

# Instrucciones de Funcionamiento del Sistema

## AntiVirus y AntiSpam Profesional

v2.0

Si su dominio ha sido incluido en el sistema de control de AntiVirus y AntiSpam Profesional de DEINFO Servicios Informáticos es recomendable que lea las siguientes instrucciones para conocer el funcionamiento del sistema y trabajar correctamente con los elementos de la *cuarentena*.

Para empezar explicaremos el recorrido de los mensajes desde que los envía un remitente en internet y llegan a su buzón. Un mensaje sigue los siguientes pasos:

- El remitente escribe un mensaje para Usted en su programa de correo y lo envía.
- El programa de correo contacta con el servidor de correo (correo saliente SMTP del remitente) y entrega el correo a dicho servidor.
- El servidor remitente valida el remitente y el mensaje y comprueba que el dominio (parte derecha de la “@”) existe en internet y que puede contactar con su servidor de correo.
- El servidor remitente y el del destinatario se ponen en comunicación, en caso de que el servidor destinatario acepte la comunicación (nota 1) el mensaje se entrega en el servidor destinatario.
- El servidor destinatario procesa el mensaje pasándolo por diferentes filtros (nota 2).
- El mensaje validado se entrega en el buzón del destinatario.
- El usuario destinatario recibe el mensaje en su buzón de correo (normalmente a través de POP3).

Todas estas transacciones y otras internas que realizan los servidores se procesan en cuestión de milésimas de segundo, aunque evidentemente pueden existir momentos en que algún servidor intermedio, líneas de comunicaciones, saturación de servidores, procesos, etc. haga que los mensajes tengan algún retraso.

Hace algunos años, cuando no existía o apenas había correo spam, siempre se decía un mensaje siempre lo recibía el destinatario o en el peor de los casos, el remitente recibía una notificación informando del error. Es decir, que teníamos la confianza de que un mensaje llegaba al destinatario. Por desgracia hoy en día esto no es así. En nuestro sistema estándar antispam (no el Profesional) se reciben cada mes unos 40.000.000 (sí, 40 millones) de mensajes de los cuales sólo el 2% ó 3% son correos buenos que llegan a sus buzones sin marcar y un 0,6% llegan como posible spam (marcado en el asunto). Esto quiere decir que se rechazan mensualmente 38.560.000 mensajes. El rechazo viene dado por diferentes razones que explicaremos a continuación. Como es obvio, no se pueden contestar estos 38 millones de mensajes dando una explicación del rechazo, se generaría un sobre tráfico impresionante además de que realmente todos estos mensajes son spam y no hay que dar ningún tipo de explicación a su remitente.

## **Causas de bloqueo de los mensajes**

Según todo lo comentado existen varios puntos de control/validación de los mensajes y varias causas por las que un mensaje o su contenido puede ser filtrado.

### **Posibles causas en el remitente:**

De entrada muchos servidores remitentes comprueban el mensaje y lo rechazan en caso que la conexión del usuario (la ADSL) esté incluida en una alguna *lista negra*.

También muchos servidores rechazan el correo si supera ciertos límites, como por ejemplo: el tamaño del mensaje, el tipo de adjuntos, el número de destinatarios en el "Para:", si el asunto está en blanco, etc.

También puede ser motivo de rechazo del mensaje si éste contiene algún virus informático. Normalmente si es el servidor remitente el que rechaza un mensaje, el usuario remitente recibe un mensaje informando de la causa y es el usuario ó administrador del servidor remitente que debe dar una solución/explicación del problema.

### **Posibles causas en el destinatario:**

En el destinatario puede haber distintas causas y, digamos efectos, por los que un mensaje se rechaza o altera.

En primer lugar los servidores realizan una comprobación de la dirección IP del remitente contra unas listas públicas de direcciones en *listas negras* (blacklist). Si un servidor está en una de estas listas es prácticamente seguro que se le bloquee el envío de correo. En este caso el correo se rechaza sin ninguna comprobación adicional. Existen listas negras generales, del sistema antispam, y personales de cada usuario/buzón. Una de las listas negras públicas más conocidas es la que se mantiene en <http://www.spamhaus.org>.

Desde esta página se pueden realizar consultas para saber si una IP está listada o no: <http://www.spamhaus.org/sbl/index.lasso>.

Una vez pasada la lista negra, los mensajes se contrastan con toda una serie de reglas. Cada una de estas reglas otorga una puntuación a cada mensaje. Dependiendo de la puntuación recibida un mensaje se clasifica como spam o no. También dependiendo de estas reglas los mensajes se eliminan, pasan a la cuarentena o se entregan al buzón del destinatario. Existen muchas reglas de comprobación diferentes y la descripción de cada una de ellas es larga, puede consultarnos si necesita más información al respecto. Los nombres de algunas de estas reglas son: black IP scan, greylist, DNSBL, header analysis, SURBL, bayesian, heuristic, dictionary scan, banned Word scan, image spam scan, etc.

Otro motivo de rechazo, o en este caso de modificación del cuerpo y contenido del mensaje es si éste contiene algún virus. En este caso se elimina el fichero que contiene el virus y se notifica al destinatario del nombre del fichero y el virus que contenía.

Tanto las reglas de antispam como las definiciones de antivirus se actualizan cada 4 horas, ya que continuamente están apareciendo reglas para combatir nuevas formas de spam, virus, etc. Todas estas reglas pueden ser configuradas para cada uno de los dominios.

## Funcionamiento de la cuarentena

Como ya hemos comentado, existe un buzón intermedio, previo al buzón donde Usted recoge los mensajes, donde se envían los mensajes con ciertas dudas sobre si es o no spam o aquellos que cumplen unas reglas concretas.

Este buzón de cuarentena está almacenado en un servidor de DEINFO y funciona de la siguiente forma:

- Es un buzón automático, se crea cuando hay mensajes que almacenar en él.
- Si tiene mensajes en el buzón de cuarentena, recibirá un mensaje cada día a las 8:00h y a las 15:00h con la lista de mensajes que hay en el buzón y las acciones que puede realizar con cada uno de los mensajes y en general.
- Puede acceder a consultar y gestionar el buzón de cuarentena en cualquier momento entrando en <https://antispam.deinfo.es> con su dirección de correo y contraseña.

En la siguiente imagen se muestra el mensaje que se recibe notificando de la existencia de mensajes en su buzón de cuarentena:

Asunto: Resumen de la Cuarentena: [ 1 mensaje(s) en cuarentena desde Sun, 12 Oct 2008 15:00:00 a Sun, 12 Oct 2008 18:40:14 ]

Date:	From:	Subject:	Web Actions:	Email Actions:
Sun, 12 Oct 2008 17:37:16	Бакнев <thumbingux6247@dayassociates.com>	Сериалы на DVD - теперь дешевле	<a href="#">Release</a> <a href="#">Delete</a>	<a href="#">Release</a> <a href="#">Delete</a>

Acciones via Web:  
Pulsa en el enlace [Release](#) para enviar una instrucción http(s) y que el mensaje se envíe a tu buzón.  
Pulsa en el enlace [Delete](#) para enviar una instrucción http(s) y que se elimine el mensaje de la cuarentena.  
[Pulsa aquí](#) para enviar una instrucción http(s) para Borrar TODOS los mensajes de la cuarentena.

Acciones por Correo:  
Pulsa en el enlace [Release](#) para enviar un mail y que el mensaje se envíe a tu buzón.  
Pulsa en el enlace [Delete](#) para enviar un mail y que el mensaje se elimine de la cuarentena.  
[Pulsa aquí](#) para enviar un mail para Borrar TODOS los mensajes de la cuarentena.

Otras acciones:  
Para ver tu bandeja de cuarentena o modificar tus preferencias, [Pulsa aquí](#)

Nota: The sender of a released message will be added to your white list.

Estos mensajes se reciben de la cuenta [release-ctrl@antispam.deinfo.es](mailto:release-ctrl@antispam.deinfo.es).

Siguiendo las indicaciones que se muestran en el mensaje, puede liberar y enviar a su buzón mensajes en cuarentena, eliminarlos o la acción global de eliminar TODOS los mensajes de la cuarentena. Los remitentes de mensajes liberados se añaden automáticamente a su lista blanca personal.

Estas acciones las puede realizar tanto de forma directa a través de web si dispone de conexión a internet en ese momento o realizarlo por correo electrónico. En este último caso se generará automáticamente un mensaje en el cual sólo deberá pulsar sobre el botón "Enviar" para enviar la instrucción seleccionada, no modifique el Asunto.

Si accede a su buzón de cuarentena en <https://antispam.deinfo.es> podrá gestionar igualmente los mensajes en la cuarentena y otras funciones personales del control antispam. En la siguiente imagen se muestra el aspecto del buzón de cuarentena:

DEINFO Gestión del servicio AntiSpam y AntiVirus Profesional

Mensajes en Cuarentena Preferencias [Desconectar] [Ayuda]

Utilización en su cuenta de correo: 1.03MB

**Correo basura** (Mensajes: 1-2 Total: 2)  
Paginas: 1

Borrar Agregar a Lista Negra Agregar a Lista Permitida Definir como SPAM Definir como Válido Liberar correo More Actions...

Estado	De	Asunto	Recibido en:
<input type="checkbox"/>	blane marvin	Регистрация на конференции RMzsc	4:19 PM
<input type="checkbox"/>	"Саша"	Классное видео с писающими крошками	4:05 PM

Borrar Agregar a Lista Negra Agregar a Lista Permitida Definir como SPAM Definir como Válido Liberar correo More Actions...

**Correo basura** (Mensajes: 1-2 Total: 2)  
Paginas: 1

Lo primero que hay que hacer al entrar en cuarentena si el buzón está en inglés, es cambiarlo de idioma. Para ello debemos entrar en la pestaña de “Preferencias” y seleccionar “Español” (o el idioma que queramos) en el desplegable “Language:”. Luego pulsamos en uno de los botones “Save” que aparece en la parte superior o inferior.

Desde esta ventana podrá realizar las siguientes acciones sobre los mensajes seleccionados:

**Borrar** los mensajes.

**Agregar a Lista Negra.** Agrega el remitente a una lista negra personal para que desde ese momento se elimine automáticamente cualquier mensaje recibido del mismo remitente.

**Agregar a Lista Permitida.** Agrega el remitente a una *lista blanca* personal para que desde ese momento se acepten y no vayan a la cuarentena los mensajes recibidos del mismo remitente.

**Definir como SPAM.** Informa a la base de datos de reglas *Bayesian* que el mensaje seleccionado es spam.

**Definir como Válido.** Informa a la base de datos de reglas *Bayesian* que el mensaje seleccionado no es spam.

**Liberar correo.** Libera el mensaje de la cuarentena y lo entrega a su buzón.

Cuando definamos un mensaje como SPAM, como Válido ó lo Liberemos, después debemos eliminarlo (opción Borrar) para que desaparezca definitivamente de la Cuarentena.

Más abajo se muestra la pantalla de “Preferencias”. Desde esta ventana podrá gestionar la base de datos Bayesian y ver el resumen de los mensajes que se le han enviado y cuántos han sido bloqueados como spam a través de la base de datos bayesiana y cuantos no.

También podrá gestionar las direcciones que ha incluido en las listas negras y blancas.

Todos los cambios de listas negras, blancas, etc. que puede realizar aquí afectan únicamente a su buzón.

En la siguiente imagen hemos resaltado en amarillo la opción de selección del Idioma y la de las “Listas Negras/Permitidas” (blacklist/whitelist).


**Gestión del servicio AntiSpam y AntiVirus Profesional**

Mensajes en Cuarentena | **Preferencias** | gpuig@deinfo.es [Desconectar] [Ayuda]

**Mostrar preferencias:**  
 Orden de mensajes(Predeterminado) :  Por Fecha en Orden Ascendiente  Por Fecha en Orden Descendiente  
 Seleccionar columnas extra:  Fecha  Tamaño  
 Mensajes por página : 25  
 Idioma : Español  
 Zona horaria: (GMT+1:00)Brussels,Copenhagen,Madrid,Paris

**Administración de cuenta de correo:**  
 Tiempo de espera máximo sin uso: Ilimitado

**Configuración Antispam:**  
 Base de datos Bayesiana:

Resumen	
Total de mensajes reconocidos como "SPAM":	564
Total de mensajes reconocidos como "NO SPAM":	102
<b>La base de datos de usuario Bayesiana NO ESTÁ aplicada/habilitada/funcional.</b>	
<b>Opciones</b>	
<a href="#">Entrenar base de datos de usuario Bayesiana con un archivo "mbox"</a>	
<a href="#">Respaldar base de datos de usuario Bayesiana</a>	
<a href="#">Restaurar base de datos de usuario Bayesiana</a>	
<a href="#">Borrar la base de datos Bayesiana de usuarios</a>	

Agregar la dirección de correo de destino a la lista "Permitida":  Activado  Desactivado  
 Listas Negras/Permitidas: Negras, Blanco  
 Recibir informe de spam:  Activado  Desactivado

**Preferencias:**  
 Cuenta principal : Ninguna  
 Cuentas secundarias : Ninguna

## Términos utilizados

**Bayesian:** Es una de las reglas a través de la que se analizan los mensajes para considerarlos o no spam. Es una base de datos que "aprende" según el tipo de mensajes recibidos. Por lo que cuanto más tiempo lleva de aprendizaje mejores son sus resultados.

**Cuarentena:** buzón temporal o intermedio donde van a parar los mensajes sospechosos antes de entregarse a su buzón o ser eliminados.

**Lista Blanca (whitelist):** lista de direcciones de correo, dominios, conexiones que se permiten.

**Lista Negra (blacklist):** lista de direcciones de correo, dominios, conexiones que se rechazan. Todo lo que esté dado de alta en una lista negra se rechaza sin ningún otro tipo de comprobación.

**Spam:** correo no deseado o no solicitado.