

# Centro Némesys

Gestión de las incidencias por uso  
indebido de Internet

Versión Septiembre 2009

## Índice

Índice .....	2
1. ¿Qué es el Centro Némesys? .....	3
2. ¿Qué son abusos de Internet?.....	3
3. ¿Cuáles son los abusos más frecuentes? .....	3
3.1 Spam.....	3
3.2. Intrusión .....	3
3.3. Phishing.....	4
3.4. Otros Abusos .....	4
4. Quiero informar de un abuso.....	4
4.1. ¿Qué es la dirección IP? .....	6
4.2. ¿Cómo comunico la incidencia?.....	6
5. ¿Qué pasa cuando llega a Telefónica una notificación sobre un abuso en Internet?..	7
6. ¿Qué puedo hacer si recibo una comunicación desde Nemesys? .....	7
7. ¿Qué son las listas negras (BLACKLIST) y en qué me afectan? .....	9
8. ¿Dónde podemos encontrar más documentación sobre seguridad en Internet? .....	9

## 1. ¿Qué es el Centro Némesys?

El Centro Némesys es una unidad de Telefónica que tiene, como actividad prioritaria, atender las incidencias que puedan surgir, por uso indebido, de las redes de Telefónica en Internet (abusos de Internet).

Estas incidencias se reciben en buzones especiales puestos a tal efecto en Internet.

Las incidencias o ataques que pueden darse son de clientes de Telefónica hacia Internet o viceversa, de Internet a clientes de Telefónica.

## 2. ¿Qué son abusos de Internet?

Como definición general, se consideran abusos de Internet a toda actividad ilícita o poco ética realizada usando los recursos de Internet. Por ejemplo, acceder a un ordenador ajeno para extraer información, destruirla, o usarlo para atacar a otro sistema.

Existen varias recomendaciones internacionales que orientan a los ISP (Proveedor de Servicios de Internet) sobre la forma correcta de atender las notificaciones sobre este tipo de actividades, siendo Telefónica uno de los más rigurosos en su cumplimiento.

Aparte de estas recomendaciones internacionales debemos tener en cuenta la legalidad vigente. Dada la naturaleza de Internet, es muy probable que haya varios países implicados en una misma incidencia, y cada nación puede tener una cobertura legal diferente para el mismo tipo de abuso. En nuestro caso, Telefónica de España está sujeta a la legislación española.

## 3. ¿Cuáles son los abusos más frecuentes?

### 3.1 Spam

Denominamos Spam al envío de correo electrónico no solicitado por el destinatario, normalmente de publicidad. La gravedad de Spam estriba en que consume recursos tanto de la red como del propio usuario. El envío de correo no solicitado supone un porcentaje muy alto del tráfico de Internet.

Perjudica al usuario porque el hecho de recibir correo electrónico no solicitado puede provocar que la cuenta de correo del destinatario se llene, dado que normalmente tiene una capacidad máxima. Esto implica que una vez alcanzada la capacidad máxima, los demás correos son rechazados hasta que se borren los que hay, con lo que puede ocurrir que no reciba un correo importante que estaba esperando. Además, el cliente tarda más en "bajar" el correo, con lo que se le fuerza a estar conectado más tiempo. Todo ello sin tener en cuenta el contenido del mensaje, que cuando trata de violencia o sexo y son accesibles por los menores, generan la consiguiente alarma social.

### 3.2. Intrusión

Denominamos intrusión (Hacking en inglés) tanto al mero intento de acceder a una máquina ajena como el hecho de conseguirlo. Englobamos bajo este término el uso de herramientas o métodos orientados a detectar la vulnerabilidad de un sistema ajeno, sin la autorización de su propietario, tales como escaneo de puertos, intentos de ejecuciones de scripts, etc.

### **3.3. Phishing.**

Phishing es un término que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se caracteriza por intentar obtener de un usuario información confidencial (sus datos, claves, contraseñas, cuentas bancarias, números de tarjetas de crédito, etc ) de forma fraudulenta. El estafador se hace pasar por una empresa o entidad pública de confianza en una aparente comunicación oficial electrónica suplantando la imagen y de esta manera hacer creer a la posible víctima que realmente los datos solicitados proceden del sitio oficial cuando en realidad no lo es.

El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida, la recepción de un correo electrónico.

### **3.4. Otros Abusos**

A parte de los anteriormente descritos (que son los más usuales) recibimos incidencias sobre vulneración de la propiedad intelectual tales como el alojamiento y distribución de música, videos, y diverso material protegido bajo las leyes internacionales del Copyright o la Ley de Propiedad Intelectual española.

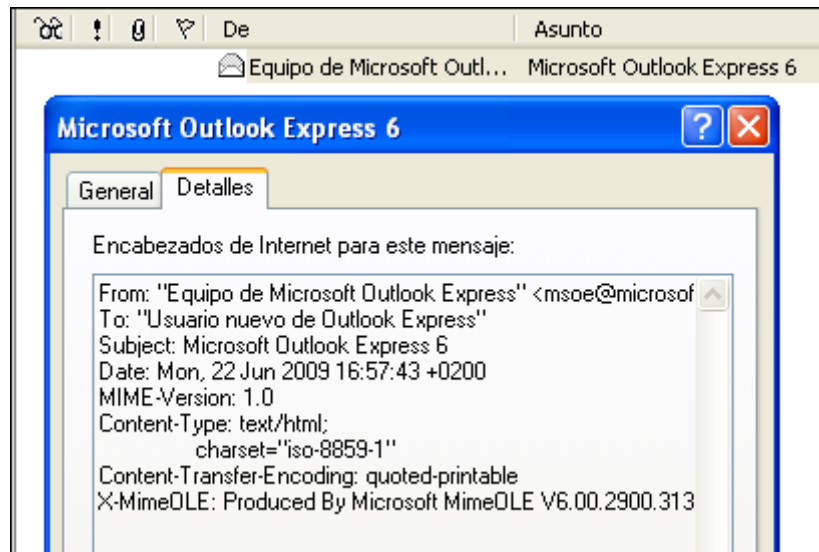
Igualmente, nos pueden llegar notificaciones sobre actividades delictivas como la pedofilia o la pornografía infantil, en cuyo caso lo remitimos a las autoridades competentes.

## **4. Quiero informar de un abuso.**

### ***Spam y phishing***

En todos los correos, además del mensaje, hay una cabecera que suele estar oculta por el programa de correo que utilizemos, pero siempre podemos verla. Es ahí donde figuran el origen, el destino y todos los sitios por donde ha pasado el correo hasta llegar a su destinatario. Aunque el correo recibido no tenga remitente, o esté falsificado, la cabecera completa del correo nos puede dar esta información por eso es fundamental aportarla al comunicar las incidencias.

Para extraer las cabeceras en todos los programas gestores de correo hay una opción para ver el código del mensaje o la cabecera. Por ejemplo si quieres consultar los encabezados en Outlook Express, haz un clic con el botón derecho sobre un mensaje y elige Propiedades. Luego, pulsa en la pestaña Detalles.



En Outlook, el proceso es aún más directo. En el menú contextual del mensaje, selecciona Opciones. Los encabezados aparecerán justo al final del cuadro de diálogo.

### Campos que aparecen en una cabecera de correo:

**Received:** Cada vez que el mensaje pasa por un servidor, aparece este campo de datos, especificándose el nombre del servidor, su dirección IP (número que se asigna a cada servidor), el programa de correo utilizado, y la fecha y la hora en que se recibió en el servidor.

**From:** Remitente original del mensaje

**Subject:** Asunto del mensaje

**To:** Destinatario del mensaje

**Content-Type:** Tipo de contenido del mensaje; en realidad, es el formato con el que se envió el mensaje.

En definitiva vemos que las cabeceras nos dan información de los servidores por donde ha pasado el correo antes de llegar a nuestro buzón (IP o nombre), la fecha, la hora, la identificación del correo en cada servidor, quién lo entregó y para quién va dirigido.

Todos estos datos son básicos para poder investigar el Correo Basura (Spam) y a los Spammers.

En la comunicación a Némesys de un correo spam debemos incluir (dentro del cuerpo del mensaje y en formato texto, nunca adjunto ni copias de pantalla) las cabeceras completas del correo

### ***Intrusión***

El cliente normalmente dispone de unos programas que detectan estos abusos, tales como el Cortafuegos (Firewall) o un Sistema de Detección de Intrusión. Estos programas, que al igual que el antivirus, es recomendable instalar, además de avisar del intento de acceso, facilitan un registro del mismo en el que normalmente aparecen la fecha y hora, el origen del ataque y la máquina atacada, así como el tipo de ataque empleado. Este registro es el que habitualmente se conoce como "Log", y el cliente debe guardarlo para adjuntarlo como prueba al informar sobre estas incidencias.

## 4.1. ¿Qué es la dirección IP?

La dirección IP es un grupo de cuatro números separados por puntos. Cada uno de ellos puede tener un valor de 0 a 255. De forma que una dirección IP es algo así como XXX.XXX.XXX.XXX. Todas las máquinas conectadas a Internet, en un momento determinado, tienen una IP distinta.

En Centro Némesys consideramos nuestro cliente a todo aquel que utilice una dirección IP asignada a Telefónica de España, independientemente de la operadora a la que pertenezca, puesto que ha utilizado un acceso a Internet de nuestra compañía.

Dado que en el "Log" o en las cabeceras de correo se registra la IP origen del ataque, aunque el usuario no sabe a quién pertenece, si puede conocer a qué ISP está asignada.

Para ello existen en Internet una serie de organizaciones que gestionan las direcciones IP y que tienen un registro de acceso público y pueden ser consultadas.

En nuestro caso, las direcciones de Telefónica de España se pueden localizar en RIPE:

<http://www.ripe.net/>

Otras organizaciones para consultar:

<https://www.arin.net/>

<http://www.apnic.net/>

<http://lacnic.net/sp/index.html>

Hay que aclarar, que muchos de los programas "Firewall" e "IDS" existentes consultan estas bases de datos en Internet y facilitan dicha información sin que el usuario deba acceder manualmente a los registros.

## 4.2. ¿Cómo comunico la incidencia?

En Telefónica de España, existen dos maneras: a través de Telefónica On Line o enviando un correo electrónico directamente a Centro Némesys.

1.- <http://www.telefonica.es/nemesys>

2.- [nemesys@telefonica.es](mailto:nemesys@telefonica.es)

De la misma forma, y siguiendo las recomendaciones internacionales, ponemos a disposición del usuario lo que podríamos denominar "buzones estándar de correo". En nuestro caso son **[abuse@telefonica.net](mailto:abuse@telefonica.net)**, **[abuse@terra.es](mailto:abuse@terra.es)** o **[oabuse@infonegocio.com](mailto:oabuse@infonegocio.com)**

En caso de acceder a la dirección de Telefónica On Line, el cliente se encuentra con un formulario de registro de incidencias en Red IP y RIMA que debe cumplimentar con los datos correspondientes (ISP que le presta el servicio de acceso a Internet, cliente particular o empresa...)

En cualquier caso, la información que le solicitamos es para identificarle como cliente nuestro si lo es. En otro caso le solicitamos información adicional sobre el ISP al que pertenece dicho usuario.

También se solicita que especifique tanto el tipo de abuso recibido, así como que copie el contenido del "Log" donde quedó registrado dicho ataque o, en el caso de Spam, que adjunte el correo recibido con las cabeceras completas.

## 5. ¿Qué pasa cuando llega a Telefónica una notificación sobre un abuso en Internet?

A Centro Némesys llegan las notificaciones sobre abusos en Internet cuando la dirección IP responsable del abuso es propiedad de Telefónica, Centro Némesys se pondrá en contacto con el usuario del servicio al que estaba asociada dicha IP en el momento del incidente, para informarle sobre el mismo. Si la actividad ilícita persiste o el volumen de spam que está provocando es muy alto, el sistema Antispam de Telefónica bloqueará el puerto 25 para ese acceso. En esta situación el cliente no podrá enviar correo a través del puerto SMTP, pero sí podrá hacerlo utilizando una de estas alternativas:

- Correo Outlook o similares en los siguientes servicios:  
Todos los proporcionados por Telefónica: servicios de correo de telefonica.net, terra.es, infonegocio.com...
- Cualquier conexión realizada a través de SMTP seguro (distinto al 25).
- Cualquier tráfico webmail de cualquier proveedor de correo

-  
El puerto 25 se bloquea porque es el más utilizado por los distribuidores de virus y troyanos para realizar su actividad.

## 6. ¿Qué puedo hacer si recibo una comunicación desde Nemesys?

Con el fin de poner sobre aviso a los clientes de los problemas de seguridad informados en nuestros buzones, el centro Nemesys de Telefónica se pone en contacto con los clientes por correo postal al domicilio de contacto del cliente, o bien por correo electrónico, a los email de contacto que haya facilitado el cliente en Telefónica, siendo este el medio preferido, debido a la inmediatez del mismo, para cualquier comunicación.

En cualquier caso, nunca se le va a solicitar que facilite ningún tipo de información personal o de cuentas de correo, siendo el origen de estos correos nuestro email nemesys@telefonica.es

Lo mas frecuente es que el cliente no esté realizando voluntariamente estas actividades ilícitas: envío de spam, phishing o intentos de intrusión; sino que un tercero haya aprovechado algún tipo de "agujero de seguridad" para llevarlas a cabo.

Como cliente de los servicios de conectividad a Internet de Telefónica, es responsable de sus equipos informáticos, así como de una correcta configuración de los mismos, por lo que es muy importante:

1- Identificar la causa que ha llevado a generar el spam o el ataque indicado, y solucionarla. De nada sirve solicitar que nos saquen de la lista negra en la que nos hayan podido incluir, o solicitar la apertura del Puerto 25, si seguimos enviando spam, porque volveremos a entrar rápidamente.

2- Analizar los equipos y servidores en busca de virus. Sería conveniente, además del antivirus actualizado del que se disponga, analizar los equipos con algún tipo de antivirus online y eliminar a conciencia cualquier amenaza que pudiera haber.

En la página web de Telefónica 'www.telefonica.es', podrá encontrar una herramienta de uso gratuito para el escaneo y eliminación de virus, llamada FreeScan, a la que podrá acceder a través de la siguiente dirección:

[http://freescan.telefonica.terra.es/FreeScan\\_EULA\\_Page.htm](http://freescan.telefonica.terra.es/FreeScan_EULA_Page.htm)

3- Si ha instalado un servidor de correo puede ser que no lo tenga bien protegido, por lo que pueden estar conectándose anónimamente a él para enviar spam.

4- Una vez eliminada la causa de la incidencia, si ha sufrido el bloqueo del puerto 25, la solución más rápida es solicitar el desbloqueo en el Centro de Atención Técnica, CAT de ADSL a través de los siguientes números de teléfono:

- 902357000 atención a clientes particulares

- 902357022 atención a empresas

[nemesys@telefonica.es](mailto:nemesys@telefonica.es)

**En Resumen:** si tenemos notificaciones que apuntan a uno de nuestros clientes, ya sea de modo deliberado o involuntario, le informamos de este hecho así como de que debe revisar sus sistemas, ya que hay abusos que pueden ser tipificados como delitos

Asimismo, en las cláusulas del contrato de ADSL (ver en cláusulas del contrato de ADSL en <http://www.telefonica.net/contratos>) se establece que un uso inapropiado del acceso a Internet facilitado por nuestra empresa puede ser motivo de suspensión unilateral del servicio, por lo que el cliente debe tomarse el interés necesario en procurar que este tipo de incidentes no vuelva a producirse.

En cualquier caso, si desea realizar cualquier consulta respecto a la incidencia o solicitar evidencias de la misma, debe ponerse en contacto con nosotros a través de esta misma dirección:

[nemesys@telefonica.es](mailto:nemesys@telefonica.es)

## 7. ¿Qué son las listas negras (BLACKLIST) y en qué me afectan?

Es importante destacar que Centro Némesys no mantiene ni gestiona ninguna lista negra.

Diferentes organismos y empresas internacionales elaboran este tipo de listas para uso propio o público.

Hay miles por todo el mundo y su inclusión en ellas responde a diferentes motivos, los más comunes, que además afectan al envío de correo son:

1) Por enviar SPAM se listan las direcciones IP que son detectadas como emisoras de este tipo de correo.

2) Por tener un servidor de correo montado sobre una IP dinámica: por procedimientos internos de seguridad en Internet, hay listas negras que incluyen todos los rangos de IP's dinámicas de las distintas operadoras que prestan servicio de acceso a Internet.

La mayoría de los administradores de servidores de correo electrónico utilizan estas listas para filtrarlo y no admiten ningún correo cuya procedencia sea un servidor montado sobre una IP dinámica incluida en estas listas. Por lo tanto será habitual que los correos enviados desde estos servidores sean devueltos.

El estar incluido en este tipo de listas no afecta al cliente de correo local ni webmail.

El servidor de correo destinatario suele enviar, en los textos de rechazo de los correos que no progresan, el motivo y el nombre de las listas negras que impiden los envíos cuando el motivo es éste.

## 8. ¿Dónde podemos encontrar más documentación sobre seguridad en Internet?

Para mayor información sobre todo lo relacionado con Internet puede consultar las siguientes URL's:

-INTECO (Instituto Nacional de Tecnologías de la Comunicación):

<http://www.inteco.es/>

-RED.es (entidad perteneciente al Ministerio de Industria, Turismo y Comercio):

<http://www.red.es/>