



**White Paper**

# **SPAM**

## **Cómo proteger a los usuarios de su empresa:**

La información incluida en este documento representa el punto de vista actual de Panda Software, S.L. sobre las cuestiones tratadas en el mismo, en la fecha de publicación. Este documento es de carácter informativo exclusivamente. Panda Software, S.L. no ofrece garantía alguna, explícita o implícita, mediante este documento.

El cumplimiento de las leyes que rigen el copyright es responsabilidad del usuario. De acuerdo con los derechos de copyright queda totalmente prohibida la reproducción total o parcial de este documento, así como su almacenamiento o introducción en un sistema de recuperación. Asimismo, queda prohibida la distribución de este documento por cualquier forma o medio (electrónico, mecánico, fotocopia, grabación u otros) o por razón alguna, sin previo consentimiento escrito de Panda Software, S.L.

Panda Software, S.L. puede tener patentes, aplicaciones de la patente, marcas registradas, derechos de autor o cualquier otro derecho de propiedad intelectual sobre la información contenida en este documento. Salvo previo acuerdo escrito con Panda Software, S.L., la posesión de este documento no proporciona derecho alguno sobre dichas patentes, marcas registradas, copyrights u otra forma de propiedad intelectual.

[www.pandasoftware.es](http://www.pandasoftware.es)



Página intencionadamente en blanco.



# ÍNDICE DE CONTENIDOS

<b>ÍNDICE DE CONTENIDOS</b> .....	<b>3</b>
<b>ÍNDICE DE ILUSTRACIONES</b> .....	<b>4</b>
<b>ÍNDICE DE TABLAS</b> .....	<b>4</b>
<b>1 INTRODUCCIÓN</b> .....	<b>5</b>
1.1 OBJETIVOS .....	5
1.2 AUDIENCIA .....	5
<b>2 ¿QUÉ ES EL SPAM?</b> .....	<b>6</b>
<b>3 ¿POR QUÉ DEBO PRESTAR ATENCIÓN AL SPAM?</b> .....	<b>7</b>
3.1 IMPACTO ECONÓMICO .....	7
3.1.1 Reducción en la productividad de la plantilla .....	7
3.1.2 Aumento de carga de trabajo en la administración .....	7
3.1.3 Aumento del consumo de recursos de red. ....	8
3.1.4 Riesgos de seguridad .....	8
3.1.5 Riesgos legales .....	8
3.2 ESTUDIOS CUANTITATIVOS .....	8
<b>4 ¿CÓMO PROTEGERSE DEL SPAM?</b> .....	<b>11</b>
4.1 ACCIONES PREVENTIVAS .....	11
4.2 ACCIONES CORRECTIVAS .....	12
4.2.1 ¿Cuándo es momento adecuado? .....	12
4.2.2 Acciones legales .....	12
4.2.2.1 California .....	13
4.2.2.2 Europa .....	14
<b>5 SOLUCIONES TECNOLÓGICAS</b> .....	<b>15</b>
5.1 TÉCNICAS DE PROTECCIÓN .....	15
5.1.1 Filtros Bayesianos .....	17
5.2 ¿QUIÉN DEBE FRENAR EL SPAM EN SU ORGANIZACIÓN? .....	18
5.2.1 Falsos positivos .....	19
5.3 ¿DÓNDE ES MEJOR PONER LOS CONTROLES? .....	19
5.4 LA VISIÓN DE PANDA SOFTWARE .....	20
5.4.1 Operativa .....	21
5.4.2 Panda ExchangeSecure .....	24
<b>6 RESUMEN Y CONCLUSIONES</b> .....	<b>25</b>



## ÍNDICE DE ILUSTRACIONES

- MECANISMO DE VALIDACIÓN DE DOMAINKEYS .....	17
- ESTRATEGIA DE PROTECCIÓN POR CAPAS DE PANDA SOFTWARE .....	19
- ARQUITECTURA DE PROTECCIÓN ANTI-SPAM DE PANDA SOFTWARE.....	22
- FIJACIÓN DEL NIVEL DE SENSIBILIDAD DE LA PROTECCIÓN ANTI-SPAM.....	22
- INCLUSIÓN DE LISTAS BLANCAS Y NEGRAS DE PROTECCIÓN ANTI-SPAM .....	23

## ÍNDICE DE TABLAS

- CORREO VS. BASURA .....	9
---------------------------	---



## 1 Introducción

El término “malware” puede ser definido como “cualquier programa, documento o mensaje susceptible de causar perjuicios a los usuarios de sistemas informáticos”. Así, los virus son tan sólo una parte de un conjunto cada vez más amplio, en el que también tienen sitio otras **amenazas informáticas**. Entre ellas se encuentran el spam, los dialers (marcadores telefónicos), o el spyware (software espía).

En la actualidad, uno de los más graves peligros de Internet es el **spam o correo electrónico no deseado**, debido, principalmente, a que pueden causar daños a muy diversos niveles.

### 1.1 Objetivos

Conocer las características del correo no deseado o spam, los principales mecanismos de **prevención** y las técnicas aplicadas por los productos comerciales para minimizar el impacto de este tipo de comunicaciones en la productividad empresarial.

### 1.2 Audiencia

- Usuarios informáticos.
- Administradores de correo electrónico.
- Administradores de red.
- Expertos en seguridad.
- CTOs (Chief Technology Officer).
- CIOs (Chief Information Officer).



## 2 ¿Qué es el spam?

El nombre de spam se origina a raíz de un gag de una serie cómica, en el que todos los platos de un restaurante tenían una marca de carne enlatada llamada spam como principal ingrediente. Así, haciendo un símil, se empezó a designar con este término el gran número de mensajes no deseados que se reciben en cualquier cuenta de correo electrónico.



Así, un mensaje se puede considerar spam si concurren los siguientes hechos:

- correo no solicitado, es decir, que ha sido enviado sin consentimiento.
- envío masivo a un número desproporcionado de destinatarios
- el receptor no conoce personalmente al emisor

Aunque no sea lo más habitual, el spam puede contener virus u otros códigos maliciosos, o direcciones de Internet que apunten a páginas web que estén preparadas para descargar algún tipo de programa en el equipo de manera no autorizada. Este ha sido, presumiblemente, el método que ha empleado el conocido gusano Sobig.F para conseguir el título del “virus que más rápidamente se ha propagado en la historia de la informática”.



### 3 ¿Por qué debo prestar atención al spam?

Por una parte, el daño que este tipo de malware provoca puede cuantificarse **económicamente** en horas de trabajo que se malgastan cada día en todo el mundo, ya no con la tarea de leer los mensajes spam, sino, simplemente, eliminándolos. Pensemos en una red corporativa con quinientos puestos de trabajo a los que llegan, diariamente, diez mensajes de este tipo.

Si debido a estos mensajes se pierden cinco minutos de tiempo, podemos calcular fácilmente el gran número de horas que cada trabajador pierde anualmente debido al spam. Además, si el contenido es lo suficientemente atractivo para que el usuario lea su contenido, o se conecte a alguna dirección de Internet que se indique en el texto, la **perdida de tiempo** aumenta exponencialmente.

#### 3.1 *Impacto económico*

El spam influye negativamente en los resultados de las empresas a través de:

##### 3.1.1 Reducción en la productividad de la plantilla

Las compañías pierden productividad cuando sus empleados tienen que gastar tiempo en descargar y borrar correo no deseado en lugar de realizar las tareas que tienen asignadas. El coste puede variar en función del coste / hora de cada empleado, pero considerando que detectar y **borrar un correo basura lleva aproximadamente 10 segundos**, para una empresa con una plantilla de 1.000 empleados donde los usuarios reciban del orden de 100 correos no deseados al mes, estos emplearan en esta tarea 3 ½ horas lo que supondría un gasto superior a los 55.000 euros.

##### 3.1.2 Aumento de carga de trabajo en la administración

Los administradores de red y correo electrónico junto a los profesionales de soporte técnico deben emplear su tiempo y esfuerzo en aconsejar y dotar de herramientas a los usuarios finales para hacer frente a este tipo de malware.



### 3.1.3 Aumento del consumo de recursos de red.

El volumen de spam en el correo electrónico es directamente proporcional al coste de los recursos informáticos que lo soportan. Así, si las **3/5 partes del correo entrante** a la empresa es spam, entonces las 3/5 partes de los servidores de correo, el ancho de banda de la red de área local y de los dispositivos dedicados a copias de seguridad están siendo utilizados en procesar y almacenar correo basura.

### 3.1.4 Riesgos de seguridad

La pieza más débil de todo sistema de seguridad es el componente humano. Los emisores de spam no pueden **acceder directamente a los escritorios** de los empleados para robar contraseñas y acceder a información confidencial. Sin embargo, si pueden engañar a los usuarios para que abran mensajes o archivos adjuntos que contengan virus o código malicioso generando así un agujero de seguridad en toda la compañía.

### 3.1.5 Riesgos legales

Muchos correos no deseados son de **contenido ofensivo, sexual o violento** que las empresas comprometidas socialmente no pueden tolerar en sus organizaciones. Además, si no se toman medidas para evitar la entrada de este tipo de contenido, la empresa podría llegar a ser denunciada por sindicatos y trabajadores por no facilitar un entorno de trabajo digno.

## 3.2 Estudios cuantitativos

El correo electrónico es hoy día el mecanismo de intercambio de comunicación preferente para empresas e individuos. Prácticamente la totalidad de las grandes corporaciones cotizadas en Bolsa cuenta con estos sistemas y de acuerdo a estudios recientes, hasta el **60 % del capital intelectual** de una empresa puede encontrarse en forma electrónico dentro de sus sistemas de correo.

La ONU estima que el spam tiene unos costes anuales a nivel mundial de 20.500 millones de dólares, y ya en el año 2002 el Ejecutivo europeo, estimó que la **pérdida de productividad** para las empresas de la UE, obligadas a limpiar masivamente sus bandejas de entrada de correo electrónico, era de **2.500 millones de euros**.



Y es que según un estudio Spamfilter Review de 2004, a nivel mundial se envían **31.000 millones de mensajes de correo electrónico al día** de los cuales el 40%, unos **12.400 millones de mensajes son correos no deseados** y se espera que el número se triplique en el año 2006, y se espera que el número se triplique en el año 2006, mientras que la firma de investigación de mercados IDC es más pesimista en sus previsiones y pronostica que el volumen de correo basura crecerá exponencialmente hasta el año 2008.

Este crecimiento ha provocado que el problema del spam se generalice entre los usuarios de Internet, pues aproximadamente el **60 % del público objetivo** (usuarios de correo electrónico) ha recibido mensajes inapropiados o de carácter sexual.<sup>1</sup>



Las cifras acerca del porcentaje de correo basura varían según la fuente como podemos ver en la Tabla 1 - Correo vs. Basura, pero parece claro que no actuar frente al spam ha dejado de ser una opción para las empresas, especialmente cuando sólo el 5% de ellas son capaces de bloquear efectivamente – 90 % de acierto – estos mensajes<sup>2</sup>.

Fuente	Porcentaje de correo basura
Gartner Group	25
AOL	33
Brightmail	50

**Tabla 1 - Correo vs. Basura**

¿Cómo se traducen estos datos en términos económicos? Según fuentes de Tech web, en el 2005 el spam costará 135 € por buzón en Estados Unidos, mientras que esta cifra asciende a 191 € por buzón de correo en Alemania, teniendo en cuenta sólo los costes por pérdida de productividad de los trabajadores y sin contabilizar los costes de infraestructura tecnológica que mencionamos en el anterior apartado. Es decir, un coste superior a los **50.000 millones de euros en todo el mundo**, de los cuáles 8.900 millones correspondían a Estados Unidos.

<sup>1</sup> Fuente: USA Today.

<sup>2</sup> Fuente: Gartner Group.



## Spam, ¿cómo proteger a los usuarios de su empresa?



Y la reacción en los departamentos de sistemas no se ha hecho esperar, ya que el estudio realizado en la Conferencia de Microsoft Exchange, muestra que el 75 % de los entrevistados consideraban el spam como un problema moderado o grave en sus empresas, y el **90 % estaba evaluando soluciones anti-spam.**



## 4 ¿Cómo protegerse del spam?

### 4.1 Acciones preventivas

La mejor manera de luchar contra el spam es evitar ser blanco del mismo. A continuación se enumeran las acciones que con más frecuencia provocan ser objeto del spam:

- Mandar un mensaje a un **grupo de noticias** o *newsgroup* .
- Dar la dirección de correo en una **tienda** online.
- Darse de alta en un **servicio de Internet** que solicite una dirección de correo.
- Mandar un correo solicitando la **baja** en la lista de distribución de un **spam**, pues lamentablemente esta acción casi siempre sirve exclusivamente para confirmar la validez de nuestra dirección de correo.
- Darse de alta o intervenir en una **lista de distribución** de correo.
- Conversaciones online en **chats**.
- Poner direcciones de correo electrónico en nuestras **páginas web** que son automáticamente extraídas por robots que buscan cadenas con el carácter @

Adicionalmente, los remitentes de spam pueden comprar listados de correos cuyos remitentes no han aprobado la recepción de mensajes promocionales. Este tipo de práctica daña seriamente la reputación de las empresas que realizan campañas de marketing online sin el permiso de sus destinatarios.

Actualmente los usuarios pueden optar por ser incluidos (*opt-in*) en programas de *permission marketing*, es decir dan su autorización expresa para recibir correos promocionales, o bien optan por excluidos de todo tipo de campaña publicitaria (*opt-out*) a través del uso de **listas Robinson** por ejemplo.

Otro mecanismo tradicionalmente utilizado por los emisores de spam es la generación aleatoria de *alias* de correo a partir de palabras y nombres habituales como **soporte**, **ventas** o **david**. A continuación, dichos alias son combinados con dominios registrados en el NIC para obtener direcciones de correos válidas.

El siguiente paso es averiguar cuáles de entre las miles de direcciones generadas son válidas. Para ello, los spammers más avanzados colocan en los correos referencias (*links*) a minúsculas imágenes que residen en sus webs y que resultan inapreciables a simple vista. Cuando el destinatario descarga y visualiza el contenido HTML del correo entonces, su cliente de correo solicita la imagen al servidor lo que genera un proceso automático de **validación de la dirección** de correo en la base de datos objetivo del spam.



Por ello, resulta recomendable **deshabilitar la vista previa** de los clientes de correo con el fin de evitar que se notifique que nuestra dirección es válida, antes incluso de abrir el mensaje.

### 4.2 Acciones correctivas

#### 4.2.1 ¿Cuándo es momento adecuado?

El momento es ya. Todos podemos empezar a actuar contra el spam que invade nuestros centros de trabajo y nuestras cuentas privadas de correo electrónico aplicando a rajatabla las siguiente reglas:

- **Nunca responda** bajo ningún concepto a un correo electrónico no deseado.
- **No adquiera ningún producto** procedente de una promoción anunciada en este tipo de correos. De esta forma disuade al emisor de realizar nuevos envíos, ya que su objetivo es obtener ganancias económicas con el mismo. Según ComputerWorld, uno de cada 400 receptores de envíos promocionales de tipo spam acaban comprando el producto o servicio anunciado.
- **No se deje llevar** por peticiones o cadenas de correos. El correo masivo de esa índole constituye spam y la lista de direcciones que aparecen en estas cadenas son utilizadas con posterioridad por los spammers.
- **No ataque electrónicamente** la cuenta de correo del emisor del spam, pues la dirección que aparece en este tipo de correos probablemente ha sido robada o ni siquiera exista.

#### 4.2.2 Acciones legales

Las acciones legales sobre el spam tienen un efecto limitado, pues si se dictan leyes contrarias a este tipo de prácticas, el generador de spam siempre puede desplazar sus **operaciones a un ISP situado en un país sin legislación** sobre la materia o penetrar ilegalmente con herramientas de *hacking* en ordenadores de personas inocentes y lanzar desde allí de forma clandestina sus correos no deseados.

A continuación, y a título de ejemplo, incluimos dos referencias importantes en materia legislativa para controlar el crecimiento del spam: California y la Unión Europea.



#### 4.2.2.1 California

La ley promulgada en el 2003 sustituye a la ley de 1998 que ya protegía mediante la **habilitación del *opt-out*** a los residentes en California. La nueva ley no sólo es aplicable a los correos enviados desde California, sino a todos los correos recibidos por residentes en dicho estado.

Además de criminalizar el envío de spam con una multa de 1.000 dólares por cada correo no deseado enviado, permite al estado de California, a los ISPs y a las personas físicas presentar cargos contra los remitentes de spam o la empresa cuya promoción o publicidad aparezca en el correo.

Esta ley surge como respuesta a estudios que muestran que el 74 % de los entrevistados estaban a favor de ilegalizar el envío masivo de correo no deseado y que sólo un 12 % se oponía. Además el **80 %** de la población estudiada consideraba el **spam como muy molesto**.

La ley ilegaliza el envío de anuncios o promoción de bienes, servicios o crédito sin el consentimiento directo del destinatario. El **consentimiento directo** queda definido en la ley como la respuesta positiva a una "solicitud clara y llamativa" del remitente preguntando si el destinatario del correo quiere recibir correo (*opt-in*) o por una solicitud directa al emisor de recibir correo por parte del receptor. La ley no especifica si las empresas que compran listados de correos electrónicos de proveedores de marketing tienen *consentimiento directo*, es decir derecho a utilizar estas direcciones.



#### 4.2.2.2 Europa

Adoptada en **julio de 2002**, la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas fija las normas comunes para asegurar mejor la protección y la confidencialidad de los datos personales en Internet. Prohíbe, entre otras cosas, el envío de 'e-mails' comerciales sin el consentimiento previo del destinatario.

Esta directiva establece reglas estrictas e impone obligaciones para garantizar la seguridad y la confidencialidad de las comunicaciones en las redes electrónicas de la UE. La norma **prohíbe el "spam"** en toda la Unión Europea, así como ocultar la identidad del remitente del correo o la utilización de una dirección de envío falsa.

El artículo 13 de la Directiva dispone que cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico durante el proceso de venta de un producto, esa **misma entidad podrá utilizar dicha dirección para la venta de productos o servicios de características similares**, a condición de que se ofrezca a los clientes, sin cargo alguno, la posibilidad de oponerse a la utilización de ese correo electrónico en el momento de la recogida de datos y, en caso de que el cliente no haya rechazado inicialmente su empleo, cada vez que reciba un nuevo mensaje.



## 5 Soluciones tecnológicas

Una gran ventaja es que el **correo no deseado** tiene, generalmente, una serie de características que lo hacen relativamente **fácil de identificar**. Prácticamente, en todos ellos se insta a la compra de algún producto utilizando unas palabras muy similares. De esa manera, un software especializado puede elaborar un determinado perfil del correo recibido para poder catalogarlo como spam y eliminarlo antes de que sea descargado en el cliente de correo electrónico o en los buzones de los usuarios.

Sin embargo, el spam también evoluciona y muchos de ellos aprovechan las capacidades del HTML para intentar engañar a los filtros de spam. Algunas de las técnicas empleadas son las siguientes:

- **Codificación.** Oculta letras codificándolas como entidades HTML o representaciones numéricas como DBCS que normalmente se utilizan para enviar caracteres especiales o en idiomas basados en ideogramas.
- **Tinta invisible.** Cambiar los colores de fondo y de la fuente para hacer que el texto no sea visible en pantalla.
- **Agujero negro.** Oculta un mensaje utilizando una fuente de tamaño cero.
- **Trocear.** Utiliza tablas HTML para trocear un mensaje en tiras diminutas.

### 5.1 Técnicas de protección

Un solución anti-spam puede utilizar una o varias técnicas para proteger a sus clientes del spam. A continuación, se muestra una relación de las técnicas más comúnmente empleadas con sus pros y contras:

- **Análisis Léxico.** Aplica filtrado de contenidos a todos los mensajes de correo para poder identificar correos no deseados. Para ello utiliza una lista de palabras o frases. Esta técnica puede aplicarse tanto al asunto del mensaje como al cuerpo, etiquetas HTML o los archivos adjuntos.

Esta técnica puede refinarse a través de expresiones regulares para capturar palabras intencionadamente mal escritas o ajustar la captura de spam a partir de la frecuencia de aparición de ciertas palabras en los mensajes no deseados.

En su contra, esta técnica no considera el contexto de ciertas palabras legítimas en un entorno y potencial spam para otras empresas. Tampoco puede analizar mensajes que sólo contengan imágenes y direcciones web (URL's). Además consume bastante tiempo de proceso y necesita de continuas actualizaciones de los pesos asignados a cada palabra.



- **Análisis heurístico.** Utiliza reglas que analizan los mensajes para asignar una probabilidad al mismo sobre si es spam. Esta técnica identifica el spam en base a varios atributos, lo que le hace efectivo en correos HTML, de texto o con imágenes. Alguna regla heurística podría ser, clasificar como spam a correos con una fecha de emisión incorrecta.

En contra de esta técnica, empleada por soluciones como SpamAssassin, juega la dificultad de establecer, probar y mantener las reglas, así como la inversión de tiempo que el administrador debe emplear en mantener actualizado el sistema.

- **Análisis de firmas.** Mantiene una base de datos de correos clasificados como spam y compara los mensajes entrantes con la base de datos en busca de un positivo. De esta manera, los mensajes no deseados conocidos son rápidamente filtrados.

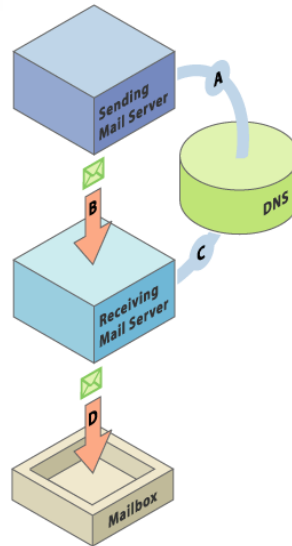
Lamentablemente, los spams están siendo continuamente modificados para evitar su clasificación en base a esta técnica, lo que ha reducido en gran medida la efectividad de este sistema.

- **Listas negras.** Las RBLs (Real time Black hole Lists) es un sistema automático y distribuido de compartir listas de spams por la red. Cuando un administrador informa de que una dirección IP está enviando spam, el sistema le manda un mensaje de prueba para validar su existencia y procede a añadirlo a la lista negra compartida.

Estas listas están en desuso debido a la incapacidad para detectar cuando la IP pertenece a un spammer real o si se trata de un usuario cuya cuenta ha sido usurpada por el remitente, en cuyo caso estaríamos bloqueando a un inocente.

- **Procesado de Lenguaje Natural.** Combina el análisis sintáctico, morfológico y práctico para correlacionar texto con categorías de significados. Permite detectar spams muy sutiles a través de conceptos multi-palabra en lugar de palabras clave. Su rendimiento suele ser muy bajo.
- **Solicitud / Respuesta.** Obliga al emisor a verificar su identidad antes de que el correo sea procesado. Esta técnica es demasiado intrusiva y aumenta la carga del servidor de correo al tener que enviar un correo al remitente por cada mensaje potencialmente clasificado como spam. Además, el proceso de validación retrasa la entrega del mensaje si el remitente ya no está conectado.
- **Autenticación.** Es una técnica consiste en facilitar la identificación del spam antes incluso de que llegue al perímetro de la empresa.

Así, por ejemplo, **DomainKeys** es un mecanismo empleado por Yahoo para verificar los dominios de cada uno de los remitentes de correo y garantizar la integridad de los correos enviados mediante firma electrónica.



**Ilustración 1 - Mecanismo de validación de DomainKeys**

De manera similar, Microsoft ha publicado su propio protocolo: **Sender-ID**, con similar objetivo, salvo que en lugar de acudir al DNS como intermediario para resolver el dominio acude al propio emisor del mensaje.

En contra de este concepto subyace la escasa base instalada hasta la fecha y los retrasos que el proceso de autenticación origina en la fase de validación.

- **Filtrado colaborativo.** El usuario final decide qué mensajes constituyen spam. Esta técnica es ideal para estaciones, pero puede provocar colisiones cuando se aplica en el servidor de correo.
- **Enfoque mixto.** Esta técnica combina varias técnicas de análisis para conseguir mayor precisión en la detección. Si no se hace correctamente, puede igualar a la suma de falsos positivos detectados por cada técnica individual en lugar de su intersección. Adicionalmente, puede presentar problemas de rendimiento.

### 5.1.1 Filtros Bayesianos

El filtrado bayesiano se basa en el principio de que la mayoría de los sucesos son dependientes de otras variables y de que la probabilidad de que un suceso sucede en el futuro puede deducirse a partir de la ocurrencia en el pasado del mismo.

Así, si una cadena de texto se repite con frecuencia en los correos no deseados, mientras rara vez se da en un correo normal, entonces la próxima vez que el sistema encuentre dicha cadena de texto en un correo es razonable que lo clasifique como spam.



Este algoritmo **permite el entrenamiento del sistema** para diferenciar automáticamente mensajes de spam de los que no lo son. Además, este filtro registra el correo saliente de la empresa, lo que le permite corregir la probabilidad en caso de que la cadena se utilice con alta frecuencia en las comunicaciones oficiales de la compañía.

Por ejemplo, si la palabra "gasolina" aparecieran en 200 de cada 5.000 spams y en 1 de cada 500 correos normales, entonces  $A_i = \{\text{correos spam, correos normales}\}$  y por el Teorema de Bayes, la probabilidad de spam condicionada por la palabra "gasolina" sería:

$$P(A_1 / gas) = \frac{P(gas / A_1)}{P(gas / A_1) + P(gas / A_2)} = \frac{200 / 5000}{(200 / 5000) + (1 / 500)}$$

Por tanto, parece razonable pedir a las soluciones tecnológicas utilizadas para minimizar los efectos del spam que sean capaces de utilizar una combinación de técnicas, incluyendo el análisis bayesiano, para frenar el spam sin importar el formato que utilicen en sus envíos e involucrando a todos los miembros de la organización en la lucha contra este tipo de amenazas.

### 5.2 ¿Quién debe frenar el spam en su organización?

Existen sistemas de filtrado de contenidos capaces de llevar a cabo esa labor, y que pueden ser fácilmente configurados por el administrador o persona encargada de mantener los equipos informáticos de la empresa. Pero si, además, el sistema anti-spam está integrado en una completa solución de seguridad como **EnterpriSecure 2006 Tecnologías TruPrevent™** que aglutina protección anti-spam tanto para puestos de trabajo (**Panda ClientShield 2006 con Tecnologías TruPrevent™**) como para servidores de correo (**Exchange, Sendmail, Qmail, Postfix**) seremos capaces de neutralizar todos los peligros del spam.

Ahora que tenemos claro la importancia de combinar la funcionalidad antivirus con la protección anti-spam, llega el momento de implantar dicha protección en la compañía. Y en este caso, como siempre, el **administrador** debe marcar la arquitectura y las políticas de seguridad anti-spam, aunque el **usuario final** debería contar con voz y voto en la clasificación de su correo (técnica de filtrado colaborativo).

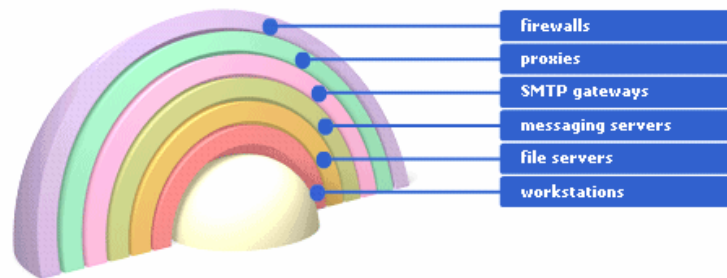


### 5.2.1 Falsos positivos

El número de soluciones que ofrecen "**cuarentena**" en los servidores de correo para mantener los mensajes sospechosos de spam para una revisión manual posterior es bastante alta. Sin embargo, este enfoque obliga al administrador a emplear mucho tiempo en dicha revisión. Es por ello, que Panda ofrece ese mecanismo de **almacenamiento temporal** en las estaciones de trabajo con el fin de reducir los costes del departamento de sistemas sin retrasar la llegada de los correos a sus destinatarios.

### 5.3 ¿Dónde es mejor poner los controles?

La protección Anti-spam se ha convertido en una necesidad para las empresas. Y sin duda, la mejor alternativa es contar con soluciones para proteger contra el spam en cada uno de los niveles o capas de la red corporativa:



**Ilustración 2 – Estrategia de protección por capas de Panda Software**

Se puede proteger cada **estación de trabajo**. Por ejemplo, Panda cuenta con ClientShield 2006 con Tecnologías TruPrevent™, que identifica el spam y evita al destinatario perder su valioso tiempo leyendo el mensaje para descubrir que no es interesante para él.

Las soluciones que trabajan en estaciones de trabajo deben permitir al usuario acceder a información que de acuerdo a sus **necesidades individuales** no es spam, tal y como hace ClientShield, pues ésta es la principal ventaja de llevar el control a los nodos capilares de la red.

Y es que la gran desventaja de las soluciones anti-spam para estaciones es la incapacidad de actualizar y **gestionar dichas soluciones de forma remota y centralizada** por parte del administrador de red que pierde el control sobre la misma si se instala en cada PC un producto mono-puesto.



Sin embargo, en el caso de ClientShield, las actualización de reglas se realiza de forma remota y automática desde la consola de **AdminSecure**, la herramienta de instalación, despliegue, mantenimiento y supervisión de las soluciones corporativas de Panda, lo que permite definir unas **políticas de protección antivirus y anti-spam para toda la organización** y conocer el grado de cumplimiento de dichas políticas en cada equipo a través del flujo de comunicación que periódicamente se establece con cada máquina, en este caso con todas aquellas que tenga Panda ClientShield instalado.

También se deben proteger los **servidores de correo** y pasarelas SMTP evitando en gran medida, la circulación de los correos basura a través de la red.

Por último, se puede proteger el **perímetro** de la red, como hace Panda con su *appliance* GateDefender. De este modo se evita que los mensajes basura lleguen a entrar en la compañía, liberando, así, de trabajo a los servidores de correo y optimizando el tráfico interno.

### **5.4 La visión de Panda Software**

Dada la **capacidad de mutación** del spam para hacerse pasar como correo legítimo, se hace necesario el **mantenimiento y actualización** de la solución anti-spam con el fin de conseguir ratios de acierto constantes en el tiempo. Mientras la primera generación de productos anti-spam eran actualizados manualmente por el administrador, la **siguiente generación** de soluciones anti-spam, de las que Panda fue un precursora, **automatiza** el proceso y lo convierte en un servicio tal y como viene haciéndose con otras protecciones basadas en firmas como el antivirus.

Las soluciones anti-spam de Panda Software utilizan distintos tipos de análisis para determinar si un mensaje de correo es spam (bayesiano, heurístico, reglas, máquina de aprendizaje, etc), repartidos en más de 300.000 algoritmos que dan como resultado una aparición de falsos positivos cercana a cero.

Cada mensaje recibido se analiza en profundidad combinando las diferentes técnicas de análisis Anti-spam, para obtener una detección óptima del spam recibido.

Además, existe un fichero de firmas de spam que crece continuamente según se detectan nuevos mensajes spam en todo el mundo y que **EnterpriSecure 2006 con Tecnologías TruPrevent™** se actualiza cada hora de manera totalmente automática y transparente para el usuario.



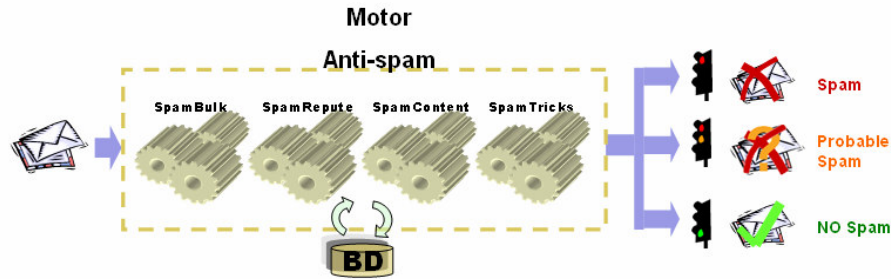
El análisis en profundidad de cada mensaje electrónico recibido hace que el resultado del análisis sea óptimo y que se reduzcan casi a cero los falsos positivos, al clasificar los mensajes recibidos como mensajes “*Spam*”, “*Probable Spam*” o “*No spam*”.

### 5.4.1 Operativa

El módulo Anti-spam de Panda **EnterpriSecure 2006 con Tecnologías TruPrevent™** cuenta con cuatro motores para analizar automáticamente el spam. Cada mensaje pasa por todos ellos para aumentar la fiabilidad del análisis. Estos motores utilizan técnicas multifunción (reglas, heurístico, bayesianos, listas, machine learning, etc...), con más de 300.000 algoritmos que reducen al máximo los falsos positivos.

Cada mensaje recibido atraviesa los cuatro motores de análisis para ser clasificado como *spam*, *probable spam*, o *no spam*, lo que dota de gran fiabilidad al sistema. Los cuatro motores son:

- **SpamBulk.**- Compara el mensaje con una lista interna de mensajes spam conocidos que han sido enviados masivamente con anterioridad
- **SpamRepute.**- Comprueba si el remitente está en la lista interna de remitentes de spam conocidos
- **SpamContent.**- Analiza el contenido del mensaje, comprobando el estilo, el diseño del mensaje, el idioma y el texto, dividiéndolo en unidades mínimas para detectar palabras clave, incluso, aunque la forma de escribir las palabras difiera de la correcta (GRATIS= G – R – A – T – I – X)
- **SpamTricks.**- Analiza si el mensaje contiene trucos técnicos utilizados habitualmente por los generadores de spam: Estos trucos pueden ser de distintos tipos. Por ejemplo, **EnterpriSecure 2006 con Tecnologías TruPrevent™** es capaz de detectar
  - Tácticas empleadas por los generadores de spam para reducir los costes de envío de grandes volúmenes de información (mensajes con una sola imagen, ocultación HTML, etc)
  - Tácticas empleadas por los generadores de spam en los mensajes para evitar los filtros Anti-spam, spam fraudulento...

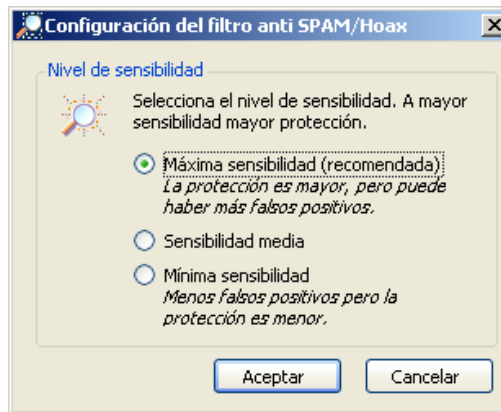


**Ilustración 3 – Arquitectura de protección anti-spam de Panda Software**

Tras atravesar los cuatro motores se obtiene un porcentaje de certeza que determina si el mensaje es *Spam* con seguridad, está cerca de serlo, en cuyo caso se considerará *Probable spam* o es un mensaje normal que no puede ser considerado como spam o probable spam.

Tanto el aprendizaje como la alimentación de los datos sobre nuevos mensajes spam o nuevos spammers se realiza remotamente y se actualiza automáticamente cada hora minutos sin necesidad de intervención del usuario.

El administrador del sistema puede definir el nivel de sensibilidad de los servidores y pasarelas de correo entre **Alto**, **Medio** y **Bajo**. Para ajustar más la solución a las necesidades de cada empresa, sin obligar al usuario final a tomar decisiones.



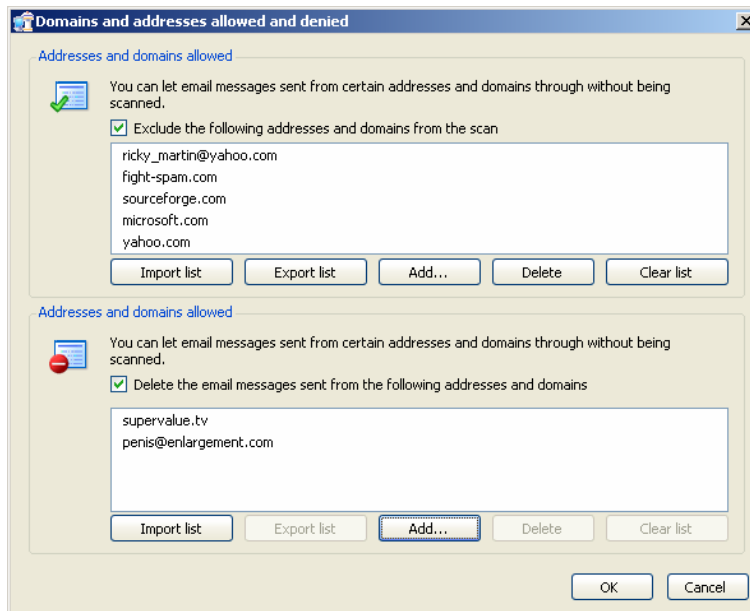
**Ilustración 4 – Fijación del nivel de sensibilidad de la protección anti-spam**

De este modo, un análisis con un nivel de sensibilidad **Alto**, detectará un mayor número de mensajes spam, aunque también aumentará el riesgo de falsos positivos. Por el contrario, con un nivel de sensibilidad **Bajo**, pocos mensajes serán clasificados como spam, pero se tendrá la certeza de no incurrir en falsos positivos.



Aparte del análisis automático que realiza siempre **EnterpriSecure 2006 con Tecnologías TruPrevent™**, el administrador puede definir manualmente una **lista blanca** con remitentes de confianza cuyos correos no serán analizados y no serán **nunca considerados spam**.

El administrador también puede definir una **lista negra** con remitentes cuyos correos serán **siempre considerados spam**, sin necesidad de analizarlos.



**Ilustración 5 – Inclusión de listas blancas y negras de protección anti-spam**

En la listas blanca y negra, los remitentes se pueden identificar:

- Por la dirección de correo del emisor del mensaje
- Por el dominio del emisor del mensaje

Las acciones a realizar con los mensajes clasificados como spam y con los clasificados como probable spam, se definen por separado, ya que pueden ser diferentes. El administrador también podrá definir **diferentes acciones** dependiendo del lugar donde se ubique la protección. Así por ejemplo, para las pasarelas SMTP es posible:

- **Dejar pasar el mensaje** y marcarlo en el asunto para que el destinatario lo identifique fácilmente como correo basura.
- **Borrar el mensaje**, es decir bloquearlo para que no llegue al destinatario final.
- **Mover el mensaje** a un buzón de spam para su posterior administración. Opcionalmente, estos mensajes también pueden marcarse, por si el administrador desea recibir una copia.



## 5.4.2 Panda ExchangeSecure

Otro tipo de soluciones anti-spam residen en el servidor de correo electrónico de la empresa, y se integra a través de *plug-ins* en Microsoft Exchange. Bloquear el spam en este punto de la red ahorra mucho a la empresa en términos de productividad del empleado, que no pierde tiempo configurando y aprendiendo a usar la herramienta anti-spam.

La protección **ExchangeSecure** verifica en su totalidad el correo electrónico de su compañía. Los archivos adjuntos son analizados en memoria, los archivos sospechosos son detectados con análisis heurístico, las políticas corporativas se garantizan al filtrar contenidos ofensivos y el **spam o correo no solicitado es bloqueado antes de llegar a los buzones** de sus destinatarios. Todo ello gestionado desde un solo punto con **AdminSecure**, la consola de administración centralizada de Panda.

En el caso de Exchange Server 2003, con ExchangeSecure es posible a las **acciones** arriba mencionadas incluir la opción de marcar la cabecera del mensaje con la valoración **SCL (Spam Confidence Level)**<sup>3</sup> de Panda sobre el mismo.

Como ha podido comprobar, las soluciones tecnológicas de Panda son capaces de resolver el problema del **spam minimizando los falsos positivos y automatizando** al máximo las tareas de **mantenimiento y actualización** sin resultar intrusivas en la privacidad de cada miembro de la organización. Todo ello empleando las **técnicas más modernas** de análisis y filtrado y dando cobertura anti-spam no sólo a estaciones de trabajo a través de **Panda ClientShield**, sino también a servidores de correo Microsoft Exchange con **ExchangeSecure** o pasarelas de correo Linux como **Sendmail, Qmail o Postfix**.

Además todas las **directivas de seguridad** relativas al spam pueden ser gestionadas a través de un **interfaz único** por el administrador de red, que utilizando la herramienta AdminSecure puede actualizar y gestionar la protección anti-spam y antimalware de las estaciones y servidores de correo de su compañía. Para ello cuenta con informes, vistas y avisos de seguridad **consolidados en tiempo real**.

---

<sup>3</sup> Sistema de valoración normalizado de las probabilidades de que un mensaje sea spam. Esta valoración puede por ejemplo, ser utilizada por otra solución anti-spam con dato adicional para mejorar la protección global.



## 6 Resumen y conclusiones

El **impacto negativo** del spam en la productividad de las empresas es un hecho, y el volumen de correo no deseado crece día a día. Como casi siempre, adoptar **medidas preventivas** resulta más rentable que tener que corregir una situación indeseable que puede aumentar el riesgo de dañar la **reputación de la organización**.

Si bien la **protección legal** ante este tipo de amenazas ha avanzado considerablemente en el último año, es necesario **informar adecuadamente** a nuestros empleados sobre cómo prevenir y actuar en caso de recibir spam.

Gestionar en las empresas el spam de manera **exclusivamente manual** no es una opción. Al igual que tampoco lo es **dejar en manos de cada usuario** las políticas de protección a adoptar. Si bien es necesario involucrar a todos los miembros de la compañía en la defensa frente al spam, alguien – administrador de correo o de la red – debe coordinar estos esfuerzos. Y esa labor de **coordinación es mucho más sencilla** si el administrador cuenta con una herramienta como **AdminSecure** que permite la instalación, mantenimiento y supervisión de las distintas protecciones anti-spam sin necesidad de desplazarse a cada máquina para conocer su nivel de protección.

Sin embargo, una correcta administración remota de los sistemas anti-spam no garantiza que los falsos positivos sean una excepción. Es necesario contar con protecciones anti-spam que como **EnterpriSecure 2006 con Tecnologías TruPrevent™** sean capaces de dotar a cada capa de la infraestructura de nuestra red de una protección basada en las últimas técnicas de detección y filtrado, al mismo tiempo que permiten que el **usuario final** pueda revisar según su propia escala de valores el correo sospechoso de ser spam en una carpeta a tal fin.



# APÉNDICES



## APÉNDICE A. Panda Software en el mundo

### Oficinas Centrales Panda Europa

Ronda de Poniente 19  
Tres Cantos  
28760 Madrid, España  
Teléfono: +34 91 806 37 00  
E-mail: [info@pandasoftware.com](mailto:info@pandasoftware.com)

Panda Software Argentina  
Calle Roque Saenz Peña 1160, piso9b  
Buenos Aires  
Teléfono: +00 5411 43823448  
E-mail: [argentina@pandasoftware.com](mailto:argentina@pandasoftware.com)

Panda Software Brasil  
R. Alvarenga, 744 2º Andar,  
Sao Paulo – SP 05509-011  
Teléfono: +00 55 11 38163000  
E-mail: [alvaro.venegas@pandaabrasil.com.br](mailto:alvaro.venegas@pandaabrasil.com.br)  
[ricardo.bachetti@pandaabrasil.com.br](mailto:ricardo.bachetti@pandaabrasil.com.br)

Panda Software China  
Room 1003, 10F, Minfang Building,  
593 Fuxing Road(M),  
200020 Shanghai  
Teléfono: +86 21 2402 8800  
+86 21 2402 8526  
E-mail: [china@pandasoftware.com](mailto:china@pandasoftware.com)

Panda Software Dinamarca  
Kirke Værlosevej 24, 1. sal, mt.  
DK 3500 – Værlose  
Teléfono: +45 60 218 738  
E-mail: [denmark@pandasoftware.com](mailto:denmark@pandasoftware.com)

Panda Software Eslovenia  
Stari trg 5A,  
SI-8210 Trebnje  
Teléfono: +386 7 34 61 020  
E-mail: [slovenia@pandasoftware.com](mailto:slovenia@pandasoftware.com)

Panda Software Francia  
33 bis Boulevard Gambetta,  
78300 Poissy  
Teléfono: +33 1 30 06 15 15  
E-mail: [france@pandasoftware.com](mailto:france@pandasoftware.com)

Panda Software Holanda  
Stephensonweg 14  
4207 HB Gorinchem  
Teléfono: +31 183 699020  
E-mail: [netherlands@pandasoftware.com](mailto:netherlands@pandasoftware.com)

Panda Software Italia  
Viale E. Marelli 165  
20099 Sesto S. Giovanni (MI)  
Teléfono: 02-24 20 22 08  
E-mail: [italy@pandasoftware.com](mailto:italy@pandasoftware.com)

### Oficinas Centrales de Panda en EE.UU.

230 N. Maryland, Suite 303  
P.O. Box 10578  
Glendale, CA 91209, USA  
Teléfono: +00 1 818 543 6901  
E-mail: [usa@pandasoftware.com](mailto:usa@pandasoftware.com)

Panda Software Austria  
Rennweg 98 Top 7  
A – 1030 Wien  
Teléfono: +49 02065 987654  
E-mail: [austria@pandasoftware.com](mailto:austria@pandasoftware.com)

Panda Software Bulgaria  
26-28, Christo Stanihev str.  
Sofia 1225  
BULGARIA  
Teléfono: +359 2 81 328 11  
E-mail: [bulgaria@pandasoftware.com](mailto:bulgaria@pandasoftware.com)

Panda Software Colombia  
Carrera 41 N.46-26 Itagui  
Antioquia  
Teléfono: + 57 4-3735588  
E-mail: [colombia@pandasoftware.com](mailto:colombia@pandasoftware.com)

Panda Software El Salvador  
63 Ave, Sur Local 3 Centro Financiero Gigante, Nivel 5, San  
Salvador, El Salvador  
Teléfono: (503) – 2287- 4194  
E-mail: [elsalvador@pandasoftware.com](mailto:elsalvador@pandasoftware.com)

Panda Software España  
Ronda de Poniente 19  
Tres Cantos  
28760 Madrid  
Teléfono: 902 365 505  
E-mail: [info@pandasoftware.es](mailto:info@pandasoftware.es)

Panda Software Gran Bretaña  
5 Signet Court, Swanns Road  
Cambridge CB5 8LA  
Teléfono: +44 (0)870 444 5640  
E-mail: [uk@pandasoftware.com](mailto:uk@pandasoftware.com)

Panda Software Hungría  
Szugló utca 54  
1145 Budapest  
Teléfono: +36 1 469 70 97  
E-mail: [hungary@pandasoftware.com](mailto:hungary@pandasoftware.com)

Panda Software Japón  
Nakameguro GT Tower 7F, 2-1-1 Kamimeguro,  
Meguro-ku, Tokyo 153-0051  
Teléfono: +81-3-6412-6020  
E-mail: [japan@pandasoftware.com](mailto:japan@pandasoftware.com)

Panda Software Alemania  
Dr.-Delllev-Karsten-Rohwedder-Str. 19  
47228 Duisburg  
Teléfono: +49 20 65 9 87 654  
E-mail: [germany@pandasoftware.com](mailto:germany@pandasoftware.com)

Panda Software Bélgica  
Mechelen Campus  
Schaliënhoedreef 20d  
2800 Mechelen  
Belgium  
Teléfono: +32 2 756 08 80  
E-mail: [belgium@pandasoftware.com](mailto:belgium@pandasoftware.com)

Panda Software Canadá  
100 Allstate Parkway  
Suite 502  
Markham  
ON L3R6H3  
Teléfono: +1 (905) 479 2208  
E-mail: [canada@pandasoftware.com](mailto:canada@pandasoftware.com)

Panda Software Corea del Sur  
3Fl. SungWoo Bldg, 114-29  
SamSung-Dong, KangNam-Gu,  
Seoul - Korea  
Teléfono: +82-2-555-8600  
E-mail: [korea@pandasoftware.com](mailto:korea@pandasoftware.com)

Panda Software Emiratos Árabes Unidos  
Bldg-5 Office No. 5G-15  
P O Box 41573 – Hamriyah  
Free Zone, Sharjah  
Teléfono: +971 (6-526.30.14)  
E-mail: [UAE@pandasoftware.com](mailto:UAE@pandasoftware.com)

Panda Software Estados Unidos  
230 N. Maryland, Suite 303  
P.O. Box 10578  
Glendale, CA 91209, USA  
Teléfono: +00 1 818 543 6901  
E-mail: [usa@pandasoftware.com](mailto:usa@pandasoftware.com)

Panda Software Grecia  
82 Zanni St.  
Piraeus, ZIP Code 18537  
Teléfono: +30 2 10 4588 085  
E-mail: [greece@pandasoftware.com](mailto:greece@pandasoftware.com)

Panda Software India  
E-9, Connaught House  
Connaught Place  
New Delhi-110001  
Teléfono: +91 11 2341 8199  
E-mail: [india@pandasoftware.com](mailto:india@pandasoftware.com)

Panda Software Letonia  
Merkela Street 1  
1050 Riga  
Teléfono: +371 7211636  
E-mail: [latvia@pandasoftware.com](mailto:latvia@pandasoftware.com)

Panda Software Arabia Saudi  
P.O.BOX # 2797,  
AL KHOBAR 31952, KSA  
Teléfono: + 966 3 897 9956  
E-mail: [saudiarabia@pandasoftware.com](mailto:saudiarabia@pandasoftware.com)

Panda Software Bolivia  
Calle Landaeta # 221,  
Edificio Gamarra 3er Piso  
La Paz – Bolivia  
Código postal 11433  
Teléfono: +591 2 211 4777  
E-mail: [bolivia@pandasoftware.com](mailto:bolivia@pandasoftware.com)

Panda Software Chile  
Mosquito 459 ofic. 202  
8320112, Santiago-Centro  
Chile  
Teléfono: +56 2 639 7541  
E-mail: [chile@pandasoftware.com](mailto:chile@pandasoftware.com)

Panda Software Costa Rica  
Calle 25, Ave 6 y 8 #648  
San José  
Teléfono: 00 506 258 0100  
E-mail: [costarica@pandasoftware.com](mailto:costarica@pandasoftware.com)

Panda Software Eslovaquia  
Lublanska 1  
83102 Bratislava  
Teléfono: +421 2 444 55 702  
E-mail: [slovakia@pandasoftware.com](mailto:slovakia@pandasoftware.com)

Panda Software Finlandia  
Hatarpään valtatie 8  
33100 Tampere  
Dirección postal: P.O BOX 636. 33101 Tampere  
Teléfono: +358 3 339 26 700  
E-mail: [finland@pandasoftware.com](mailto:finland@pandasoftware.com)

Panda Software Guatemala  
5 Av. 5-55 Zona 14, Euro plaza Torre 1 Nivel 2.  
Ciudad de Guatemala  
Teléfono: +502 2386-8866/67/68  
E-mail: [guatemala@pandasoftware.com](mailto:guatemala@pandasoftware.com)

Panda Software Israel  
43 Hamelacha street,  
New Industrial Zone  
42504 Natanya  
Teléfono: +972 9 – 8859611  
E-mail: [israel@pandasoftware.com](mailto:israel@pandasoftware.com)

Panda Software Lituania  
Žemaitės st. 21,  
LT – 2009 Vėlnius  
Teléfono: +370 5 2397833  
E-mail: [lituania@pandasoftware.com](mailto:lituania@pandasoftware.com)



## Spam, ¿cómo proteger a los usuarios de su empresa?



### Panda Software Luxemburgo

Mechelen Campus  
Schalènhoevredreef 20d  
2800 Mechelen  
Belgium  
Teléfono: +32 2 756 08 80  
E-mail: [luxembourg@pandasoftware.com](mailto:luxembourg@pandasoftware.com)

### Panda Software Paraguay

Eliseo Reclus 247 Calle Guido Spano  
Asunción  
Teléfono: +00 595 21 607594

E-mail: [paraguay@pandasoftware.com](mailto:paraguay@pandasoftware.com)

### Panda Software Puerto Rico / Rep. Dominicana

Avenida Muñoz Rivera 1058  
Edificio Fomento Corporativo  
Esquina Yale  
Río Piedras 00927 Puerto Rico  
Teléfono: +1 787 296 1139

E-mail: [caribe@pandasoftware.com](mailto:caribe@pandasoftware.com)

### Panda Software Suiza

Route Champ-Colin, 10  
1260 Nyon  
Teléfono: +41 22 994 89 40

E-mail: [switzerland@pandasoftware.com](mailto:switzerland@pandasoftware.com)

### Panda Software Venezuela

Av. Libertador  
C.C. Libertador, PH-7  
Caracas  
Teléfono: +(58 212) 700.7596  
E-mail: [venezuela@pandasoftware.com](mailto:venezuela@pandasoftware.com)

### Panda Software Malasia

Unit A-10-6, Megan Phileo Promenade,  
189 Jalan Tun Razak,  
50400 Kuala Lumpur  
Teléfono: +60 3 2163 2468  
E-mail: [malaysia@pandasoftware.com](mailto:malaysia@pandasoftware.com)

### Panda Software Peru

Calle Lord Cochrane 521  
Miraflores – Lima 18  
Teléfono: 00 51 1 221 6001/ 221 0159

E-mail: [peru@pandasoftware.com](mailto:peru@pandasoftware.com)

### Panda Software Rusia

64-47 Tokarey St.,  
620109 Yekaterinburg, Sverdlovsk region  
Teléfono: +7 3432 78-31-27  
E-mail: [russia@pandasoftware.com](mailto:russia@pandasoftware.com)

### Panda Software Tailandia

192 Soi Laprao 107  
Bangkapi, Bangkok 10240  
Teléfono: 00 662 7311480

E-mail: [thailand@pandasoftware.com](mailto:thailand@pandasoftware.com)

### Panda Software México

Tuxpan 39# 104 y 105,  
06760 México, D.F.  
Teléfono: +52 5 2642127

E-mail: [mexico@pandasoftware.com](mailto:mexico@pandasoftware.com)

### Panda Software Polonia

Ul. Wiktorska 63  
02-587 Warszawa  
Teléfono: +48 (22) 540 18 06

E-mail: [poland@pandasoftware.com](mailto:poland@pandasoftware.com)

### Panda Software Singapur

10 Ubi Crescent, # 05-37  
Ubi Techpark, Singapur 408564  
Teléf:+ (65) 6742 2660  
E-mail: [singapore@pandasoftware.com](mailto:singapore@pandasoftware.com)

### Panda Software Turquía

Darulaceze Cad  
Karatlas Sok. SNS Plaza N° 6  
80270 OKMEYDANI – ISTANBUL  
Teléf.: 90 212 222 1520/90 212 210 2200  
E-mail: [turkey@pandasoftware.com](mailto:turkey@pandasoftware.com)

### Panda Software Noruega

ViroSafe Norge AS  
Skogveien 41  
2318 Hamar  
Teléfono: 00 47 62 53 96 80

E-mail: [norway@pandasoftware.com](mailto:norway@pandasoftware.com)

### Panda Software Portugal

Quinta da francelha - Edificio Sagres, 7B  
2685-338 Prior Velho  
Teléfono: + 35 1 219426800

E-mail: [portugal@pandasoftware.com](mailto:portugal@pandasoftware.com)

### Panda Software Suecia

Industrivägen 7,  
S-171 48 Solna  
Teléfono: +46 8-545 25030

E-mail: [sveeden@pandasoftware.com](mailto:sveeden@pandasoftware.com)

### Panda Software Uruguay

Jose Enrique Godó 1955  
11200 Montevideo  
Teléfono: +5982 4020673

E-mail: [uruguay@pandasoftware.com](mailto:uruguay@pandasoftware.com)



## APÉNDICE B. Glosario de términos.

Nombre	Descripción
<b>Algoritmo</b>	Secuencia detallada de acciones a realizar para llevar a cabo una tarea. Así denominado, en honor del matemático iraní Al-Khwarizmi.
<b>Análisis heurístico</b>	Consiste en el método, estrategia o técnica empleada para hacer más fácil la resolución de problemas. Aplicado al mundo informático, se entiende como una técnica utilizada para detectar virus que en ese momento son desconocidos.
<b>Expresiones regulares</b>	Las expresiones regulares son metalenguajes que describen los lenguajes aceptados por los autómatas finitos, es decir, describen los lenguajes regulares. Un lenguaje regular está compuesto de combinaciones de símbolos y tres operadores: <u>Concatenación</u> . A concat B es cierto si un acierto de A va seguido de un acierto de B. <u>Or</u> – el patrón A OR B es cierto si A es cierto o B es cierto <u>Cierre</u> – cero o más aciertos para un patrón.
<b>Filtro de contenidos (Parental Lock)</b>	El filtrado de contenidos, también denominado "Parental Lock", permite definir a que tipos de contenidos Web no se permitirá el acceso. La definición se realiza por el tipo de contenido y no por la dirección Web, con lo que todas las Web que estén dentro de la categoría del contenido elegido como prohibido, no se les debe de permitir el acceso.
<b>Filtro de cookies</b>	Las cookies son pequeños ficheros de texto utilizados por los servidores Web para almacenar y consultar información del usuario al entrar en una de sus páginas Web desde un navegador.  La principal finalidad de la cookies es identificar al usuario y personalizarle las páginas que consulta.  Pero las cookies se pueden utilizar para almacenar información de navegación del usuario, gustos, etc., sin que tenga conciencia de ello  El filtro de cookies consiste en la posibilidad del bloqueo de cookies salientes (enviadas desde el navegador hacia el servidor), o entrantes (enviadas desde el servidor hacia el navegador para que se graben en el disco duro).
<b>Herramienta de hacking</b>	Programa que permite a los hackers realizar acciones que conllevan un riesgo de seguridad en otros ordenadores (spam, chequeo de puertos de comunicaciones, ataques de denegación de servicio -DoS-, etc.).
<b>Malware</b>	Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de los sistemas informáticos. MALicious softWARE.



<b>Plug-in</b>	Los navegadores soportan plug-ins o programas pequeños que visualizan o interpretan un formato de archivo o protocolo como: Shockwave, RealAudio, PDF, CMX (gráficos vectoriales). El archivo a visualizar queda incluido en la página web a través de una etiqueta HTML de tipo EMBED.
<b>Protección contra Dialers</b>	Un Dialer o marcador telefónico es un programa capaz de utilizar sin autorización el Modem de un equipo.
<b>Spam</b>	El Spam o correo electrónico basura, consiste en la recepción de forma indiscriminada de correos conteniendo anuncios de algún producto, provenientes de fuentes no solicitadas.
<b>Spyware</b>	<p>Se llama Spyware a aquellos programas, componentes ActiveX o elementos de código embebidos en correos y páginas Web, cuya finalidad es la obtención de información personal del Usuario (hábitos de navegación, gustos, preferencias de compra, datos bancarios, etc.) sin que este tenga conocimiento de ello, o haya dado su consentimiento conscientemente.</p> <p>Spyware son:</p> <p><b>WebBugs</b> Elementos incrustados en correos electrónicos y capaces de enviar a un servidor predeterminado información personal del usuario cuando este abre el e-mail.</p> <p><b>Cookies.</b> Programas que monitorizan los hábitos de navegación: programas que actúan de forma inadvertida registrando las páginas a las que se conecta un usuario, los programas que ejecuta, etc.).</p>
<b>Virus</b>	Los virus son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.



## APÉNDICE C. Abreviaturas y siglas.

- CIO – Chief Information Officer
- CTO – Chief Technology Officer
- DBCS – Double Byte Character Set
- HTML – Hyper Text Markup Language
- ISP – Internet Service Provider
- IT – Information Technology
- NIC – Network Information Center
- RBL – Real time Black hole List
- SCL – Spam Confidence Level
- SMTP – Simple Mail Transfer Protocol
- UE – Unión Europea
- URL – Uniform Resource Locator

## APÉNDICE D. Bibliografía.

### Legislación de California

#### Restrictions On Unsolicited Commercial E-mail Advertisers

<http://www.spamlaws.com/state/ca1.html>

### Directiva Europea 2002/58/CE

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=ES&numdoc=32002L0058&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=ES&numdoc=32002L0058&model=guichett)

### Microsoft Sender-ID

<http://www.microsoft.com/mscorp/safety/technologies/senderid/overview.aspx>

### Yahoo DomainKeys

<http://es.antispam.yahoo.com/domainkeys>