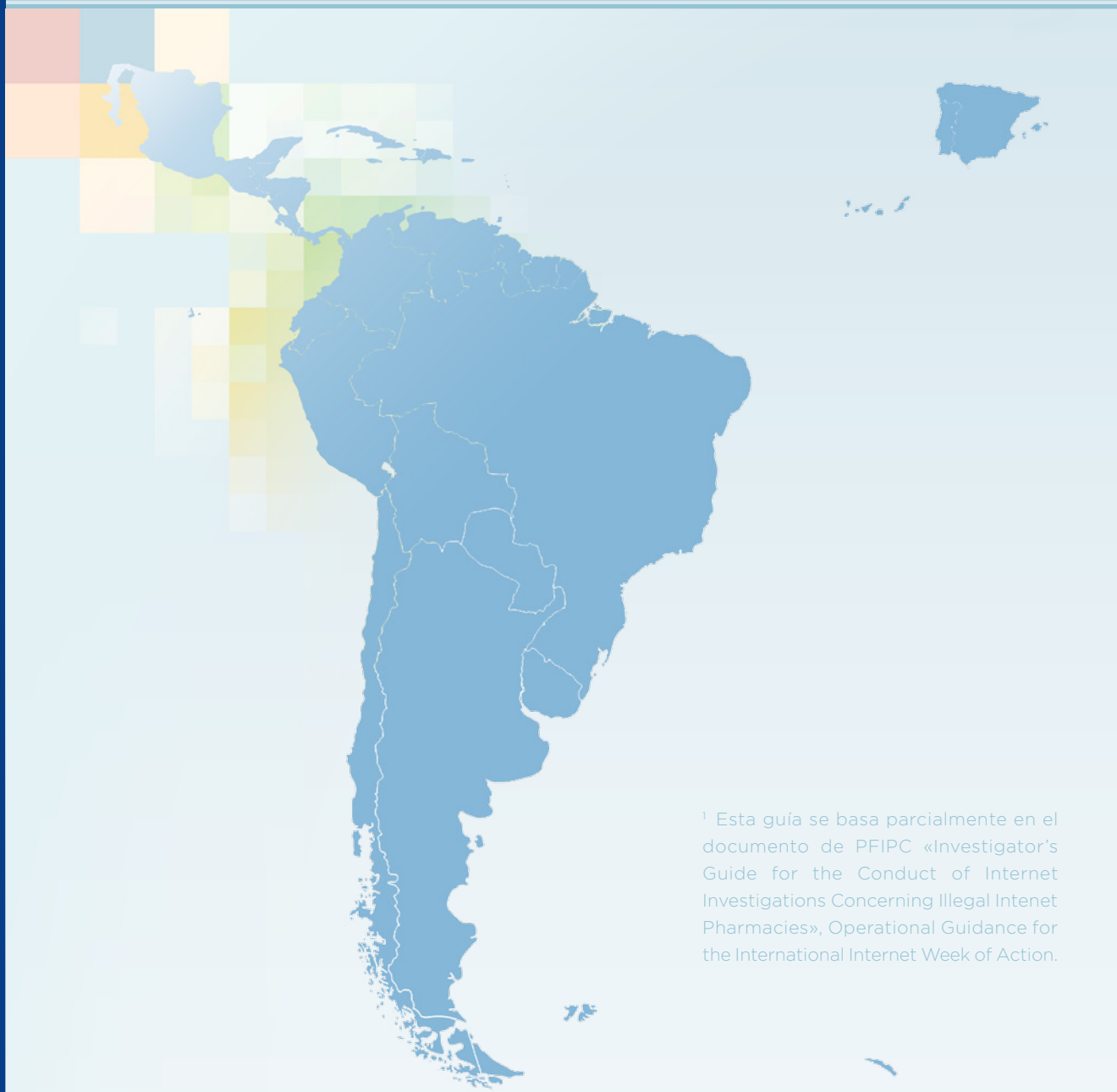


# GUÍA BÁSICA DE INVESTIGACIONES sobre la venta a través de Internet, de medicamentos falsificados o fraudulentos<sup>1</sup>



<sup>1</sup> Esta guía se basa parcialmente en el documento de PFIPC «Investigator's Guide for the Conduct of Internet Investigations Concerning Illegal Internet Pharmacies», Operational Guidance for the International Internet Week of Action.

**Edita y distribuye**

**Red EAMI [www.redeami.net](http://www.redeami.net)**

**Revisado por:** Red PUCs Sistema FALFRA

**En:** Cartagena de Indias, Colombia 11 al 15 de mayo 2015

**Aprobado por:** Secretariado de la Red EAMI

**Fecha de aprobación:** 16 de diciembre de 2015

**Fecha de publicación web:** Septiembre 2016

**Version 1.0**



# ÍNDICE

<b>1. INTRODUCCIÓN Y OBJETIVO</b>	<b>3</b>
<b>2. ESTRUCTURA DE INTERNET, ELEMENTOS BÁSICOS</b>	<b>4</b>
<b>3. HARDWARE Y SOFTWARE NECESARIO</b>	<b>5</b>
<b>4. IDENTIFICAR UNA FARMACIA EN LÍNEA FRAUDULENTA</b>	<b>7</b>
Características y elementos comunes que ayudan a identificar farmacias en línea fraudulentas	<b>7</b>
<b>5. IDENTIFICAR A LOS RESPONSABLES</b>	<b>9</b>
<b>6. COMPRA DE PRUEBA EN SITIOS WEB FRAUDULENTOS</b>	<b>12</b>
<b>7. SEGUIR LA TRANSACCIÓN</b>	<b>13</b>
<b>8. OFERTA DE MEDICAMENTOS EN PORTALES DE VENTA</b>	<b>14</b>
Glosario	15
Anexo 1. Flujograma	18
Anexo 2. <i>Check list</i> de investigación de una web	19



# 1. INTRODUCCIÓN Y OBJETIVO

La expansión de las nuevas tecnologías, como es Internet, ha incrementado los flujos de información y ha dado lugar a nuevas aplicaciones comerciales. Una de las consecuencias de esta amplia red de comunicación es el crecimiento sostenido que viene experimentando el comercio electrónico. Entre otros productos y servicios que se ofertan y se comercializan a través de Internet, están los medicamentos u otros productos relacionados con la salud (complementos alimenticios o productos sanitarios, entre otros productos de uso y consumo humano).

El propósito de esta guía es poder servir a las autoridades competentes como manual básico y de referencia para la investigación de sitios web que puedan estar promocionando y/o vendiendo medicamentos u otros productos falsificados o fraudulentos.

Sin embargo, estas actuaciones están condicionadas tanto por la normativa que regula la venta de medicamentos en cada país como por la capacidad de actuación o investigación que la referida normativa atribuya a las autoridades competentes.

Existen países cuya legislación permite la venta a través de Internet de medicamentos. Sin embargo, en otros países, la venta a distancia a través de Internet, de medicamentos o de algunos tipos de medicamentos (p.e. aquellos sujetos a prescripción médica) está sometida a ciertas restricciones legales. Cuando la venta de medicamentos o de ciertas categorías de medicamentos (p.e. medicamentos no sujetos a prescripción u OTC) esté permitida, existe, generalmente, una normativa que establece los requisitos que debe cumplir esta venta al público o las condiciones para su importación.

En todo caso, las actuaciones y medidas que puede adoptar cada autoridad vendrán determinadas por la capacidad y competencias, atribuidas por la normativa, en la lucha contra la venta de medicamentos falsificados o fraudulentos a través de Internet.

La constante evolución del comercio electrónico de productos relacionados con la salud nos obliga a adoptar nuevas estrategias de investigación y medidas de control de mercado, dentro del marco que establece el sistema normativo y de competencias vigente en cada país.



## 2. ESTRUCTURA DE INTERNET, ELEMENTOS BÁSICOS

Para realizar investigaciones básicas es necesario entender algunos conceptos sobre la estructura y funcionamiento de Internet. En el Glosario, al final del presente procedimiento, se han incluido algunos de estos conceptos.

Internet es una red de redes; un conjunto de redes interconectadas en las que no existe un nodo central, sino una multitud de conexiones. Cada ordenador que se conecta a Internet se identifica con una dirección IP, formada por un grupo de 4 números entre 0 y 255 separados por puntos (p.e. 123.146.2.34). En la mayoría de los casos, este número lo asigna la compañía que es proveedor del servicio de conexión a Internet y puede ser fijo (invariable) o cambiar y ser reasignado periódicamente por el servidor del proveedor de servicios de acceso.

Los sitios web a los que accedemos están físicamente alojados en ordenadores llamados servidores. Cuando tecleamos una dirección URL (p.e. [www.aemps.gob.es](http://www.aemps.gob.es)), dicha dirección debe «traducirse» a una dirección IP (la del ordenador donde se aloje el sitio) para que nuestro equipo pueda acceder al mismo. Esta «traducción» se realiza a través de servidores específicos (servidores DNS o *Domain Name Servers*).



### 3. HARDWARE Y SOFTWARE NECESARIO

Las investigaciones de sitios web requieren disponer de un equipo conectado a Internet y de software, que puede llegar a ser muy especializado. En este procedimiento se propone únicamente el empleo de software gratuito y acceso a bases de datos que no conllevan coste.

Para las investigaciones de sitios web que realizan ventas ilegales es recomendable disponer del siguiente equipo:

- Un ordenador con una dirección IP dinámica, independiente y separado del resto de los ordenadores de la institución en la que trabajemos. De esta manera, el responsable del sitio Web investigado, no vinculará la dirección IP del equipo con la institución desde la que se acceda. Este número es visible para los operadores de sitios web a los que conectamos y puede identificar a ordenadores que se conectan desde redes institucionales. Cuando navegamos por Internet, el responsable del sitio web sabe desde qué nodo accedemos y dejamos un rastro de visita revelando un acceso desde una red de la agencia o web ministerial.

Esto permitiría (al menos teóricamente) al titular del sitio web solo bloquearnos el acceso, o redirigirnos a determinadas páginas Web. Por ejemplo, se han visto casos en que, tras un primer acceso desde un ordenador de la red institucional, se ha retirado el sitio web tras identificarse la dirección IP.

Si se quiere echar un vistazo a una página de un sitio Web sin revelar la identidad, puede acudir al cache de Google<sup>1</sup>. Google rastrea la Web y toma periódicamente instantáneas de cada página. Las páginas almacenadas pasan así a formar parte de la «caché» de Google.

- Impresora conectada al ordenador (preferiblemente de color).



<sup>1</sup> Para ver cómo acceder a las páginas en caché de Google: <https://support.google.com/websearch/answer/1687222?hl=es>, acceso 20/02/2015.

- Tener a disposición dispositivos de almacenamientos de datos, como por ejemplo, un disco duro externo o una grabadora de DVD/CD, necesarios para guardar descargas de la página o elementos de prueba.

Con un software adecuado se podrá hacer registro de todas las acciones de vigilancia realizadas:

- Realizar una descarga del sitio web investigado para examinarlo off-line o fuera de conexión. Se pueden utilizar, entre otros, programas gratuitos como WinHTTrackWebsite-Copier: [www. HTTrack.com](http://www.HTTrack.com).
- La información sobre el ranking que ocupa el sitio Web, el porcentaje de personas que la visitan, y desde qué países lo hacen, se pueden consultar en páginas web como: [www. alexa.com](http://www.alexa.com).
- Alternativamente a disponer de un ordenador independiente, para acceder a los sitios web ilícitos de forma anónima puede navegarse a través de servidores o proxys que anonimizan la navegación al ocultar nuestra identidad IP. De esta manera, el Web master del sitio Web investigado no nos identifica, por ejemplo: navegación web a través del portal [www.anonymouse.org](http://www.anonymouse.org) o de [www.collegeproxy.us](http://www.collegeproxy.us).
- Tener actualizado el Antivirus en el ordenador, así como el Firewall y el software anti-spyware si se dispone de él.
- Si queremos ver versiones antiguas de la Web, y ver los cambios que se han introducido, podemos consultar «Wayback Machine» en <https://archive.org/web/web.php>, en el que podremos encontrar capturas automáticas de versiones anteriores de algunas de las páginas web que investiguemos.



En algunos casos, solo podemos reunir pruebas del sitio web que está vendiendo sólo o únicamente medicamentos falsificados o fraudulentos si nos registramos, o incluso, si simulamos realizar un pedido de medicamentos, siempre que lo permita la normativa nacional (tener en cuenta la inducción al delito). Comenzar con el proceso de compra de manera simulada es fundamental si queremos saber, por ejemplo, si la página en la que estamos realmente vende o nos redirige a otra u otras páginas. En estos casos, es útil crear distintas identidades de posibles compradores con cuentas en servidores de correo gratuitos (tipo Gmail o Outlook) para los supuestos en los que se realicen intentos de compra de productos. Es importante documentar todo el proceso de compra simulada (p.ej. mediante «pantallazos» o capturas dinámicas de pantalla, impresión de correos...).

## 4. IDENTIFICAR UNA FARMACIA EN LÍNEA FRAUDULENTA

La investigación puede comenzar motivada por una denuncia; en otros casos, es la autoridad la que puede realizar una búsqueda de sitios web que vendan medicamentos no autorizados o fraudulentos que no deban ofertarse por medios telemáticos. Para ello utilizamos buscadores como Google o Bing, definiendo las palabras clave de búsqueda necesarias. Existen buscadores automáticos configurables (*Web crawlers* o *Web spiders*) disponibles comercialmente.

Muchas veces es necesario filtrar o restringir la búsqueda (p.ej. páginas en español, o con el dominio del país de interés en la investigación). Es aconsejable conocer los criterios de filtrado que ofrecen los distintos buscadores<sup>2</sup>.

### CARACTERÍSTICAS Y ELEMENTOS COMUNES QUE AYUDAN A IDENTIFICAR FARMACIAS EN LÍNEA FRAUDULENTAS.

Estos son algunos de los elementos que pueden ayudarnos en la identificación de sitios web que realizan venta ilícita de medicamentos o productos falsificados o fraudulentos (siempre de acuerdo con la legislación nacional):

- La dirección que se facilita en la información de contacto del sitio Web o en las condiciones generales de uso es falsa o no facilita ninguna información sobre los responsables. Solo ofrece un formulario de contacto electrónico.
- El número de teléfono que se facilita en la información de contacto del sitio web o en las condiciones de uso parece falso o redirige a otro teléfono.
- El sitio web tiene errores ortográficos y/o gramaticales en la traducción que lo hacen sonar extraño. Esto puede ser consecuencia de que el diseñador del sitio web se ubique en otro país.



<sup>2</sup> P. ej. para Google:

[https://support.google.com/websearch/answer/2466433?hl=es&ref\\_topic=3081620](https://support.google.com/websearch/answer/2466433?hl=es&ref_topic=3081620)  
y <https://support.google.com/websearch/answer/142143?hl=es>



- El sitio web usa spam para promocionarse.
- El sitio web no dispone de un sistema de pago electrónico seguro o el pago se realiza a través de transferencia o por un depósito a cuenta bancaria, Western Union o Moneygram.
- El sitio web oferta única o principalmente lo que se conocen como «lifestyle-drugs», medicamentos para el estilo de vida (adelgazantes, medicamentos para la disfunción eréctil, hipnóticos, anabolizantes, abortivos anticonceptivos y otros) o que ofrecen información sesgada, exagerada, confusa o errónea sobre los medicamentos.
- El sitio web oferta medicamentos que requieren receta médica contraviniendo la normativa nacional.
- En el sitio web, se presenta información que afirma, entre otros, lo siguiente: *«medicamentos científicamente probados», refiere a «un descubrimiento científico», «tratamientos milagrosos», «productos exclusivos», «los medicamentos/productos no cuentan con efectos adversos», aportan testimonios de clientes o gente famosa curados exitosamente o el testimonio del investigador que patentó el medicamento, entre otros.*



## 5. IDENTIFICAR A LOS RESPONSABLES

El titular de un **sitio web** es el responsable de la actividad ilícita que en el mismo se desarrolle. En la Unión Europea, la normativa obliga a que el titular de un sitio web muestre en el mismo toda la información para permitir su identificación y datos de contacto; no obstante, los titulares de sitios web que venden medicamentos falsificados o fraudulentos incumplen sistemáticamente esta obligación. A veces esta información no se muestra en la página principal, pero sí puede estar en otras secciones de la página (p. ej. «Condiciones legales»).

A pesar de que con frecuencia estos datos no se encuentran en el sitio web, a veces se muestra una dirección de correo electrónico o un número de teléfono. La búsqueda en Google con estos datos, puede dar como resultado otras web o anuncios donde sí figure una identidad o una dirección.

En caso de que no aparezca ningún tipo de información en el sitio web la identificación del titular puede realizarse a través de bases de datos de acceso público, tipo WHOIS de la ICANN o a través de las autoridades que conceden los nombres de dominio nacionales (p. ej. RED. ES para los dominios. ES).

Es importante conocer al organismo responsable de los dominios de nivel nacional en cada país a fin de poder gestionar estas acciones y solicitar su colaboración a la hora de cancelar nombres de dominio (p.ej. si se han registrado empleando una información falsa).

En el modelo de información remitida por la autoridad de nombre de dominio, se facilitan, entre otros, los datos del titular que tiene el derecho de uso y utilización de un nombre de dominio «.XX». Así mismo se remite la información sobre la persona de contacto administrativo que contará con poder de representación en relación con los derechos de uso del nombre de dominio; los datos de la persona de contacto de facturación que tiene atribuida las funciones relacionadas con el pago de las cantidades correspondientes a las tarifas de asignación y renovación del nombre de dominio.es y finalmente la persona de contacto técnico encargada de los aspectos técnicos relacionados con la configuración y operativa del nombre de dominio.



En caso de tratarse de un dominio «.com» o de otro tipo, se utiliza la base de datos WHOIS de la ICANN: <http://whois.icann.org/es>, que es de acceso público, y, facilita los datos de identificación y contacto del responsable del sitio web, así como los datos de los contactos técnicos y administrativos. Por ejemplo, si hacemos una búsqueda WHOIS de la web <http://www.redeami.net> podemos averiguar que:

- Está registrada por el Ministerio de Sanidad y Política Social, y podemos consultar los datos de su dirección.
- Su dirección IP (195.64.186.72), que está, además, en un servidor dedicado (solo aloja esta web) y localizado en Madrid.

En el supuesto de que se tratara de una persona jurídica y no se aporte la información necesaria para realizar una notificación, se puede solicitar la colaboración del Registro Mercantil correspondiente que remite la información disponible en el mismo.

Además, con la dirección IP podemos ubicar dónde se aloja el servidor <http://www.iplocation.net/> y también saber cuál es la dirección IP del equipo desde el que estamos accediendo a internet.

En ocasiones estas bases de datos no nos facilitan ningún tipo de información sobre el titular del dominio.com porque existen empresas constituidas para proteger los datos personales de los titulares. Como resultado de la actividad de estas empresas se mantiene en el anonimato al titular del dominio.com y la dirección, teléfono y demás información que se aporta, en estas bases de datos de acceso público, son los que corresponden a la empresa. En ocasiones podemos plantearnos dirigirnos a estas empresas para que cancelen el registro del nombre de dominio si la actividad de la página supone una infracción de sus términos legales o condiciones de uso.

En otras ocasiones no ha sido posible identificar al titular de la web, o este se encuentra fuera de nuestro territorio, o la web se encuentra alojada en un servidor que no está a nuestro alcance. En estos casos no es posible tomar una medida directa contra la misma (su retirada o cancelación), pero aún puede ser posible acudir a los proveedores de acceso a redes (Glosario). Estas empresas dan acceso a Internet a los usuarios finales y disponen de mecanismos para impedir o bloquear el acceso a determinados URLs. Este bloqueo no es efectivo en todos los casos, ya que solo afecta a los clientes de los proveedores de acceso que procedan al bloqueo; además, puede evitarse si se emplean conexiones indirectas (a través de servidores proxys). No obstante, es una medida útil cuando no pueden adoptarse otras.



Una vez conocida esta información, se pueden considerar diversas opciones, dependiendo de la legislación nacional y de las ubicaciones de los responsables de los sitios web:

- Dirigir un escrito requiriendo, al titular del sitio web, la suspensión del servicio. Esto será posible cuando haya sido posible su identificación y el titular se ubique en nuestro país. Podemos igualmente considerar solicitar a otro país la colaboración para que se dirija al titular que se ubique en dicho país, por si fuera posible actuar en base a la jurisdicción local. Esta comunicación se realizará, salvo que se determine otra cosa, al punto de contacto único, dentro de la red EAMI.
- Cuando el registro de un sitio web se haya realizado a través de una empresa, podemos dirigir un requerimiento a la empresa registradora, con posibilidades de éxito si la actividad de la web infringe los términos legales de la compañía registradora (p.ej. infracción de derechos de patente, productos que pongan en riesgo la salud pública).
- Dirigir un requerimiento al servidor que aloja el sitio web, si éste se ubica en nuestro territorio, para que retire el sitio o impida el acceso al mismo.
- Compromiso de comunicar al país de la Red EAMI.
- Mercado libre e identificar al nombre de dominio nacional.



## 6. COMPRA DE PRUEBA EN SITIOS WEB FRAUDULENTOS

Un trámite importante en la investigación de un sitio web es la verificación y comprobación de que efectivamente se realiza la venta telemática de medicamentos no autorizados<sup>3</sup>.

Para obtener una prueba de compra es recomendable crear un perfil de usuario ficticio. Se deben utilizar sistemas o métodos que permitan al investigador realizar una compra sin que sea identificado y poder así recopilar las pruebas de la venta ilícita.

Para ello deben guardarse/archivarse cada uno de los pasos que se siguen a lo largo de la compra y en todo caso:

No se debe utilizar el ordenador de la institución. Tendremos a disposición un ordenador con una I. P. que no permita la identificación.

No utilizar como dirección de entrega la dirección de la institución o Autoridad.



<sup>3</sup> En algunos países la compra puede ser considerada instigación al delito, por lo que deberá evaluarse esta posibilidad.

## 7. SEGUIR LA TRANSACCIÓN

El seguimiento de la transacción económica o financiera es uno de los métodos más eficientes para identificar al titular de un sitio web que realiza una actividad ilícita. Sin embargo la posibilidad de utilizar este método depende o queda condicionado por la capacidad que tenga atribuida la autoridad competente.

Los titulares de sitios web ilícitos tienen como objetivo obtener un beneficio económico: dinero; y por ello para ganarse la confianza de los consumidores y usuarios presentan sus sitios web como si fueran lícitos utilizando sistemas de pago como: tarjetas de crédito, transferencias de dinero; Paypal e incluso procesadores de pago falso.

Establecer una colaboración con estas entidades bancarias, cuyo ámbito de actuación está más regulado que Internet, puede resultar realmente útil a la hora de identificar a los titulares de sitios web que realizan actividades ilícitas.



## 8. OFERTA DE MEDICAMENTOS EN PORTALES DE VENTA

Es común en algunos países encontrar oferta de medicamentos en sitios web de venta, donde además se oferta otros productos. Dependiendo de la legislación de cada país y toda vez que la comercialización de medicamentos se encuentre prohibida por estos canales, se podrán llevar adelante las siguientes acciones:

- Contactar con responsables del portal para informar las dificultades de comercializar medicamentos fuera de la cadena legal de distribución.
- Realizar convenios que permitan cancelar las ofertas rápidamente y obtener los datos de los anunciantes.
- Proporcionar al portal palabras claves para, en un primer momento, realizar un filtro en las solicitudes de publicación.
- Constatada la oferta, solicitar la baja a las autoridades del portal web.
- Recibir la información referente al ofertante.
- Prohibir de uso y comercialización productos que carecen de la debida autorización de la autoridad sanitaria.
- Realizar la denuncia ante las autoridades judiciales siempre que esto represente un delito en el país donde ocurra.
- Realizar procedimientos en conjunto con las fuerzas policiales a fin de investigar los domicilios desde donde se estuviera realizando la oferta.



# GLOSARIO

**Internet:** conocida como la Red de redes donde reside toda la información; es una red global que consiste en un grupo interconectado de redes locales que se conectan entre sí mediante la utilización del protocolo TCP/IP. La finalidad de esta red global es permitir el intercambio libre de información entre los usuarios.

**Dirección I. P:** es un número único e irrepetible con el cual se identifica un dispositivo (de hardware) dentro de la red. Está formado por 4 números (0-255) separados por puntos. Este dispositivo utiliza el protocolo IP para conectarse a Internet. Para convertir una dirección IP en el nombre de dominio que forma parte de la URL se utiliza el sistema de nombres de dominio (DNS).

**DNS:** Domain Name System, o en español, sistema de nombres de dominio es una tecnología que utiliza una base de datos que sirve para resolver nombres de dominio en las redes, esto es, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder.

Los sitios web tienen tanto una dirección descriptiva, denominada URL, como una dirección IP. Para buscar sitios web, los usuarios usan las URLs, pero los equipos usan las direcciones IP. DNS convierte las URLs en direcciones IP (y viceversa). Por ejemplo, si se escribe <http://www.aemps.es> en la barra de direcciones del navegador, el equipo envía una solicitud a un servidor DNS. El servidor DNS convierte la URL en una dirección IP, para que el equipo pueda encontrar el servidor web de AEMPS.

**World Wide Web (WWW):** es básicamente un medio de comunicación de texto, gráficos y otros objetos multimedia a través de Internet, es decir, la web es un sistema de hipertexto que utiliza Internet como su mecanismo de transporte.

**Nombre de dominio:** un dominio o nombre de dominio es el nombre que identifica un sitio web. Cada dominio tiene que ser único en Internet. Un ejemplo de nombre de dominio: [aemps.gob.es/](http://www.aemps.gob.es/)

**URL:** es una secuencia de caracteres que se usa para nombrar recursos de Internet para su identificación y localización (ejemplo: imágenes, vídeos, presentaciones, documentos de texto...). El formato general de un URL es: esquema://máquina.directorio.archivo; ej.: <http://www.aemps.gob.es/>

**Red EAMI** Guía de investigaciones sobre la venta a través de internet, de medicamentos falsificados o fraudulentos





**Sitio Web:** un sitio web es un sitio (localización) en la World Wide Web que contiene documentos (páginas web) organizados jerárquicamente.

**Página Web:** es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, adaptada para la llamada World Wide Web, y que puede ser accedida mediante un navegador. Esta información se encuentra generalmente en formato HTML o XHTML, y puede proporcionar navegación (acceso) a otras páginas web mediante enlaces de hipertexto.

**Servidor:** servidor en informática será un ordenador u otro tipo de dispositivo que suministra la información requerida por unos de los clientes entendiéndose por estos otros ordenadores o máquinas.

**Whois:** WHOIS (en inglés sería whois) es un protocolo de Internet utilizado para consultar bases de datos y obtener información sobre el registro de un nombre de dominio o dirección IP.

(Especificar que en este caso son las definiciones contenidas en la normativa española resultado de la transposición de la Directiva comunitaria).

**Servicios de la Sociedad de la información:** todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

**Servicio de intermediación:** servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

**Proveedor de Servicios de Internet:** persona física o jurídica que proporciona un servicio de la sociedad de la información.

**Registro de nombres de dominio (*Registry*):** autoridad de registro de nombres de dominio de alto nivel, que pueden o no estar vinculados a un país (p. ej., COM, NET o MX, AR...).

**Empresa registradora (*Registrar*):** empresa que realiza la inscripción en el Registro de nombres de dominio (*Registry*) a solicitud



de un cliente (*Registrant*). Tienen que haber sido acreditados por ICANN (p. ej., GoDaddy).

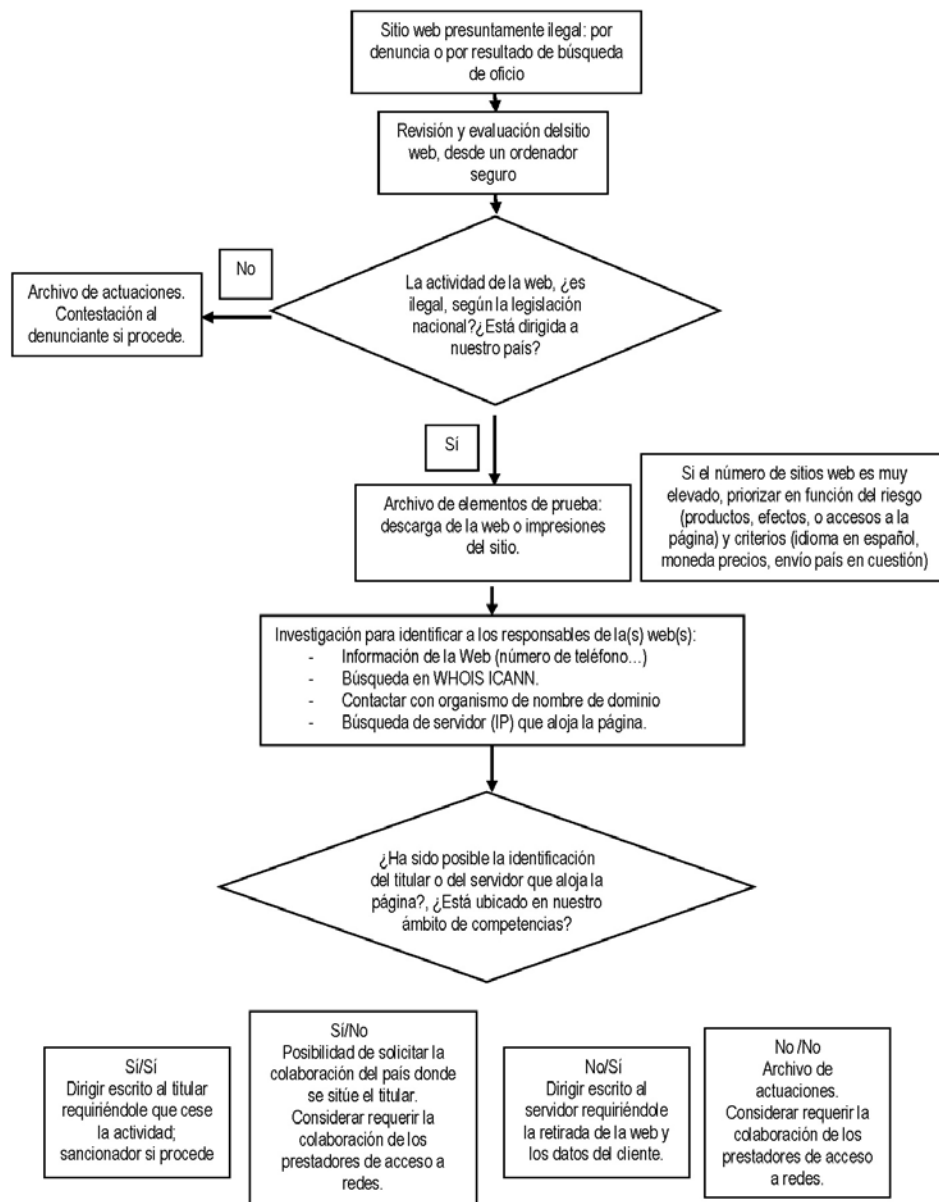
**Titular del nombre de dominio (*Registrant*):** persona que inscribe el nombre de dominio en el registro, tiene los derechos exclusivos de uso del mismo y suele ser responsable de la información que consta en la web.

**Proveedor de acceso a redes:** facilitan el acceso a una red de telecomunicaciones.

**Medicamento falsificado y fraudulento:** a los efectos previstos en el presente procedimiento se aplicará la definición incluida en el protocolo de actuaciones del sistema FALFRA.



# ANEXO 1. FLUJOGRAMA



## ANEXO 2. CHECK LIST DE INVESTIGACIÓN DE UNA WEB

<b>INFORMACIÓN DEL CASO</b>		
	Web investigada (URL)	
	Datos del denunciante/ Investigación de oficio	
	Fecha de inicio de la investigación	
	Descripción de los hechos denunciados	
<b>INVESTIGACIÓN</b>		
1	Acceso desde un ordenador seguro, con conexión a internet anónima (IP dinámico)	
2	Información mostrada en la página web	
	Titular, datos de contacto (e-mail, teléfono)	
	Producto(s)	
	Actividad (venta, publicidad...)	
	Impresión o descarga de la página web	
3	Identificador del titular	
	Datos WHOIS	
	Datos de contacto (e-mail, dirección, teléfono...)	
4	Servidor que aloja la página	
	IP	
	Servidor exclusivo (aloja solo esta página o no)	
	Proveedor de servicios de alojamiento	
<b>ACTUACIONES</b>		
5	Actuaciones	
	Requerimiento al titular de la página	
	Requerimiento	

