|  |
| --- |
| CONSALUD S.A. |
| Reporte Herramienta “mailcleaner” |
|  |
|  |
| **Francisco Abarca** |
| **17/01/2019** |

|  |
| --- |
| Reporte descriptivo sobre el funcionamiento, estado y posibles configuraciones de la herramienta “mailcleaner”, la cual monitorea el estado del servicio de correo y su seguridad. |

Contenido

[Sistema Base 4](#_Toc535566988)

[Ajuste de Redes 4](#_Toc535566989)

[Ajustes de DNS 4](#_Toc535566990)

[Localización 5](#_Toc535566991)

[Hora y Fecha 5](#_Toc535566992)

[Proxies 6](#_Toc535566993)

[Registro 6](#_Toc535566994)

[Ajustes Generales 7](#_Toc535566995)

[Predeterminados 7](#_Toc535566996)

[Compañía 7](#_Toc535566997)

[Cuarentenas 8](#_Toc535566998)

[Tareas Periódicas 8](#_Toc535566999)

[Logging del Sistema 9](#_Toc535567000)

[Archivado 9](#_Toc535567001)

[Dominios 10](#_Toc535567002)

[SMTP (Simple Mail Transfer Protocol) 11](#_Toc535567003)

[SMTP Checks 11](#_Toc535567004)

[Control de Conexiones 12](#_Toc535567005)

[Control de Recursos 13](#_Toc535567006)

[TLS (Transport Security Layer)/SSL (Secure Socket Layer) 14](#_Toc535567007)

[Greylisting (Lista gris) 15](#_Toc535567008)

[DKIM (DomainKeys Identified Mail) 15](#_Toc535567009)

[Anti-Spam 16](#_Toc535567010)

[Ajustes Globales 16](#_Toc535567011)

[Módulos Anti-Spam 17](#_Toc535567012)

[TrustedSources 17](#_Toc535567013)

[Spamc 18](#_Toc535567014)

[PreRBLs 19](#_Toc535567015)

[NiceBayes 20](#_Toc535567016)

[UriRBLs 20](#_Toc535567017)

[ClamSpam 21](#_Toc535567018)

[Protección de Contenido 22](#_Toc535567019)

[Ajustes Globales 22](#_Toc535567020)

[Anti-Virus 22](#_Toc535567021)

[Control HTML 23](#_Toc535567022)

[Control en el formato de los Mensajes 23](#_Toc535567023)

[Nombre de Archivos Adjuntos 24](#_Toc535567024)

[Tipo de Archivos Adjuntos 24](#_Toc535567025)

[Accesos 25](#_Toc535567026)

[Observaciones 26](#_Toc535567027)

[Remitente no Verificado 26](#_Toc535567028)

[No hay una búsqueda de DNS inversa 26](#_Toc535567029)

[SSL/TLS no configurado 27](#_Toc535567030)

[DKIM no configurado 27](#_Toc535567031)

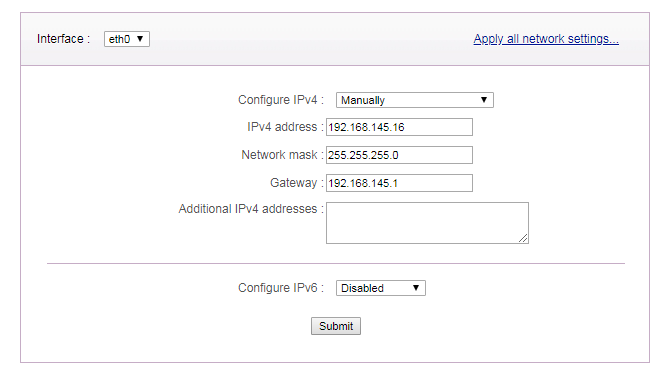
[Comportamiento extraño del spool 28](#_Toc535567032)

Configuración

# Sistema Base

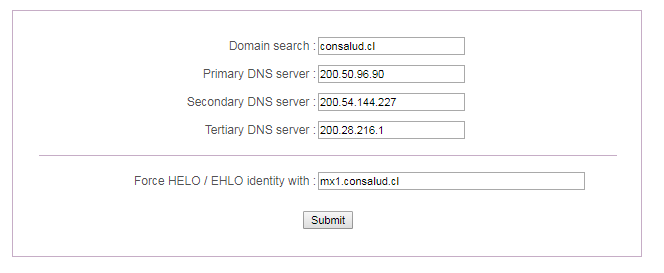
## Ajuste de Redes

Menú en el cual, mediante la selección de una interfaz (red o inalámbrica), es posible configurar su IPv4, tanto manual o seleccionar su configuración automática, en caso de configuración manual tenemos la dirección, la máscara de red, la puerta de enlace (gateway) y direcciones adicionales en caso de ser necesario. Además, tenemos la posibilidad de configurar el IPv6.



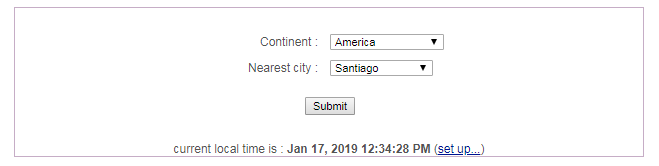
## Ajustes de DNS

En este menú, tenemos la búsqueda del DNS (registro A), y la definición del DNS primario, secundario y terciario. La identidad con la cual se identifica puede ser forzada e ingresada manualmente.



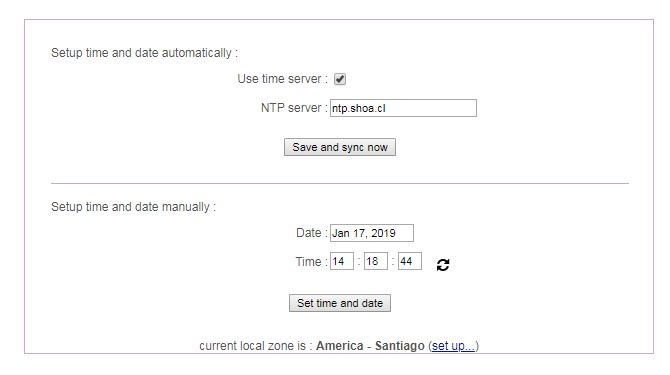
## Localización

Acá configuramos la zona del sistema con dos filtros, Continente y ciudad más cercana.



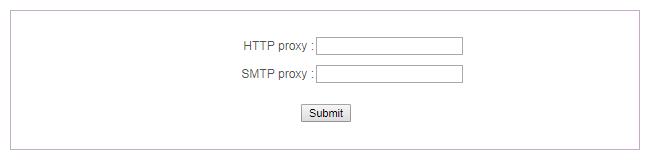
## Hora y Fecha

Sección en la cual podemos proveer un servidor NTP del cual obtendremos nuestros datos horarios, o bien hacerlo de manera manual.



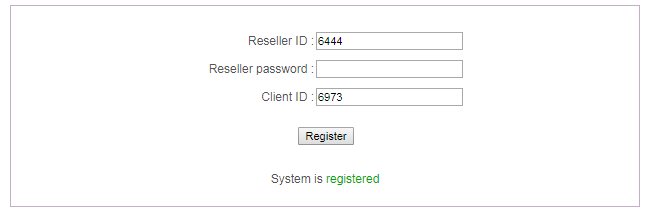
## Proxies

Esta pestaña posibilita la opción de configurar un proxy, tanto para el protocolo HTTP como para el protocolo de los mensajes (SMTP).



## Registro

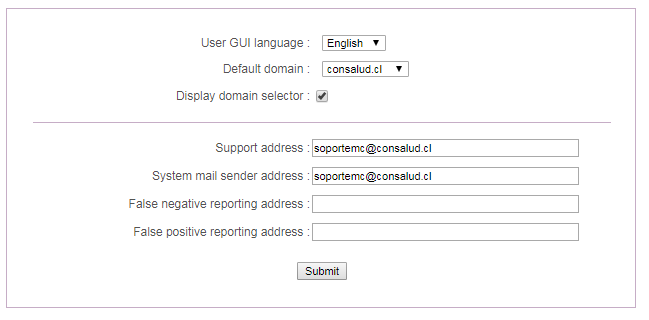
Sección en donde podemos verificar el estado de registro del sistema, y en caso de vencimiento o fin del término de la licencia renovarla.



# Ajustes Generales

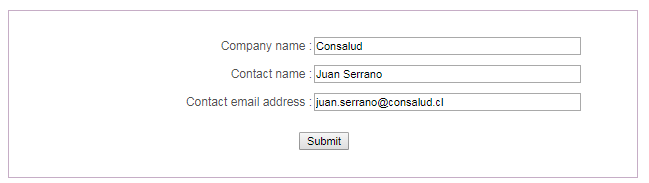
## Predeterminados

En esta sección podemos elegir opciones tales como, el idioma de la interfaz, el dominio por defecto, la dirección de correo para el soporte como el sistema, además de las direcciones para la notificación de falsos positivos o negativos.



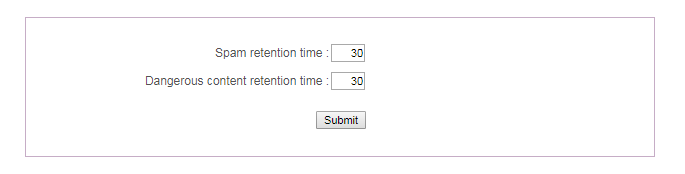
## Compañía

Lugar en donde van las configuraciones sobre el nombre de la compañía, nombre de contacto y dirección de correo del contacto.



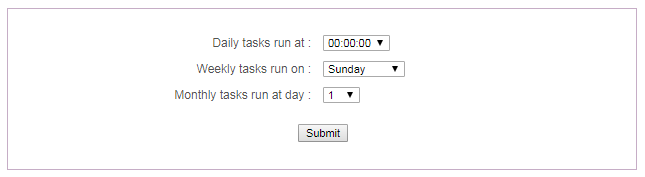
## Cuarentenas

Acá están las opciones de tiempo que mantendrán la existencia de archivos en cuarentena para su posterior eliminación y/o examinación. Hay dos tipos de retenciones que se pueden configurar, retención de spam (en días), y tiempo de retención de contenido peligroso, en días también.



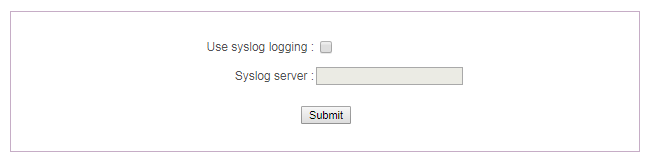
## Tareas Periódicas

En este menú están las configuraciones para las tareas programadas, las cuales se dividen en diarias, semanales y mensuales. Para cada una hay que elegir una hora, un día de la semana y un día del mes respectivamente.



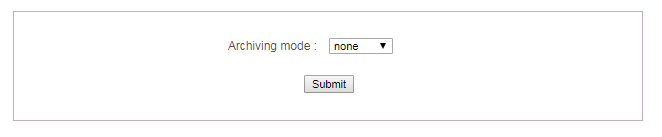
## Logging del Sistema

En esta pestaña podemos habilitar un log del sistema (syslog) con su respectivo server para recopilar información.



## Archivado

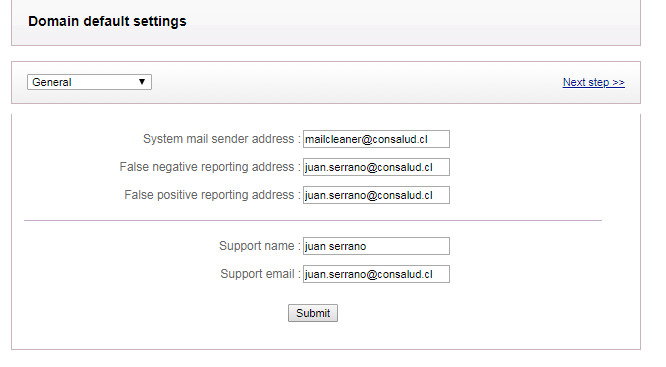
Tenemos la opción de habilitar un archivado externo el cual es configurable al seleccionarlo en donde debemos proveer un servidor objetivo.

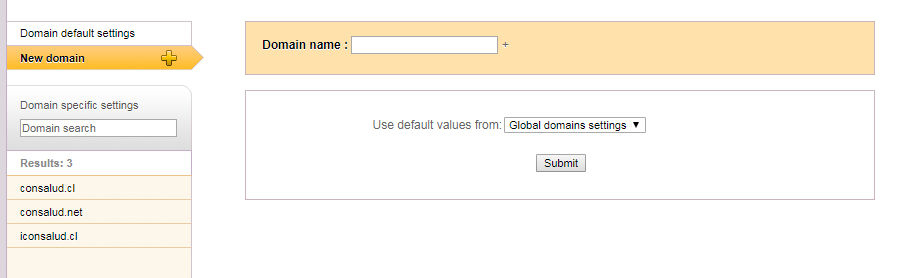


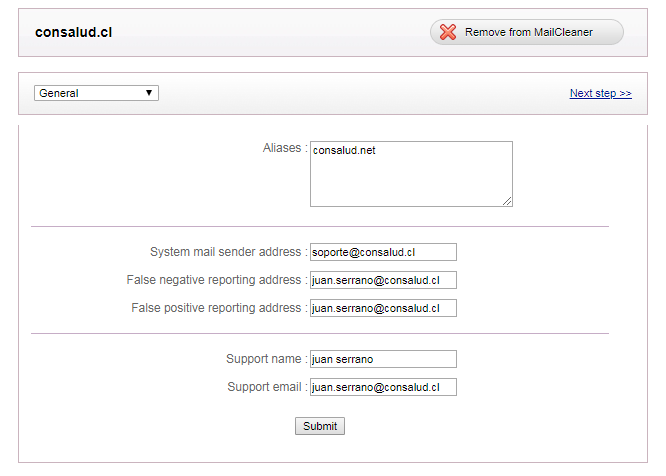
# Dominios

Acá podemos configurar las opciones globales de nuestros dominios, como los correos del administrador, en caso de falla o falsos negativos/positivos y el encargado de soporte.

En esta ventana también podemos revisar los dominios ya configurados y añadir nuevos, ya sean con las variables definidas anteriormente (ajustes de dominio globales) o alguno en particular de los que ya tenemos.



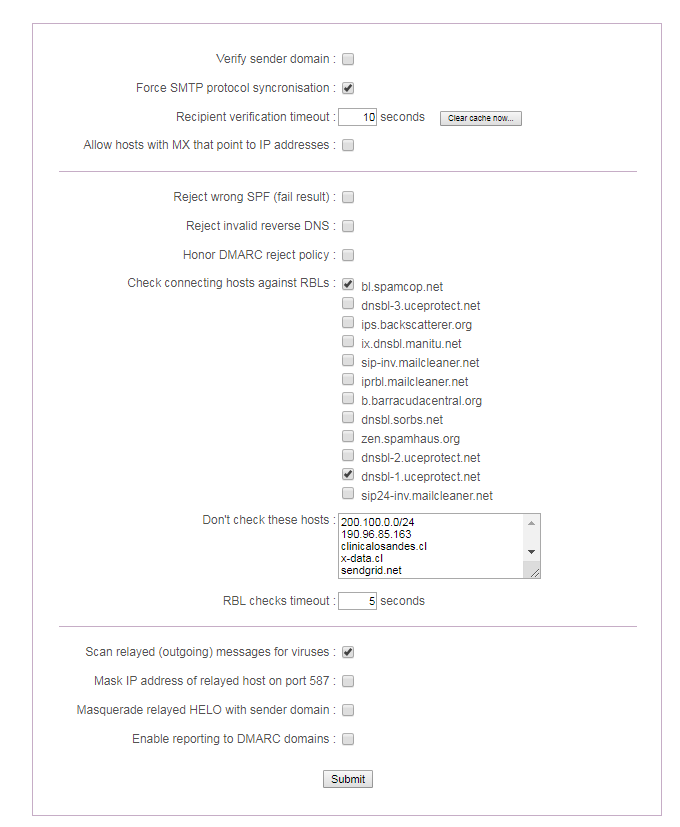




# SMTP (Simple Mail Transfer Protocol)

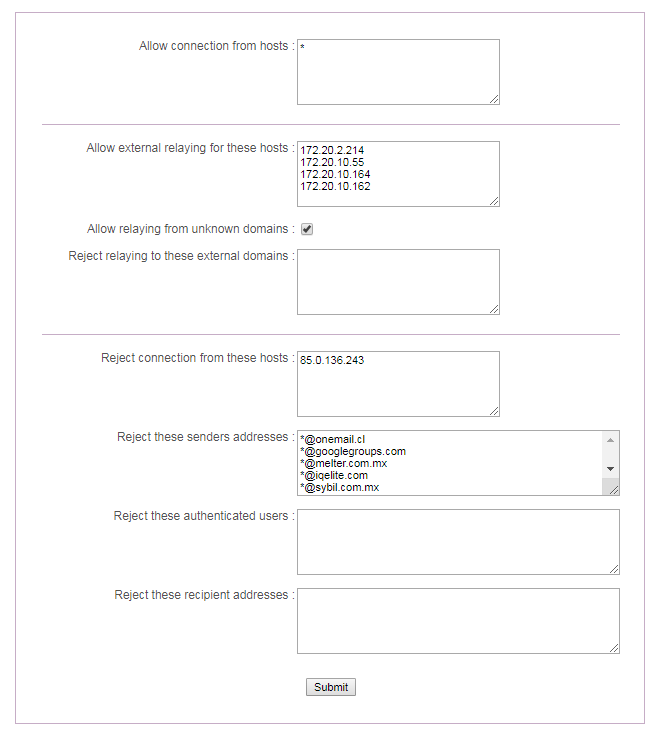
## SMTP Checks

Dentro de esta pestaña podemos controlar el funcionamiento del protocolo de transferencia de los correos, ya sea verificando el dominio, forzando la sincronización del protocolo, hacer timeout a la verificación del recipiente, filtrar DNS con una o varias bases de datos a seleccionar, hacer una lista blanca sobre hosts, modificar el timeout para la verificación con la base de datos, entre otras opciones.



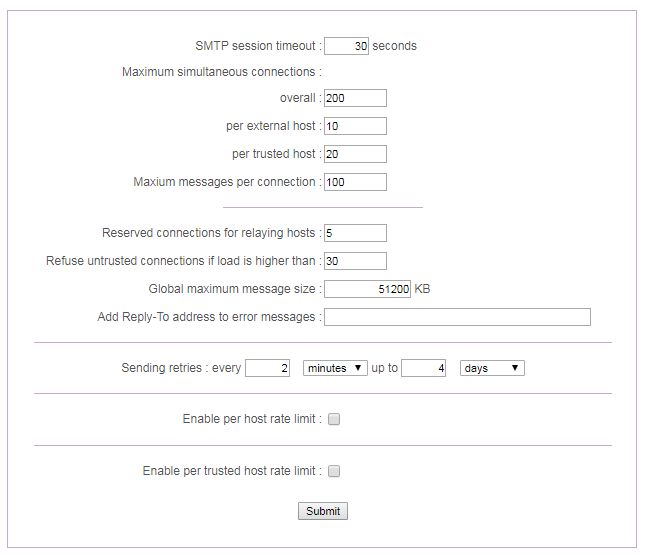
## Control de Conexiones

Desde acá tenemos las opciones delimitar a quién aceptamos/rechazamos dentro del protocolo sea por IP como por dominio/direcciones, también tenemos la opción de bloquear ciertos destinatarios.



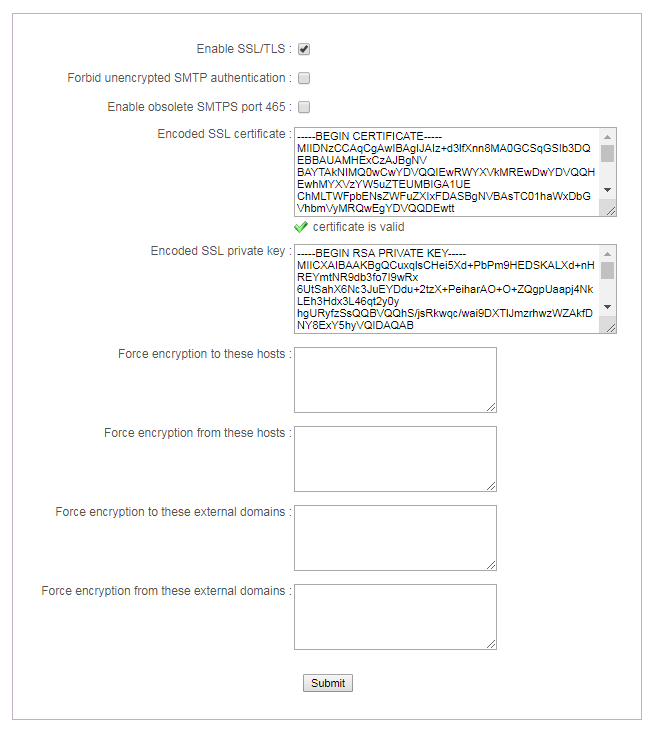
## Control de Recursos

En esta sección determinamos cuantos recursos se entregan, pudiendo limitar la cantidad de conexiones simultáneas, la máxima cantidad de mensajes por conexión, negar conexiones si estas superan cierta carga, el tamaño máximo por mensaje, cada cuanto son los reintentos de envío y límites por host.



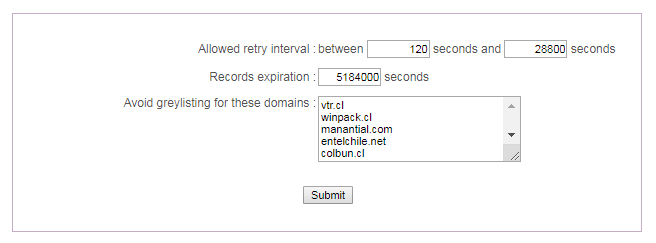
## TLS (Transport Security Layer)/SSL (Secure Socket Layer)

Acá podemos habilitar las opciones sobre los certificados e ingresar las claves correspondientes.



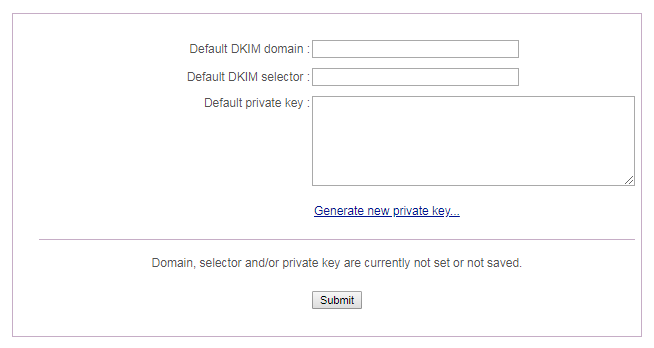
## Greylisting (Lista gris)

Esta sección nos habilita el uso de la lista gris dentro del sistema, la cual rechazará temporalmente cualquier correo desde un dominio/remitente el cual no reconozca, también tenemos un filtro para colocar dominios para que no entren en esta lista.



## DKIM (DomainKeys Identified Mail)

DKIM, es un método de autentificación de correos destinado para detectar direcciones de remitentes falsificados, esto es muy útil contra el phishing. Acá podemos generar y colocar las llaves necesarias para el método, así como el dominio del DKIM.

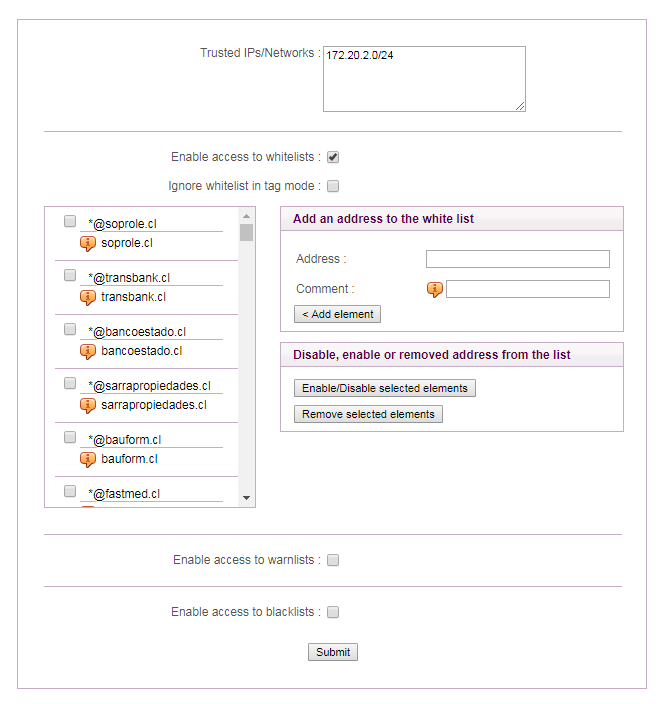


# Anti-Spam

## Ajustes Globales

Dentro de esta pestaña tenemos los ajustes generales sobre las herramientas anti-spam, tanto la configuración de la lista blanca, negra y la de avisos. También tenemos una pequeña sección al inicio con nuestras IP/Redes confiadas.

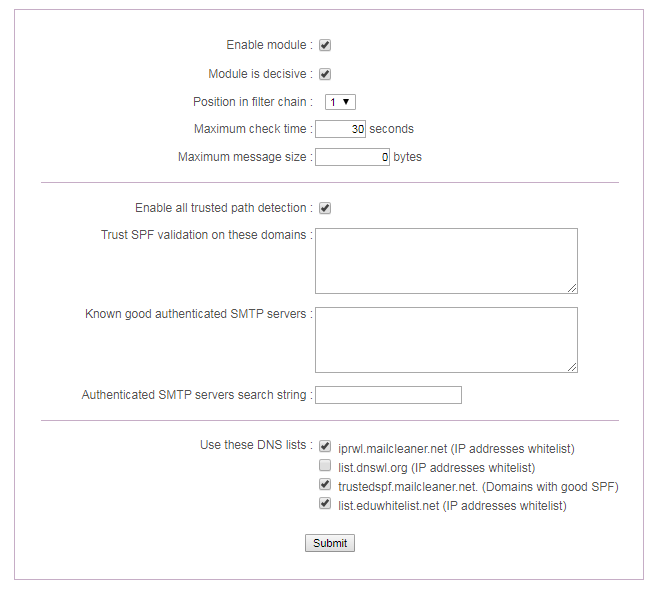
Nuestras listas son modificables y los elementos pueden ser retirados/deshabilitados/agregados a placer del administrador.



## Módulos Anti-Spam

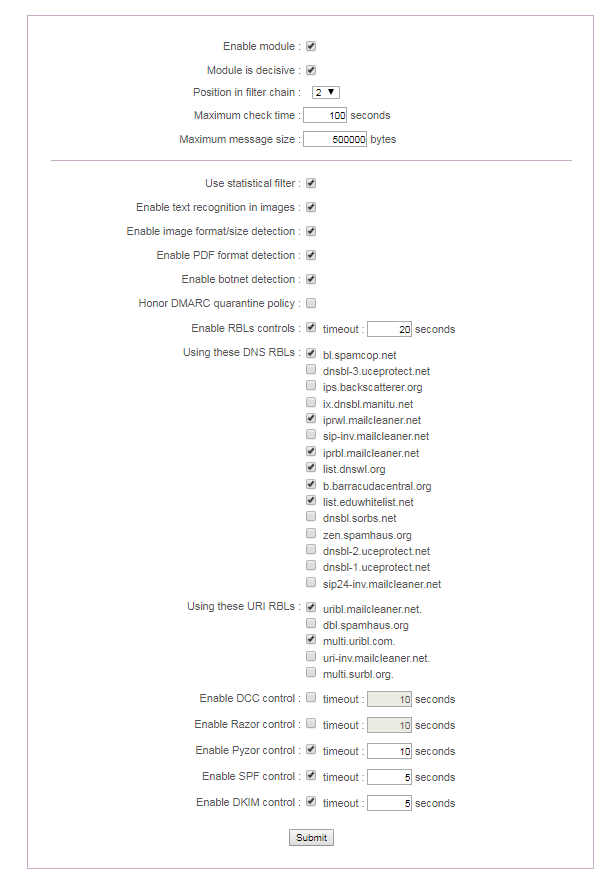
### TrustedSources

Este módulo cuando está habilitado administra las listas blancas y añade filtros propios de bases de datos en el internet. También se pueden modificar las variables de tiempo que puede tomar y tamaño máximo del mensaje, además tenemos la opción de añadir servidores SMTP conocidos desde acá.



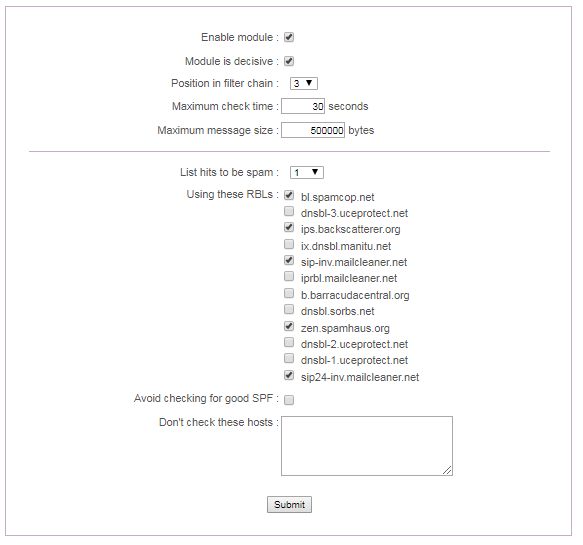
### Spamc

Este módulo es similar al anterior pero enfocado al spam, en donde filtra mediante bases de datos DNSBL (Domain Name System-based Blackhole List) o RBL (Real-time Blackhole List), enfocadas a DNS o URI (Uniform Resource Identifier).



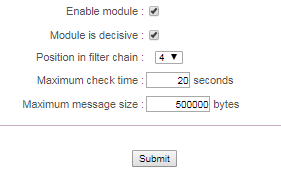
### PreRBLs

Módulo idéntico al anterior el cual genera un filtro más complementando al anterior sus opciones son similares, la función es idéntica pero el input de las RBL puede variar atrapando correos que pasaron el filtro anterior.



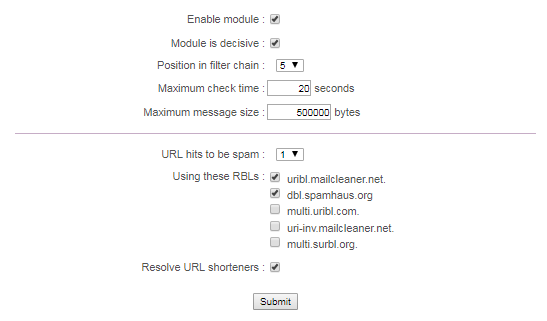
### NiceBayes

Este módulo se comunica con bases de datos con modelos estadísticos e información para identificar el spam de una manera más personalizada (la cual debe ser mantenida en base a reglas) similar a smapassasin.



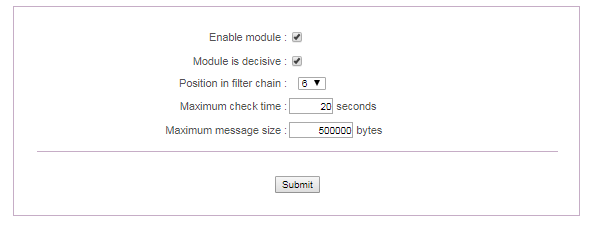
### UriRBLs

Con este módulo hacemos un filtrado mediante URI con las bases de datos seleccionadas, siempre cuando el filtro este habilitado, además de tener bases activas y/o elegidas.



### ClamSpam

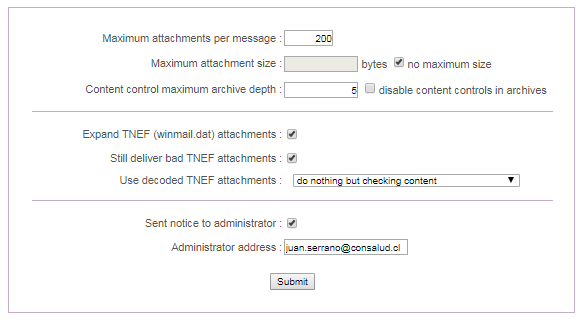
Este módulo filtra spam con reglas internas provistas por terceros, con las opciones de máximo tiempo de chequeo y máximo largo del mensaje.



# Protección de Contenido

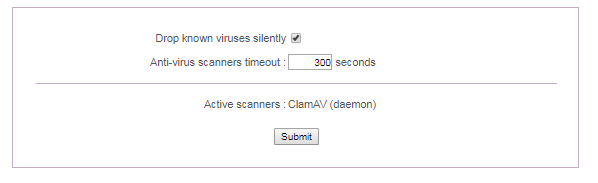
## Ajustes Globales

En esta sección podemos configurar la cantidad de adjuntos máximos por mensaje, así como máximo tamaño por archivo adjunto, configuraciones sobre los adjuntos de forma TNEF (Transport Neutral Encapsulation Format), y la utilidad de notificar al administrador en caso de ocurrencias con los archivos adjuntos.



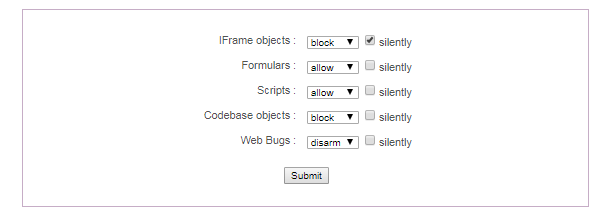
## Anti-Virus

Acá podemos elegir el comportamiento del antivirus en caso hallar un archivo malicioso, si queremos que haga su trabajo silenciosamente en caso que el virus ya sea conocido y el tiempo que puede demorar el escáner.



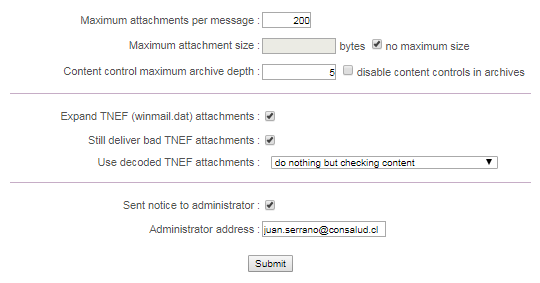
## Control HTML

En este menú podemos elegir que funcionalidades de HTML habilitamos, bloqueamos o desarmamos y si genera un aviso al administrador/log.



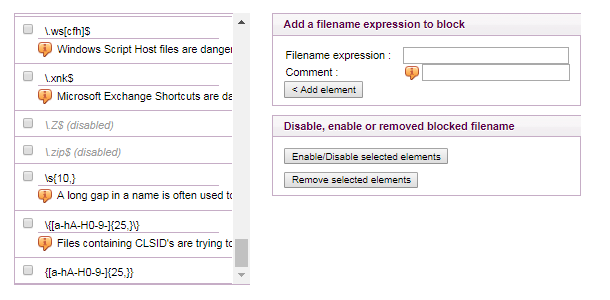
## Control en el formato de los Mensajes

Similar al menú anterior pero con el enfoque de las funcionalidades y cualidades de los mensajes, según estas habilitamos o no los mensajes.



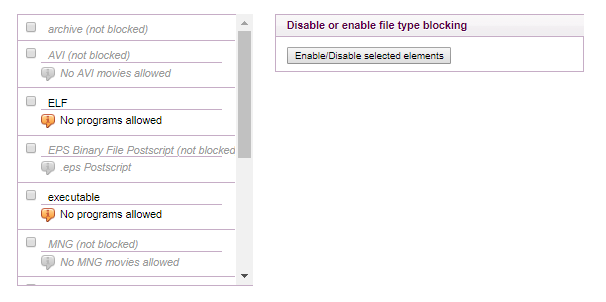
## Nombre de Archivos Adjuntos

Dentro de esta sección podemos usar expresiones regulares para generar reglas, para filtrar ciertos nombres o extensiones de archivos que consideremos peligrosos.



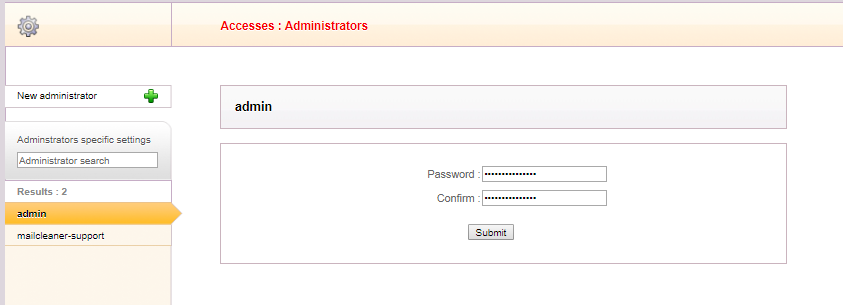
## Tipo de Archivos Adjuntos

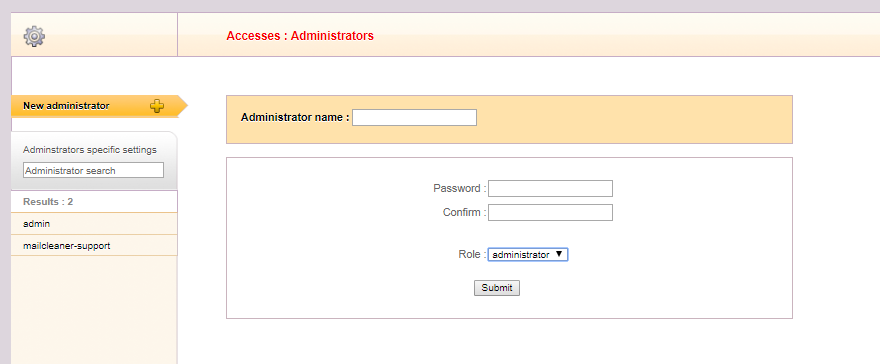
Este menú es similar al anterior, pero la diferencia es que las reglas están predefinidas y solo se puede activar/desactivar, obteniendo un filtro por tipo de archivos más generalizado.



# Accesos

Esta ventana recopila las opciones de acceso, crear usuarios nuevos para acceder a la herramienta y cambiar contraseñas.

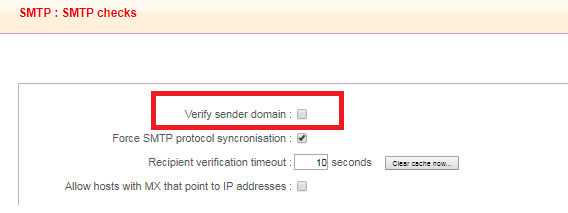




# Observaciones

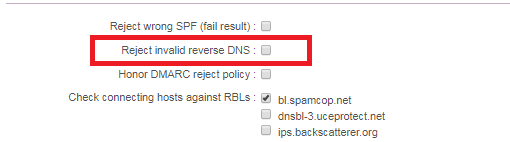
## Remitente no Verificado

Dentro de las opciones de *“SMTP checks”*, tenemos la opción para verificar si el remitente corresponde al dominio que dice ser, esta opción es útil y se verifica su configuración para evitar ataques de tipo phishing.



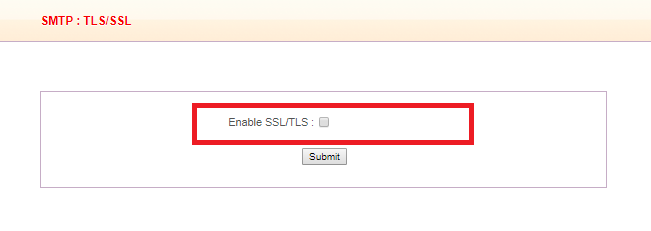
## No hay una búsqueda de DNS inversa

Dentro de las opciones de *“SMTP checks”*, está la opción para verificar el DNS mediante una [búsqueda inversa](https://en.wikipedia.org/wiki/Reverse_DNS_lookup) del dominio para llegar a la IP, esto se hace mediante el ISP, lo cual lo hace más difícil de falsificar, por ende si el DNS no calza con la IP que el ISP mantiene en su base de datos el correo es rechazado por supuesto spoofing.



## [SSL](http://info.ssl.com/article.aspx?id=10241)/[TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) no configurado

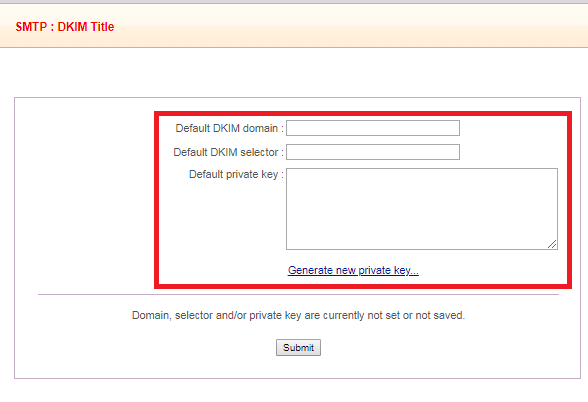
Dentro de las medidas de seguridad del protocolo SMTP, no existe una forma de encriptación nativa, por ende para tener una capa de seguridad y no tener texto plano navegando por internet se recomienda tener uno de los protocolos de seguridad para tener una capa de seguridad en el protocolo de envío de mensajes.



## DKIM no configurado

[DKIM](http://www.dkim.org/) es un método de autentificación de correos el cual ayuda en la detención del spoofing, el cual es usado para ataques de phishing y spam. Este método verifica que el remitente que envió el correo está autorizado por el administrador/dueño del dominio, esto se realiza mediante firmas digitales, las cuales son publicadas en conjunto al DNS. Esto también verifica que los archivos adjuntos no puedan ser modificados luego que salen del servidor en cuestión.

Este método es un estándar definido en [**RFC 6376**](https://tools.ietf.org/html/rfc6376), con actualizaciones [**RFC 8301**](https://tools.ietf.org/html/rfc8301)y [**RFC 8463**](https://tools.ietf.org/html/rfc8463).



## Comportamiento extraño del [spool](https://unix.stackexchange.com/questions/150715/what-is-the-purpose-of-mail-spools)

Dentro del spool, podemos ver el almacenamiento temporal de algunos correos que están siendo enviados, analizados o con intento de reenvío. Si nos fijamos en la imagen inferior la sección de correos entrantes, su lista de remitentes son direcciones locales lo cual debería ser al revés, esto genera confusión en si la herramienta está mal configurada o la documentación dice algo al respecto. Cabe notar que sucede lo mismo para el correo saliente.

