

Panda Security

Email Protection

Manual de Administrador

Versión 4.3.2-2



Tabla de contenidos

Tabla de contenidos	2
1. Introducción a Email Protection	3
2. Interfaz de Email Protection	5
3. Funciones adicionales	68
4. Soporte técnico	69

1. Introducción a Email Protection

1.1 ¿Qué es Email Protection?

Email Protection es una solución de seguridad para email basada en software como servicio (SaaS). El Software como Servicio le permite centrarse en su negocio, liberándolo de las tareas de gestión y de los costes operativos de las soluciones de seguridad tradicionales.

Email Protection consta de un sistema multicapas que combina distintos filtros y mecanismos de protección que emplean tanto tecnologías propias (Email Protection PROACTIVE, Listas de Confianza...) como tecnologías estándar (reputación de IPs, redes de Bayes, listas blancas y negras, greylists, traffic shaping...) para asegurar la máxima efectividad. Mediante la eliminación de spam, virus y phishing - empleando más de diez filtros diferentes -, no sólo se reduce la carga del servidor de correo electrónico, sino que también disminuyen los problemas de productividad relacionados al tiempo dedicado a la eliminación del spam.

Aparte de los filtros por conexión se proporcionan dos modos de filtrado: modo automático y modo garantizado.

Email Protection posee una interfaz intuitiva y de fácil configuración que permitirá al administrador poner en funcionamiento rápidamente los elementos de protección necesarios para la seguridad de la empresa.

1.2 Funcionalidades

Algunas de las funcionalidades de Email Protection son:

- Configuración centralizada
- Fácil administración
- Antispam multicapas
- Backup de correo entrante
- Alta de usuarios:
 - Manualmente
 - Importación desde archivo
 - LDAP call out con descubrimiento de Alias
 - SMTP call out
- Administrador por dominio

- Log de correos con posibilidad de abrir los correos (si se decidió por esta posibilidad al hacer la compra), agregar remitentes/IP's a lista blanca/negra, clasificar correos como Válido/Spam
- Listas de Confianza por usuario
- Filtros personalizados
- Notificador informativo

2. Interfaz de Email Protection

2.1 Acceso administrador

Se puede acceder al Panel de Control de Email Protection utilizando cualquier navegador en el que se introducirá la URL asignada por su administrador, agregando “/admin/” al final.



Le aparecerá un panel Web donde se tendrá que identificar con sus datos de usuario o administrador.

Si desea entrar como usuario y no recuerda su contraseña, puede pulsar la opción: “¿Ha olvidado su contraseña?”

2.2 Panel de Administrador

La interfaz de Email Protection es muy intuitiva y fácil de utilizar. Incluye cinco secciones:

- Gestión
- Filtrado
- Personalización
- Configuración
- Ayuda

2.2.1 Nota aclaratoria

Algunos de los Paneles de Administración están divididos en dos secciones:

- Configuración global: se escogen ciertas opciones que se aplicarán por defecto a todos los dominios.
- Configuración por dominio: se escoge si se quiere usar la opción estándar para todo el Servicio (opción Global) o se prefiere escoger otras opciones para el dominio en concreto.

Todos los Paneles de Administración han sido probados y funcionan en los siguientes navegadores:

- Internet Explorer ® 9
- Mozilla Firefox desde 6.x

Las resoluciones de pantalla soportadas son 1024x768 y superiores.

2.3 Gestión

En esta sección podrá administrar todos los aspectos relacionados a: usuarios, dominios y modos de alta a emplear.

2.3.1 Creación y edición de contraseñas

Email Protection solo acepta contraseñas seguras.

Al ingresar una contraseña, el sistema evalúa su seguridad, impidiendo ingresar contraseñas cuya fortaleza sea débil.

Sugerencias y restricciones para la creación de una contraseña segura:

- Letras minúsculas y mayúsculas de "a" a "z", exceptuando "ñ"
- Números del 0 a 9
- Símbolos permitidos: _ . -
- Longitud mínima de 8 caracteres y máxima de 64 caracteres.

2.3.2 Estado

Estado de suscripción

- Fecha de contratación.
- Fecha de expiración.
- Cantidad de licencias consumidas.
- Cantidad de licencias disponibles.

Email Protection

Fecha de contratación	22/02/2013
Fecha de expiración	22/04/2014
Cantidad de licencias disponibles	83
Cantidad de licencias consumidas	17

Estadísticas de correo entrante

- **Spam rechazados:** Número de mensajes spam rechazados por el Firewall de correos, ya sea por su alto contenido de Spam o por los filtros de conexión.

- **Spam:** Número de mensajes clasificados como spam. Se pueden consultar o recuperar mediante el Panel de Administrador, Panel de Usuario, informe de correo bloqueado o Notificador.
- **Correos pendientes de validación:** Número de mensajes provenientes de remitentes que aún no pertenecen a las listas blancas o negras de los destinatarios que utilizan el modo de filtrado garantizado.
- **Avisos de virus:** Número de mensajes que informan sobre correos en los que se ha detectado virus.
- **Avisos de servidor:** Número de mensajes que informan a los remitentes sobre problemas en la entrega de un correo.
- **Listas de correo:** Número de mensajes categorizados como lista de correo.
- **Correo válido:** Número de mensajes que han pasado todos los filtros y han sido entregados.
- La información descrita anteriormente se muestra para los siguientes tres períodos de tiempo:
 - **Total** - Estadísticas de los últimos 30 días.
 - **Hoy** - Estadísticas para el día actual (a partir de la medianoche).
 - **Ultima hora** - Estadísticas de la hora anterior a la actual.

Tabla resumen estadísticas Correo Entrante

Referencia	Total	Hoy	Ultima hora
Spam rechazados	25	0	0
Spam	200	0	0
Correos pendientes de validación	83	0	0
Avisos de virus	23	0	0
Avisos de servidor	60	0	0
Listas de correo	60	0	0
Correo válido	180	0	0

Estadísticas de correo saliente

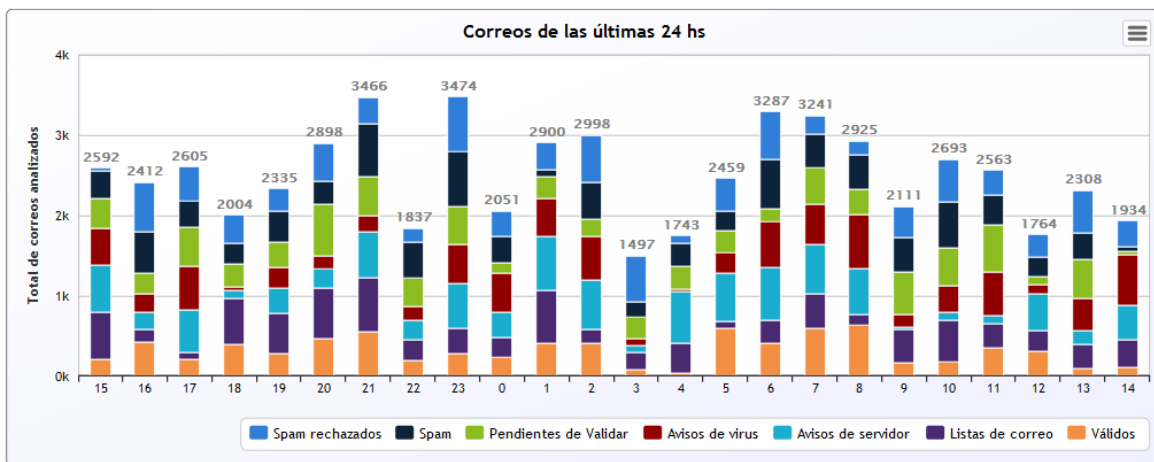
- **Spam rechazados:** Número de mensajes spam rechazados por el Firewall de correos por su elevado contenido de Spam.
- **Virus:** Número de mensajes en los que se ha detectado virus.
- **Correo válido:** Número de mensajes que han pasado todos los filtros y han sido entregados.
- La información descrita anteriormente se muestra para los siguientes tres períodos de tiempo:
 - **Total** - Estadísticas de los últimos 30 días.
 - **Hoy** - Estadísticas para el día actual (a partir de la medianoche).
 - **Ultima hora** - Estadísticas de la hora anterior a la actual.

Tabla resumen estadísticas Correo Saliente

Referencia	Total	Hoy	Ultima hora
Spam rechazados	12	0	0
Virus	3	0	0
Correo válido	60	0	0

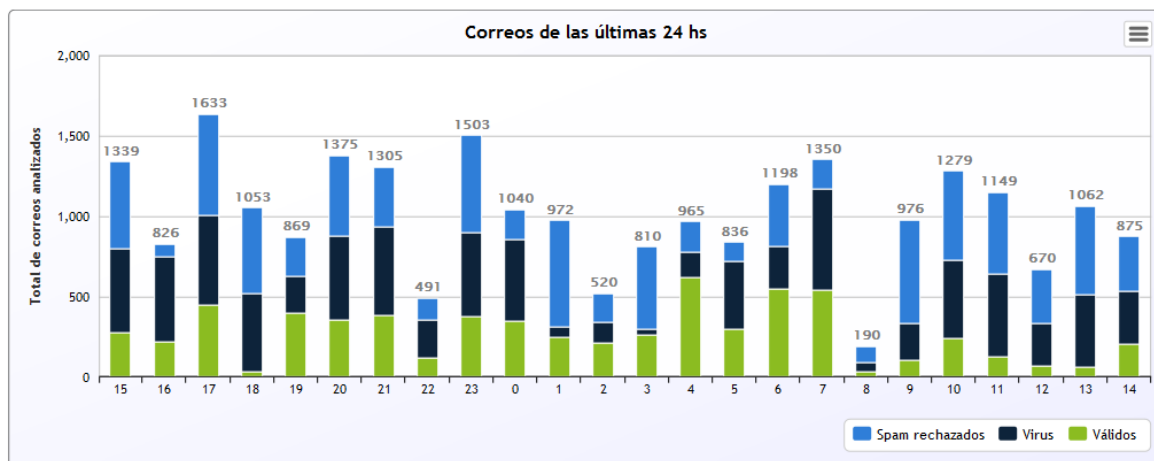
Estadísticas de correo entrante por hora

Muestra el desglose de la actividad de mensajes entrantes de las últimas 24 horas del día.



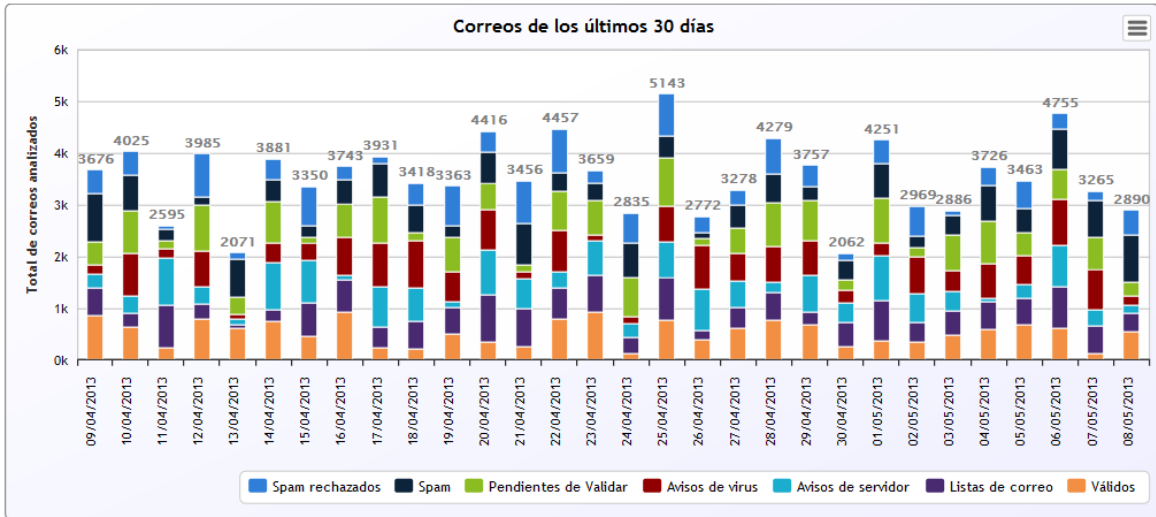
Estadísticas de correo de correo saliente por hora

Muestra el desglose de la actividad de mensajes salientes de las últimas 24 horas del día.



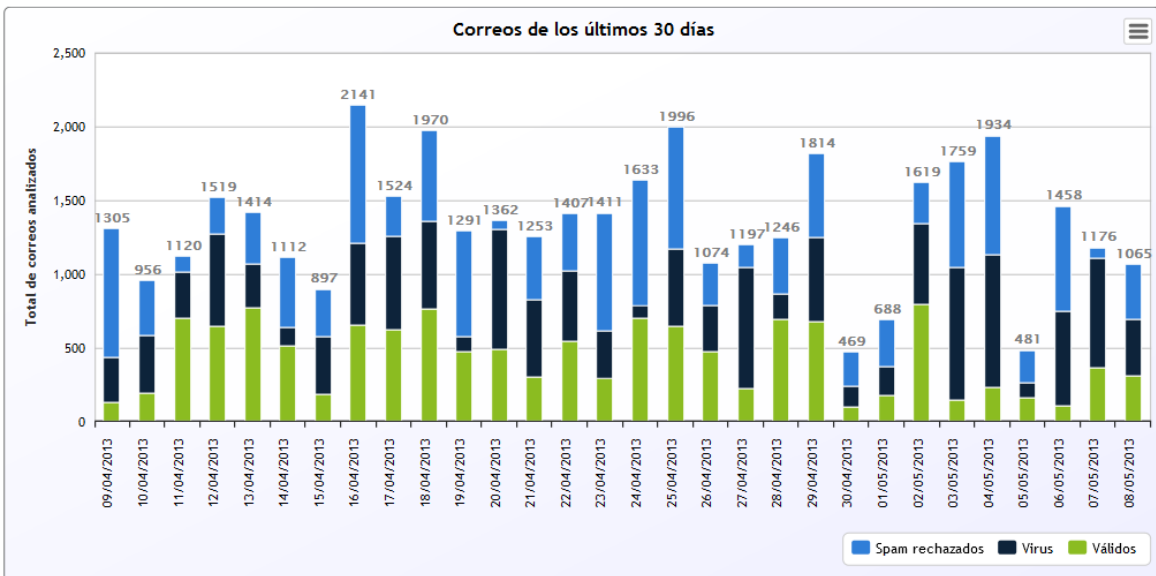
Estadísticas de correo entrante por día

Muestra el desglose de la actividad de mensajes entrantes en los últimos 30 días.



Estadísticas de correo saliente por día

Muestra el desglose de la actividad de mensajes salientes en los últimos 30 días.



2.3.3 Dominios



Muestra el listado de los dominios dados de alta en Email Protection incluyendo información como el Host SMTP destino y la cantidad de usuarios actuales.

Los dominios alias¹ se muestran al hacer clic sobre el enlace *[ver alias]* que se muestra junto al nombre del dominio principal.

Para editar el dominio o ver los usuarios del mismo se debe hacer clic en el icono correspondiente.

Puede realizar búsquedas de dominios por los siguientes criterios: *Nombre de dominio* y *Nombre de alias*, seleccionando una de esas opciones de la lista de selección que aparece en el formulario de búsquedas.


Desde el menú de edición del dominio se puede crear un administrador específico que tendrá derechos de administración sobre el mismo.

Si al comprar Email Protection se elige la opción de acceder a los paneles de usuario, se permitirá la gestión de los paneles de usuario al administrador de empresa y de dominios.

Si al comprar Email Protection se eligió la opción de acceder a los correos desde Log de Correos, se permitirá la gestión de los correos desde el listado de Log de Correos al administrador de empresa y de dominios.

¹ Un dominio alias es aquel que se crea dependiendo de otro dominio y por defecto tiene las mismas cuentas que su dominio principal (sin necesidad de crearlas). Los dominios alias sólo existen virtualmente y no tienen buzón físico

Dominios

[Mostrar información](#) 

La empresa dispone de **0** licencias

Datos del dominio: domain.com

Datos del dominio
Registros MX
Datos del administrador del dominio

El dominio es un **alias**

* Correo electrónico de contacto:

Idioma: Español Propagar cambios en cascada

Máximo de usuarios permitidos: [Ayuda](#)

Licencias consumidas: **1**

Licencias consumidas por dominios alias: **0**

(*) Campos requeridos

Para importar una lista de dominios se debe seguir el siguiente formato:

- El archivo a importar debe contener:
- Nombre de dominio
- Servidores Mx (separados por ; si son más de uno)
- Correo electrónico de contacto
- Nombre y apellido del administrador del dominio (1)
- Nombre de usuario (login Administrador) (2)
- Contraseña válida (3)
- Dominio canónico (en caso de ser dominio alias) (4)

(1, 2, 3 y 4) Indican datos opcionales.

Un dominio con administrador debe especificar los tres campos (1) (2) (3), la ausencia de uno de ellos hará que el dominio no sea dado de alta. Un dominio alias sin administrador, debe completar las opciones (1), (2) y (3) (datos del administrador) con vacío, por ejemplo: 'alias.com, mx1.com:10 ; mx2.com:9 , user@domain.com, canonico.com'.

Cada línea del archivo debe representar un dominio.

Estos archivos pueden ser tanto .txt como .csv

Estructura del archivo:

Nombre de Dominio, Servidor Mx:Prioridad, Correo de Contacto, Nombre y Apellido del Administrador de Dominio[opcional], Nombre de Usuario (login)[opcional], Contraseña[opcional]

Para dominio ALIAS: Nombre de Dominio, Servidor Mx:Prioridad, Correo de Contacto, Nombre y Apellido del Administrador de Dominio [opcional], Nombre de Usuario (login)[opcional], Contraseña[opcional], Dominio Canónico

Archivo final (ejemplo):

dominio.com, servidorMx_1:10;servidorMx_2:20, administrador_empresa@ejemplo.com, Andrés Lopez, andres_lopez, 1234567891

dominioAlias.com,servidorMx_1:10;servidorMx_2:20,administrador_empresa@ejemplo.com, Andrés Lopez, andres_lopez, 1234567891, dominio.com

dominioAliasSinAdmin.com,servidorMx_1:10;servidorMx_2:20, administrador_empresa@ejemplo.com, , , , dominio.com

Importante:

- Una contraseña se considera válida sólo si no es débil
- Este proceso puede tardar varios minutos, el resultado de la importación será notificado por correo electrónico a la cuenta maru@Panda.com
- El dominio no debe poseer caracteres inválidos
- El login del Administrador es único
- Los registros Mx deben ser válidos
- No pueden faltar campos obligatorios

HostMX y servidores Mx (*este último para la importación de dominios*):

Se permite el agregado de IPs tanto del tipo IPv4 como IPv6. Cada dirección IPv6 debe ser representada en ocho grupos separados por ":"; cada grupo debe contener 4 dígitos hexadecimales.

Es posible utilizar la notación comprimida IPv6, eliminando los ceros a la derecha de cada grupo.

Por ejemplo:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

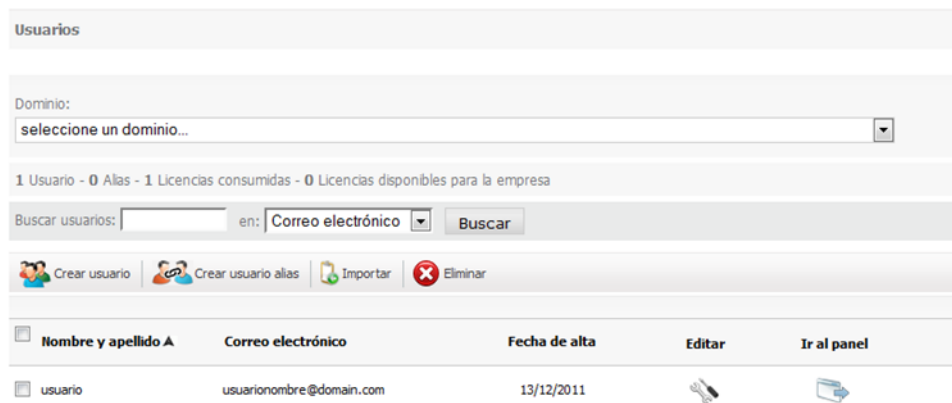
2001:0DB8::1428:57ab

2.3.4 Usuarios

Muestra el listado de usuarios y alias de usuarios, y permite: crear de forma manual, importar desde un archivo o eliminar usuarios o alias de usuarios, ignorar o admitir un usuario.

Puede realizar búsquedas de usuarios por los siguientes criterios: *Nombre y apellido*, *Correo electrónico* y *Alias*, seleccionando una de esas opciones de la lista de selección que aparece en el formulario de búsquedas.

Desde el icono "Editar" se accede a un formulario donde se pueden modificar los datos del usuario. En ningún caso se permite cambiar su dirección de correo.










Usuarios

Dominio:
seleccione un dominio...

1 Usuario - 0 Alias - 1 Licencias consumidas - 0 Licencias disponibles para la empresa

Buscar usuarios: en: Correo electrónico

 Crear usuario  Crear usuario alias  Importar  Eliminar

 Nombre y apellido A	Correo electrónico	Fecha de alta	Editar	Ir al panel
 usuario	usuarionombre@domain.com	13/12/2011		

Para importar una lista de usuarios se tiene que seguir el siguiente formato:

El archivo a importar debe contener: nombre y apellido, dirección de correo electrónico (incluyendo o no @dominio; este último caso se da cuando la importación de usuarios se realiza habiendo seleccionado previamente un dominio), y la contraseña del usuario², separados por coma.

² En ausencia de la contraseña del usuario, se generará una al azar que será enviada al mismo en el correo de bienvenida.

Cada línea del archivo debe representar un usuario.
Estos archivos pueden ser tanto .txt como .csv

Estructura del archivo:

Nombre y apellido, Correo, Contraseña

Ejemplo:

Miguel Sanchez, msanchez@ejemplo.com, aras249g
Andrés López, alopez@ejemplo.com, 32kios5

La importación de usuarios puede tardar varios minutos (entre 5 y 10 segundos por usuario) y se va a realizar en segundo plano, por lo que no debe esperar a su completa finalización antes de realizar otra acción en el sistema. El resultado de la importación será notificado por correo electrónico a la cuenta.

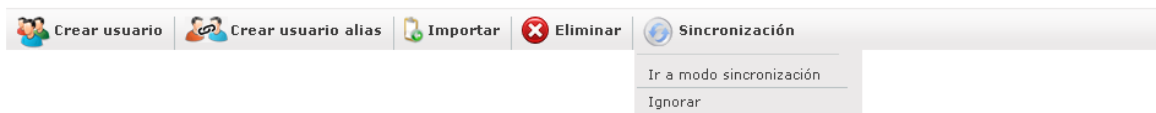
2.3.4.1 Sincronización de Usuarios.

Un usuario ignorado es aquel que no será sincronizado en caso de estar activo el modo de Sincronización.

El botón "Ir a modo de sincronización" permite visualizar aquellos usuarios que:

- serán ignorados por el proceso de sincronización.
- serán eliminados por el proceso de sincronización.
- serán actualizados por el proceso de sincronización.

En caso de estar activo el modo de sincronización manual, la vista de sincronización mostrará sólo aquellos usuarios que serán ignorados, eliminados o actualizados. En el caso de estar activo el modo de sincronización automático, la vista de sincronización mostrará sólo aquellos usuarios que serán ignorados.

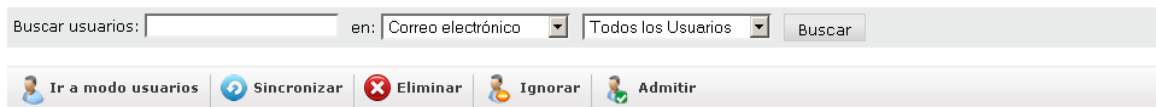


El botón "Sincronizar", que sólo está disponible cuando el modo de sincronización es Manual, permite realizar la sincronización de todos los usuarios del dominio o empresa que se haya seleccionado.

Un usuario que ha sido ignorado, puede volver a incluirse en el proceso de sincronización mediante el botón "Admitir".

En el modo de sincronización se pueden realizar búsquedas de usuarios utilizando los filtros "Usuarios ignorados", "Usuarios a borrar" o "Usuarios a modificar".

Mediante el botón "Ir a modo usuarios", se retorna a la vista de gestión de usuarios.



2.3.5 Usuarios con filtrado básico

Los usuarios con filtrado básico recibirán correo, pero sólo se les aplicará el filtrado por conexión. No tendrán filtrado por contenido, así como tampoco podrán tener ningún tipo de cuarentena.



Los usuarios con filtrado básico pueden pasar a ser usuarios normales si el administrador lo cree necesario.


Es importante recordar que todos los usuarios tienen que estar dados de alta en Email Protection para que no se rechace su correo. Si se decide que no se quiere hacer uso de los filtros por contenido ni de los paneles de usuario, entonces la mejor opción es crearlos como usuarios con filtrado básico.

Estos usuarios no cuentan como licencias de Email Protection.

2.3.6 Modo de Alta

Existen diferentes modos de alta de usuarios para dar la mayor flexibilidad posible al cliente.

Modo de alta

[Mostrar información sobre modos de alta](#) 

Modo de alta global

Manual	LDAP
<input checked="" type="radio"/>	<input type="radio"/> configurar

Modo de alta por dominio

Dominio	Por defecto	Manual	SMTP	LDAP	Catch All
domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> configurar	<input type="radio"/>

2.3.6.1 Alta Manual

El administrador de Email Protection es el encargado de dar de alta cada una de las cuentas de los usuarios manualmente. Esta opción se recomienda únicamente en el caso de querer añadir un número reducido de cuentas. Para agregar una cuenta debe dirigirse a la pestaña **“Gestión”** y luego al menú **“Usuarios”**.

2.3.6.2 Alta Automática por SMTP call out o LDAP

Email Protection permite dar de alta los usuarios de forma automática a medida que empiecen a recibir correo. Para ello comprueba que las direcciones de correo de los destinatarios existan en el servidor final. Estas comprobaciones se pueden realizar con un servidor SMTP o LDAP (ver 2.3.6.2.1 Configuración de parámetros para descubrimiento de usuarios en LDAP corporativo), creando el usuario en Email Protection si éste existe o rechazando el correo si no existe. En caso de seleccionar SMTP, asegúrese que su servidor de correo está configurado para poder realizar esa comprobación³. En caso de duda puede ponerse en contacto con nuestro departamento de soporte.

³ El servidor SMTP debería responder afirmativamente sólo para aquellos usuarios válidos dentro del dominio.

2.3.6.2.1 Configuración de parámetros para descubrimiento de usuarios en LDAP corporativo

La configuración del descubrimiento de usuarios en LDAP corporativo, empleada en el modo de alta LDAP, se divide en siete secciones, que se describen a continuación.

2.3.6.2.1.1 Servidor de LDAP

Servidor de LDAP

Servidor: [Ayuda](#)

- Open LDAP
- Open LDAP
- Lotus Domino
- Active Directory
- Otro

En esta sección debe especificar el servidor LDAP que está utilizando; esto permite sugerir ciertos valores de configuración ya conocidos.

2.3.6.2.1.2 Conexión

Utilizar SSL [Ayuda](#)

* Host: [Ayuda](#)

* Puerto: [Ayuda](#)

Conexión anónima

Nombre de usuario: [Ayuda](#)

Contraseña: [Ayuda](#)

En esta sección deberá especificar la información necesaria para conectarse al servidor LDAP:

- Utilizar SSL: permite establecer una conexión cifrada (Secure Socket Layer).

Host: indique la dirección IP o el nombre DNS del servidor LDAP.

Se permite el uso de IPs tanto del tipo IPv4 como IPv6. Cada dirección IPv6 debe ser representada en ocho grupos separados por ":"; cada grupo debe contener 4 dígitos hexadecimales.

Es posible utilizar la notación comprimida IPv6, eliminando los ceros a la derecha de cada grupo.

Por ejemplo:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000:1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0:0:1428:57ab

2001:0DB8:1428:57ab

- Puerto: indique el puerto TCP/IP usado para conectarse al servidor LDAP. Normalmente existen dos puertos estándar empleados por los servidores LDAP:
 - 389: para conexiones regulares (no-seguras)
 - 636: para conexiones seguras (SSL)

También deberá especificar la información de conexión, es decir, los parámetros que se usarán para identificar al usuario que se conectará al servidor LDAP. Basándose en esta información, el servidor determina los privilegios para una conexión específica.

En caso de seleccionar "Conexión anónima", no deberá especificar ninguno de los parámetros de esta sección.

- Nombre de usuario: representa un DN de usuario, por ejemplo: uid=jperez,ou=People,dc=dominio,dc=com
- Contraseña, por ejemplo: supersecreto2008

2.3.6.2.1.3 Alcance de la búsqueda

Alcance de la búsqueda

* DN Base: [Ayuda](#)

un nivel [Ayuda](#)

subárbol [Ayuda](#)

En esta sección deberá especificar el alcance de la búsqueda, seleccionando uno de los siguientes valores:

- DN Base: la "raíz" para enlazar (bind) al servidor. Para el caso de servidores con LDAPv3, puede dejar este campo en blanco para así conectarse al RootDSE del servidor.
- Un nivel: especifica que la búsqueda de objetos se realizará en el nivel inmediatamente inferior al valor indicado en DN Base, sin utilizar recursión.
- Subárbol: especifica que la búsqueda de objetos se realizará en el nivel inmediatamente inferior al valor indicado en DN Base, utilizando recursión.

Sintaxis de DN Base

En el caso en que el valor del campo contenga:

- Un carácter espacio « » (ASCII 32) o numeral «#» (ASCII 35) al principio.
- Un carácter espacio « » (ASCII 32) al final.
- Alguno de los caracteres: «,» (ASCII 44), «+» (ASCII 43), «'» (ASCII 34), «\» (ASCII 92), «<» (ASCII 60), «>» (ASCII 62) o «;» (ASCII 59)

El carácter debe ser escapado anteponiendo al mismo el carácter «\» (ASCII 92)

Por ejemplo, si el valor de "Organization Name" (O) es de la siguiente forma: CN=L. Eagle,O=Sue, Grabbit and Runn,C=GB

Entonces, el mismo debe ser escapado como se indica a continuación: CN=L. Eagle,O=Sue\\, Grabbit and Runn, C=GB

2.3.6.2.1.4 Búsqueda del nombre de usuario

Búsqueda del nombre de usuario

* Atributo que contiene la dirección de correo electrónico: [Ayuda](#)

El atributo almacena sólo el nombre del usuario

El atributo almacena la dirección de correo electrónico completa

* Filtro LDAP: [Ayuda](#)

En esta sección deberá especificar los parámetros que permiten realizar el descubrimiento de usuarios en el LDAP corporativo:

- Atributo que contiene la dirección de correo electrónico, por ejemplo: mail, rfc822Mailbox, entre otros.
- Deberá indicar si el atributo especificado anteriormente almacena sólo el nombre del usuario o la dirección de correo electrónico completa.
- Filtro LDAP: especifique aquí la clase más apropiada para refinar la búsqueda (esto afecta al rendimiento en el proceso de búsqueda, pues se mantienen índices de acuerdo a las clases de objetos). El patrón genérico indicado por defecto (objectClass=*) permite que el filtro coincida con todas las clases de objeto LDAP.

2.3.6.2.1.5 Búsqueda de Alias

Búsqueda de Alias

Activar descubrimiento de Alias:

* Atributo que contiene el alias: [Ayuda](#)

* Filtro LDAP: [Ayuda](#)

El campo es multivaluado

Si

No

Separador de alias: [Ayuda](#)

El alias está en el mismo objeto que la dirección de correo?

Si

No

Atributo que contiene el DN del objeto del usuario real: [Ayuda](#)

Verificar

Si se activa el descubrimiento de alias, deberá configurar los siguientes parámetros:

- Atributo que contiene el alias, por ejemplo: uid, userId, entre otros.
- Indicar, para el atributo anterior, si este es multivaluado; en caso de no serlo, deberá indicar un separador de alias usado dentro de ese atributo⁴.
- Debe determinar si el alias se encuentra en el mismo objeto LDAP que la dirección de correo; en caso de no ser así, deberá indicar el atributo que contiene el DN del objeto del usuario real (por ejemplo: cn, userId)

2.3.6.2.1.6 Grupos

Esta configuración es utilizada por el motor de reglas, para determinar si un usuario de un dominio protegido, pertenece a un grupo dado en el LDAP corporativo.

Grupos

Pertenencia en Grupos:

* Atributo que contiene los grupos a los que pertenece un usuario: [Ayuda](#)

¿El campo es multivaluado?

Si

No

Separador de grupos: [Ayuda](#)

(*) campos requeridos

⁴ No puede ser utilizado ningún carácter que pueda formar parte de una dirección de correo electrónico, es decir: letras de la A a la Z (mayúsculas y minúsculas), números del 0 al 9 y el siguiente conjunto de símbolos: ?) @ ! # \$ % & ' * + - / = ^ _ ` ~ . { | } "

En esta sección deberá especificar la información necesaria para la pertenencia en grupos:

- Atributo que contiene los grupos a los que pertenece un usuario.
- Especificar si el campo es multivaluado.
- Separador de grupos.

2.3.7 Administradores

La gestión de múltiples administradores le permite definir los usuarios que tendrán permiso para gestionar el Firewall de correos para toda su organización, así como también para determinados dominios.

Es posible distinguir dos tipos de administradores, tanto a nivel de la empresa como de un dominio:

- Administrador principal
- Administrador secundario

En el contexto de la empresa, el administrador principal es el único que posee los privilegios para dar de baja la empresa o modificar sus credenciales de acceso.

Tanto a nivel de empresa como a nivel de dominio, sólo es posible definir un único administrador principal.

Para crear un administrador se requiere la siguiente información:

- Tipo de administrador
 - Administrador de empresa
 - Administrador de dominio. En este caso debe indicarse el dominio que será administrado.
- Nombre completo
- Nombre de usuario: se utilizará para iniciar sesión de administrador
- Contraseña
- Dirección de correo electrónico de contacto: a esta dirección se enviarán los informes de actividad de filtrado, así como también las notificaciones de los resultados de las acciones realizadas en segundo plano (por ejemplo: importación de usuarios, cambio de configuraciones en cascada, etc).

Es posible editar los datos de un administrador o eliminar el mismo sólo si este es de tipo "secundario". La edición de los datos de un administrador principal se realiza desde las siguientes secciones:



- Administrador de dominio: Solapa "Gestión", opción de menú "Dominios", edición de los datos del dominio.
- Administrador de empresa: Solapa "Configuración", opción de menú "Datos del administrador".


Administradores

Filtro:

Administradores 3

Buscar usuarios: en:

 Crear administrador  Eliminar

<input type="checkbox"/> Usuario (login) ▲	Nombre y apellido	Correo electrónico	Dominio	Editar
<input type="checkbox"/> secundario1	usuario secundario 1	secundario1@dominio.com	empresa	
<input type="checkbox"/> secundario2	usuario secundario 2	secundario2@dominio.com	empresa	
<input type="checkbox"/> usuario	corp	corp@dominio.com	empresa	





2.3.8 Auditoría de acciones

Esta funcionalidad le permite acceder a los registros de las acciones realizadas por todos sus administradores y usuarios finales registrados en el sistema.

Auditoría de acciones

(13 de 13 Acciones seleccionadas)

Cantidad de registros encontrados: 4

Acción	Fecha ▲	Usuario	Tipo de usuario	Datos	Avisos / Errores
Configuración datos de la empresa	2012-05-21 13:22:21	prueba	Empresa		
Configuración datos personales	2012-05-21 13:23:29	prueba	Empresa		
Configuración cambio de contraseña	2012-05-21 13:24:28	prueba	Empresa		Errores encontrados [+]
Configuración cambio de contraseña	2012-05-21 13:24:49	usuario	Empresa		

Entre los tipos de acciones registradas pueden mencionarse:

- Altas, bajas y actualización de datos dominios
- Altas, bajas y actualización de datos de administradores de empresa y dominio
- Altas, bajas y actualización de datos de usuarios finales
- Modificaciones de configuraciones de filtrado de correo
 - Listas blancas y negras

- Modo de filtrado
- Filtros de correo entrante y saliente
- Marcado de Spam
- Reglas de clasificación
- ...
- ...

El motor de búsquedas le permite establecer los siguientes filtros:

- Tipo de usuario que ha realizado la acción: permite escoger entre los siguientes valores
 - Todos
 - Empresa (administradores de empresa)
 - Dominio (administradores de dominio)
 - Usuario final
- Categoría principal de la acción: permite escoger entre los siguientes valores
 - Gestión
 - Filtrado
 - Personalización
 - Configuración
 - Notificador
 - Webservice
- Acciones concretas. Éstas dependen de los filtros anteriores que hayan sido aplicados.
- Rango de fechas entre las que se haya ejecutado la acción
 - Fecha inicial
 - Fecha final
- Nombre del usuario que haya ejecutado la acción: en caso de utilizar esta opción, debe indicar el nombre de usuario completo.

Los resultados obtenidos tras realizar una búsqueda muestran la siguiente información:

- Nombre de la acción
- Fecha en la que ha sido realizada
- Nombre del usuario (aquel con el que inicia sesión en cualquiera de los paneles o notificador)
- Tipo de usuario
 - Administrador de empresa
 - Administrador de dominio
 - Usuario final
- Datos de la acción: indica, para cada una de ellas, los datos utilizados para su realización.
- Descripción de los errores que pudieran haberse producido durante la ejecución de la acción.

Haciendo clic sobre las columnas "Acción", "Fecha" o "Usuario", es posible ordenar el resultado de la búsqueda por cualquiera de esos criterios, de forma ascendente o descendente.

2.4 Filtrado

En esta sección podrá administrar todos los aspectos relacionados al filtrado que realiza Email Protection, aplicando configuraciones a nivel global, de dominios y de usuarios.

2.4.1 Listas

2.4.1.1 Lista Blanca

La Lista Blanca puede contener direcciones de correo electrónico, dominios o IPs. A los correos provenientes de dominios o remitentes pertenecientes a esta lista, se les aplicarán los filtros de conexión, antivirus, motor de reglas y ningún filtro de contenido.

A los correos provenientes de las IPs que aplican a nivel de empresa no se les aplicará el filtrado de contenido y filtros de conexión pero si los filtros de antivirus y motor de reglas; asimismo estas IPs tienen menor prioridad que aquellas definidas en las listas blanca y negra globales.

No podrá eliminar aquellas IPs que aplican a nivel global; éstas se muestran sólo a efectos informativos y sólo pueden ser gestionadas por administradores del sistema.

Al Introducir un remitente en una Lista Blanca o Lista Negra, este se comparará con el Header-From y el Envelope-From.

Al enviar el remitente de un correo desde los logs a Lista Blanca o Lista Negra, se agrega a las mismas el Envelope-From.

Los filtros de contenidos sólo abarcan análisis bayesiano.

Se podrán importar direcciones de correo electrónico, dominios de correo y direcciones IPs.

- El archivo a importar debe contener elementos separados por los caracteres , (coma), ; (punto y coma) o salto de línea
- Cada línea del archivo puede contener varios elementos separados por los separadores anteriormente comentados
- El archivo puede ser tanto .txt como .csv
- La cantidad máxima de elementos por archivo es de 2000

A fin de evitar redundancia en las listas blancas de remitentes y dominios, no será posible agregar un remitente cuando el dominio ya existe en la lista. Caso contrario, al agregar un dominio en lista blanca, los remitentes pertenecientes a este dominio serán eliminados.

Se permite el agregado de IPs tanto del tipo IPv4 como IPv6. Cada dirección IPv6 debe ser representada en ocho grupos separados por ":"; cada grupo debe contener 4 dígitos hexadecimales.

Es posible utilizar la notación comprimida IPv6, eliminando los ceros a la derecha de cada grupo.

Por ejemplo:

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
```

```
2001:0DB8:0000:0000:0000::1428:57ab
```

```
2001:0DB8:0:0:0:0:1428:57ab
```

```
2001:0DB8:0::0:1428:57ab
```

```
2001:0DB8::1428:57ab
```

2.4.1.2 Lista Negra

La Lista Negra puede contener direcciones de correo electrónico, dominios o IPs. Los correos provenientes de dominios o remitentes pertenecientes a la lista negra serán colocados en cuarentena después de pasar por los filtros de conexión.

Aquellos correos provenientes de IPs de esta lista, serán rechazados.

No podrá eliminar aquellas IPs que aplican a nivel global; éstas se muestran sólo a efectos informativos y sólo pueden ser gestionadas por administradores del sistema.

Al introducir un remitente en una Lista Blanca o Lista Negra, este se comparará con el Header-From y el Envelope-From.

Al enviar el remitente de un correo desde los logs a Lista Blanca o Lista Negra, se agrega a las mismas el Envelope-From.

Se podrán importar direcciones de correo electrónico, dominios de correo y direcciones IP's.

- El archivo a importar debe contener elementos separados por los caracteres , (coma), ; (punto y coma) o salto de línea
- Cada línea del archivo puede contener varios elementos separados por los separadores anteriormente comentados
- El archivo puede ser tanto .txt como .csv
- La cantidad máxima de elementos por archivo es de 2000

A fin de evitar redundancia en las listas negras de remitentes y dominios, no será posible agregar un remitente cuando el dominio ya existe en la lista. Caso contrario, al agregar un dominio en lista blanca, los remitentes pertenecientes a este dominio serán eliminados.

Se permite el agregado de IPs tanto del tipo IPv4 como IPv6. Cada dirección IPv6 debe ser representada en ocho grupos separados por ":"; cada grupo debe contener 4 dígitos hexadecimales.

Es posible utilizar la notación comprimida IPv6, eliminando los ceros a la derecha de cada grupo. Por ejemplo :

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

2.4.2 Anti Virus

2.4.2.1 Dominios

Desde aquí podrá gestionar la activación o desactivación de los filtros antivirus disponibles para su empresa y dominios, tanto para los correos entrantes como para los salientes.

Por defecto el filtrado antivirus está activo para ambos tipos de tráfico de correos.

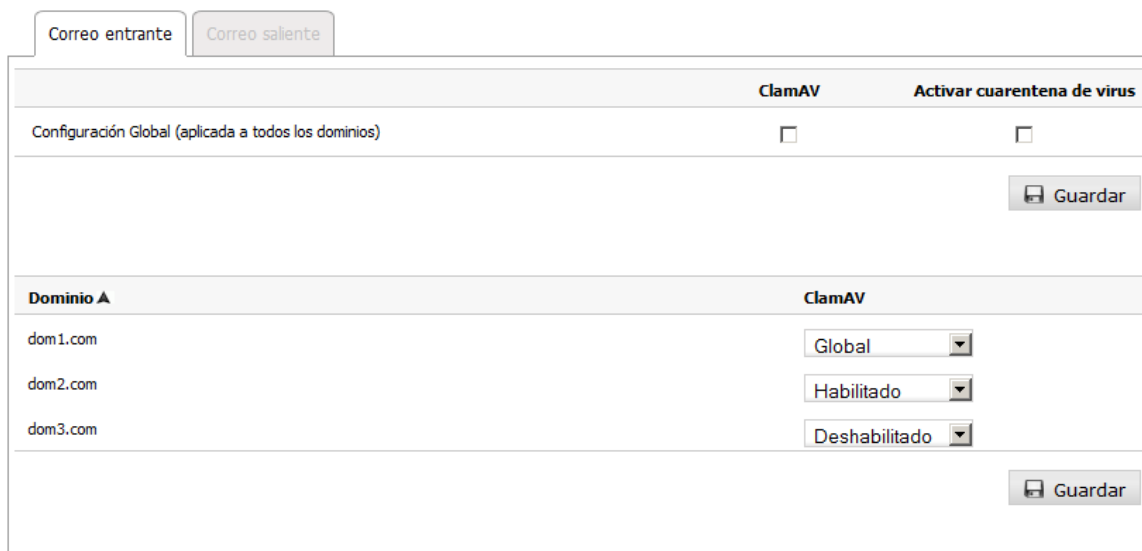
Si desactiva todos los antivirus de los que dispone para un tráfico de correos en particular, los mismos no serán sometidos al control de antivirus.

Para activar la cuarentena de virus (disponible sólo para el correo entrante), deberá tener previamente activado al menos uno de los antivirus disponibles. Cuando la cuarentena de virus se encuentra activada, cada vez que llega un correo infectado, se envía una notificación al destinatario del correo y se almacena una copia del correo infectado que es accesible para los administradores de empresa desde la solapa "Filtrado", opción de menú "Virus en cuarentena".

Para aplicar el filtrado antivirus al correo saliente **es necesario** que esos correos se envíen a través de la plataforma identificándose con las credenciales de acceso que utiliza para iniciar sesión en la consola de gestión:

1. Habilitar el filtrado antivirus para el correo saliente.
2. Indicar a su SMTP que utilice como SMARHOST al servidor indicado para su plataforma de servicio.
3. En la configuración para SMARHOST de su SMTP debe indicar que la sesión SMTP es autenticada y que el usuario y contraseña a utilizar son los mismos con los que inicia sesión en su consola de administrador.

Sin esta configuración no tendrá efecto la configuración de filtrado antivirus para el correo saliente.



Configuración Global (aplicada a todos los dominios)	
ClamAV	<input type="checkbox"/>
Activar cuarentena de virus	<input type="checkbox"/>
<input type="button" value="Guardar"/>	

Dominio A	ClamAV
dom1.com	Global
dom2.com	Habilitado
dom3.com	Deshabilitado
<input type="button" value="Guardar"/>	

2.4.2.2 Usuarios

Desde aquí podrá gestionar la activación o desactivación de los filtros antivirus disponibles para sus usuarios, tanto para los correos entrantes como para los salientes.

Por defecto los usuarios utilizan la configuración de filtrado antivirus definida por el dominio al que pertenecen (opción "Global"), tanto para el correo entrante como para el saliente.

Si desactiva todos los antivirus de los que dispone para un tráfico de correos en particular, los mismos no serán sometidos al control de antivirus.

Los usuarios que tengan los filtros antivirus desactivados siguen contando como licencias.

Dominio: Buscar: en:

Cantidad de usuarios: 3

Configuración del dominio: ClamAV (Habilitado)

Nombre ▲	Login	ClamAV
Nombre Usuario 1	u1@dom1.com	<input type="text" value="Global"/>
Nombre Usuario 2	u2@dom1.com	<input type="text" value="Habilitado"/>
Nombre Usuario 3	u3@dom1.com	<input type="text" value="Deshabilitado"/>

2.4.3 Anti Spam

2.4.3.1 Dominios

Desde aquí podrá gestionar la activación o desactivación del filtrado anti spam para su empresa y dominios, tanto para los correos entrantes como para los salientes.

Por defecto el filtrado anti spam está activado tanto para el correo entrante como para el correo saliente. Los dominios utilizan la configuración de filtrado definida por la empresa.

Si desactiva el filtrado anti spam para un tráfico de correos en particular, se pasará a un modo en el que los filtros por contenido no se aplicarán, pero seguirán aplicándose los filtros por conexión.

En el caso de que un correo saliente sea considerado spam será rechazado y se comunicará la decisión al remitente del mensaje.

Para aplicar el filtrado anti spam al correo saliente **es necesario** que esos correos se envíen a través de la plataforma identificándose con las credenciales de acceso que utiliza para iniciar sesión en la consola de gestión:

4. Habilitar la opción filtrado anti spam para el correo saliente.

5. Indicar a su SMTP que utilice como SMARHOST al servidor indicado para su plataforma de servicio.
6. En la configuración para SMARHOST de su SMTP debe indicar que la sesión SMTP es autenticada y que el usuario y contraseña a utilizar son los mismos con los que inicia sesión en su consola de administrador.

Sin esta configuración no tendrá efecto la configuración de filtrado anti spam para el correo saliente.

Correo entrante
Correo saliente

	Antispam	Activar Marcado de Spam
Configuración Global (aplicada a todos los dominios)		
	<input type="checkbox"/>	<input checked="" type="checkbox"/> configurar
Guardar		
Dominio A	Antispam	Activar Marcado de Spam
dom1.com	Habilitado	<input checked="" type="checkbox"/> configurar
dom2.com	Global	<input type="checkbox"/> configurar
Guardar		

Nota: El servicio se proporciona a miles de clientes, al igual que todos los principales servicios de correo electrónico. Existe la posibilidad de que algunas de nuestras IPs públicas sean listadas por RBLs de terceros (listas negras reputación). Contamos con medidas de seguridad para evitar que esto ocurra. Sin embargo, en el caso improbable de que las IPs sean incluidas en una RBL, haremos todo lo necesario para revertir rápidamente esa situación. Si esto sucede, los clientes pueden minimizar el impacto en la organización, y la posibilidad de que un correo electrónico saliente sea rechazado, cambiando de forma temporal la configuración de sus MTAs para enviar el correo directamente a través de Internet.

La opción Activar Marcado de Spam, disponible sólo para el correo entrante, le permite etiquetar el correo clasificado como spam. Haciendo clic en el enlace "configurar" podrá especificar dónde insertar la marca de SPAM, seleccionando:

- La marca se ubicará antes del asunto: para insertar la etiqueta especificada al comienzo (es decir, como prefijo) del asunto del correo.

Por ejemplo, '[SPAM] Viaje gratis!'.

- La marca se ubicará después del asunto: para insertar la etiqueta especificada al final (es decir, como sufijo) del asunto del correo.

Por ejemplo, 'Viaje gratis [SPAM]'.

Los valores permitidos para la Marca de spam son: **caracteres ASCII**.

La configuración que proporciona el sistema por defecto es:

- Cuarentena activada.
- Marca de Spam: **[SPAM], *SPAM*, [Maybe SPAM]**.
- La marca se ubicará antes del asunto.

Activar Marcado de Spam tiene las siguientes implicaciones:

1. No se enviarán los siguientes "mensajes automáticos" a usuarios finales:
 - Mensaje de bienvenida.
 - Informe de correos bloqueados.
 - Mensaje de validación de remitentes (modo de filtrado Garantizado).
2. El "Marcado de Spam" es compatible sólo con el modo de filtrado Automático; por tanto, si algún dominio o usuario tenía modo de filtrado Garantizado se pasa a Automático. No podrá seleccionar el modo garantizado a ningún nivel (empresa/dominio/usuario) que haya optado por el uso del marcado de Spam.
3. La configuración "Cuarentena" afecta a todos los correos, no sólo a los correos clasificados como Spam.

2.4.3.2 Usuarios

Desde aquí podrá gestionar la activación o desactivación del filtrado anti spam para sus usuarios, tanto para los correos entrantes como para los salientes.

Los usuarios utilizan la configuración de filtrado anti spam definida por el dominio al que pertenecen.

Si desactiva el filtrado anti spam para un tráfico de correos en particular, se pasará a un modo en el que los filtros por contenido no se aplicarán, pero seguirán aplicándose los filtros por conexión.

En el caso de que un correo saliente sea considerado spam será rechazado y se comunicará la decisión al remitente del mensaje.

Para aplicar el filtrado anti spam al correo saliente **es necesario** que esos correos se envíen a través de la plataforma identificándose con las credenciales de acceso que utiliza para iniciar sesión en la consola de gestión:

7. Habilitar la opción filtrado anti spam para el correo saliente.
8. Indicar a su SMTP que utilice como SMARHOST al servidor indicado para su plataforma de servicio.

- En la configuración para SMARTHOST de su SMTP debe indicar que la sesión SMTP es autenticada y que el usuario y contraseña a utilizar son los mismos con los que inicia sesión en su consola de administrador.

Sin esta configuración no tendrá efecto la configuración de filtrado anti spam para el correo saliente.

Dominio:
 Buscar:
 en:

Cantidad de usuarios: 13

Configuración del dominio: Habilitado

Nombre ▲	Login	Antispam
Nombre Usuario 1	u1@dom1.com	<input type="text" value="Global"/>
Nombre Usuario 2	u2@dom1.com	<input type="text" value="Habilitado"/>
Nombre Usuario 3	u3@dom1.com	<input type="text" value="Deshabilitado"/>

Nota: El servicio se proporciona a miles de clientes, al igual que todos los principales servicios de correo electrónico. Existe la posibilidad de que algunas de nuestras IPs públicas sean listadas por RBLs de terceros (listas negras reputación). Contamos con medidas de seguridad para evitar que esto ocurra. Sin embargo, en el caso improbable de que las IPs sean incluidas en una RBL, haremos todo lo necesario para revertir rápidamente esa situación. Si esto sucede, los clientes pueden minimizar el impacto en la organización, y la posibilidad de que un correo electrónico saliente sea rechazado, cambiando de forma temporal la configuración de sus MTAs para enviar el correo directamente a través de Internet.

2.4.4 Virus en cuarentena

Desde esta opción el administrador podrá:


- Ver los correos listados
- Descargar archivos adjuntos de los correos
- Eliminar los correos



El tiempo de almacenamiento de los correos se muestra en la pestaña Configuración, opción Almacenamiento, Correo válido.

Virus en cuarentena

[Mostrar información sobre virus en cuarentena](#) 

2 correos infectados

 Eliminar

<input type="checkbox"/> Remitente	Asunto	Fecha	Tamaño
 virus2@virus.com	our vacations photos	02/09/2009	1.71 KB
 virus@virus.com	look at this	02/09/2009	1.7 KB

2.4.5 Listas de confianza


2.4.5.1 Listas de confianza para el dominio

Las Listas de Confianza son unas listas blancas automáticas y personalizadas por dominio. De esta manera se consigue que no se aplique el filtrado a los correos de la gente con la que normalmente se intercambia información y así evitar falsos positivos.

Estas listas se van llenando automáticamente con las direcciones de correo de los remitentes que Email Protection considera que no ofrecen ningún tipo de duda sobre su procedencia.


Desde este panel se habilitan/deshabilitan las Listas de Confianza para todo el servicio o para ciertos dominios.

Lista de confianza para el dominio

[Mostrar información sobre lista de confianza](#) 


Configuración global

	Habilitado	Deshabilitado
Todos los dominios	<input type="radio"/>	<input checked="" type="radio"/>

 Guardar

Configuración por dominio.

Nombre Dominio	Global	Habilitado	Deshabilitado
domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

 Guardar

2.4.5.2 Listas de confianza por usuario

Las Listas de Confianza son unas listas blancas automáticas y personalizadas por usuario.

De esta manera se consigue que no se aplique el filtrado a los correos de la gente con la que normalmente se intercambia información y así evitar falsos positivos.

Estas listas se van llenando automáticamente con las direcciones de correo de los remitentes que Email Protection considera que no ofrecen ningún tipo de duda sobre su procedencia.

Desde este panel se habilitan/deshabilitan las Listas de Confianza para los usuarios individuales.

Lista de confianza por usuario

Dominio:

Configuración: **Lista de confianza deshabilitada**

Buscar: en:

Nombre y apellido A	Correo electrónico	Según dominio	Habilitado	Deshabilitado
usuario	usuarionombre@domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.4.6 Modo de filtrado

2.4.6.1 Modo de filtrado por dominio

El filtrado de mensajes por contenido se lleva a cabo para determinar si un mensaje es o no válido cuando se da el caso que Email Protection no puede determinar si el remitente es un spammer mediante alguno de los filtros por conexión o las listas blancas/negras.

Para ello Email Protection permite elegir entre dos modos de filtrado:

2.4.6.1.1 Modo Automático

Analiza y clasifica los mensajes recibidos como correo válido o Spam en función de la puntuación que obtiene cada uno de ellos tras la verificación de más de 600 reglas. A mayor puntuación mayor probabilidad de que un mensaje sea Spam.

Cuanto más alto es el nivel de protección que se elija mayor es la probabilidad de encontrar mensajes Spam, pero también de considerar Spam mensajes que no lo son (falsos positivos). Un valor de 5 debería ser suficiente para un usuario estándar.

2.4.6.1.2 Modo Garantizado

Comprueba y valida el origen de los mensajes, verificando si los emisores figuran en la lista de remitentes válidos del usuario (lista blanca).


Cualquier remitente que no se encuentre en la lista blanca del destinatario recibirá automáticamente un mensaje de validación. Tras hacer un simple clic en un enlace del correo de validación, el remitente será añadido a la lista blanca del destinatario y su correo será entregado. A partir de entonces todos sus mensajes serán entregados automáticamente sin pasar por los filtros de contenido.


Si el modo de filtrado garantizado se encuentra habilitado, la función Evitar suplantación de identidad se desactiva en aquel nivel donde se aplique (usuario, dominio o empresa).

En el caso de que el remitente no se validara, el destinatario puede hacerlo manualmente desde su Panel de Control, desde el Notificador o desde el Informe de correo bloqueado.

Propagar en cascada, a nivel global, aplica la configuración a todos los dominios y usuarios de la empresa, a nivel de dominio, aplica la configuración a todos los usuarios del dominio.

Modo de filtrado por dominio

[Mostrar información sobre la configuración de filtros](#) 

 La carpeta **"Correo pendiente de validación"** correspondiente al modo de filtrado Garantizado se muestra siempre, independientemente del modo de filtrado del Usuario.

Configuración Global

	Automático	Garantizado	
Todos los dominios	<input checked="" type="radio"/> 5 <small>▼</small>	<input type="radio"/>	<input type="checkbox"/> Propagar en cascada

Modo de filtrado de mensajes Spam

Nombre Dominio	Global	Automático	Garantizado	
domain.com	<input checked="" type="radio"/>	<input type="radio"/> 5 <small>▼</small>	<input type="radio"/>	<input type="checkbox"/> Propagar en cascada


2.4.6.2 Modo de filtrado por usuario

Se permite cambiar el modo de filtrado de Email Protection para cada usuario individualmente.

Ver el apartado Modo de filtrado por dominio para más información sobre los modos de filtrado.

Modo de filtrado por usuario

[Mostrar información sobre la configuración de filtros por usuario](#) ?

 La carpeta "Correo pendiente de validación" correspondiente al modo de filtrado Garantizado se muestra siempre, independientemente del modo de filtrado del Usuario.

Dominio:

Buscar: en:

Nombre y apellido A	Correo electrónico	Según dominio	Automático	Garantizado
usuario	usuarionombre@domain.com	<input checked="" type="radio"/>	<input type="radio"/> 5	<input type="radio"/>

2.4.7 Motor de reglas

2.4.7.1 Motor de reglas entrantes

Las reglas de filtrado que defina le permitirán administrar el flujo de mensajes entrantes de los usuarios del sistema. Mediante el uso de estas reglas, podrá:

- Eliminar los archivos adjuntos de un correo.
- Marcar un correo como SPAM o Válido.
- Eliminar el correo sin dejarlo en papelera.
- Reenviar o enviar copia de un correo a uno o varios destinatarios.
- No realizar acciones sobre el correo.

Para crear una regla:

1. Defina los criterios (condiciones) bajo los que se aplicará la regla.
2. Seleccione una o más acciones a aplicar sobre el mensaje.
3. Puede optar por desactivar la regla durante su creación; por defecto, la regla se creará en estado "activa".
4. Finalmente, haga clic en "crear regla".

Motor de reglas entrantes

[Mostrar información sobre motor de reglas](#) ?

 Si bien puede crear tantas reglas como crea necesarias, es importante advertir que el uso de **demasiadas** reglas podría impactar en el desempeño del sistema, produciendo retrasos en la recepción/entrega del correo.

Mostrar reglas de:

Empresa

Existe: 1 regla de filtrado

 Crear regla  Eliminar

<input type="checkbox"/>	Prioridad	Condición	Acción	Activa	Editar
<input type="checkbox"/>	1  	Aplicar a Correos con Tamaño > 10 Kb	Quitar los archivos adjuntos.		

Es importante mencionar que el empleo de la acción "Reenviar a", excluye al resto de las acciones.

La acción de "enviar copia a" envía una copia del correo recibido originalmente a un destinatario o varios separados por coma.

La acción de "reenviar a" no se puede combinar con otras acciones. Se reenvía el correo original a la dirección indicada o a varias separadas por coma.

En el caso de seleccionar "Archivo adjunto del tipo Mime", el motor evaluará el campo Mime del archivo adjunto. Para imágenes jpg se debe ingresar **image/jpeg**, para avi se debe ingresar **video/avi**, etc.

Es importante mencionar que el empleo de la acción "eliminar archivos adjuntos" modificará el contenido del correo; esto afectará a aquellos que hayan sido firmados mediante PGP o X.509, invalidando la firma digital. Panda no se responsabiliza por las implicaciones legales de los efectos producidos por estas modificaciones.

En el caso de seleccionar "Archivo adjunto de tamaño...", los valores que especifique serán considerados en KB; por ejemplo, si indica 25, se interpretará 25 KB; si indica 25000, se interpretará 25000 KB ó, lo que es equivalente 25 MB.

La condición **Tamaño del correo**, se refiere al tamaño total del correo, incluyendo archivos adjuntos.

La definición de condiciones de una Regla le permite hacer uso de la búsqueda de patrones de tipo URL como parte del contenido de un correo.

Es importante mencionar que el empleo de Contiene tarjetas de crédito, reconoce los siguientes formatos de tarjetas de crédito:

Visa: XXXX XXXX XXXX XXXX

MasterCard: XXXX XXXX XXXX XXXX

Maestro: XXXX XXXX XXXX XXXX

American Express: XXXX XXXXXX XXXXX

Diners: XXXX XXXXXX XXXX

Si bien puede crear tantas reglas como crea necesarias, es importante advertir que el uso de demasiadas reglas podría impactar en el desempeño del sistema, produciendo retrasos en la recepción/entrega del correo.

Es posible definir condiciones para archivos adjuntos que se evalúen también para el contenido de esos archivos. En el caso de archivos comprimidos que contienen otros archivos comprimidos, la evaluación de la regla se realizará hasta el cuarto nivel de compresión. Las búsquedas dentro de archivos comprimidos se podrán activar cuando la condición involucre los siguientes operadores:

- Todo o parte del nombre
- De tamaño >
- De tamaño <=

El operador "Contiene expresión regular" puede utilizarse para los campos:

- Asunto
- Cuerpo

Las expresiones regulares soportadas son del tipo PERL. Para más información sobre este tipo de expresiones, puede consultar la siguiente referencia oficial:

http://en.wikipedia.org/wiki/Regular_expression#Perl-derived_regular_expressions

2.4.7.2 Motor de reglas salientes

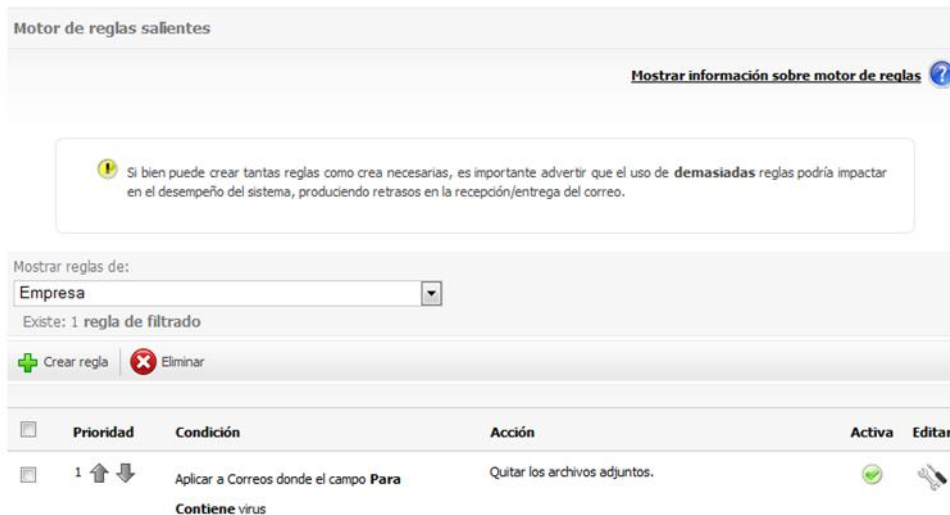
Las reglas de filtrado que usted defina le permitirán administrar el flujo de mensajes salientes de los usuarios del sistema. Mediante el uso de estas reglas, podrá:

- Eliminar los archivos adjuntos de un correo.
- Rechazar por política de empresa.
- Aceptar como válido.
- Eliminar el correo sin dejarlo en papelera.
- Reenviar o enviar copia de un correo a uno o varios destinatarios.
- No realizar acciones sobre el correo.

Para crear una regla:

1. Defina los criterios (condiciones) bajo los que se aplicará la regla.

2. Seleccione una o más acciones a aplicar sobre el mensaje.
3. Puede optar por desactivar la regla durante su creación; por defecto, la regla se creará en estado "activa".
4. Finalmente, haga clic en "crear regla".



Motor de reglas salientes

[Mostrar información sobre motor de reglas](#) ?

⚠ Si bien puede crear tantas reglas como crea necesarias, es importante advertir que el uso de **demasiadas** reglas podría impactar en el desempeño del sistema, produciendo retrasos en la recepción/entrega del correo.

Mostrar reglas de:
 Empresa

Existe: 1 regla de filtrado

+ Crear regla - Eliminar

Prioridad	Condición	Acción	Activa	Editar
1	Aplicar a Correos donde el campo Para Contiene virus	Quitar los archivos adjuntos.	<input checked="" type="checkbox"/>	

Es importante mencionar que el empleo de la acción "Reenviar a", excluye al resto de las acciones.

La acción de "enviar copia a" envía una copia del correo recibido originalmente a un destinatario o varios separados por coma.

La acción de "reenviar a" no se puede combinar con otras acciones. Se reenvía el correo original a la dirección indicada o a varias separadas por coma.

En el caso de seleccionar "Archivo adjunto del tipo Mime", el motor evaluará el campo Mime del archivo adjunto. Para imágenes jpg se debe ingresar image/jpeg, para avi se debe ingresar video/avi, etc.

Es importante mencionar que el empleo de la acción "eliminar archivos adjuntos" modificará el contenido del correo; esto afectará a aquellos que hayan sido firmados mediante PGP o X.509, invalidando la firma digital. Panda no se responsabiliza por las implicaciones legales de los efectos producidos por estas modificaciones.

En el caso de seleccionar "Archivo adjunto de tamaño...", los valores que especifique serán considerados en KB; por ejemplo, si indica 25, se interpretará 25 KB; si indica 25000, se interpretará 25000 KB ó, lo que es equivalente 25 MB.

La condición Tamaño del correo, se refiere al tamaño total del correo, incluyendo archivos adjuntos.

La definición de condiciones de una Regla le permite hacer uso de la búsqueda de patrones de tipo URL como parte del contenido de un correo.

Es importante mencionar que el empleo de Contiene tarjetas de crédito, reconoce los siguientes formatos de tarjetas de crédito:

Visa: XXXX XXXX XXXX XXXX

MasterCard: XXXX XXXX XXXX XXXX

Maestro: XXXX XXXX XXXX XXXX

American Express: XXXX XXXXXX XXXXX

Diners: XXXX XXXXXX XXXX

Si bien puede crear tantas reglas como crea necesarias, es importante advertir que el uso de demasiadas reglas podría impactar en el desempeño del sistema, produciendo retrasos en la recepción/entrega del correo.

Es posible definir condiciones para archivos adjuntos que se evalúen también para el contenido de esos archivos. En el caso de archivos comprimidos que contienen otros archivos comprimidos, la evaluación de la regla se realizará hasta el cuarto nivel de compresión. Las búsquedas dentro de archivos comprimidos se podrán activar cuando la condición involucre los siguientes operadores:

- Todo o parte del nombre
- De tamaño >
- De tamaño <=

El operador "Contiene expresión regular" puede utilizarse para los campos:

- Asunto
- Cuerpo

Las expresiones regulares soportadas son del tipo PERL. Para más información sobre este tipo de expresiones, puede consultar la siguiente referencia oficial:

http://en.wikipedia.org/wiki/Regular_expression#Perl-derived_regular_expressions

2.4.8 Logs de correos

2.4.8.1 Listado de logs

El listado de Logs de correo permite ver la información básica de todos los correos que han pasado por Email Protection así como cambiar su estado o incluso ver dichos correos (si es que se definió esta opción en el momento de la compra de Email Protection).

Se pueden filtrar los correos usando cualquiera de los campos dispuestos a tal efecto o con la combinación de varios de ellos.

Logs de correos

Listado de logs

[Mostrar información sobre listado de logs ?](#)

Buscar logs de correo para:

Asunto:

De:

Para:

IP Origen:

Clasificación:

Período: (dd/mm/aaaa)

Desde:

Hasta:


El rango de las fechas para la búsqueda de logs de correo estará limitado según el tiempo de almacenamiento.

La lista de selección de clasificación le permitirá filtrar los Logs por las siguientes categorías:

- Todos sin rechazados ni saliente
- Avisos de servidor
- Avisos de virus
- Correo con virus
- Listas de correo
- Pendientes de validar
- Spam
- Válidos
- Correo saliente válido
- Correo entrante rechazado
- Correo saliente rechazado

Los posibles estados⁵ en los que puede encontrar un correo son los siguientes:

- Entregado: el correo ha sido entregado al destinatario.
- Pendiente: el correo aún se encuentra en la cola de envío, o se está reenviando debido a algún tipo de error en destino.
- Error: se ha producido algún error en la entrega del correo; el motivo se podrá ver haciendo clic en "Más detalles".
- Error temporal: Se ha producido algún error en la entrega del correo; el motivo se podrá ver haciendo clic en "Más detalles".
- Retenido: correos que han sido clasificados como SPAM o que debido a la configuración indicada por el usuario, no deben serle entregados (avisos de virus, avisos de servidor y listas de correo).
- Procesando: no se ha determinado aún el estado del correo. Se debe esperar una próxima actualización de Logs para ver el estado del correo.
- Eliminado: correos que han sido clasificados como VIRUS y han sido eliminados.
- Cuarentena: correos que han sido clasificados como VIRUS y fueron pasados a cuarentena.

Si se realiza algún cambio que afecte a la clasificación de un correo (por ejemplo, pasar de SPAM a Correo válido, o viceversa), la columna clasificación mostrará un icono () que reflejará tal situación.

Un correo puede ser clasificado como uno de los siguientes valores:

- Válido
- Lista de correo
- Aviso de servidor
- Spam
- Pendiente de validar
- Aviso de virus
- Correo con virus
- Saliente válido

⁵ En la lista de Logs se muestra, para un correo determinado, el estado actual del mismo; es decir, no se exhiben todos los estados por los que ha pasado ese correo (por tanto, un determinado correo aparecerá sólo una vez en la lista de Logs)

- Eliminado
- Spam rechazado

Esas clasificaciones son generadas por alguno de los siguientes componentes del sistema:

- Antispoofing
- Sistema anti-virus
- Lista negra
- Condición de lista de correo
- Clasificador bayesiano
- Anti-spam desactivado por ser usuario con filtrado básico
- Condición de correo pendiente de validación
- Condición de aviso de servidor
- Correo auto-generado
- Motor de reglas
- RBLw: La IP del remitente se encuentra en una DNSBL
- RPDS (Sistema de detección de patrones recurrentes)
- Clasificador heurístico
- Ningún filtro lo clasifica, es válido porque nadie dice lo contrario
- SPFw: El correo ha sido enviado desde una IP no autorizada para tal fin por los administradores del dominio remitente
- Lista de confianza
- Cantidad de destinatarios excedida: La cantidad de destinatarios del correo excede el máximo permitido
- Ruteo fijo: Existen políticas de plataforma que han forzado esta clasificación

Se proporciona además la posibilidad de *descargar* un fichero con los Logs que han resultado de una consulta o, simplemente, del listado obtenido por defecto. El formato del fichero es compatible con Microsoft® Excel®.

Para cada Log de correo, dependiendo de su clasificación y estado, pueden existir las siguientes acciones a realizar con los datos del mismo:

- Enviar IP de origen a lista blanca: A los correos provenientes de IPs pertenecientes a esta lista, se les aplicarán los filtros de conexión y antivirus, y ningún filtro de contenido.
- Enviar IP de origen a lista negra: Aquellos correos provenientes de IPs de esta lista, serán directamente rechazados.
- Enviar dominio de origen a lista blanca: A los correos provenientes de dominios pertenecientes a esta lista, se les aplicarán los filtros de conexión y antivirus, y ningún filtro de contenido.
- Enviar dominio de origen a lista negra: Los correos provenientes de dominios pertenecientes a esta lista, serán colocados en cuarentena después de pasar por los filtros de conexión.
- Enviar remitente a lista blanca: A los correos provenientes de remitentes pertenecientes a esta lista, se les aplicarán los filtros de conexión y antivirus, y ningún filtro de contenido.
- Enviar remitente a lista negra: Los correos provenientes de remitentes pertenecientes a esta lista, serán colocados en cuarentena después de pasar por los filtros de conexión.
- Pasar a Correo Válido: Mueve un correo de su carpeta de origen a la carpeta válidos.
- Pasar a Correo Spam: Mueve un correo válido a la carpeta spam.
- Ver Correo: Permite visualizar el correo electrónico al cual se hace referencia. Esta acción estará disponible sólo en el caso en que la misma haya sido incluida al momento de comprar Email Protection.
- Reentregar: Re entrega el correo al cual se hace referencia.

Acciones masivas de Logs de Correo:

Las acciones masivas permiten realizar diferentes operaciones sobre un conjunto de logs de correos, de manera simultánea. Dado que el proceso puede llevar varios minutos, el resultado de cada operación será notificado por correo electrónico a la cuenta de contacto configurada.

Las acciones solicitadas sólo tendrán efecto sobre los logs seleccionados en la página actual de resultados de la búsqueda.

No todas las acciones son aplicables a todos los tipos de correos:

- Re-entrega: sólo los correos válidos podrán ser re-entregados.
- Pasar a Lista Blanca / Pasar a Lista Negra: podrán incluirse dominios, IPs o remitentes.

A fin de evitar redundancias en las listas de remitentes y dominios, no será posible agregar un remitente cuando el dominio ya exista en la misma lista. Por esta razón, al

agregar un dominio a una lista, todas las direcciones de correo de ese dominio serán eliminadas de la lista.

Pasar a Lista Blanca



Pasar a Lista Negra



2.4.9 Validación NDR

Es posible desde el Panel de Administrador de empresa configurar esta validación tanto a nivel de dominios como a nivel de usuarios. Estas opciones se encuentran en la solapa "Filtrado" en las secciones "Validación NDR por Dominios" y "Validación NDR por Usuarios" respectivamente.

Validación NDR implica que a todos los mensajes enviados a través de nuestro servidor se les agregará una firma digital (SRS), que será verificada en caso de que el mensaje sea rechazado por parte del servidor SMTP del destinatario. Si esta firma es validada correctamente, se procede con el resto de los filtrados sobre el correo electrónico entrante; en caso de no coincidir, el correo entrante es automáticamente rechazado.

La activación de la validación de NDRs para empresa, dominio o usuario implica lo siguiente:

1. Si un correo viene con codificación SRS válida entonces se aplica filtrado.
2. Si un correo viene con codificación SRS inválida entonces es rechazado.
3. Si un correo viene sin codificación SRS, es rechazado.

2.4.9.1 Validación NDR por Dominio

La gestión de validación NDR de correo entrante por dominios le permitirá definir configuraciones que podrán aplicarse de forma global a todos los dominios, o para cada dominio en particular.

Por defecto, este tipo de validación se encuentra desactivada, tanto para la empresa como para cada dominio dentro de ella. Para activarlo, tanto a nivel empresa como

dominio, deberá: seleccionar **Configuración propia**, luego hacer clic en **Validación NDR**; si no selecciona esa opción, la validación quedará desactivada.

- Validación por NDR:** La activación de esta validación implica que Email Protection verificará la existencia y validez de una firma digital en todos los correos entrantes rechazados (esa firma fue agregada en el momento de hacer el envío de un correo de forma autenticada). Esta validación previene el ingreso de SPAM en forma de falsos rechazos de correos.

Validación NDR por dominio

[Mostrar información sobre validación NDR por dominios](#) 

Configuración de la empresa

	Validación NDR
Configuración global (aplicada a todos los dominios)	<input type="checkbox"/>

Dominio A	Configuración global	Configuración propia	Validación NDR
domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

Aquellos mensajes que no sean enviados a través de Email Protection, son susceptibles de no recibir avisos de servidor o respuestas automáticas en el caso de que la validación de NDRs se encuentre activada.

2.4.9.2 Validación NDR por Usuario

La gestión de validación NDR por usuarios le permitirá definir, para cada usuario, si desea o no activar la **Validación NDR**. Esta validación implica que Email Protection verificará la existencia y validez de una firma digital en todos los correos entrantes rechazados (esa firma fue agregada en el momento de hacer el envío de un correo de forma autenticada). Esta validación previene el ingreso de SPAM en forma de falsos rechazos de correos.

Por defecto, la configuración de la **Validación NDR** para cada usuario es la que utiliza el dominio al que pertenece.

Aquellos mensajes que no sean enviados a través de Email Protection, son susceptibles de no recibir avisos de servidor o respuestas automáticas en el caso de que la validación de NDRs se encuentre activada.

Validación NDR por usuario

[Mostrar información sobre validación NDR por usuarios](#) ?

Dominio:

Configuración: **global**

Buscar: en:

Nombre y apellido A	Correo electrónico	Según dominio	Configuración propia	Validación NDR
usuario	usuarionombre@domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

2.4.10 Detección de suplantación de identidad

Es posible desde el Panel de Administrador de empresa configurar detección de suplantación de identidad tanto a nivel de dominios como a nivel de usuarios. Estas opciones se encuentran en la solapa "Filtrado" en las secciones "Detección de suplantación de identidad por dominio" y "Detección de suplantación de identidad por usuarios" respectivamente.

Si el modo de filtrado garantizado se encuentra habilitado, la función Evitar suplantación de identidad se desactiva en aquel nivel donde se aplique (usuario, dominio o empresa).

Se permite el agregado de IPs tanto del tipo IPv4 como IPv6. Cada dirección IPv6 debe ser representada en ocho grupos separados por ":"; cada grupo debe contener 4 dígitos hexadecimales.

Es posible utilizar la notación comprimida IPv6, eliminando los ceros a la derecha de cada grupo.

Por ejemplo:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

2.4.10.1 Detección de suplantación de identidad por dominio

La gestión de Detección de suplantación de identidad por dominio le permitirá definir configuraciones que podrán aplicarse de forma global a todos los dominios, o para cada dominio en particular.

Por defecto, esta prueba se encuentra deshabilitada, tanto para la empresa como para cada dominio dentro de ella.

- **Detección de suplantación de identidad por dominio:** Verificará que el emisor del correo es quien dice ser, cuando el emisor y el receptor del correo son cuentas protegidas por el Firewall de correo y pertenecen al mismo dominio. Si se habilita esta prueba no será necesario agregar el propio dominio a la lista negra como práctica preventiva de SPAM. Este tipo de práctica tiene como motivación evitar que correos electrónicos no deseados sean recibidos cuando el emisor ha suplantado la identidad con una cuenta protegida.

Si se deshabilita la prueba, o si se desea usar la configuración indicada por la empresa para un dominio, no se podrá definir Listas de direcciones IP habilitadas para el envío.

Las IP's incluidas en la **Lista de direcciones IP habilitadas para el envío**, no serán chequeadas por este filtro. Si se deshabilita la prueba, o si se desea usar la configuración indicada por la empresa para un dominio, no se podrán definir IPs en **Lista de direcciones IP habilitadas para el envío**.

Detección de suplantación de identidad por dominio

[Mostrar información sobre Detección de suplantación de identidad por dominio](#) ?

Mostrar configuración de:

Empresa ▼

Configurar

Habilitar

+
-

Guardar cambios

2.4.10.2 Detección de suplantación de identidad por usuario

La gestión de detección de suplantación de identidad por usuario le permitirá definir, para cada usuario, si desea o no activar la Detección de suplantación de identidad. De habilitarse el comportamiento por usuario, las pruebas se aplicarán para aquellos correos cuyo emisor es el mismo usuario protegido.

Detección de suplantación de identidad por usuario

Dominio:

domain.com ▼

Buscar: en: Correo electrónico ▼ Aplicar filtro Mostrar todos

Nombre y apellido A	Correo electrónico	Según dominio	Habilitada	Deshabilitada
usuario	usuariionombre@domain.com	●	●	●

Guardar cambios

2.5 Personalización

En esta sección podrá configurar:

- Aspectos referidos a los mensajes automáticos: "Mensaje de bienvenida" e "Informe de correo bloqueado".
- Logotipo corporativo y por dominio.
- Idioma de las consolas de administración de empresa y de dominio.

2.5.1 Mensajes automáticos

Email Protection puede enviar automáticamente tres tipos de mensajes a los usuarios:

2.5.1.1 Mensaje de bienvenida

Se envía una única vez a cada nuevo usuario del servicio. En él se explican aspectos relacionados con la configuración de la cuenta de correo electrónico y la utilización eficiente del servicio.

Adjunto con el mensaje de bienvenida se podrá enviar el manual de usuario Email Protection o cualquier archivo que se desee.

Puede optar por enviar el mensaje de bienvenida por defecto o el mensaje de bienvenida personalizado. Puede personalizar el mensaje de bienvenida, haciendo clic sobre el link "**Modificar**".

Atención: si se decide que no se envíe el mensaje de bienvenida y se usa la creación automática de usuarios, éstos no recibirán la contraseña para acceder a su Panel de Control.

Mensajes automáticos

Mostrar configuración de:

empresa

Mensaje de bienvenida Informe de correo bloqueado Mensaje validación filtrado Garantizado

El mensaje de bienvenida se envía una sola vez a cada nuevo usuario del Servicio. En él se explican aspectos relacionados con la configuración de la cuenta de correo electrónico, y a la utilización eficiente del Servicio.

Adjunto con el mensaje de bienvenida podrá enviar el manual de usuario SPAMINA ó algún archivo que usted desee. El mismo puede ser de cualquier formato. En cuanto al tamaño del archivo, no debe superar los 6 MB.

Atención: Si decide que no se envíe el mensaje de bienvenida y usa la creación automática de usuarios, éstos no recibirán la contraseña para acceder a su Panel de Control.

Permitir al administrador de dominio la personalización del mensaje

Mensaje por defecto SPAMINA

Mensaje personalizado [Modificar](#)

No enviar mensaje de bienvenida

Enviar sin adjunto

Enviar con manual

Enviar con el archivo...

2.5.1.1.1 Modificar Mensaje

Aparecerá una pantalla con un campo con el texto por defecto del mensaje y un campo con el asunto del correo que se enviará. En esta pantalla puede cambiar el contenido y asunto del mensaje para la empresa o para cada dominio. El mensaje por defecto para la empresa, será aquel que se usa actualmente en las distribuciones de Email Protection. Antes de guardar el mensaje puede pre visualizarlo haciendo clic en el botón **“Previsualizar”**.

2.5.1.2 Informe de correo bloqueado

En él se informa sobre los mensajes que han sido bloqueados por Email Protection; dando la opción de recuperar los correos clasificados como spam, y agregar sus remitentes a la lista blanca del usuario. Puede optar entre el no envío de este mensaje, o el envío con periodicidad diaria o semanal.

Puede optar por enviar el informe Email Protection por defecto o personalizar el mensaje mediante la implementación de plantillas.

Las plantillas pueden ser gestionadas haciendo clic sobre el enlace **“Ver plantillas”**. Las mismas se encuentran en un desplegable, con el cual podrá seleccionar la plantilla que desea utilizar.

Mensaje de bienvenida
Informe de correo bloqueado
Mensaje validación filtrado Garantizado

El informe de correo bloqueado se envía de forma diaria (por defecto), y en él se informa sobre los mensajes que han sido bloqueados por SPAMINA.

En este informe se permite a los usuarios recuperar mensajes clasificados como Spam por error, agregando a sus remitentes a la Lista Blanca.

De esta manera, el informe es una potente herramienta que permite adecuar el Servicio a las necesidades de cada usuario.

Permitir al Administrador de dominio la personalización del informe

Mensaje por defecto [Previsualizar](#)

Mensaje Personalizado [Ver plantillas](#)

Plantilla seleccionada:

No enviar informe

Enviar informe diariamente

Enviar informe semanalmente

Propagar en cascada

Propagar **en cascada**: Aplica la configuración a todos los dominios y usuarios de la empresa.

2.5.1.2.1 Ver plantillas

Aparecerá una nueva interfaz donde los botones que estarán disponibles son:

- **Crear Plantilla:** crea un nuevo mensaje basado en el mensaje por defecto de Email Protection. Para crear un mensaje se debe definir un tema, un contenido del mensaje y el asunto correspondiente que se enviará en el correo electrónico. También se permite definir el nombre y correo del remitente del mensaje, por defecto aparecerá el correo de contacto de la empresa y la posibilidad de seleccionar los contenidos que desea que aparezcan en el informe y los que desea quitar.
- **Puede pre visualizar el mensaje** antes de ser guardado.
- **Eliminar:** elimina el mensaje, asunto, remitente y la plantilla. La relación es 1 a 1 y son obligatorios todos los campos.
- **Formulario de Búsqueda:** se puede buscar una plantilla por nombre de plantilla y asunto.



2.5.1.3 Mensaje de validación del modo de filtrado Garantizado

Cualquier remitente que no se encuentre en la lista blanca del destinatario recibirá automáticamente un mensaje de validación. Tras hacer un simple clic en un enlace del correo de validación, el remitente será añadido a la lista blanca del destinatario y su correo será entregado. A partir de entonces todos sus mensajes serán entregados automáticamente sin pasar por los filtros de contenido.

Puede optar por personalizar el mensaje de validación a través de la opción "Mensaje Personalizado", en caso contrario se utilizará un mensaje por defecto.



2.5.2 Informes de administradores

La gestión de Informes de administrador le permite habilitar/deshabilitar el envío de cada informe y configurar sus destinatarios.

El informe de actividad contiene información sobre su/s:


- Dominio de correo electrónico.
- Cuentas de correo electrónico.
- Tráfico de correos.
- Mensajes.

- Modo de filtrado.

Se podrá configurar tanto a nivel empresa (configuración global) como a nivel dominio, en la cual el envío de informe de actividad estará por defecto habilitado.

La configuración de destinatarios le permite definir los destinatarios del informe de actividad a nivel global o para cada dominio.

Informes de administradores

[Mostrar información sobre gestión de informes](#) 

El envío del **Informe del Actividad por Dominio** comenzará el día: Miércoles, 1:20 horas

Configuración de la empresa

Configuración global	Enviar informe	Destinatarios
Aplica a todos los dominios	<input checked="" type="checkbox"/>	[+ Ver] Configurar

[Guardar](#)

Configuración por dominio:

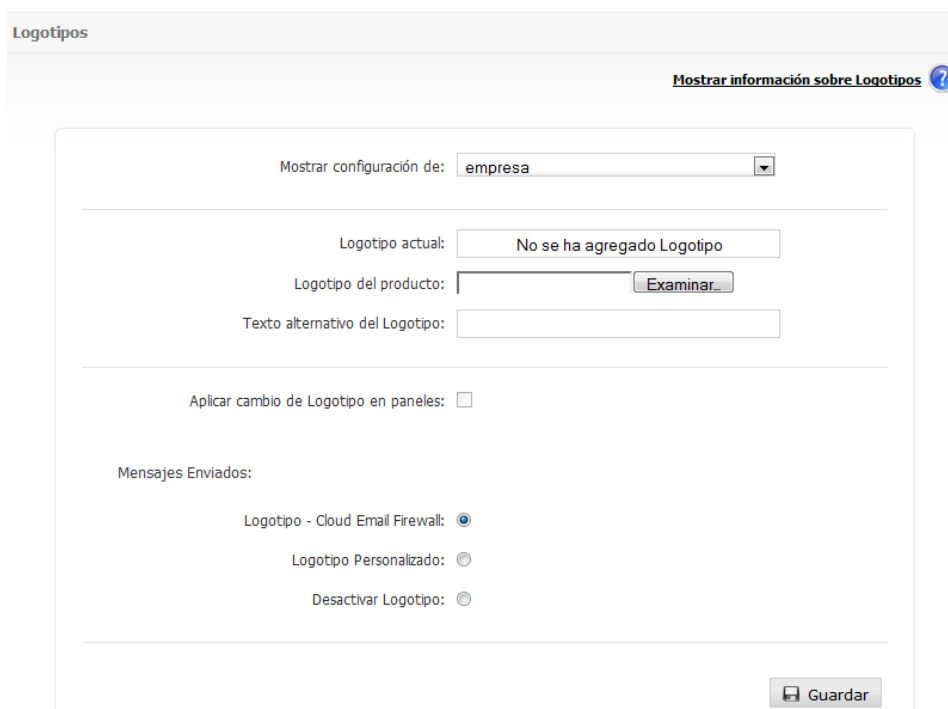
Dominio	Global	Enviar informe	Destinatarios
domain.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[+ Ver] Configurar

[Guardar](#)

Se podrán agregar hasta un máximo de 10 destinatarios y además seleccionar (para el envío de informe) tanto al administrador de empresa como al administrador de dominio.

2.5.3 Logotipos

La lista de opciones "Mostrar configuración de" le permite seleccionar la configuración a nivel de empresa o dominio para el logotipo que utilizará en los mensajes enviados.



Al seleccionar la configuración de un dominio, se estará configurando el logotipo secundario. El mismo se ubicará en el sector superior derecho de los mensajes enviados.

El archivo puede estar en los siguientes formatos: PNG, GIF o JPG. No hay restricciones en cuanto a las dimensiones del archivo original, sin embargo es aconsejable que el logotipo posea transparencia (PNG) y su formato sea rectangular, en caso contrario el mismo será adaptado de forma automática para ser utilizado por el sistema.



Además de tener la posibilidad de eliminar el logotipo actual, usted puede introducir un texto alternativo para el mismo.

El nuevo logotipo será aplicado a los paneles eligiendo la opción "Aplicar cambio de logotipo en Paneles".

En el caso de los mensajes enviados, podrá optar por:

- Utilizar el logotipo por defecto del Firewall de correo
- Utilizar un logotipo personalizado (opción "Logotipo Personalizado")
- No utilizar logotipos (opción "Desactivar Logotipo")

2.5.4 Idioma


En esta sección es posible elegir un idioma, el cual será el utilizado tanto para el Panel como para los mensajes enviados automáticamente. Esta opción está en la pestaña de "Configuración", en el apartado "idioma".

Desde el Panel de Administrador de empresa es posible al crear un dominio optar por un idioma que no necesariamente tiene que ser el mismo que utiliza la empresa, por defecto aparecerá el que tiene el administrador de empresa.

Para los dominios alias pertenecientes a la empresa también tendrán la opción de seleccionar un idioma, por defecto aparecerá el mismo idioma que el dominio principal del cual proceden.

En la creación de usuarios también, se permite seleccionar el idioma. En la modificación también se dará la opción.

Propagar cambios en cascada, aplica la configuración de idioma a todos los dominios y usuarios de la empresa, a nivel de dominio, aplica la configuración a todos los usuarios del dominio.



The screenshot shows a configuration panel with the following elements:

- Top right: [Mostrar información](#) with a question mark icon.
- Section: "Mostrar configuración de:" with a dropdown menu currently set to "empresa".
- Section: "Seleccionar Idioma:" with a dropdown menu set to "Español" and a checkbox for "Propagar cambios en cascada".
- Bottom right: A "Guardar" button with a floppy disk icon.

2.6 Configuración

En esta sección podrá configurar aspectos del sistema tales como: datos del Administrador; qué hacer frente a ciertos mensajes pertenecientes a la clasificación de listas/mensajes de servidor/avisos de virus; o qué periodicidad emplear para los mensajes que puede generar Email Protection de forma automática, entre otros.

2.6.1 Datos de la empresa

Se deben introducir los campos referentes a información de la empresa.

El campo **correo electrónico de contacto** indica la dirección de correo desde la que se enviarán todos los mensajes generados automáticamente por Email Protection.

El campo **remite** de mensajes automáticos será usado como remitente para todos los Mensajes Automáticos; si no indica uno, se utilizara por defecto no-reply@mep.pandasecurity.com

Datos de la empresa

* Nombre de la empresa:

Dirección:

Dirección 2:

Código postal:

* Teléfono:

Dirección Web:

* Persona de contacto:

* Correo electrónico de contacto:

Remite de mensajes automáticos: [Ayuda](#)

Fecha de alta: 20/10/2011

Fecha de caducidad: 20/10/2012

Licencias contratadas: 1

Licencias en uso: 1


(*) Campos requeridos

2.6.2 Datos del Administrador

Se deben introducir los datos referentes a información del administrador.

Se permite cambiar la contraseña de administración así como el número de mensajes por página que se mostrarán en los distintos paneles.

Datos del Administrador

[Mostrar información](#) 

* Nombre y Apellido:

Teléfono:

Dirección:

Ciudad:

País:

(*) Campos requeridos

Datos del administrador

Datos Personales **Cambiar Contraseña** Mensajes por página

(*) Nombre de usuario: [Ayuda](#)

(*) Contraseña anterior: [Ayuda](#)

(*) Contraseña: [Ayuda](#)

(*) Confirmación de contraseña:

(*) Campos requeridos

Datos del administrador

Datos Personales Cambiar Contraseña **Mensajes por página**

Aquí podrá configurar la cantidad de resultados que desea obtener por página.

Resultados por página:

2.6.3 Acceso a panel de usuarios finales

Es posible determinar si un conjunto de usuarios finales pueden o no acceder a su panel. Aquellos usuarios a los que se les haya deshabilitado el acceso a su panel, recibirán una notificación indicando esta situación ante cualquier intento de acceso.


2.6.3.1 Configuración por dominio

Permite configurar el acceso a paneles de los usuarios finales a nivel de empresa y dominio.

Tanto para la empresa como para cada uno de los dominios que pertenecen a ésta, las opciones de configuración disponibles son:

- **Global:** Se utiliza la configuración definida por el nivel superior: empresa para el caso del dominio y Protection de correo para el caso de la empresa.
- **Propia:** Permite aplicar una configuración diferente a la especificada por el nivel superior.
- **Acceso a panel para usuarios finales:** Indica que los usuarios de la empresa / dominio tendrán permitido acceder a sus paneles de usuario.
- **Propagar en cascada la configuración global:** Aplica la configuración a todos los dominios y usuarios de la empresa.
- **Propagar en cascada la configuración definida para un dominio específico:** Aplica la configuración a todos los usuarios del dominio seleccionado.

Configuración por dominio

[Mostrar información sobre acceso a paneles](#) 

Configuración Global

	Acceso a panel para usuarios finales
Todos los dominios	<input checked="" type="checkbox"/> <input type="checkbox"/> Propagar en cascada

[Guardar](#)

Acceso a panel usuarios finales

Nombre Dominio	Configuración global	Configuración propia	Acceso a panel para usuarios finales	
domain.com	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Propagar en cascada

[Guardar](#)

2.6.3.2 Configuración por usuario

Permite configurar el acceso a paneles a nivel de usuario final.

Para cada uno de los usuarios que pertenecen al dominio seleccionado, las opciones de configuración disponibles son:

- **Según dominio:** Se utiliza la configuración definida a nivel dominio.
- **Propia:** Permite aplicar una configuración diferente a la especificada por el dominio.
- **Acceso a panel para usuarios finales:** Indica si el usuario tendrá permitido acceder a su panel de usuario.

Configuración por usuario

[Mostrar información sobre acceso a panel para usuarios](#) 

Dominio:

Buscar: en: [Aplicar filtro](#)

Nombre y apellido A	Correo electrónico	Según dominio	Configuración propia	Acceso a panel para usuarios finales
usuario	usuarionombre@domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

[Guardar cambios](#)

2.6.4 Listas y avisos

Existen tipos de correo que no tienen ninguna utilidad para la mayoría de usuarios (aunque sean muy útiles para otros) o que son utilizados especialmente por los spammers para hacer llegar su correo al usuario final.

Se han creado unos menús especiales para decidir qué hacer con las listas de correo, los avisos de servidor y los avisos de virus.

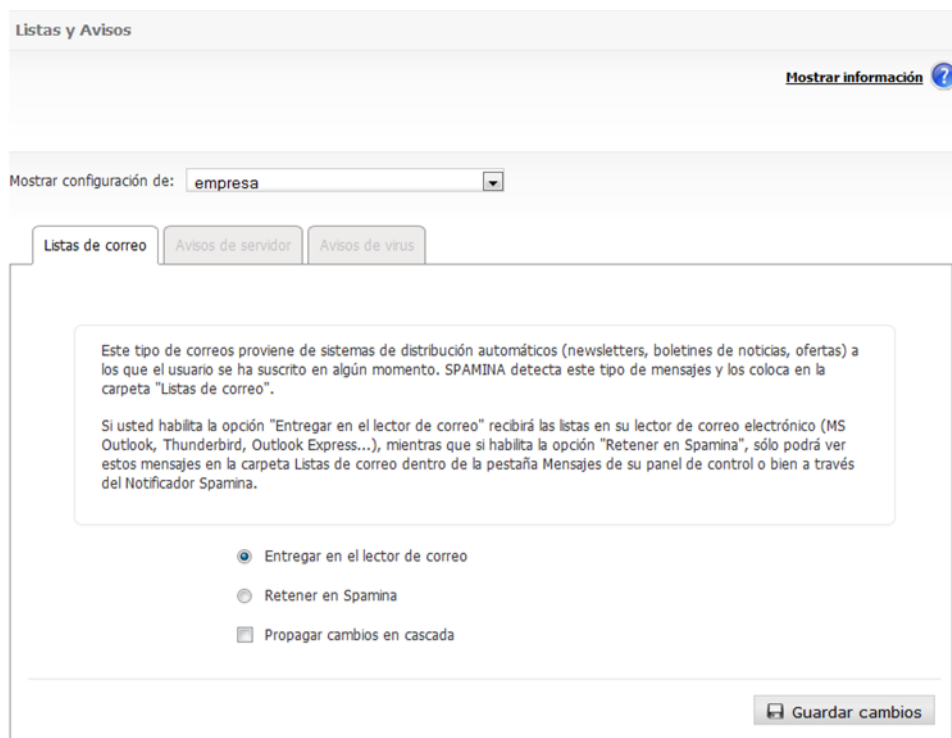
Se permite decidir, tanto para el servicio completo como para los dominios específicos, si dichos correos se entregarán al usuario final o si se guardarán en carpetas separadas para su consulta puntual si se cree necesario.

2.6.4.1 Listas de correo

Este tipo de correos proviene de sistemas de distribución automáticos (newsletters, boletines de noticias, ofertas...) a los que el usuario se ha suscrito en algún momento. Email Protection detecta este tipo de mensajes y los mueve a la carpeta **"Listas de correo"**.

Si se habilita la opción **"Entregar en el lector de correo"**, se recibirán las listas en el lector de correo electrónico (MS Outlook, Thunderbird, Outlook Express...), mientras que si se habilita la opción **"Retener"**, sólo se podrán ver estos mensajes en la carpeta **"Listas de correo"** dentro de la pestaña **"Mensajes"** del Panel de Control, o bien a través del Notificador Email Protection.

Propagar cambios en cascada, aplica la configuración a todos los dominios y usuarios de la empresa, a nivel de dominio, aplica la configuración a todos los usuarios del dominio.



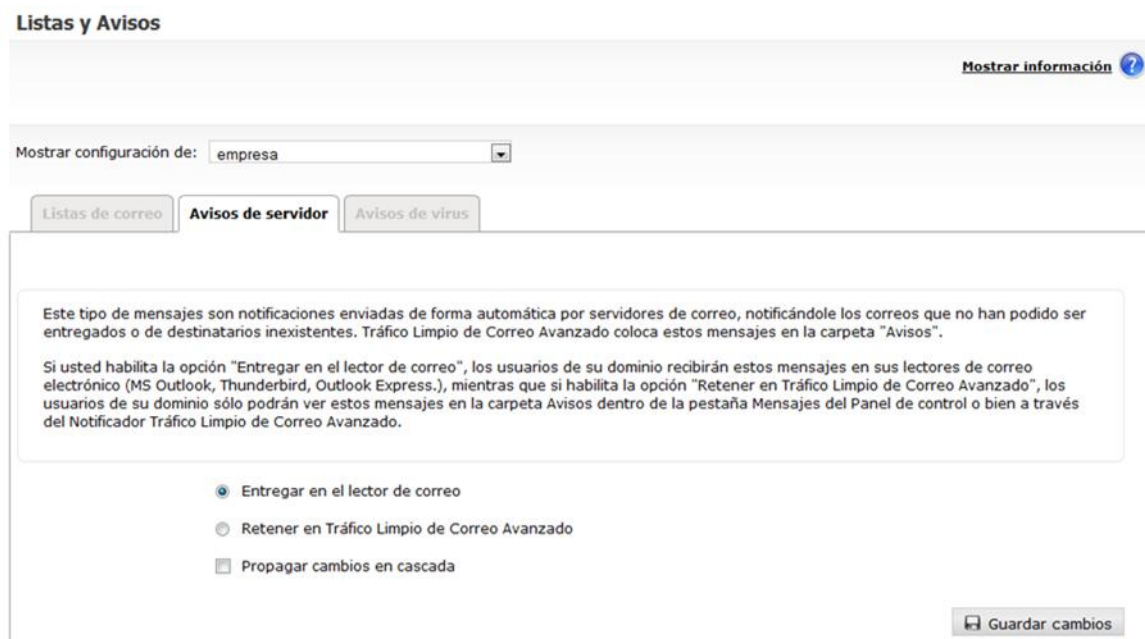
The screenshot shows the 'Listas y Avisos' configuration page. At the top, there is a 'Mostrar información' link with a question mark icon. Below that, a dropdown menu shows 'empresa' selected. There are three tabs: 'Listas de correo' (active), 'Avisos de servidor', and 'Avisos de virus'. The main content area contains a text box explaining that this type of email comes from automatic distribution systems and is moved to the 'Listas de correo' folder. Below the text box are three radio button options: 'Entregar en el lector de correo' (selected), 'Retener en Spamina', and 'Propagar cambios en cascada'. At the bottom right, there is a 'Guardar cambios' button.

2.6.4.2 Avisos de servidor

Este tipo de mensajes son notificaciones enviadas de forma automática por servidores de correo notificando los correos que no han podido ser entregados normalmente por ser los destinatarios inexistentes. Email Protection mueve estos mensajes a la carpeta **“Avisos”**.

Si se habilita la opción **“Entregar en el lector de correo”**, los usuarios recibirán estos mensajes en sus lectores de correo electrónico (MS Outlook, Thunderbird, Outlook Express...), mientras que si habilita la opción **“Retener en Email Protection”**, los usuarios sólo podrán ver estos mensajes en la carpeta **“Avisos”** dentro de la pestaña **“Mensajes”** del Panel de Control, o bien a través del Notificador Email Protection.

Propagar cambios en cascada, aplica la configuración a todos los dominios y usuarios de la empresa, a nivel de dominio, aplica la configuración a todos los usuarios del dominio.



Listas y Avisos [Mostrar información](#) ?

Mostrar configuración de: empresa

Este tipo de mensajes son notificaciones enviadas de forma automática por servidores de correo, notificándole los correos que no han podido ser entregados o de destinatarios inexistentes. Tráfico Limpio de Correo Avanzado coloca estos mensajes en la carpeta "Avisos".

Si usted habilita la opción "Entregar en el lector de correo", los usuarios de su dominio recibirán estos mensajes en sus lectores de correo electrónico (MS Outlook, Thunderbird, Outlook Express...), mientras que si habilita la opción "Retener en Tráfico Limpio de Correo Avanzado", los usuarios de su dominio sólo podrán ver estos mensajes en la carpeta Avisos dentro de la pestaña Mensajes del Panel de control o bien a través del Notificador Tráfico Limpio de Correo Avanzado.

Entregar en el lector de correo
 Retener en Tráfico Limpio de Correo Avanzado
 Propagar cambios en cascada

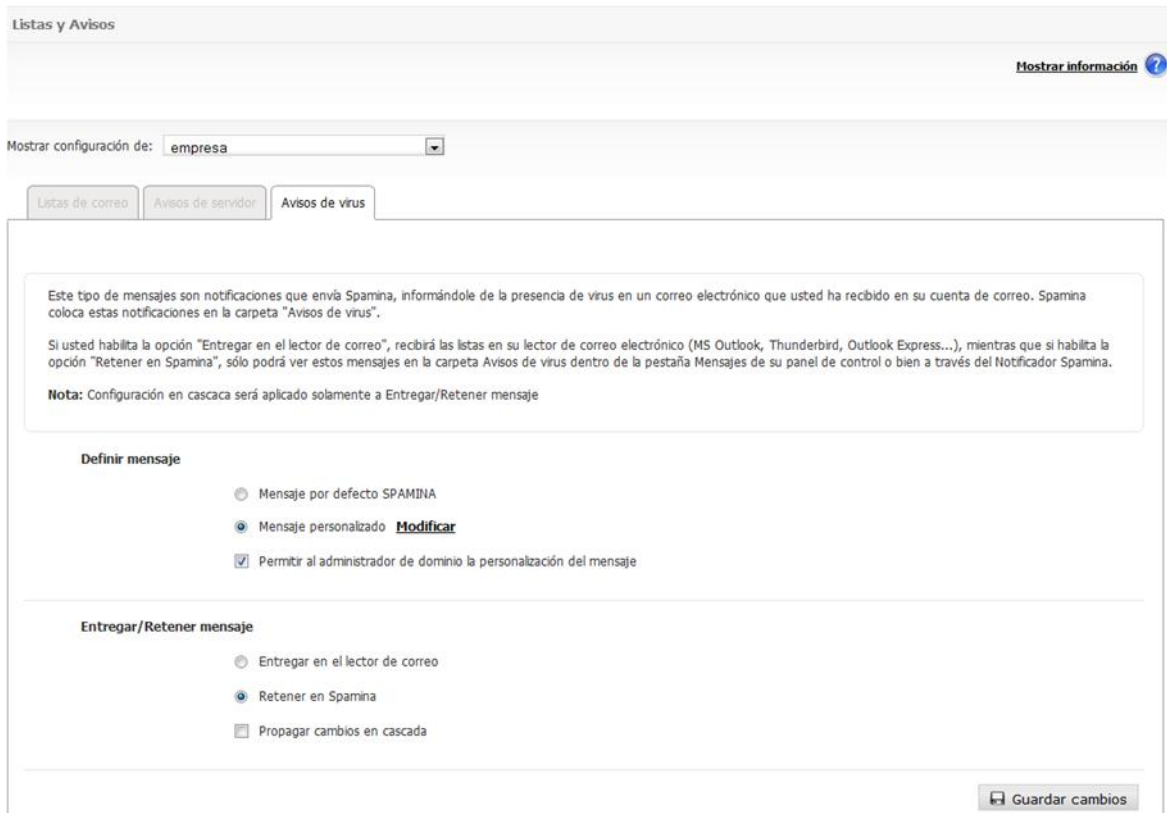
2.6.4.3 Avisos de virus

Este tipo de mensajes son notificaciones que envía Email Protection, informando de la presencia de virus en un correo electrónico. Email Protection mueve estas notificaciones a la carpeta **“Avisos de virus”**.

Si se habilita la opción **“Entregar en el lector de correo”**, se recibirán las listas en el lector de correo electrónico (MS Outlook, Thunderbird, Outlook Express...), mientras que si se habilita la opción **“Retener en Email Protection”**, sólo se podrán ver estos mensajes en la carpeta **“Avisos de virus”** dentro de la pestaña **“Mensajes”** del Panel de Control, o bien a través del Notificador Email Protection.

Propagar cambios en cascada, aplica la configuración a todos los dominios y usuarios de la empresa, a nivel de dominio, aplica la configuración a todos los usuarios del dominio.

Puede optar por personalizar el mensaje de aviso de virus desde la opción "Mensaje Personalizado", en caso contrario se utilizará un mensaje por defecto.



Mostrar configuración de: **empresa**

Este tipo de mensajes son notificaciones que envía Spamina, informándole de la presencia de virus en un correo electrónico que usted ha recibido en su cuenta de correo. Spamina coloca estas notificaciones en la carpeta "Avisos de virus".

Si usted habilita la opción "Entregar en el lector de correo", recibirá las listas en su lector de correo electrónico (MS Outlook, Thunderbird, Outlook Express...), mientras que si habilita la opción "Retener en Spamina", sólo podrá ver estos mensajes en la carpeta Avisos de virus dentro de la pestaña Mensajes de su panel de control o bien a través del Notificador Spamina.

Nota: Configuración en cascada será aplicado solamente a Entregar/Retener mensaje

Definir mensaje

Mensaje por defecto SPAMINA
 Mensaje personalizado [Modificar](#)
 Permitir al administrador de dominio la personalización del mensaje

Entregar/Retener mensaje

Entregar en el lector de correo
 Retener en Spamina
 Propagar cambios en cascada

Nota: Propagar cambios en cascada será aplicado solamente a Entregar/Retener mensaje.

2.6.5 Disclaimers

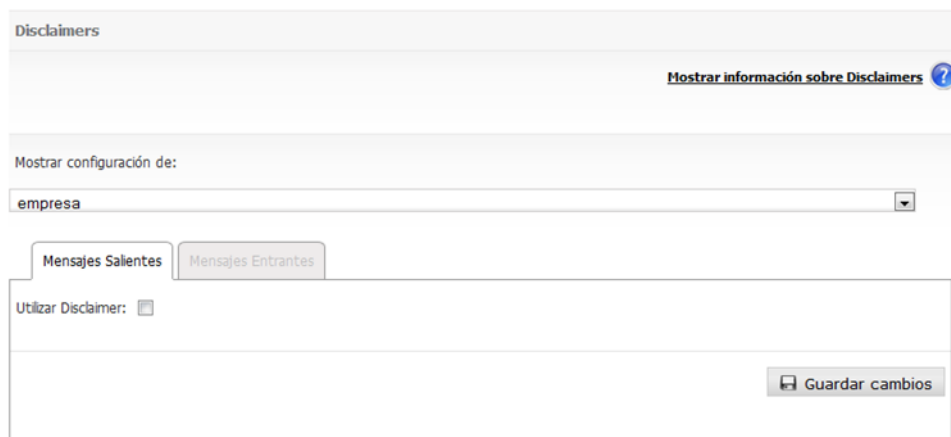
En esta sección, podrá establecer un tipo texto (disclaimer) que será colocado automáticamente al final de un correo, tanto entrante como saliente; a su vez, podrá establecer una configuración diferente para cada uno de ellos. Para que estos disclaimers apliquen a correo saliente, deberá tener activo y correctamente configurado el correo saliente a través de esta solución usando una conexión autenticada.

Esta configuración permite:

- Definir los Disclaimers tanto a nivel de la empresa como a nivel de cada dominio en particular.
- Establecer versiones del mensaje tanto en texto plano como en HTML
- Utilizar un conjunto de palabras reservadas (DATE, SENDER y RECIPIENT) que se sustituirán de forma automática para cada mensaje. Para que esa sustitución se realice de forma correcta, el cuerpo del disclaimer debe contener las palabras reservadas entre corchetes dobles, tal y como se muestra a continuación:

- Fecha de recepción del mensaje: [[DATE]]
- Remitente del mensaje: [[SENDER]]
- Destinatario del mensaje: [[RECIPIENT]]

IMPORTANTE: el empleo de disclaimers modificará el contenido del correo; esto puede afectar a aquellos que hayan sido firmados mediante PGP o X.509, invalidando la firma digital. Panda no se responsabiliza por las implicaciones legales de los efectos producidos por estas modificaciones.



2.6.6 Sincronización

En esta sección, podrá configurar la sincronización de usuarios. Dicha sincronización mantiene la coherencia entre los datos del repositorio externo y el Firewall de correo.

Las distintas opciones de configuración de la Sincronización son:

1. Sincronización: Permite activar o desactivar el uso de la sincronización
2. Ejecución de Sincronización: Permite elegir la frecuencia en que se ejecuta el proceso de sincronización.
3. Modo de Sincronización: El modo de sincronización puede ser Automático o Manual.
 - a. Automático: Realiza la sincronización sin interacción del administrador. Todos los usuarios detectados son modificados o borrados según corresponda.
 - b. Manual: Permite al administrador decidir que usuarios van a ser borrados o modificados una vez realizada la detección de usuarios a sincronizar. De esta forma se podrán Ignorar usuarios para que no sean tenidos en cuenta por el proceso de sincronización.
4. Envío de reporte de Sincronización: Si el proceso de sincronización es manual, se envía un mensaje notificando los usuarios a modificar o a eliminar. Una vez que el

administrador aplica la sincronización, los resultados son enviados en otro informe. Si el proceso de sincronización es automático, solo se envía un único informe con los resultados de la sincronización.

La configuración global es para el caso en que el administrador de empresa decida que los dominios tengan la misma configuración que la empresa.

La configuración propia es para que cada dominio tenga una configuración distinta para sí.

Sincronización

[Mostrar información sobre sincronización por dominios](#) ?

Configuración de la empresa

	Sincronización	Ejecución de sincronización	Modo de Sincronización	Envío reporte de sincronización
Configuración global (aplicada a todos los dominios)	<input type="checkbox"/>	Domingo	Manual	<input checked="" type="checkbox"/>

La empresa tiene sincronización: deshabilitada

Dominio A	Configuración global	Configuración propia	Sincronización	Ejecución de sincronización	Modo de Sincronización	Envío reporte de sincronización
domain.com	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	Domingo	Manual	<input checked="" type="checkbox"/>

2.6.7 Informes

Informes

1 informe

Buscar: en: Nombre

<input type="checkbox"/>	Nombre ▲	Asunto	Destinatarios	Frecuencia	Activo	Generar ahora	Editar
<input type="checkbox"/>	Plantilla	envío de informe	corp@dominio.com [+detalles]	Semanal	Si	<input type="button" value="Generar ahora"/>	<input type="button" value="Editar"/>

- Es posible seleccionar una de las siguientes frecuencias para el envío de un informe:
 - Diaria: El informe es enviado diariamente, con los datos correspondientes al flujo de correo que se haya producido entre las 0 y las 23hs del día anterior.
 - Últimos 7 días: El informe es enviado diariamente, con los datos correspondientes al flujo de correo que se haya producido entre los últimos 7 días y el día actual.

- **Semanal:** El informe será enviado semanalmente, con los datos correspondientes al flujo de correo que se haya producido entre el lunes y el domingo de la última semana.
 - **Mensual:** El informe es enviado mensualmente, con los datos correspondientes al flujo de correo que se haya producido entre el primero y el último día del mes.
 - **Mes actual:** El informe es enviado diariamente, con los datos correspondientes al flujo de correo que se haya producido entre el día 01 del mes y el día actual del mismo mes.
- Para cualquier informe gestionado desde la solapa "Configuración", opción de menú "Reportes", se puede solicitar su ejecución inmediata mediante el botón "generar ahora".
 - La siguiente tabla resume las acciones que se realizarán al presionar el botón "generar ahora" de acuerdo a la periodicidad del reporte:

Periodicidad	Comportamiento al presionar el botón "generar ahora"
Mensual	Se enviarán los datos correspondientes al mes anterior
Diaria	Se enviarán los datos correspondientes al día anterior
Semanal	Se enviarán los datos correspondientes a la semana anterior
Mes actual	Se enviarán los datos desde el primer día del mes actual hasta el día anterior a hoy
Últimos 7 días	Se enviarán los datos correspondientes a los últimos 7 días a partir de ayer

Puede especificar hasta 10 destinatarios para cada informe.

El informe se enviará por correo electrónico en formato PDF, tanto a los destinatarios indicados como a la dirección de contacto del administrador.

Es posible crear informes por categoría o informes predefinidos:

Por categorías

Durante las creación/edición de informes, debe seleccionar al menos una de las categorías de filtrado tanto para correo entrante como para correo saliente. Es posible no seleccionar categorías de filtrado de correo entrante, siempre que haya al menos una categoría de filtrado de correo saliente seleccionada, y viceversa. Asimismo, también es necesario seleccionar al menos un dominio.

Si selecciona una categoría de filtrado de correo entrante/saliente, debe seleccionar al menos un gráfico de filtrado de correo entrante/saliente respectivamente.

Predefinidos

Durante la creación/edición de informes predefinidos, debe seleccionar al menos una de los informes predefinidos que se encuentran disponibles.

Los reportes predefinidos disponibles son:

- Top emisores de correo: Muestra los N usuarios que más correo envían a través de la plataforma.
- Top emisores de correo por tamaño: Muestra los N usuarios que más volumen de correo envían a través de la plataforma.
- Top destinatarios de correo: Muestra los N usuarios que más correo reciben.
- Top destinatarios de correo por tamaño: Muestra los N usuarios que más volumen de correo reciben.
- Top destinatarios de Spam: Muestra los N usuarios que más correo Spam reciben.
- Top virus bloqueados: Muestra los N virus más bloqueados.

Para cada uno de estos informes predefinidos, se debe seleccionar un límite para el TOP. Los valores posibles son:

- 10
- 15
- 20
- 30

Informes

[Mostrar información sobre reportes](#)

Datos para el envío del informe

Habilitado:

(*) Nombre plantilla:

(*) Asunto:

Dominios

Todos los dominios:

Seleccione los dominios deseados:

Destinatarios

Administrador de empresa: (user@mail.com)

Otros destinatarios:

Período:

Diario: (El informe se generará a las: 00:30 horas)

Últimos 7 días: (El informe se generará todos los días a las: 00:30 horas)

Semanal: (El informe se generará a las: 00:30 horas del día lunes)

Mensual: (El informe se generará a las: 00:30 horas del primer día del mes)

Mes actual: (El informe se generará todos los días a las: 00:30 horas)

Tipo de informe:

Por categorías:

Predefinidos:

Informes predefinidos:

Top emisores de correo: Límite:

Top emisores de correo por tamaño: Límite:

Top destinatarios de correo: Límite:

Top destinatarios de correo por tamaño: Límite:

Top destinatarios de Spam: Límite:

Top virus entrantes bloqueados: Límite:

Top virus salientes bloqueados: Límite:

(*) Campos requeridos

2.6.8 Notificación por límite de licencias

Habilitado:

Porcentaje de licencias disponibles: %

Destinatarios

Administrador de empresa: (admin@domain.com)

Otros destinatarios:

other@domain.com

+
-

En esta sección podrá definir:

- Si desea recibir notificaciones por límite de licencias. El sistema notificará por correo electrónico a las direcciones configuradas, cuando el porcentaje de licencias disponibles de la empresa, sea inferior al establecido.
- Porcentaje de licencias disponibles que disparará la notificación, debe ser un valor entero comprendido entre 0 y 100.
- Destinatarios, hasta un máximo de 10 direcciones de correo electrónico.

2.6.9 Zona horaria

Esta configuración permite indicar la zona horaria predeterminada para la empresa, cada uno de sus dominios y los usuarios. En cada caso, es posible seleccionar del menú desplegable una zona horaria específica o un valor «Global». Este último valor establece que se utilizará la zona horaria seleccionada por una entidad superior: un usuario utilizará la zona horaria definida por el dominio, un dominio utilizará la zona horaria definida por la empresa, la empresa utilizará la zona horaria de la plataforma.

Los usuarios pueden configurar su propia zona horaria, pero si se escoge una configuración en este punto, se les facilitará el uso de sus consolas en lo que se refiera a tratamiento de fechas.

La zona horaria seleccionada sólo se aplica a aquellos usuarios que no hayan configurado una zona horaria específica. El cambio de esta configuración tanto para la empresa como para un dominio se aplica a la zona horaria de los usuarios que no tengan un valor de zona horaria ya seleccionado.

2.6.10 Darse de baja

En vistas a mejorar nuestro servicio, le agradeceríamos que nos indique brevemente los motivos por los cuales ha decidido darse de baja.

Darse de baja

En vistas a mejorar nuestro servicio, le agradeceríamos que nos indique brevemente los motivos por los cuales ha decidido darse de baja.

La empresa **Company**, todos sus dominios y usuarios serán dados de baja.

Motivos:

Empty text area for providing reasons for cancellation. Includes a vertical ellipsis icon in the bottom right corner.

Confirmar

3. Funciones adicionales

3.1 Notificador Panda

El Notificador de correo es una utilidad⁶ que se instala y le permite controlar y gestionar totalmente su correo electrónico.

Una vez instalado el Notificador, se visualiza un pequeño icono en la bandeja de sistema, que parpadea cuando el servicio tiene actividad y nos proporciona distintos avisos: llegada de nuevo correo electrónico, notificaciones sobre la presencia de virus, correos electrónicos que no han podido ser entregados o destinatarios inexistentes. El Notificador dispone de unos menús muy intuitivos y nos permite acceder a todas las opciones del servicio. Le permite gestionar los mensajes, marcándolos como correo válido, no válido o eliminándolos, así como configurar el modo de filtrado (Automático o Garantizado), y el nivel de protección deseado, pudiendo gestionar varias cuentas de correo a la vez. Existe la opción de acceder a las mismas acciones en su panel de control de la página Web de Panda.

3.1.1 Especificaciones técnicas

El Notificador funciona en sistemas operativos Windows (XP, Vista y Windows 7), Mac OS X, Linux x86-64, Linux PowerPC y Linux i386; en todos los casos se requiere de sistemas operativos que soporten multiusuario.

⁶ Es un programa opcional para mejorar el uso del filtro externo de correo, pero no es necesaria su instalación para proteger una cuenta de correo electrónico.

4. Soporte técnico

Como cliente de Panda dispone de varias alternativas para contactar con nuestro equipo internacional de Soporte Técnico. Por favor, acceda al sitio web de **soporte** (<http://www.pandasecurity.com/enterprise/support/>) para localizar el centro de soporte y la opción de contacto que más le convengan.