Panda Security

Email Protection

Manual de Administrador de Dominio

Versión 4.3.2-2

Tabla de contenidos

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, liberándole de las tareas de gestión y de los costes operativos de las soluciones de seguridad tradicionales.

Email Protection consta de un sistema multicapa que combina distintos filtros y mecanismos de protección que emplean tanto tecnologías propias (Email Protection PROACTIVE, Listas de Confianza...) como tecnologías estándar (reputación de IP's, 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.

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 Interfaz de Email Protection

La interfaz de Email Protection es muy intuitiva y fácil de utilizar.

Incluye cinco secciones:

- Gestión
- Filtrado
- Personalización
- Configuración
- Ayuda

Todos los paneles de administración han sido probados y funcionan en los siguientes navegadores:

Internet Explorer ® 9

Mozilla Firefox desde 3.6

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 sólo acepta contraseñas seguras. Al introducir una contraseña, el sistema evalúa su seguridad, impidiendo el uso de 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: guión bajo (_), punto (.) y guión medio (-).
- 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:

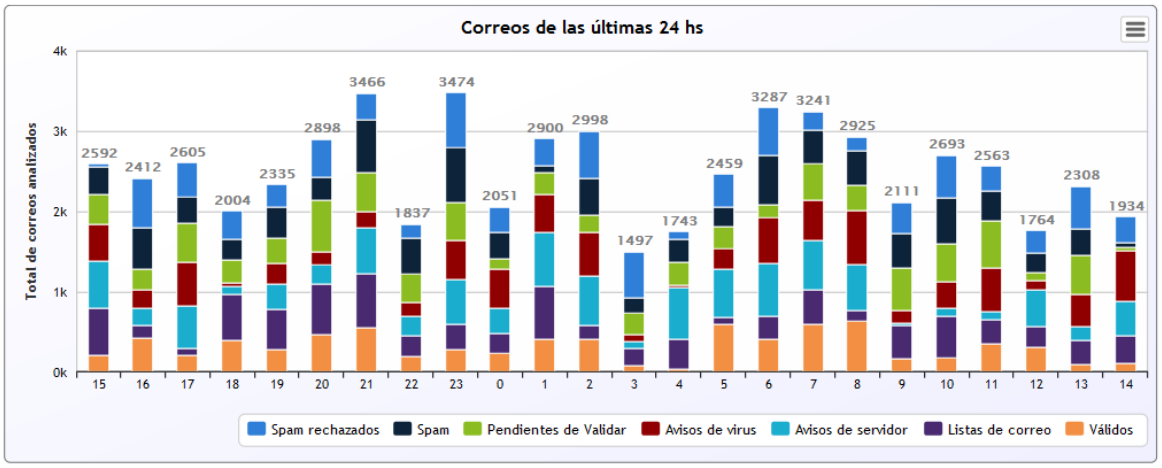
    - **Total** - Estadísticas de los últimos 30 días.
    - **Hoy** - Estadísticas para el día actual (a partir de la medianoche).
    - **Ultima hora** - Estadísticas de la hora anterior a la actual.

Tabla resumen estadísticas Correo Saliente

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

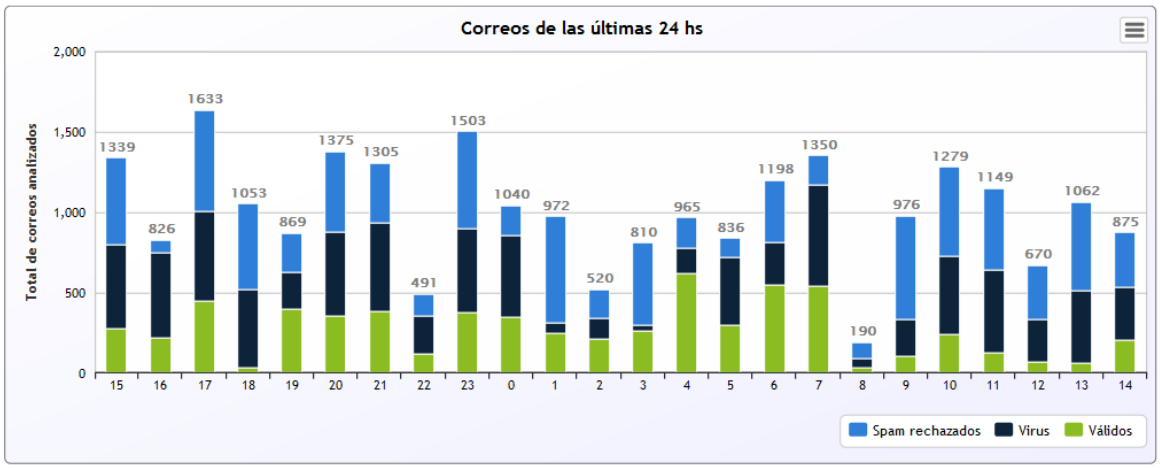
Estadísticas de correo entrante por hora

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



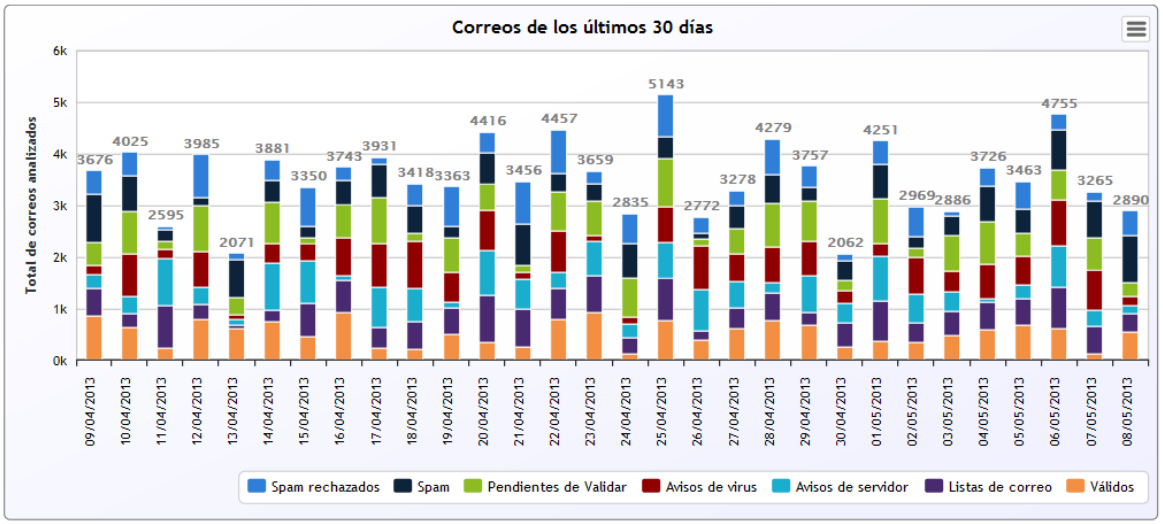
Estadísticas de correo de correo saliente por hora

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



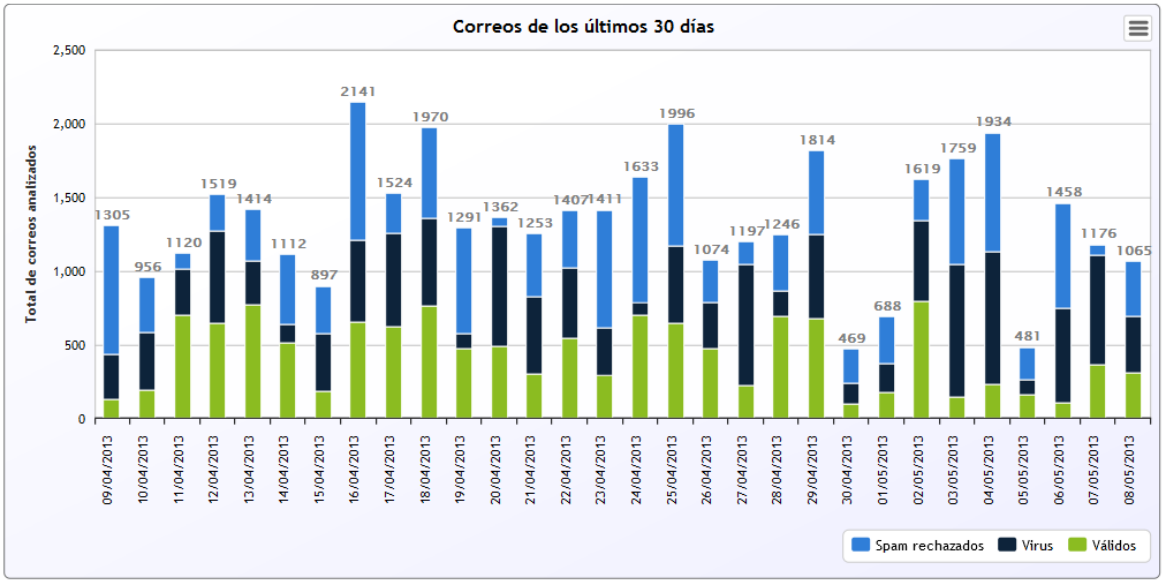
Estadísticas de correo entrante por día

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



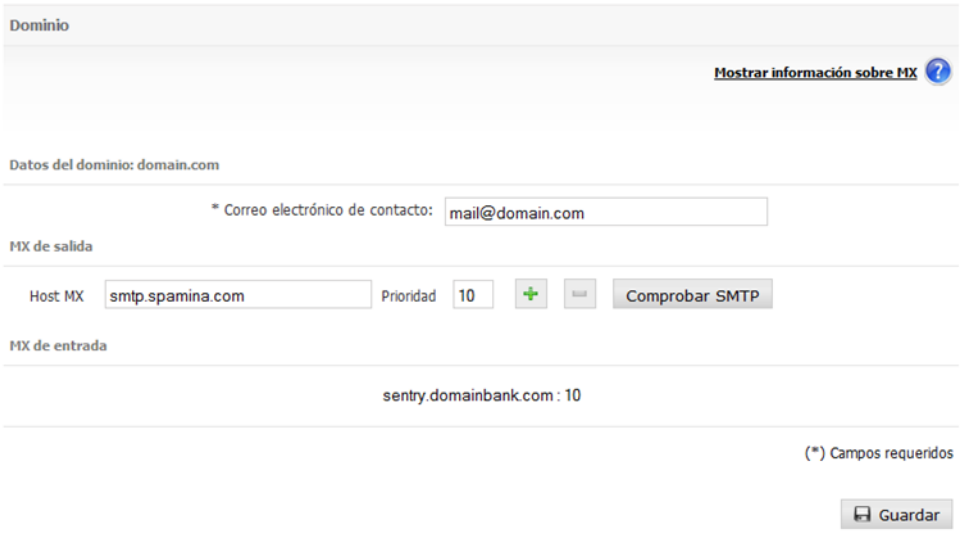
Estadísticas de correo saliente por día

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



2.3.3 Dominio

Se deben añadir tantos servidores, donde entregar el correo válido, como sea necesario. La entrega se intentará contra el servidor con el número de prioridad menor, probando con el siguiente si este fallara, y así sucesivamente.



HostMX:

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

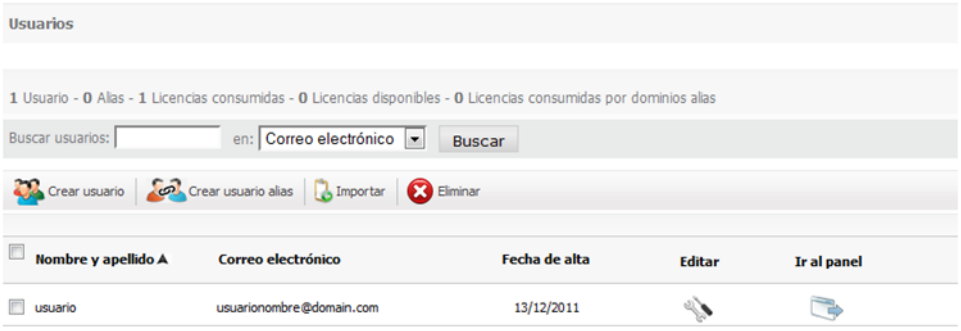
2001:0DB8::1428:57ab

2.3.4 Usuarios

Muestra el listado de usuarios y alias de usuarios, y permite crearlos de forma manual, importarlos desde un archivo (solo usuarios) o eliminarlos.

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.



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 (sin incluir @dominio), y la contraseña del usuario1, separados por coma.

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
Una contraseña se considera válida sólo si no es débil.

Cada línea del archivo debe representar un usuario.

Estos archivos pueden ser tanto .txt como .csv

Estructura del archivo:

Nombre y apellido, Correo, Contraseña

En el caso del correo "miusario@midominio.com" solo será necesario agregar el nombre de usuario (miusario).

Ejemplo:

Miguel Sanchez, msanchez, aras249g

Andrés López, alopez, 32kios5

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

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. Automáticamente se le enviara un mail al administrador de dominio notificando dicha importación.

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.

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*".

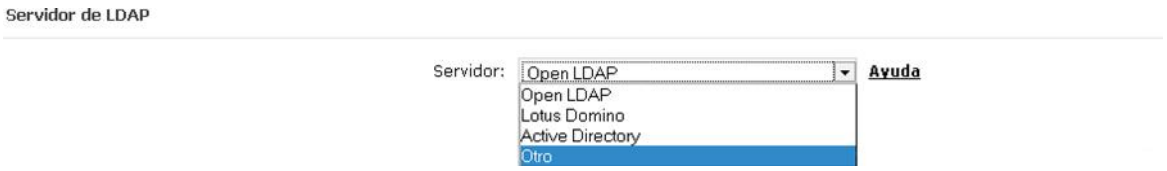
2.3.6.2 Alta Automática por SMTP call out o LDAP

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 **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 comprobación[2]. En caso de duda puede ponerse en contacto con nuestro departamento de soporte.

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.

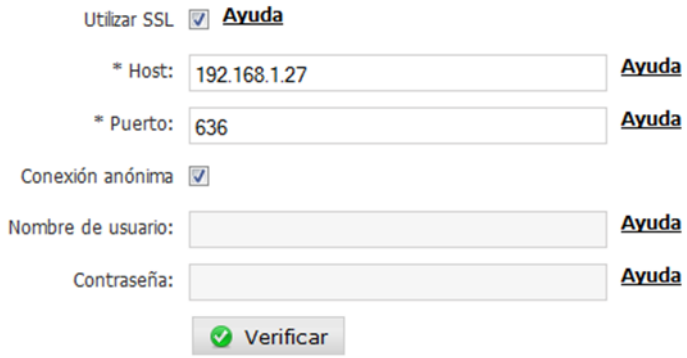
2.3.6.2.1.1 Servidor de LDAP



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

[2] El servidor SMTP debería responder afirmativamente sólo para aquellos usuarios válidos dentro del dominio.



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

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:

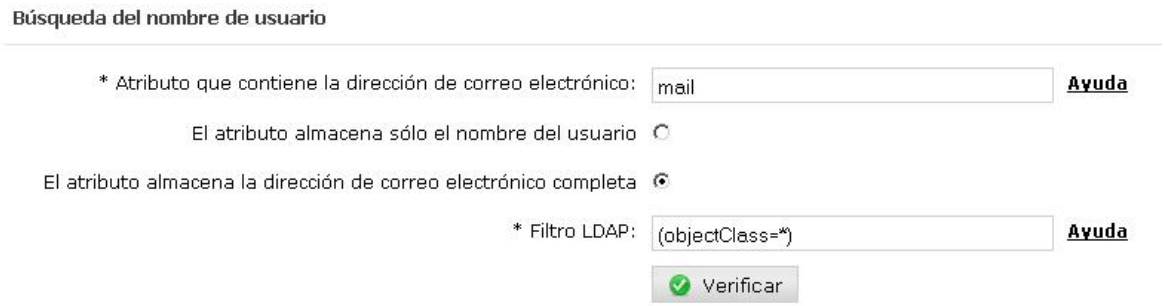
- Un carácter espacio « » (ASCII 32) o numeral «#» (ASCII 35) al principio.
- Un carácter espacio « » (ASCII 32) al final.
- Alguno de los caracteres: «,» (ASCII 44), «+» (ASCII 43), «"» (ASCII 34), «\» (ASCII 92), «<» (ASCII 60), «>» (ASCII 62) o «;» (ASCII 59)

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



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

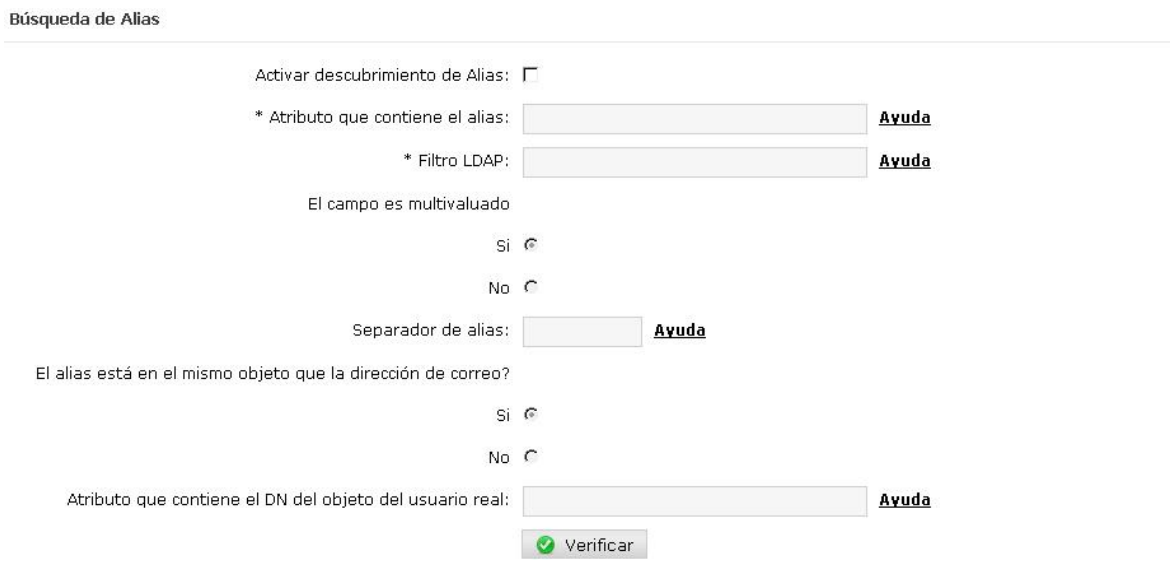
- Atributo que contiene la dirección de correo electrónico, por ejemplo: mail, rfc822Mailbox, entre otros.
- Deberá indicar si el atributo especificado anteriormente almacena sólo el nombre del usuario o la dirección de correo electrónico completa.
- Filtro LDAP: especifique aquí la clase más apropiada 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

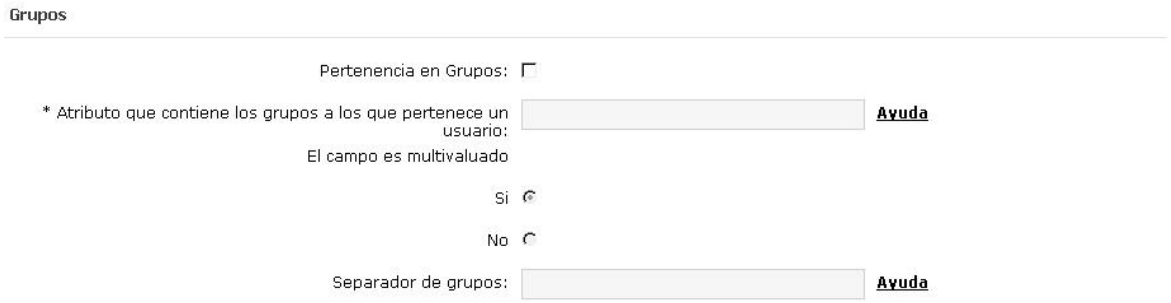
Si se activa el "*descubrimiento de alias*", deberá configurar los siguientes parámetros:

- 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 atributo[3].
- 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).

[3] 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: ?) @ ! # $ % &' * + - / = ^ _ ` ~ . { | }"



2.3.6.2.1.6 *Grupos*



Ésta 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.

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 su dominio.

Es posible distinguir dos tipos de administradores:

- Administrador principal

- Administrador secundario

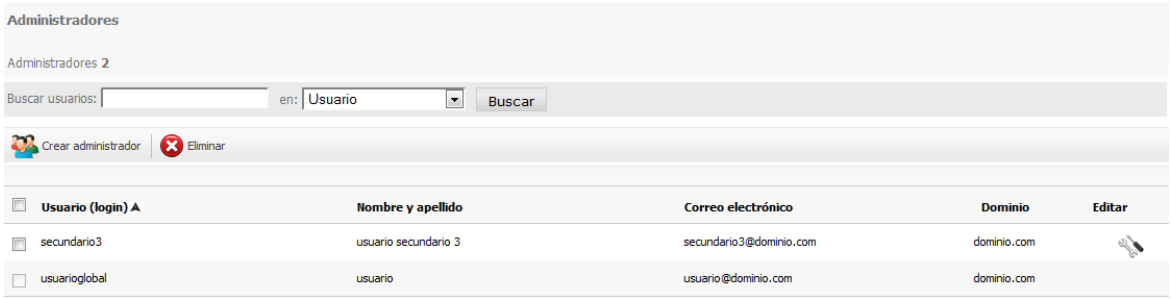
Sólo existe un único administrador principal del dominio.

Para crear un administrador se requiere la siguiente información:

- 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 la siguiente sección:

- Solapa "Configuración", opción de menú "Datos del administrador".

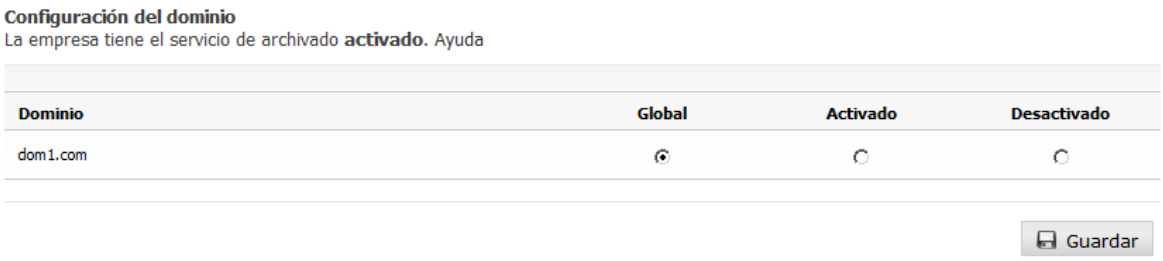


2.3.8 Archivo

2.3.8.1 Dominio

Teniendo contratado el servicio de archivado de correos, Ud. puede decidir el tipo de configuración que desea utilizar para su dominio.

La opciones de «activar» o «desactivar» el servicio de archivado aplican desde el momento en el que se establecen y no propagan esos cambios en cascada a todos los niveles inferiores.



2.3.8.2 Usuarios

Teniendo contratado el servicio de archivado de correos, Ud. puede decidir el tipo de configuración que desea utilizar para cada uno de sus usuarios.

Sólo podrá «activar» el servicio de archivado si la cantidad de licencias disponibles así lo permite.

Importante: Las cuentas de tipo alias utilizan la misma configuración definida para las cuentas reales a las que éstas hacen referencia. Como consecuencia, todas las cuentas de tipo alias asociadas a una cuenta determinada consumen licencias del servicio de archivado cuando éste es activado para tal cuenta.

2.3.8.3 Búsquedas

Podrá utilizar la interface de búsquedas para realizar consultas sobre los correos archivados.

La sección «Filtros» permite especificar, de forma opcional:

1. Usuario del que se desean obtener los correos. La lista de usuarios está disponible sólo después de haber seleccionado un dominio.

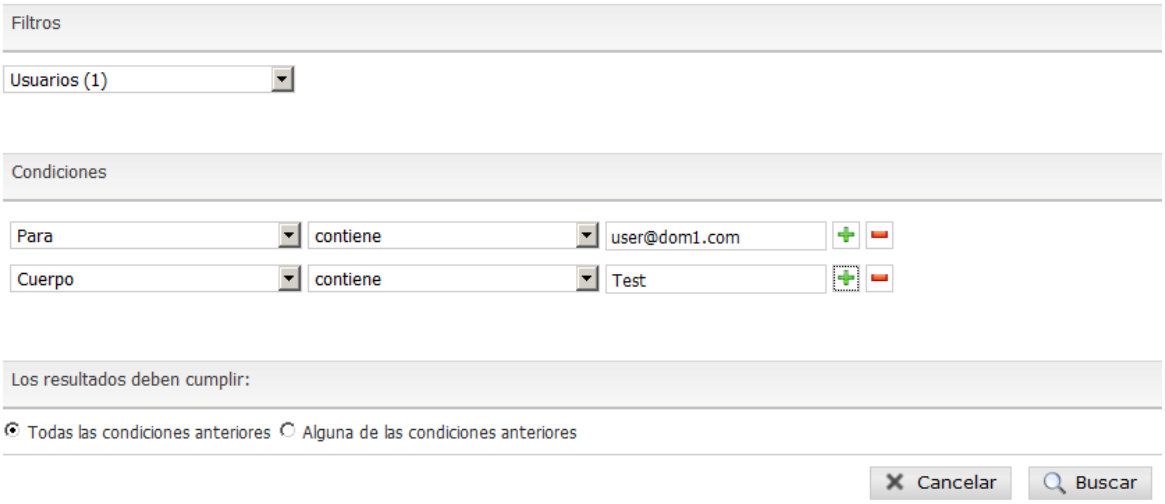
En la sección «Condiciones» podrá indicar todos los criterios de búsqueda que desea utilizar. Esos criterios pueden hacer uso de los campos y operaciones que se indican en la siguiente tabla:

Campo	Operación	Valor
Para	▪ Contiene ▪ No contiene	Todo o parte de una dirección de correo electrónico.
De	▪ Contiene ▪ No contiene	Todo o parte de una dirección de correo electrónico.
Cc	▪ Contiene ▪ No contiene	Todo o parte de una dirección de correo electrónico.
Asunto	▪ comienza con ▪ no comienza con ▪ termina con ▪ no termina con ▪ contiene ▪ no contiene ▪ es igual a ▪ es diferente de	Texto que desea localizar en el asunto de un correo.
Asunto	▪ contiene ▪ no contiene	Texto que desea localizar en el cuerpo de un correo.
Correos con fecha	▪ es igual a ▪ es diferente de ▪ es mayor o igual que ▪ es menor o igual que	Fecha en la que el correo ha sido enviado.

Finalmente, podrá especificar la operación lógica que desea aplicar para combinar las condiciones de su búsqueda:

- **Todas las condiciones anteriores**: Los resultados de la búsqueda serán aquellos que cumplan con todas las condiciones que ha indicado.

- **Alguna de las condiciones anteriores**: Los resultados de la búsqueda serán aquellos que cumplan con cualquiera de las condiciones que ha indicado.



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 dominio no se les aplicará el filtrado de contenido y filtros de conexión pero si los filtros de antivirus y motor de relgas; asimismo estas IPs tienen menor prioridad que aquellas definidas en las listas blanca y negra globales.

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 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 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 IPs.

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 Dominio

Desde aquí podrá gestionar la activación o desactivación de los filtros antivirus disponibles para su dominio, 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.

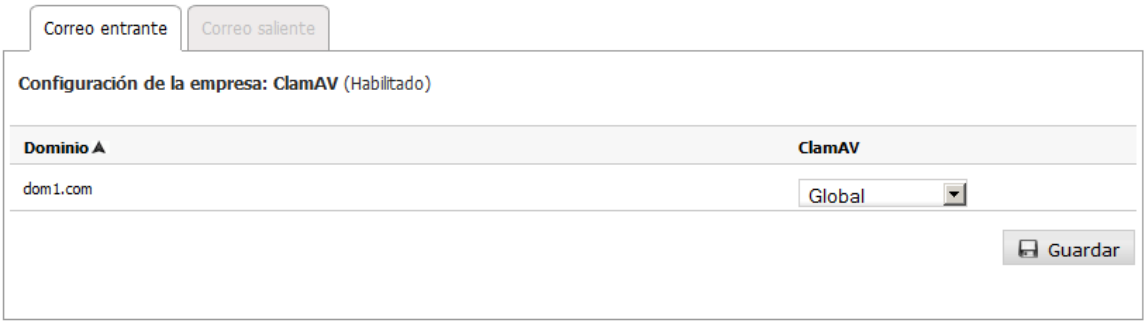
Para aplicar el filtrado antivirus al correo saliente **es necesario** que esos correos se envíen a través de la plataforma identificándose con las credenciales de acceso que utiliza para iniciar sesión en la consola de gestión:

1. Habilitar el filtrado antivirus para el correo saliente.

2. Indicar a su SMTP que utilice como SMARTHOST al servidor indicado para su plataforma de servicio.

3. 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 antivirus para el correo saliente.



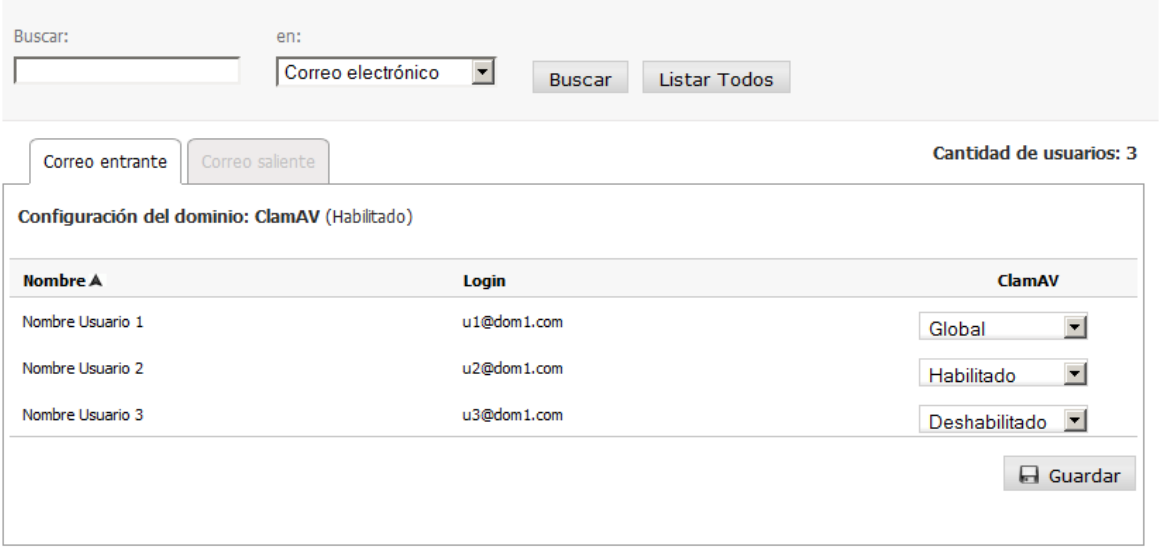
2.4.2.2 Usuarios

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.



2.4.3 Anti Spam

2.4.3.1 Dominio

Desde aquí podrá gestionar la activación o desactivación del filtrado antispam para su dominio, tanto para los correos entrantes como para los salientes.

Por defecto el dominio utiliza la configuración de filtrado antispam definida por la empresa.

Si desactiva el filtrado antispam 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 antispam 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 antispam para el correo saliente.

5. Indicar a su SMTP que utilice como SMARTHOST al servidor indicado para su plataforma de servicio.

6. 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 antispam para el correo saliente.

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 tenia 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 antispam para sus usuarios, tanto para los correos entrantes como para los salientes.

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

Si desactiva el filtrado antispam 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.

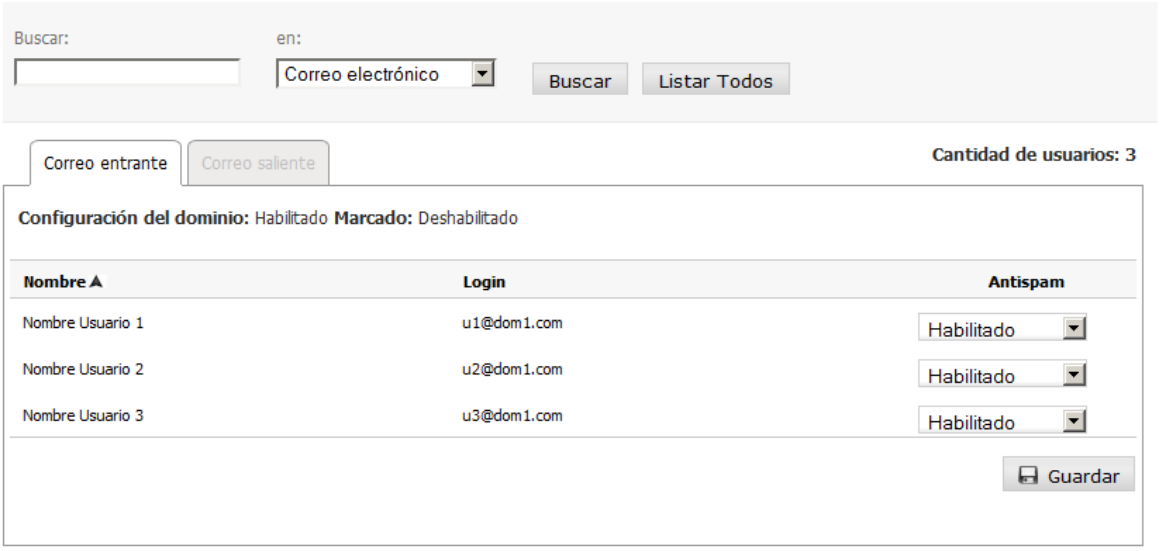
Para aplicar el filtrado antispam al correo saliente **es necesario** que esos correos se envíen a través de la plataforma identificándose con las credenciales de acceso que utiliza para iniciar sesión en la consola de gestión:

1. Habilitar la opción filtrado antispam para el correo saliente.

2. Indicar a su SMTP que utilice como SMARTHOST al servidor indicado para su plataforma de servicio.

3. 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 antispam para el correo saliente.



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.

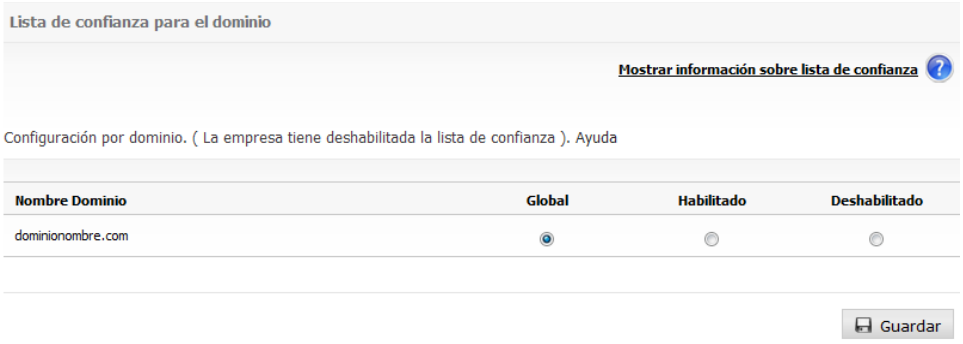
2.4.4 Listas de confianza

2.4.4.1 Listas de confianza para el dominio

Las Listas de Confianza son unas listas blancas automáticas y personalizadas para el 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 el dominio.



2.4.4.2 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.

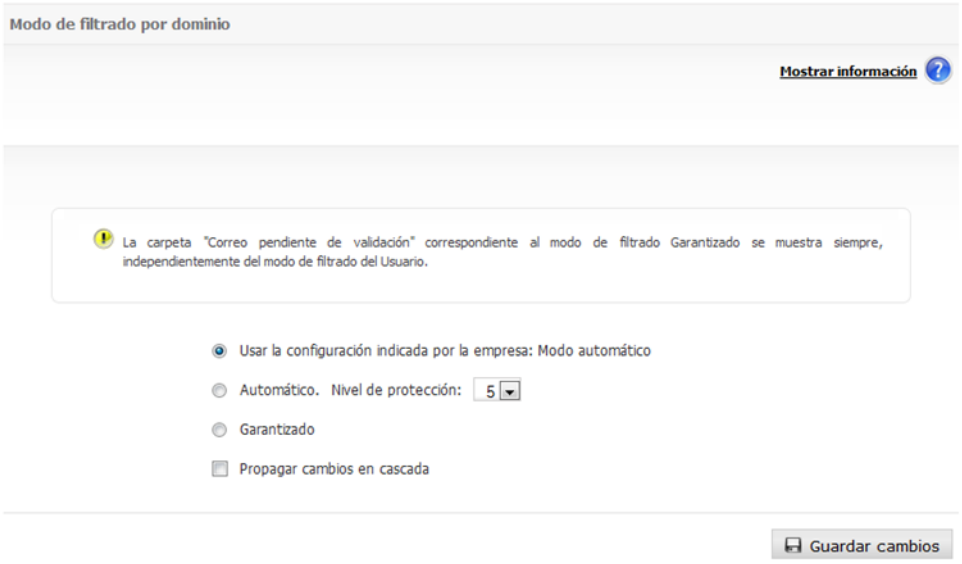
Desde este panel se habilitan/deshabilitan las Listas de Confianza para los usuarios individuales.

2.4.5 Modo de filtrado

2.4.5.1 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:



La opción de "Propagar cambios en cascada", propaga la configuración del dominio a todos los usuarios existentes en el mismo.

2.4.5.1.1 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.

2.4.5.1.2 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.

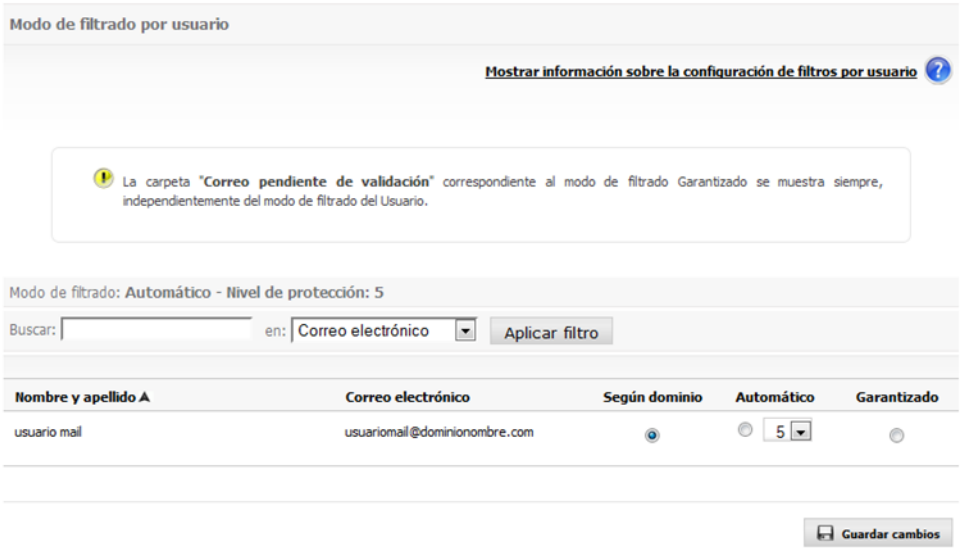
En el caso de que el remitente no se validara, el destinatario puede hacerlo manualmente desde su Panel de Control, desde el Notificador o desde el Informe de correo bloqueado.

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

2.4.5.2 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.



2.4.6 Motor de reglas

2.4.6.1 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".

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

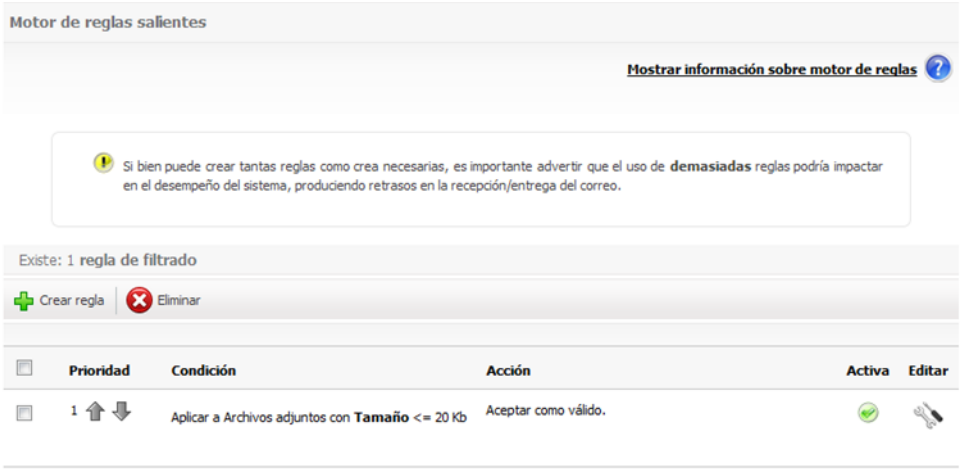
2.4.6.2 Motor de reglas salientes

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".



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

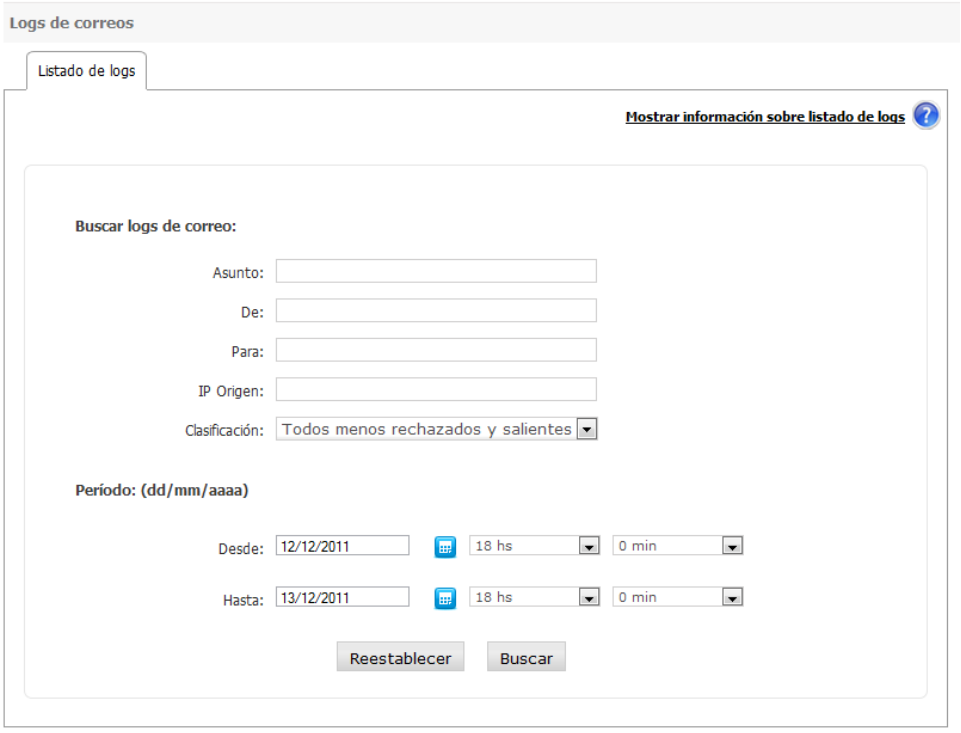
2.4.7 Logs de correos

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.

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

- Todos menos rechazados y 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



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

Los posibles estados[4] 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

[4] 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 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.
- Reentregar: Re entrega el correo al cual se hace referencia.

Esta acción estará disponible en el caso en que la empresa al comprar Email Protection eligiera la opción de poder ver correos desde Log de Correos:

- Ver Correo: Permite visualizar el correo electrónico 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.

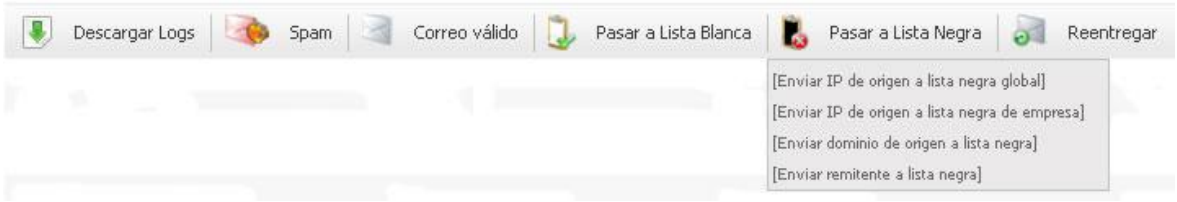
No todas las acciones son aplicables a todos los tipos de correos:

- 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



2.4.8 Validación NDR

Es posible desde el Panel de Administrador de dominio configurar esta validación tanto para el dominio como para sus usuarios. Estas opciones se encuentran en la pestaña "Filtrado" en las secciones "Validación NDR por Dominios" y "Validación NDR por Usuarios" respectivamente.

La 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 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.

2.4.8.1 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 su dominio.

Por defecto, este tipo de validación adopta la configuración indicada por su empresa. Puede establecer una configuración propia; para activar esta validación 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 (esta 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.

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.

2.4.8.2 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 (esta 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.

2.4.9 Detección de suplantación de identidad

Es posible desde el Panel de Administrador de dominio configurar detección de suplantación de identidad tanto a nivel de dominio 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 o dominio).

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

2.4.9.1 Detección de suplantación de identidad por dominio

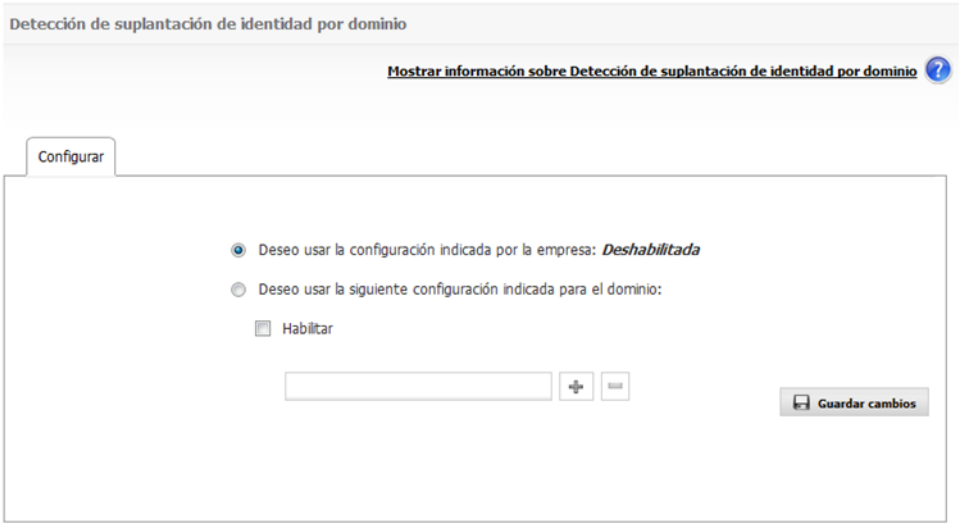
Por defecto, esta prueba se encuentra deshabilitada.

- **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 Firewal 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.

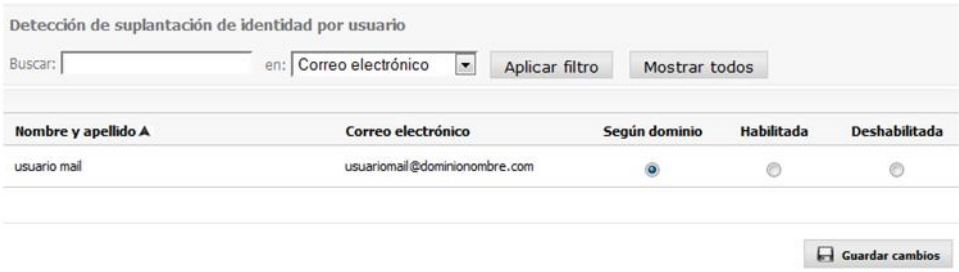
Si se deshabilita la prueba, o si se desea usar la configuración indicada por la empresa para un dominio, no se podrá definir Listas de direcciones IP habilitadas para el envío.

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**.



2.4.9.2 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.



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:

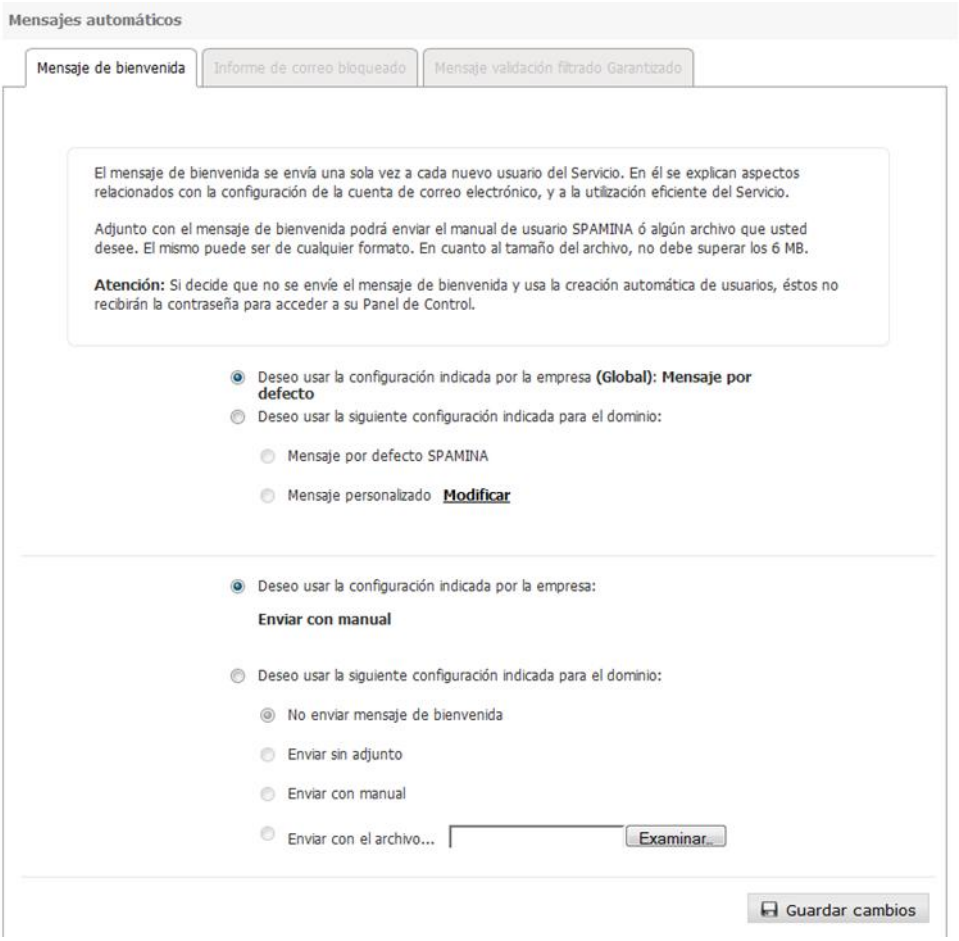
2.5.1.1 Mensaje de bienvenida

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: La opción de personalización debe ser habilitada por su administrador de empresas. 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.



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 previsualizarlo 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.

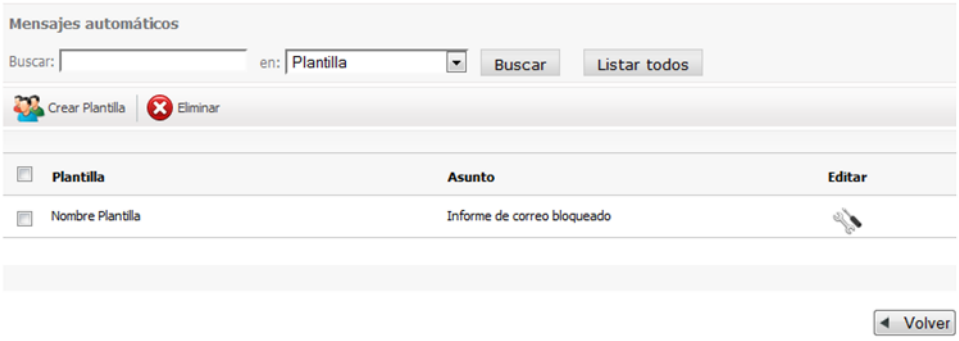
Puede optar por usar la configuración indicada por la empresa, enviar el informe Email Protection por defecto o personalizar el mensaje mediante la implementación de plantillas.

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.

Atención: la opción de personalización debe ser habilitada por su administrador de empresas.

Propagar en cascada: Aplica la configuración a todos los usuarios.

2.5.1.2.1 Ver plantillas

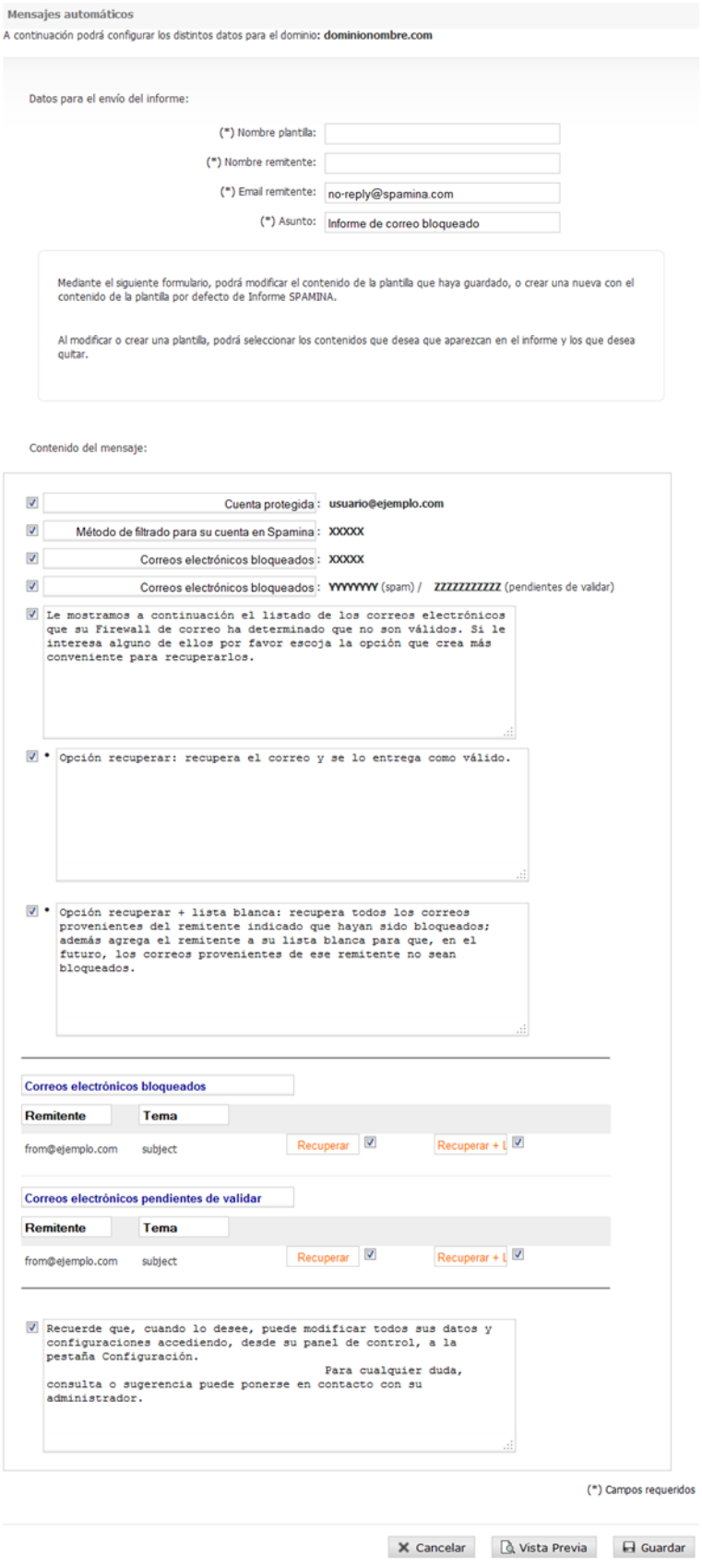


Aparecerá una nueva interfaz donde los botones que estarán disponibles son:

- ***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.

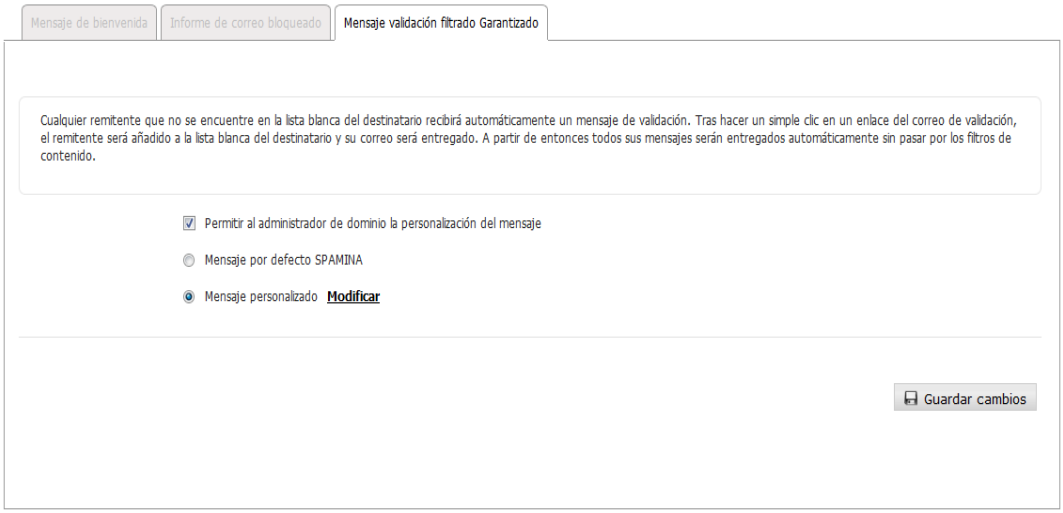
- Puede pre visualizar el mensaje antes de ser guardado.
- ***Eliminar***: elimina el mensaje, asunto, remitente y la plantilla. La relación es 1 a 1 y son obligatorios todos los campos.
- ***Formulario de Búsqueda***: se puede buscar una plantilla por nombre de plantilla y asunto.


Mensajes automáticos
A continuación podrá configurar los distintos datos para el dominio: dominionombre.com
Datos para el envío del informe:
(*) Nombre plantilla:
(*) Nombre remitente:
(*) Email remitente: no-reply@spamina.com
(*) Asunto: Informe de correo bloqueado
Mediante el siguiente formulario, podrá modificar el contenido de la plantilla que haya guardado, o crear una nueva con el contenido de la plantilla por defecto de Informe SPAMINA.
Al modificar o crear una plantilla, podrá seleccionar los contenidos que desea que aparezcan en el informe y los que desea quitar.
Contenido del mensaje:
Cuenta protegida : usuario@ejemplo.com
Método de filtrado para su cuenta en Spamina : XXXXX
Correos electrónicos bloqueados : XXXXX
Correos electrónicos bloqueados : YYYYYYY (spam) / ZZZZZZZZZZ (pendientes de validar)
Le mostramos a continuación el listado de los correos electrónicos que su Firewall de correo ha determinado que no son válidos. Si le interesa alguno de ellos por favor escoja la opción que crea más conveniente para recuperarlos.
Opción recuperar: recupera el correo y se lo entrega como válido.
Opción recuperar + lista blanca: recupera todos los correos provenientes del remitente indicado que hayan sido bloqueados; además agrega el remitente a su lista blanca para que, en el futuro, los correos provenientes de ese remitente no sean bloqueados.
Correos electrónicos bloqueados
Remitente
Tema
from@ejemplo.com
subject
Recuperar
Recuperar + l
Correos electrónicos pendientes de validar
Remitente
Tema
from@ejemplo.com
subject
Recuperar
Recuperar + l
Recuerde que, cuando lo desee, puede modificar todos sus datos y configuraciones accediendo, desde su panel de control, a la pestaña Configuración.
Para cualquier duda, consulta o sugerencia puede ponerse en contacto con su administrador.
(*) Campos requeridos
Cancelar
Vista Previa
Guardar

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 envió de cada informe y configurar sus destinatarios.

El informe de actividad contiene información sobre su:

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

Por defecto el envió de informe de actividad estará habilitado para el dominio.

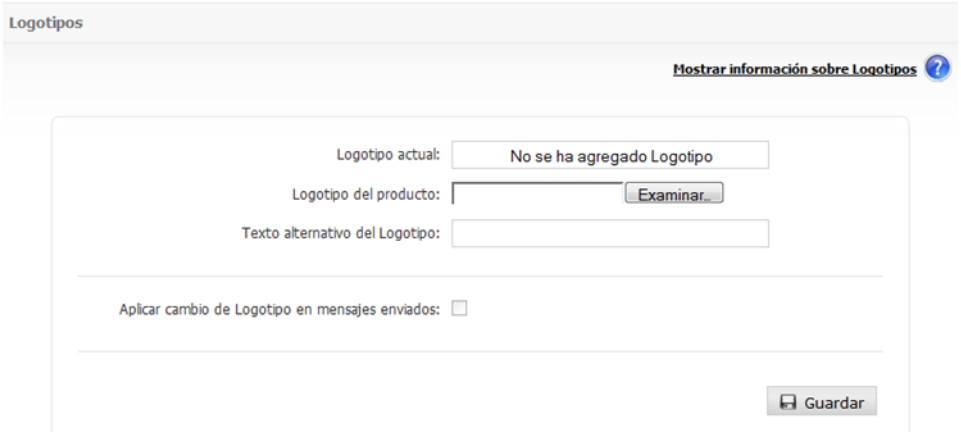
La configuración de destinatarios le permitirá definir los destinatarios del informe.

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

2.5.3 Logotipos

Aquí podrá gestionar el logotipo que utilizarán los mensajes enviados.

El logotipo 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 ingresar un texto alternativo para el mismo.

El nuevo logotipo será aplicado a los mensajes automáticos, al dejar seleccionada la opción "Aplicar cambio de logotipo en mensajes enviados".

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".

Por defecto aparecerá el que tiene el administrador de empresa.

La opción de "Propagar cambios en cascada", propaga la configuración de idioma del dominio a todos los usuarios existentes en el mismo.

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

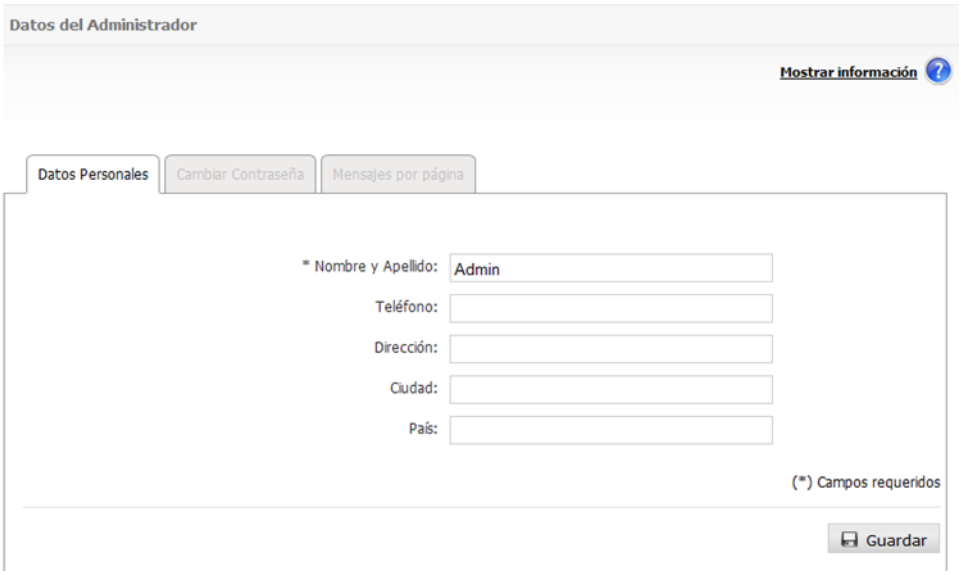
2.6 Configuración

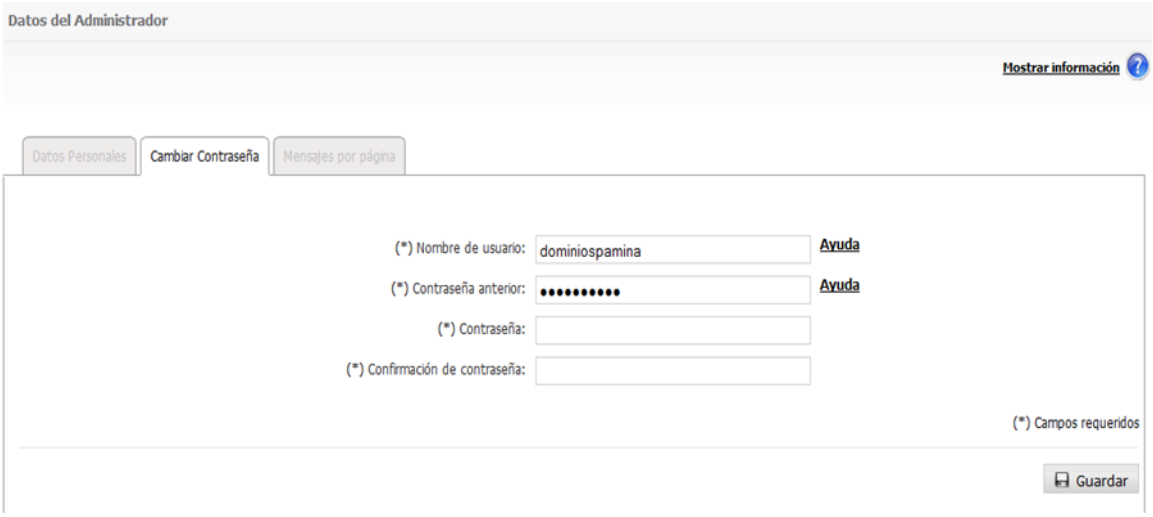
En esta sección podrá configurar aspectos del sistema tales como: datos del Administrador; qué hacer frente a ciertos mensajes pertenecientes a la clasificación de listas/mensajes de servidor/avisos de virus; o qué periodicidad emplear para los mensajes que puede generar Email Protection de forma automática,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

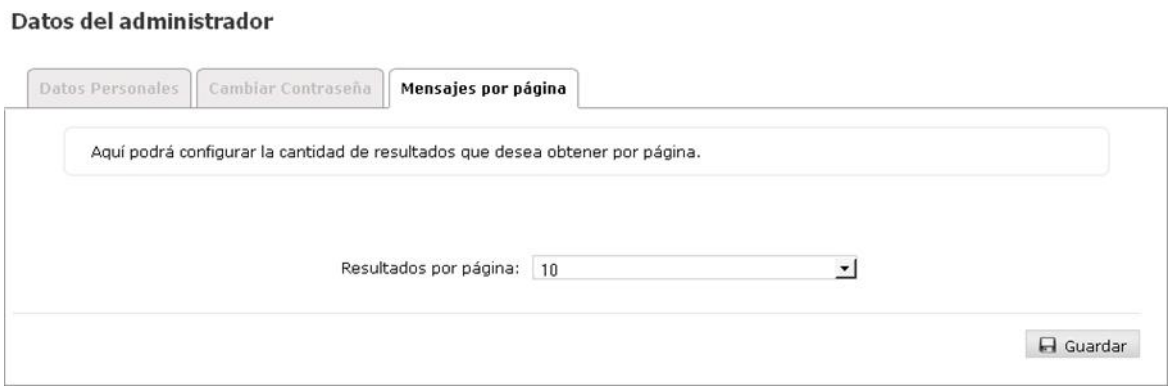
2.6.1 Datos del Administrador

Se deben introducir los datos referentes a información del administrador.

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







2.6.2 Acceso a panel para 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.

2.6.2.1 Configuración por dominio

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

Las opciones de configuración disponibles son:

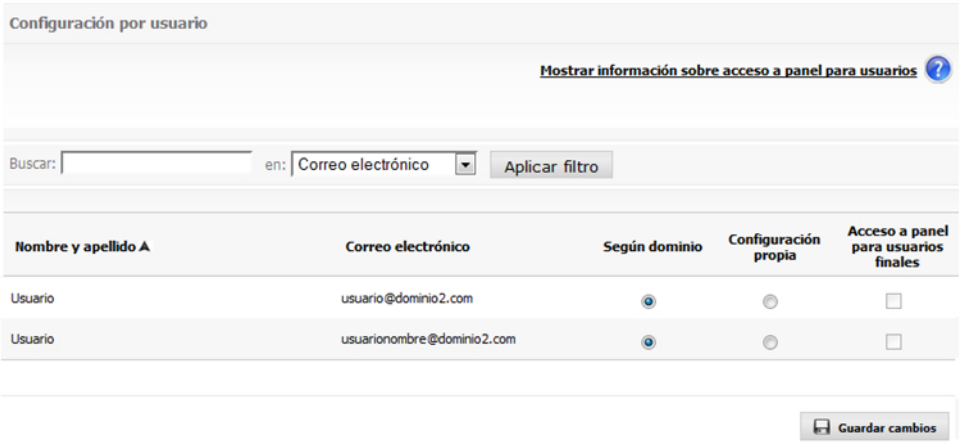
- **Global:** Se utiliza la configuración definida por el nivel superior.
- **Propia:** Permite aplicar una configuración diferente a la especificada por el nivel superior.
- **Acceso a panel para usuarios finales:** Indica que los usuarios del dominio tendrán permitido acceder a sus paneles de usuario.
- **Propagar en cascada:** Aplica la configuración a todos los usuarios del dominio.

2.6.2.2 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.



2.6.3 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.

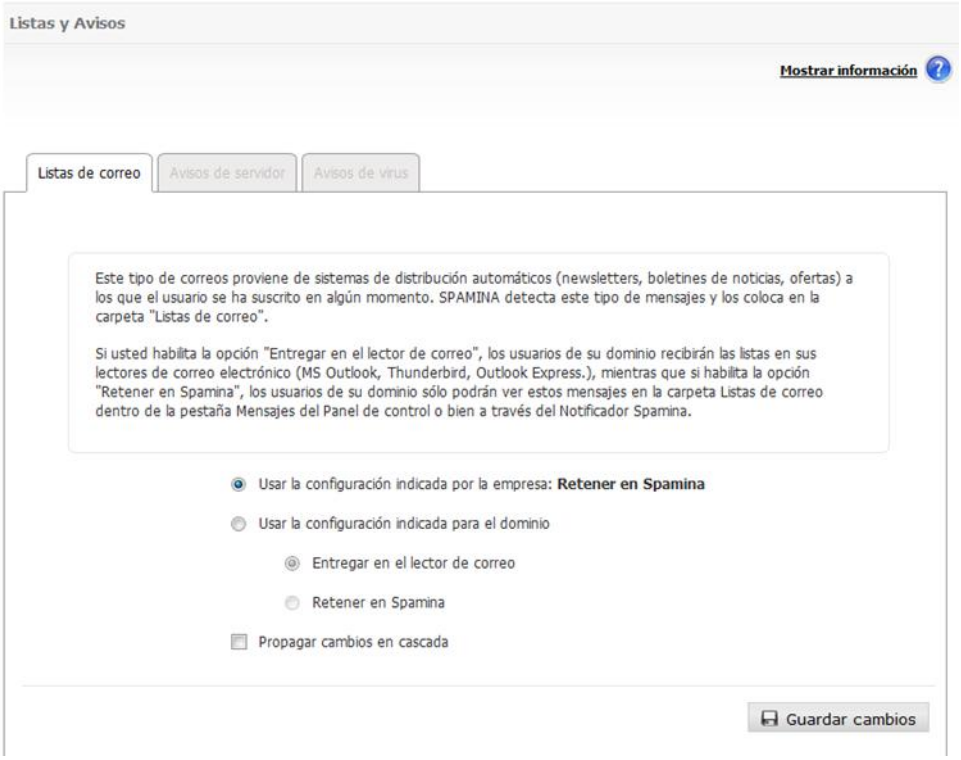
Se permite decidir, tanto para el servicio completo como para los dominios específicos, si dichos correos se entregarán al usuario final o si se guardarán en carpetas separadas para su consulta puntual si se cree necesario.

2.6.3.1 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 en Email Protection*", 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.

La opción de "Propagar cambios en cascada", propaga la configuración del dominio a todos los usuarios existentes en el mismo.

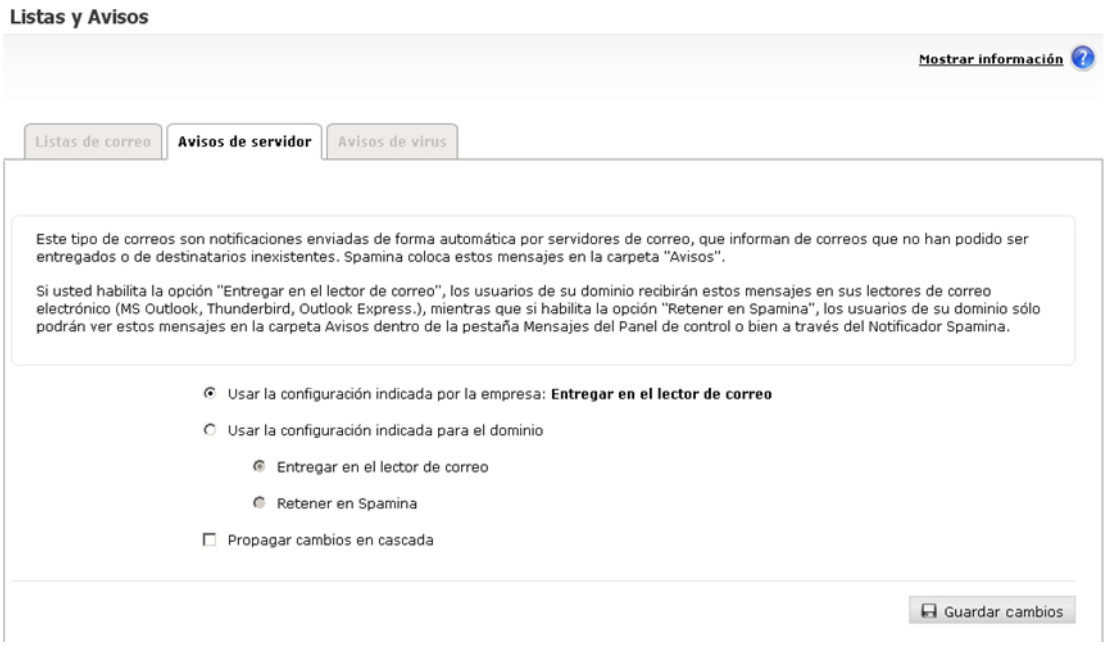


2.6.3.2 Avisos de servidor

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.

La opción de "Propagar cambios en cascada", propaga la configuración del dominio a todos los usuarios existentes en el mismo.



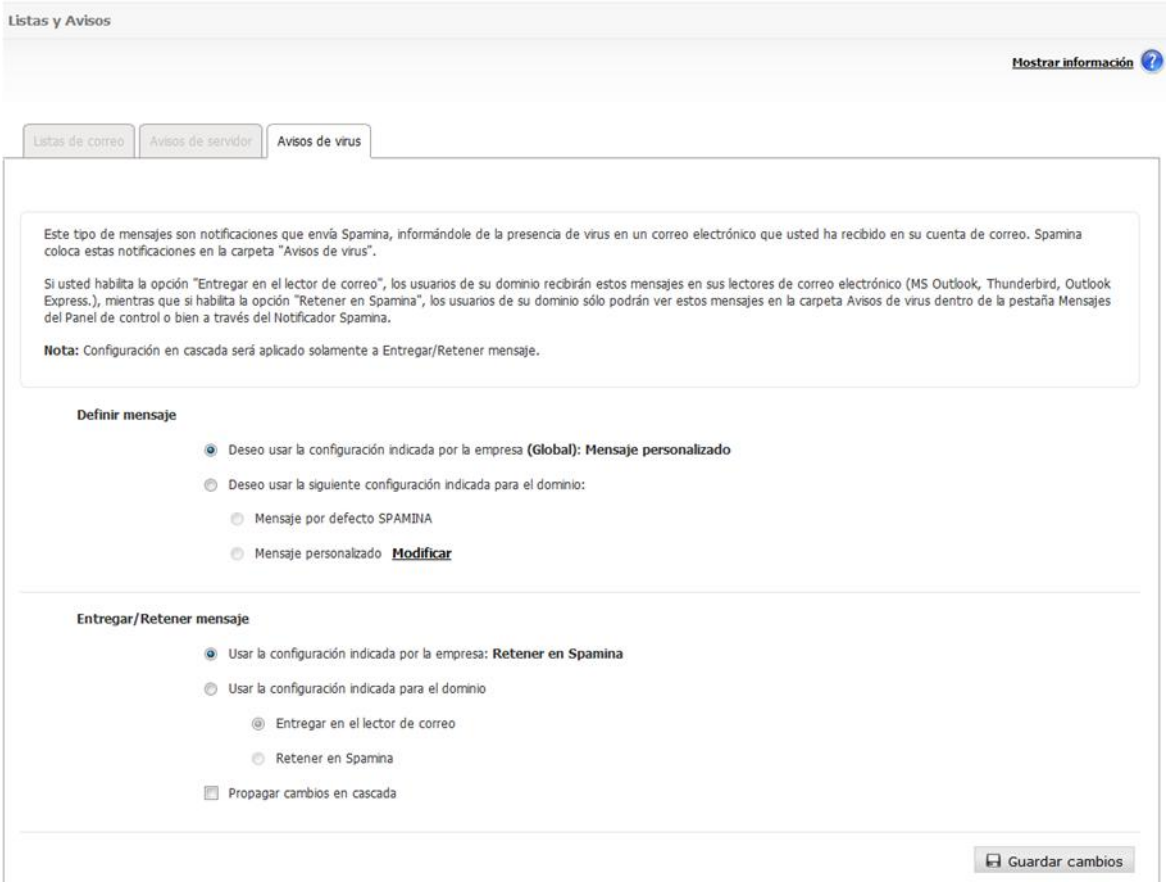
2.6.3.3 Avisos de virus

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.

La opción de "Propagar cambios en cascada", propaga la configuración del dominio a todos los usuarios existentes en el mismo.

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



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

2.6.4 Disclaimers

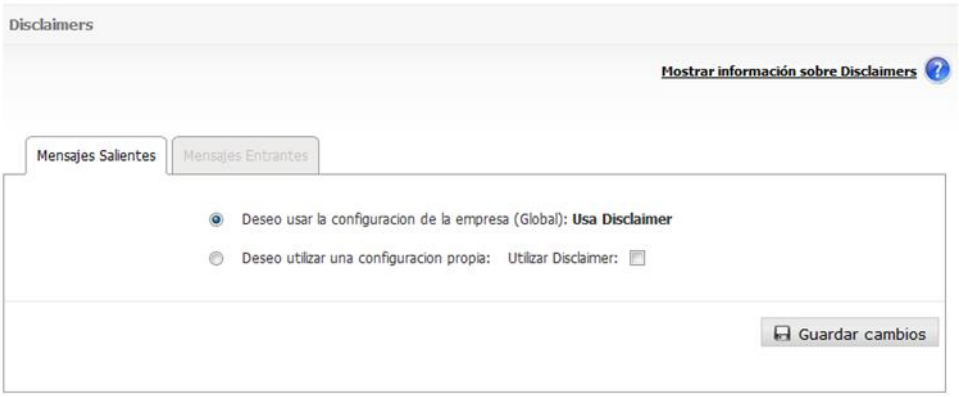
En esta sección, podrá establecer un tipo texto (disclaimer) que será colocado automáticamente al final de un correo, tanto entrante como saliente; a su vez, podrá establecer una configuración diferente para cada uno de ellos. Para que estos disclaimers apliquen a correo saliente, deberá tener activo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



Es importante mencionar que el uso 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. Email Protection no se responsabiliza por las implicaciones legales de los efectos producidos por estas modificaciones.

2.6.5 Sincronización

Esta sección describe cómo configurar la sincronización de usuarios. Esta funcionalidad permite mantener consistencia 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 con el administrador. Todos los usuarios detectados son modificados o borrados según corresponda.
    b. Manual: Permite al administrador decidir qué 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, sólo se envía un único informe con los resultados de la sincronización.

La configuración global permite al administrador de empresa determinar que los dominios tendrán la misma configuración que la empresa.

La configuración propia permite definir a cada dominio una configuración particular.

2.6.6 Informes

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

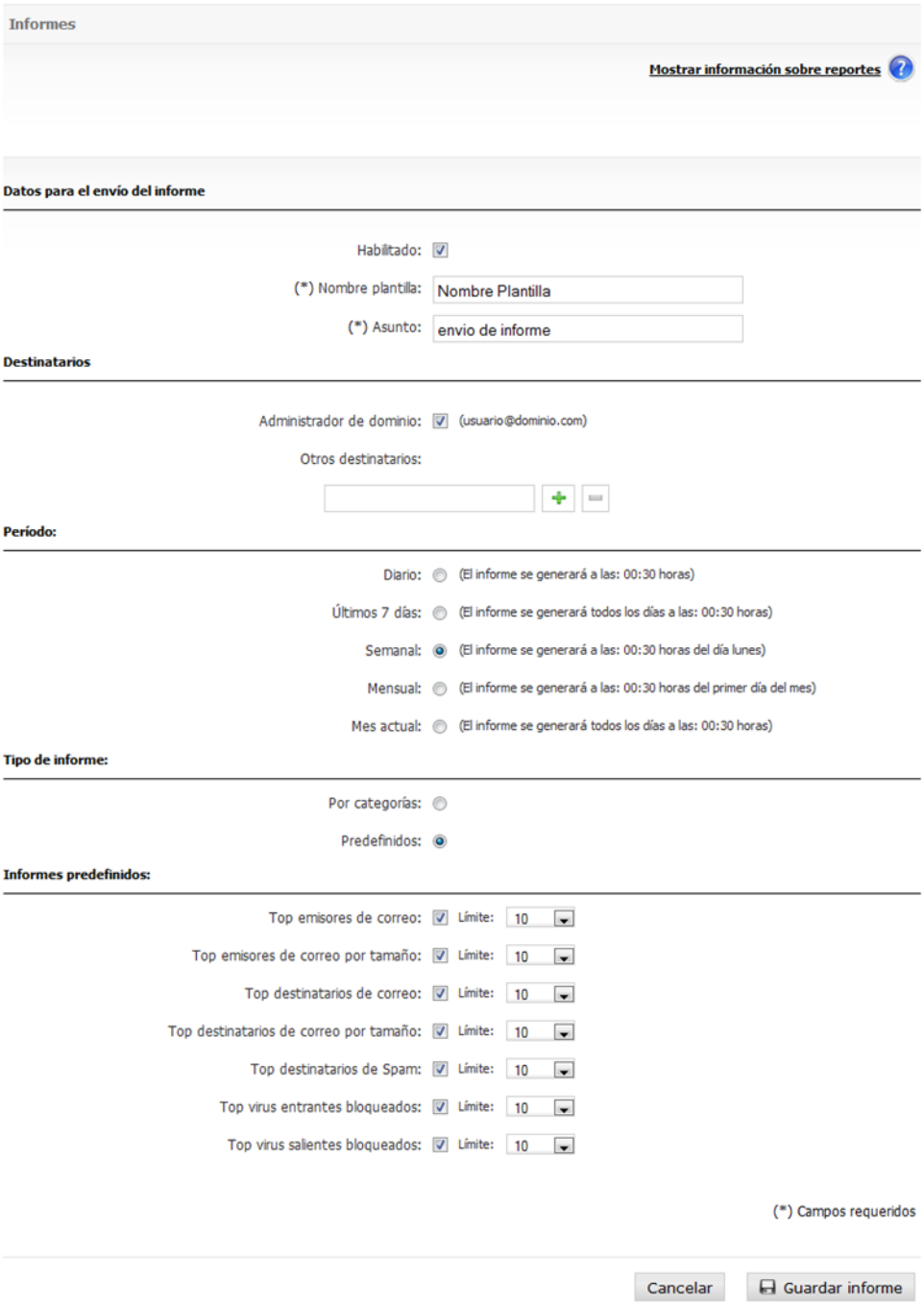
Los reportes predefinidos disponibles son:

- 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 volúmen 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 volúmen 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



2.6.7 Zona horaria

Esta configuración permite indicar la zona horaria predeterminada para su dominio y 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, el dominio utilizará la zona horaria definida por la empresa.

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 para su dominio se aplica a la zona horaria de los usuarios que no tengan un valor de zona horaria ya seleccionado.

3 Funciones adicionales

3.1 Notificador Panda

El Notificador de correo es una utilidad[5] 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.

[5] 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.