										
138										
139										
140										
141										
142										
143										
144										
145										
146										
147										
148										
149										
150										
151										
152										
153										
154										
155										
156										
157										
158										
159										
160										
161										
162										
163										
164										
165										
166										
167										
168										
169										
170										
171										
172										
173										
174										
175										
176										
177										
178										
179										
180										
181										
182										
183										
184										
185										
186										
187										
188										
189										
190										
191										
192										
193										
194										
195										
196										
197										
198										
199										
200										
201										
202										
203										
204										
205										
206										
207										
208										
209										
210										
211										
212										
213										
214										

IMPACTO

RIESGO RESIDUAL					
PROBABILIDAD	10	MUY ALTA			
	8	ALTA			
	6	MODERADA		006	003
	3	BAJA	001, 002, 004, 009, 010		
	1	MUY BAJA	007, 008	005	
RIESGO		MÍNIMO	LEVE	MEDIO	CRÍTICO
		1	3	6	30
IMPACTO					
					

Estadísticas del libro: Promedio: 5,6 Cuenta: 56 Suma: 36 100%

Pruebas de respaldo

#	A	B	C	D	E	F	G	H	I	J	K	L
#	Activo	Ataque	Medio	Problema	Prioridad	Antivirus (Salvaguarda)	Intervención	Resolución	Responsable	Fecha inicio	Fecha fin	Comentario
001	Portal de Dirección	Ciberataque	Aceptable	Alarma	Sistema de alarma	Sistema de alarma	Sistema de alarma	Sistema de alarma	Sistema de alarma	01/09/2024	01/12/2024	Configuración avanzada
002	Portal de Dirección	Fuga de información	Aceptable	Antivirus	Software anti-malware	Software anti-malware	Software anti-malware	Software anti-malware	Software anti-malware	01/09/2024	01/12/2024	Incluye formación
003	Servidor web	Denegación de servicios	Tolerable	Sistema de prevención de ataques	Mitigación de ataques DDoS	Mitigación de ataques DDoS	Mitigación de ataques DDoS	Mitigación de ataques DDoS	Mitigación de ataques DDoS	01/09/2024	01/12/2024	Configuración avanzada
004	CFO	Acceso no autorizado	Aceptable	Vigilante	Vigilancia física	Vigilancia física	Vigilancia física	Vigilancia física	Vigilancia física	01/09/2024	01/12/2024	Vigilancia 24/7
005	Aplicación web	Intrusión	Aceptable	Firewall y monitoreo de aplicaciones	Protección con firewall y monitoreo	Protección con firewall y monitoreo	Protección con firewall y monitoreo	Protección con firewall y monitoreo	Protección con firewall y monitoreo	01/09/2024	01/12/2024	Configuración continua
006	Base de datos	Intrusión	Aceptable	Encriptación de base de datos	Software de en Base de datos	Software de en Base de datos	Software de en Base de datos	Software de en Base de datos	Software de en Base de datos	01/09/2024	01/12/2024	Claves actualizadas
007	Estación de trabajo	Malware	Aceptable	Antivirus y formación continua	Antivirus y formación para usuarios	Antivirus y formación para usuarios	Antivirus y formación para usuarios	Antivirus y formación para usuarios	Antivirus y formación para usuarios	01/09/2024	01/12/2024	Actualizaciones periódicas
008	Red corporativa	Interrupción de servicio	Aceptable	Redundancia y respaldo	Respaldo y redundancia	Respaldo y redundancia	Respaldo y redundancia	Respaldo y redundancia	Respaldo y redundancia	01/09/2024	01/12/2024	Pruebas periódicas
009	Sistema de correo	Phishing	Tolerable	Formación y filtros de spam	Filtros de spam y formación	Filtros de spam y formación	Filtros de spam y formación	Filtros de spam y formación	Filtros de spam y formación	01/09/2024	01/12/2024	Revisión semestral
010	Servidor de archivos	Pérdida de datos	Tolerable	Respaldo regular de los datos	Respaldo de datos	Respaldo de datos	Respaldo de datos	Respaldo de datos	Respaldo de datos	01/09/2024	01/12/2024	Pruebas de respaldo
011	0	0	0	0	0	0	0	0	0	0	0	0
012	0	0	0	0	0	0	0	0	0	0	0	0
013	0	0	0	0	0	0	0	0	0	0	0	0
014	0	0	0	0	0	0	0	0	0	0	0	0
015	0	0	0	0	0	0	0	0	0	0	0	0
016	0	0	0	0	0	0	0	0	0	0	0	0
017	0	0	0	0	0	0	0	0	0	0	0	0
018	0	0	0	0	0	0	0	0	0	0	0	0
019	0	0	0	0	0	0	0	0	0	0	0	0
020	0	0	0	0	0	0	0	0	0	0	0	0
021	0	0	0	0	0	0	0	0	0	0	0	0
022	0	0	0	0	0	0	0	0	0	0	0	0
023	0	0	0	0	0	0	0	0	0	0	0	0
024	0	0	0	0	0	0	0	0	0	0	0	0
025	0	0	0	0	0	0	0	0	0	0	0	0
026	0	0	0	0	0	0	0	0	0	0	0	0
027	0	0	0	0	0	0	0	0	0	0	0	0
028	0	0	0	0	0	0	0	0	0	0	0	0
029	0	0	0	0	0	0	0	0	0	0	0	0
030	0	0	0	0	0	0	0	0	0	0	0	0
031	0	0	0	0	0	0	0	0	0	0	0	0

Estadísticas del libro: Promedio: 45576,5 Cuenta: 122 Suma: 911570 100%

Riesgos que son prioritarios de tratar: **001, 006, 008**.

Estos riesgos se encuentran en la zona de muy alta probabilidad y alto impacto, lo que los convierte en la mayor preocupación y tratar lo antes posible.

#### 4. NORMATIVA APLICABLE PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL:

La normativa que regula el tratamiento de datos personales en España ha experimentado cambios significativos en los últimos años, buscando garantizar la protección de los derechos de las personas físicas en relación con el tratamiento de sus datos. Las normas son las siguientes:

- **Reglamento General de Protección de Datos (RGPD):** Este reglamento europeo (UE) 2016/679 es directamente aplicable en todos los estados miembros de la Unión Europea, incluyendo

España. Establece un marco jurídico común y elevado para la protección de los datos personales.

- **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** Esta ley española (Ley Orgánica 3/2018) adapta el RGPD al ordenamiento jurídico español y desarrolla algunos aspectos específicos.

La normativa implica lo siguiente:

- **Principios:** Establece principios fundamentales como la licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad, así como la responsabilidad proactiva del responsable del tratamiento.
- **Derechos de los interesados:** Reconoce y garantiza los derechos de los individuos sobre sus datos, como el derecho de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos.
- **Obligaciones de los responsables del tratamiento:** Impone diversas obligaciones a quienes tratan datos personales, como la realización de evaluaciones de impacto, la designación de un delegado de protección de datos en determinados casos, la notificación de brechas de seguridad, etc.

### **Figuras del delegado de Protección de Datos, responsable del tratamiento y encargado del tratamiento**

Dentro del marco normativo de protección de datos, encontramos tres figuras clave:

<b>FIGURA</b>	<b>RESPONSABILIDADES PRINCIPALES</b>
Delegado de Protección de Datos	<p>Figura obligatoria en determinadas organizaciones. Actúa como un punto de contacto interno y externo en materia de protección de datos.</p> <p>Asesoramiento, supervisión, cooperación con la autoridad de control, etc.</p>
Responsable del tratamiento	<p>Persona física o jurídica, autoridad pública, servicio u organismo que, individualmente o conjuntamente con otros, determina los fines y medios del tratamiento de datos personales.</p> <p>Determinación de los fines y medios del tratamiento, garantía del cumplimiento de la normativa.</p>
Encargado del tratamiento	<p>Persona física o jurídica, autoridad pública, servicio u organismo que trata datos personales por cuenta del responsable del tratamiento.</p> <p>Tratamiento de datos por cuenta del responsable, bajo sus instrucciones.</p>