SPAMINA
Securing Digital Communications

SEGURIDAD DE CORREO EN LA NUBE

PROPUESTA TÉCNICA

SPAMINA
Securing Digital Communications

ÍNDICE

1. DATOS DE LA PROPUESTA

SPAMINA			
Account Manager	EDUARDO BOBADILLA		
Teléfono	+55 3711 5660	E-mail	eduardo.bobadilla@spamina.com
Contacto Técnico	OSCAR ALVAREZ / ADAN BARBABOSA		
Teléfono	+34 673 391 408 | +52 55 4341 2361	E-mail	oscar.alvarez@spamina.com adan.barbabosa@spamina.com

DATOS DEL CLIENTE	
Empresa	UNIVERSIDAD AUTÓNOMA DE CHIHUAHUA

DATOS DEL PARTNER	
Empresa	

Fecha Presentación	
Fecha Propuesta	MARZO.2017 rev.A

2. SPAMINA - FABRICANTE DE SOLUCIONES DE SEGURIDAD

2.1. ACERCA DE SPAMINA

Aegis Security, S.L. (en adelante Spamina), empresa de seguridad europea, ofrece una plataforma segura de comunicación en la nube, que garantiza la seguridad del correo electrónico y demás sistemas modernos de comunicación cada día en mayor uso en las corporaciones, como es el caso de la mensajería instantánea. Además, ofrecemos a las empresas la tranquilidad de saber que su información se encuentra completamente protegida bajo la legislación vigente de la Unión Europea.

En Spamina somos desarrolladores de nuestra propia tecnología, que se diseña y desarrolla en las sedes de España y Argentina. En estos términos, ofrece cumplimiento legal estricto en el ámbito comercial de producto español(europeo) y americano (centro y sur), para las empresas públicas.

Nuestro modelo de seguridad para el entorno del correo electrónico desde la nube de Spamina garantiza la continuidad del negocio, la escalabilidad del servicio contratado, eliminando la necesidad de mantener infraestructura propia al igual que mantenimiento y control de la misma.

Las soluciones de Spamina, van desde el propio servicio de correo en la nube (Parla), con las capas de seguridad integradas; pasando por la protección perimetral del correo, los servicios de archivado, cifrado y control de fuga de datos y seguridad web.

Spamina cuenta con oficinas en Madrid, Barcelona, Milán, Buenos Aires, México DF y Lima. Nuestros productos y servicios se distribuyen a través de los principales mayoristas y distribuidores autorizados a nivel nacional, y a través de partners clave a nivel internacional, con Oficinas de Representación en Portugal, México, Chile, Perú, Bolivia, Perú, Ecuador, Colombia, Brasil, Guatemala y Dubái.

Los productos desarrollados para la protección del correo electrónico que ofrece Spamina han obtenido el certificado ISO 9001:2008, que especifica los requisitos necesarios para disponer de un buen sistema de gestión de la calidad. Se asegura de este modo que se ha llevado a cabo un profundo análisis técnico de las funcionalidades más demandadas por los usuarios para incorporarlas a su portfolio de soluciones, además de mejorar constantemente las existentes.

Spamina ha recibido en el 2010 el premio de la revista SIC al "Reconocimiento a la excelencia de las soluciones tecnológicas en el ámbito de la protección del correo electrónico".

SUN MICROSYSTEMS ha otorgado a Spamina el "Premio a la innovación y trabajo conjunto con SUN", en reconocimiento al éxito de la colaboración entre ambas compañías.

SPAMINA viene respaldada por su reconocimiento internacional, avalado por el premio CfEL 2005 de Cambridge* al mejor proyecto tecnológico, así como por la apuesta de multinacionales como HP, SUN MICROSYSTEM, IBM, VMWARE, CITRIX y BLACKBERRY que han certificado nuestra solución integrándola en sus programas de partners oficiales.

Gartner ha reconocido a Spamina en el Cool Vendor Report de 2016. El informe de Gartner refleja los productos y servicios de IT que consideran interesantes, innovadores y con visión estratégica.

*Centro de innovación tecnológica más importante del mundo.

Esta confianza es el resultado del esfuerzo constante de un equipo de más de 50 ingenieros. Los Centros de seguimiento Spamina repartidos por todo el mundo nos permiten alimentar nuestras redes de spam, lo que significa una garantía de confianza para todos los usuarios.

2.2. REFERENCIAS SPAMINA

A continuación, reflejamos algunas referencias de clientes de Spamina:

ADESLAS	CEPSA	MAZ
AENA	CLECE	MEDIASET
AHORRAMAS	COFARES	MINISTERIO INDUSTRIA
AIR EUROPA	CORTEFIEL	NUTREXPA
ASISA	DKV	OMEGA PHARMA
AVANZA	FCC	ONCE
AYESA	FIESTA HOTELES	PARADORES
AYUNTAMIENTO BILBAO	GLOBALIA	PROSEGUR
BANCA CIVICA	GOBIERNO ARAGON	REDIRIS
BANCO GALLEGO	GOBIERNO CANTABRIA	SANTANDER CONSUMER
BANKINTER	GRUPO PLANETA	SERVICAIXA
C.G. FARMACEUTICOS,	HOTELES NH	TECKNON
C.G. MEDICOS	HOTELES SILKEN	TELEFONICA
CAP ARAG	INE	TUBOS REUNIDOS
CARREFOUR	ISOLUX	UMIVALE
CECOFAR	JAZZTEL	UNCETA

3. SOLUCION SPAMINA SEGURIDAD CORREO - CLOUD EMAIL SECURITY SUITE

3.1. CLOUD EMAIL FIREWALL

Cloud Email Firewall (CEF) ofrece protección integral del correo electrónico de las empresas desde la nube de manera eficiente, escalable y siempre actualizada de forma automática. El filtrado CEF está diseñado para proteger el servidor de correo de spam, virus, spoofing, *phising* y spyware. El filtrado almacena el Spam y *malware* en la nube de Spamina liberando al servidor de correo electrónico y redundado el uso de ancho de banda en la red corporativa, CEF ofrece a los administradores un completo sistema de informes y una gestión sencilla.

La solución de filtrado de correo no se limita a ofrecer la seguridad integral, sino que incorpora varios módulos para garantizar la continuidad del servicio de correo electrónico, como Email Backup que permite 5 días de copias de seguridad del correo electrónico, o también, el módulo de Email Continuity que se activa en caso de caída del servidor de correo, garantizando 4 días de entrega en modo "relay". Así mismo, para facilitar el acceso alternativo al correo electrónico, Cloud Email Firewall incluye un acceso al Emergency Webmail que garantiza la disponibilidad, en cualquier circunstancia y desde cualquier lugar.

El servicio CEF incorpora, además, un filtrado automático desarrollado por Spamina, Simile Fingerprint Filter (SFF® v2.0) para protección de la reputación de la plataforma, permitiendo el envío de correos masivos de clientes a la vez que se aseguran niveles de servicio en la entrega de correo corporativo a internet.

SFF ha sido ampliado para ser capaz de identificar una gama más amplia de tipos de correo electrónico salientes: spam débil, fuerte y email masivo (correo legal).

¿Cómo actúa SFF® v2.0?
Cada plataforma de filtro de correo electrónico Cloud Email Firewall está dotada de una plataforma de mailing. El objetivo es ser capaz de entregar el correo legal sin interrupción del servicio para el resto de los clientes del servicio. La plataforma monitoriza en tiempo real todo el correo para reaccionar cuando cualquiera de sus IP cae en listas negras. Sólo los nodos "más limpios" se utilizan para la entrega de correo electrónico y mensajes de correo electrónico salientes, permitiendo garantizar que el tráfico corporativo saliente que procesa la plataforma Cloud Email Firewall se entrega de manera eficiente y atendiendo a unas latencias mínimas.

Los correos electrónicos con clasificación "spam débil" se reenvían a través de la Plataforma de Mailing, donde se intenta garantizar la entrega de los correos masivos (no Spam), enviados a través de CEF.

Los correos electrónicos con clasificación "spam fuerte" son rechazados.

3.1.1. CARACTERISTICAS CLAVE

- Privacidad de datos. El servicio de protección de correo Cloud Email Firewall ofrecido desde la nube de Spamina cumple con la exigente normativa de la Unión Europea en materia de protección de datos, ayudando a su empresa a mantener la máxima seguridad. El

almacenado de correos electrónicos se realiza únicamente en Centros de Proceso de Datos dónde la legislación establecida garantiza la privacidad de datos de nuestros clientes.

- Filtrado Multicapa para correo entrante y saliente: Incluyendo filtros de conexión, antivirus, antispam y anti-*malware*, y análisis con patrones heurísticos & bayesianos y propios Spamina (SFF® v2.0).
- Continuidad de negocio ofreciendo:
  - Relay de correo durante 4 días.
  - Backup del correo entrante (5 días de correo válido y 28 de correo Spam en cuarentena).
  - Interfaz Webmail de emergencia, permite a los usuarios de su organización mantener siempre disponible el acceso al correo en caso de caída del servicio mail del cliente.
- Dashboard: Visión dinámica del estado del sistema y la actividad de filtrado para distintos periodos de tiempo.
- Tecnologías avanzadas de filtrado, incluyendo
  - Filtros propios de Spamina, como el reputado filtro de similitud de patrones, SFF (Simile Fingerprint Filter) versión 2.0.
  - Protección ante suplantación de identidad, Anti-spoofing.
  - Filtros de verificación de autenticación y firmado DKIM, SPF y DMARC.
  - Protección de ataques de DNS (DNSSEC) como envenenamiento, pharming o suplantación de DNS.
- Auditoría de acciones: Proporciona información sobre la actividad que los administradores y usuarios finales realizan sobre el sistema, permitiendo conocer y analizar la totalidad de acciones realizadas por los usuarios sobre el servicio.
- Motor de gestión de informes: configuración de envío de información de filtrado para administradores de empresa y dominio. Facilidad de uso a través de reportes predefinidos.
- Cuarentena centralizada: Permite a los administradores revisar todos los correos de la empresa en cuarentena.
- Acciones masivas sobre correos desde listados de logs: Información detallada sobre las clasificaciones y filtros aplicados.
- **Tecnología CYREN™ integrada**: Se integran los motores de Antispam, virus por patrones y listas de reputación de esta prestigiosa marca.
- Solución perimetral: La arquitectura de la solución está basada en una arquitectura distribuida y escalable (SDA).
- WebServices API: Permite la interoperabilidad con aplicaciones de terceros.
- Motor de Políticas: Gestión de las políticas de uso del correo electrónico (correo entrante / saliente).
- Distintos niveles de administración: Administrador de empresa, administrador dominio y usuario final.
- IpV6: Compatibilidad con IPv4 e IPv6.
- Centro de Soporte Spamina: sistema de monitorizado 24x7x365 incluido en el modelo Cloud, y con la garantía de continuidad del Servicio.
- Soporte Técnico 24x7 (opcional [1]).

[1] Se incluye soporte 8x5 con la licencia estándar y 24x7 como un añadido en la licencia.

- Integrable con cualquier Plataforma de Email existente en el cliente [2].

3.1.2. BENEFICIOS

- Correo 99,9% libre de amenazas.
- 5 días de Backup de correo entrante.
- Gestión centralizada de los correos de toda la organización o del dominio.
- Garantiza la entrega de correo en caso de caída del servidor de correo del cliente gracias al servicio de continuidad de negocio.
- Correo 100% accesible ante caídas temporales del servidor del cliente.
- Adaptable a las políticas de seguridad de la compañía, permitiendo la gestión del correo entrante y saliente ayudando al cumplimiento de normativas de la organización.
- Permite obtener una visión dinámica del estado del sistema (dashboard) y de la actividad de filtrado.
- Acceso en tiempo real a información sobre acciones realizadas en el sistema.
- Los usuarios de su organización accederán al correo que ya ha sido protegido por el servicio de filtrado, independientemente de la ubicación de sus usuarios y de los dispositivos utilizados.
- Reducción de costes, ahorro de recursos e inversión inicial mínima.
- Plataforma adaptable a cualquier tipo de organización y futuras necesidades.
- Protección contra posibles amenazas y problemas de seguridad asociados a IPv6.
- API's adicionales que permiten que servicios software de terceros puedan integrarse fácilmente con el servicio Cloud Email Firewall.
- Disponibilidad inmediata del servicio y puesta en marcha en menos de 24h.

3.1.3. ADMINISTRACIÓN

- Distintos niveles de administración en la plataforma (administrador general, o de dominio).
- Gestión de usuarios y listas de distribución en tiempo real.
- Acceso HTTPS/SSL y tráfico cifrado TLS.
- Múltiples configuraciones posibles a nivel de empresa, dominio y usuario.
- Motor de políticas de correo entrante y saliente, a nivel de empresa, domino o usuario final.
- Módulo de informes de actividad del tráfico de correo electrónico, por dominio.
- Integración con LDAP para la gestión de usuarios (Active Directory, OpenLDAP, Lotus Domino, etc).
- Integración PUSH para provisión de usuarios de Directorio Activo mediante un agente de sincronización de usuarios a la nube de Spamina.
- Gestión de Cuarentenas de Spam y Virus por usuario o de forma centralizada.
- Configuración de listas blancas y listas negras aplicables a nivel de empresa y dominio.
- Configuración de listas blancas y negras personales por usuario.
- Listas blancas personales auto-alimentadas (Auto-whitelisting).
- Marcado de correo Spam con y sin envío a cuarentena.

[2] La compatibilidad está garantizada para correo entrante. Para realizar el filtrado de correo saliente es necesario que la plataforma de correo del cliente pueda enviar todo el correo saliente a través de un Smart Host.

- Configuración de informes periódicos para usuarios y administradores.
- Actualizaciones automáticas y transparentes, inherentes al modelo Cloud.
- Notificador de correo multiplataforma (Windows, Mac, Linux).
- Gestión en múltiples idiomas (EN/ES/CAT/DE/IT/FR/PO/RU).

3.1.4. SEGURIDAD Y FILTRADO MULTI-CAPA

El servicio de filtrado de correo Cloud Email Firewall proporciona una protección completa (filtrado de conexión, anti-virus/malware y contenido) para el correo electrónico empresarial con antispam, antivirus, anti-*malware, phishing* y anti-spoofing que de manera perimetral bloquea el correo malicioso, entregando sólo correo limpio hacia su organización.

- Filtrado de reputación y métodos de protección contra amenazas avanzadas.
- Protección contra ataques de directorio (por ejemplo, Delay y GreyListing).
- Modos de Filtrado Automático y Garantizado.
- Detección de correos pertenecientes a listas comerciales de distribución (greymail).
- El filtrado automático incluye hasta 4 motores de detección de Spam por análisis de contenido del correo.
- Análisis de malware mediante dos motores, con la opción de tener un tercer motor adicional (Advanced Malware Engine).
- Funciones de Firewall de correo con definición de reglas de uso y configuración para administrador y usuarios finales.
- Gestión de Listas Blancas/Listas Negras por parte del administrador y del usuario final.
- Análisis de archivos adjuntos comprimidos (zip, rar, etc...) con hasta 10 niveles de compresión.
- Reglas avanzadas de filtrado (múltiples condiciones AND/OR, uso de expresiones regulares, filtrado basado en diccionarios, comprimidos protegidos, tipos MIME, etc...)
- Archivado completo del correo entrante válido y de cuarentena.
- Auto-whitelisting: configuración de alimentación automática de listas blancas, aplicable por empresa, dominio o usuario final.

A continuación, se explica la tecnología de filtrado utilizada en la protección de correo entrante y saliente de la organización que contrata la solución:

Filtrado de correo entrante:

La siguiente imagen muestra la cadena de filtrado que se aplica a todo correo proveniente de internet de forma que ofrece una protección eficaz para poder bloquear amenazas dirigidas a su organización:

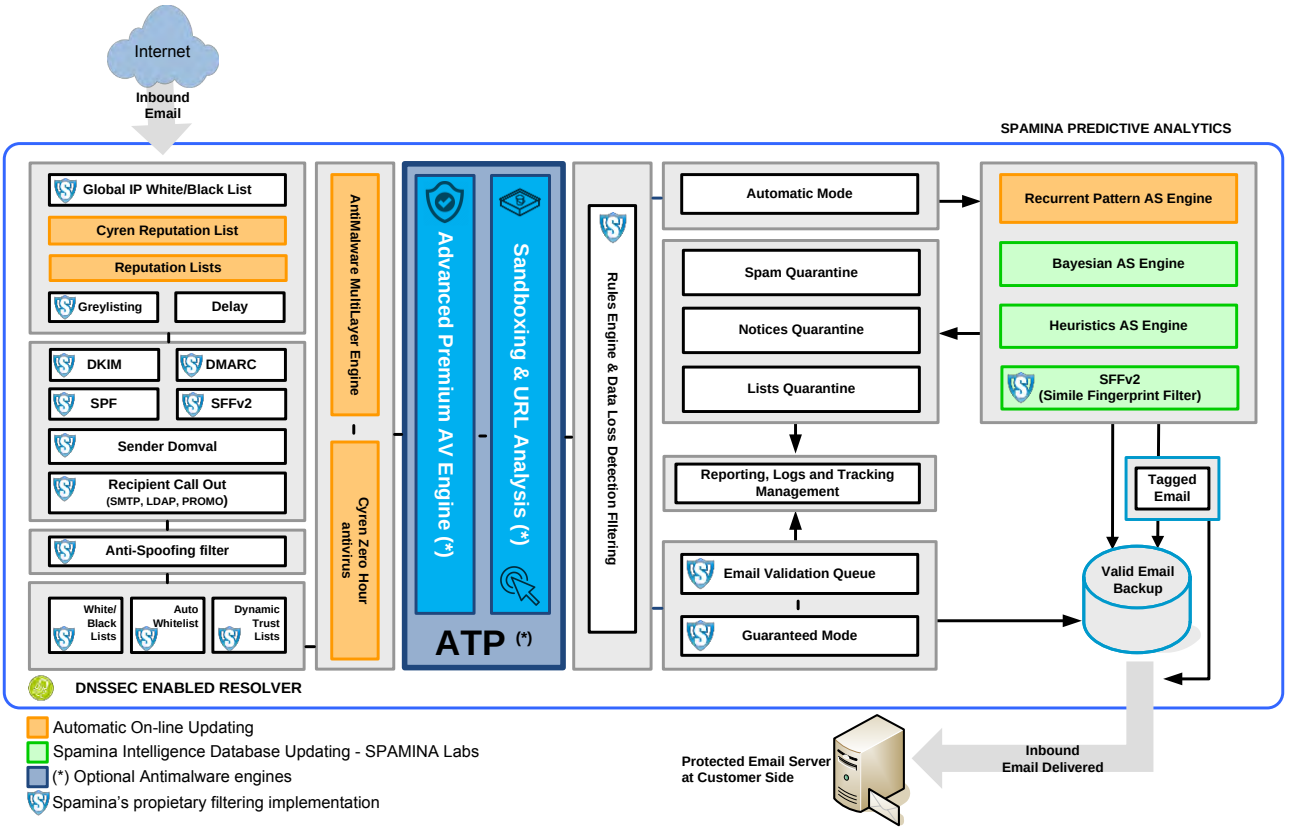


Imagen. - Visión del filtrado Cloud Email Firewall de correo (entrante).

La cadena de filtrado está dividida en 3 grandes bloques de filtrado:

Filtros de conexión:

En esta cadena de filtrado se aplican diversas técnicas orientadas a rechazar correos provenientes de fuentes conocidas de spam o programas automatizados de envío de correo spam. Un correo que sea clasificado como Spam en este bloque será rechazado por la plataforma y por tanto su contenido nunca será aceptado. Esto implica que nunca se procederá al almacenado interno (en cuarentena) o envío al servidor de correo del cliente final. Esta cadena de filtrado aplica las siguientes técnicas de filtrado:

- Listas de reputación globales / RBLs: Listas negras en tiempo real de varios proveedores bien conocidos y reputados a nivel mundial.
- Greylisting, Delay: Técnica orientada a disuadir a programas automáticos de envío de spam para que cesen su actividad, introduciendo retrasos en la entrega de correo a la plataforma de Spamina.
- DKIM, SPF y DMARC: Técnicas que se apoyan en la infraestructura pública de DNS para poder verificar que el remitente dice ser quien es y dar veracidad a su correo.
- Sender Domain validation: Técnica de validación del dominio del remitente que comprueba que sea un dominio válido en internet y con capacidad de recibir correo.
- Recipient Call Out: Validación del usuario destino, evita hacer entrega de correos a usuarios no existentes en la organización que protege la solución.
- Antispoofing Filter: Filtro para evitar la suplantación de identidad de los remitentes, y así evitar que se entregue correo proveniente de remitentes falsificados.

- Whitelists / Blacklists: Listas blancas y negras que pueden ser definidas por el administrador del sistema para ser aplicadas a todos o algunos de los dominios de la empresa e incluso listas blancas y negras personales por usuario de la organización.
- Auto-Whitelist: Generación automática de listas blancas personales de los usuarios basada en la comunicación de los usuarios de la organización con otros destinatarios de internet.
- Dynamic Trusts Lists: Listas de confianza de remitentes que se generan dinámicamente cuando esos remitentes envían correos válidos a los usuarios.

Filtro Anti-Malware:

El siguiente bloque de filtrado consiste en hacer un análisis de los correos para bloquear los correos que contengan algún tipo de malware. Por defecto Spamina utiliza dos motores:

- Antivirus basado en firmas de virus: Este motor contiene una base de datos de firmas conocidas de virus. Cuando se escanean los adjuntos o el cuerpo de los correos se pueden detectar estos patrones en el contenido de los correos y sus adjuntos, bloqueando la entrega de esos correos maliciosos.
- Antivirus de detección hora cero (Zero-hour): Motor antimalware que se apoya en una red de detección de patrones recurrentes a nivel mundial, donde se analizan más de 80 billones de correos diarios y se clasifican aquellos que sean maliciosos. Las técnicas de detección de esta red son variadas, incluyendo un complejo sistema de detección de varias capas que incluye técnicas heurísticas, basadas en firmas de virus, emulación y algorítmicas.

Spamina ofrece una protección adicional mediante un tercer motor de antivirus y malware con sandoxing de ficheros y URLs para amenazas avanzadas de ransomware, y "hora cero", denominado Advanced Threat Protection (ATP) que requiere una licencia adicional complementaria para el servicio de Cloud Email Firewall.

Filtro de contenido de correos:

El siguiente bloque de filtrado consiste en hacer una inspección del contenido del correo para detectar si es Spam. En caso de que se detecte un correo como spam en este bloque de filtrado, será puesto en la cuarentena del sistema. Se aplican los siguientes 4 motores de filtrado:

- Motor de detección de Spam por patrones recurrentes: Este motor se poya en una red de detección global que procesa billones de correos diarios, teniendo una tasa de detección de spam de más del 99% y sin prácticamente falsos positivos (aproximadamente 1 entre 1.5 millones).
- Motor Bayesiano de detección de Spam: Técnica estadística de clasificación de Spam.
- Motor Heurístico de detección de Spam: basado en puntuaciones examinando varias características de los correos.
- Red SFF – Simile Fingerprint Filter: Esta técnica se apoya en huellas digitales de correos similares para determinar si son Spam.

Un correo que sea detectado por este bloque de filtrado como Spam será puesto en la cuarentena del sistema durante un máximo de 28 días, periodo durante el cual tanto administradores finales como usuarios finales pueden hacer una revisión de estos correos y realizar su desbloqueo de la cuarentena si fuera necesario.

Filtrado de correo saliente:

La siguiente imagen muestra la cadena de filtrado que se aplica a todo correo saliente de su organización y dirigido a internet, de forma que ofrece una protección eficaz para poder bloquear posibles amenazas salientes de su organización, así como proteger su reputación de envío de correo:

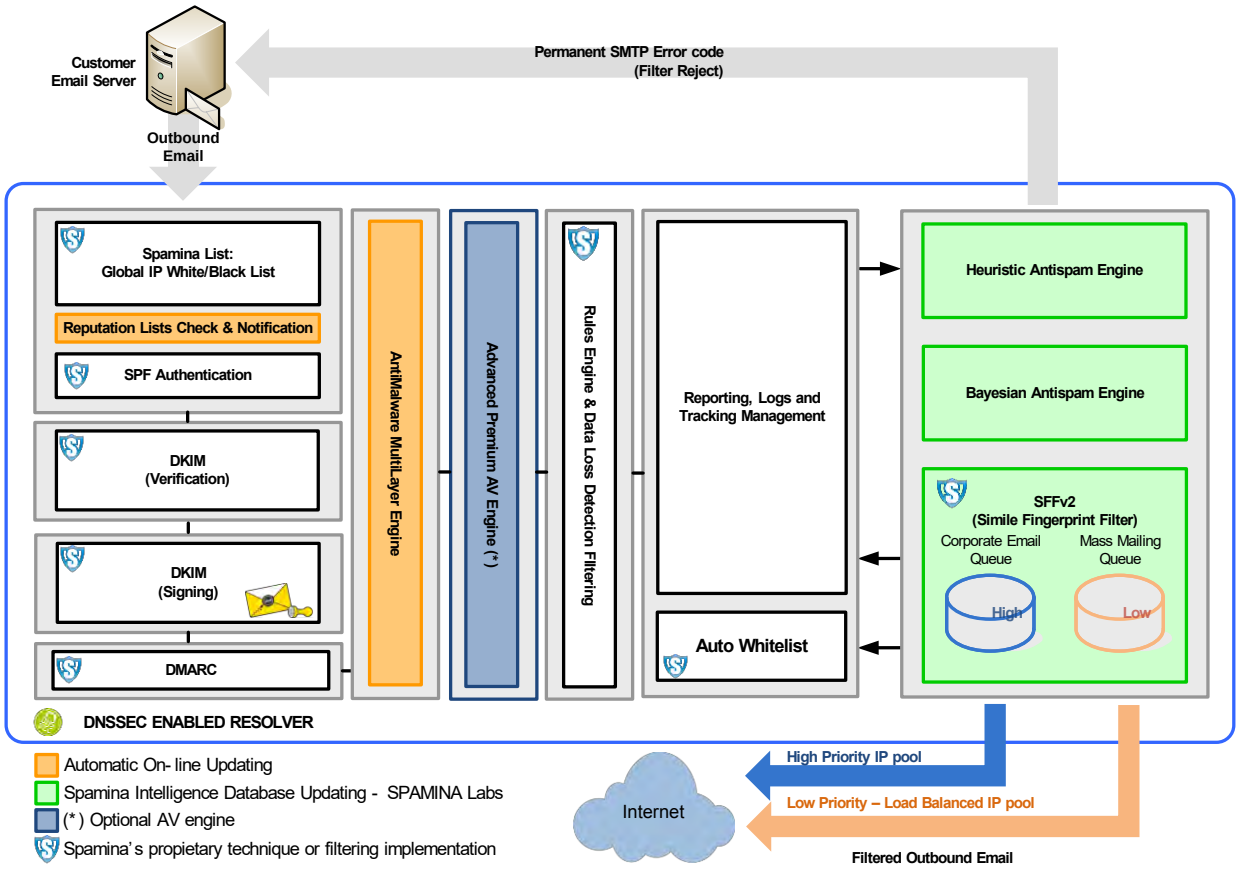


Imagen. - Visión del filtrado Cloud Email Firewall de correo (saliente).

La cadena de filtrado de correo saliente también está dividida en 3 grandes bloques de filtrado:

Filtros de conexión:

En esta cadena de filtrado se aplican diversas técnicas orientadas a denegar el envío de correo saliente y por tanto rechazar la entrega de correos a internet que provengan de fuentes conocidas de spam, de programas automatizados de envío de correo spam o correos que no pasen las verificaciones pertinentes. Un correo que sea clasificado como Spam en este bloque será rechazado por la plataforma y por tanto su contenido nunca será aceptado. Esto implica que nunca se procederá al almacenado interno (en cuarentena) o envío al servidor de correo del cliente final. Esta cadena de filtrado aplica las siguientes técnicas de filtrado:

- Listas Blancas y listas Negras Globales: Se trata de listas mantenidas por Spamina ya que se ha detectado que estas IPs realizan envío de correo en la plataforma o por el contrario Spamina puede optar por meter una IP remitente en lista blanca. Estas listas no son administrables por el cliente final.
- Comprobación y notificación en listas de reputación: La plataforma realiza comprobaciones periódicas de las direcciones IP desde las que nuestros clientes nos hacen entrega de sus correos para su envío a internet. Estas comprobaciones se realizan utilizando múltiples proveedores de listas negras. En caso de que algunas de las IPs de nuestros clientes se encuentren en lista negra, mandamos una notificación al administrador de la solución de Spamina en el cliente advirtiéndole de esta situación. Esta acción no implica que Spamina rechazará el correo proveniente del cliente, simplemente se trata de advertencias para indicar al cliente final de que:
  - Sistemas remotos de protección antispam pueden proceder al rechazo de ese correo al que damos salida debido a que alguna de las IPs de tránsito presentes en la cabecera se encuentran en sistemas de lista negra en tiempo real (DNSRBL).
  - El cliente final puede tener un problema de envío de Spam a través de su infraestructura de comunicaciones.

  En ningún momento esta técnica previene a Cloud Email Firewall de realizar la entrega de los correos del cliente hacia internet.
- Verificación de firma DKIM: En caso de que el correo que nos entrega el cliente para su envío a internet contenga un firmado por DKIM, este se comprueba y si fuera inconsistente la verificación de dicha firma, se rechazaría el correo por tratarse de una posible suplantación de identidad.
- Firmado de correos por DKIM: La solución Cloud Email Firewall permite hacer el firmado del mensaje por DKIM. El cliente únicamente debe proporcionar la clave privada y el selector del DNS donde se puede localizar la clave pública para que los receptores puedan comprobar la validez del mensaje. Esta técnica permite añadir una verificación adicional a los correos que envía Cloud Email Firewall.
- DMARC: Cloud Email Firewall permite actuar acorde a las acciones especificadas por el administrador del dominio remitente del correo en el registro DMARC presente en el DNS.

Filtro Anti-Malware:

El siguiente bloque de filtrado consiste en hacer un análisis de los correos para rechazar y no dejar que sean enviados a los destinatarios los correos que contengan algún tipo de malware. Por defecto Spamina utiliza un único motor antimalware para correo saliente:

- Antivirus basado en firmas de virus: Este motor contiene una base de datos de firmas conocidas de virus. Cuando se escanean los adjuntos o el cuerpo de los correos se pueden detectar estos patrones en el contenido de los correos y sus adjuntos, bloqueando la entrega de esos correos maliciosos.

En caso de que el cliente ha contratado la protección adicional Advanced Threat Protection, este tercer motor antivirus/malware, se aplicaría a todo el tráfico de correo entrante y saliente analizado por Cloud Email Firewall. Mientras que, el motor de Sandbox de archivos y la protección de URLs se aplicaría con todos los correos entrantes.

Filtro de contenido de correos:

El siguiente bloque de filtrado consiste en hacer una inspección del contenido del correo para detectar si es Spam. En caso de que se detecte un correo como spam en este bloque de filtrado, será puesto en la cuarentena del sistema. Se aplican los siguientes 3 motores de filtrado para correo saliente:

- Motor Bayesiano de detección de Spam: Técnica estadística de clasificación de Spam.
- Motor Heurístico de detección de Spam: basado en puntuaciones examinando varias características de los correos.
- Red SFF – Simile Fingerprint Filter: Esta técnica se apoya en huellas digitales de correos similares para determinar si son Spam, posible spam o si se trata de un envío masivo de correo que realiza el cliente. En caso de tratarse de un correo spam, la huella digital de este correo es introducida en una base de conocimiento que Spamina mantiene a nivel global y que es consultada por el resto de filtros de la tecnología de spamina, para su clasificación de correo entrante. En caso de tratarse de un correo masivo enviado por el cliente, se realizará el envío a través de una serie de equipos destinados al envío de este tipo de correo. La plataforma monitoriza en tiempo real todo el correo saliente por la plataforma para reaccionar cuando cualquiera de sus IP cae en listas negras. Sólo los nodos "más limpios" se utilizan para la entrega de correo electrónico y mensajes de correo electrónico salientes, permitiendo garantizar que el tráfico corporativo saliente que procesa la plataforma Cloud Email Firewall se entrega de manera eficiente y atendiendo a unas latencias mínimas.

Un correo que sea detectado en el análisis de filtrado de correo saliente como Spam será rechazado por el sistema a nivel SMTP, provocando un envío de un NDR – Non Delivery Report – de vuelta al usuario. No existe un sistema de cuarentena saliente en la cadena de filtrado de correo saliente, para evitar que posibles falsos positivos queden retenidos en la plataforma sin posibilidad de notificación al remitente del correo.

3.1.5. ADVANCED THREAT PROTECTION

Advanced Threat Protection (ATP) ofrece protección exhaustiva y definitiva contra una amplia gama malware, ransomware y amenazas avanzadas persistentes, que intentan infiltrarse a través del correo electrónico.

La solución ATP de Spamina aporta una capa adicional de protección al correo electrónico por encima de los servicios antimalware y antispam.

La solución ATP de Spamina incorpora las siguientes tecnologías:

- Advanced Premium Antivirus
- Sanboxing de Ficheros & URLs

El servicio está totalmente integrado en las consolas de gestión, ofreciendo a los directores de TI el control para su configuración y auditorías, así como generación de informes del servicio. Igualmente, los usuarios son notificados cuando reciben emails que son sometidos a análisis, así como cuando pinchan en URLs que pueden ser potencialmente peligrosos.

La tecnología de Sandboxing ofrece un mecanismo de seguridad para ejecutar programas/ficheros en un entorno controlado, para así analizar las acciones y los efectos que puedan ocasionar.

El análisis por técnicas de Sandboxing se utiliza frecuentemente para comprobar en tiempo real emails o programas que no han sido verificados y puedan contener un virus, códigos o enlaces maliciosos, evitando así que estos afecten al dispositivo del usuario final.

3.1.6. MOTOR DE POLITICAS

Los administradores pueden habilitar reglas basadas en políticas granulares sobre la entrada y salida del correo electrónico, así como fijar una amplia gama de acciones sobre la base de atributos del mensaje y el contenido del mismo.

El motor de filtrado de contenido ofrece la definición de políticas corporativas sin necesidad de cambiar la forma en la que los empleados utilizan su correo electrónico. El motor de políticas incluye funcionalidades avanzadas tales como la identificación de mensajes según la especificación MIME en adjuntos, la posibilidad de utilizar operadores lógicos AND/OR en la definición de reglas o el uso de diccionarios y expresiones regulares.

3.1.7. LOGS DE CORREO

El proceso de filtrado avanzado multi-capa que analiza cada uno de los correos electrónicos entrantes y salientes del dominio, ofrece una gestión con control completo para los administradores del servicio.

Cloud Email Firewall permite desde el panel de administración realizar un análisis forense y un seguimiento exhaustivo, de todo el flujo de correos de la organización:

- Gestión de los correos en cuarentena. El administrador podrá interactuar con el servicio de filtrado:
  - validando el spam o reenviando los mensajes.
  - reasignar a listas blancas de la empresa, del dominio o del usuario final.
  - reasignar a listas negras de la empresa, del dominio o del usuario final.
- Búsquedas de mensajes por múltiples criterios: Dominio, De, Para, Asunto, Dirección IP origen, clasificación y/o filtro aplicado, fecha, hora y minutos.
- Seguimiento de políticas aplicadas: agrupar reglas y establecer un nombre identificativo por medio del cual realizar un seguimiento de su aplicación.
- Visualizar las cabeceras o el correo completo analizado (configurable según la política de la empresa).
- Almacenamiento de la cuarentena durante 28 días.
- Reenvío de los resultados de las búsquedas en formato CSV para un procesamiento posterior.
- El resultado de las búsquedas permite obtener detalles de: IP origen, De/Para, Asunto, Fecha/Hora, Tamaño, Estado y clasificación (razón del bloqueo) ofreciendo posibilidad de tomar decisiones sobre el filtrado aplicado
- Los resultados de clasificación pueden ser por correos con antivirus/antivirus por patrón recurrente, anti-spoofing, antispam, listas de confianza, validación SPF, patrones bayesianos/heurísticos, validación DKIM / DMARC, lista de confianza/negras/de correos, max. nº de destinatarios, entre otros.

3.1.8. INFORMES

Spamina Cloud Email Firewall ofrece un completo módulo de informes que permite conocer y controlar en todo momento, y al detalle, lo que sucede en el correo de su empresa, y tomar acciones

necesarias para corregirlo. Desde el panel de administración se pueden configurar notificaciones, informes y estadísticas de filtrado:

- Estadísticas de filtrado: gráficas instantáneas del estado del servicio (entrante y saliente) seleccionable por empresa o dominio. Permite mostrar un reporte gráfico del correo y estadístico de la última hora, de 24h, mensual o volumen total (válidos, virus, spam, intentos de ataque/spam rechazado y listas de correo).
    - Estadísticas imprimibles o exportables en múltiples formatos (PDF, JPEG, PNG, etc...)
- Informes a medida o predefinidos con detalles por usuario o dominio completo.
    - Origen: correos entrantes y salientes.
    - Periodicidad: diarios, últimos 7 días, semanales, mensuales, etc.
    - Presentación: gráfico, tabla o resumen.
    - Categorías:
        - Correos válidos, spam, virus, listas de correos, spam rechazado, avisos de virus, etc...
        - Top usuarios que reciben correo con virus.
        - Top usuarios que envían correo.
        - Top usuarios que más reciben/envían correo (por tamaño y nº).
        - Top correos entrantes / salientes bloqueados con virus
- Informes de correo bloqueado: los usuarios pueden recibir en su buzón los resultados diarios o semanales del correo bloqueado por Spamina. El mensaje es personalizable con plantillas y permite opciones de recuperación y paso a listas blancas o negras.

3.1.9. NOTIFICADOR DESKTOP

Spamina Cloud Email Firewall proporciona una herramienta que se instala [3] en PC de escritorio proporcionando notificaciones en tiempo real cada vez que se retiene un correo en la cuarentena de Spamina. Esta herramienta de notificación permite, también, a los usuarios acceder a sus listas blancas y listas negras personales, así como interactuar con las preferencias de filtrado que realiza la plataforma de Spamina en la nube.

[3] Windows, Mac y Linux.

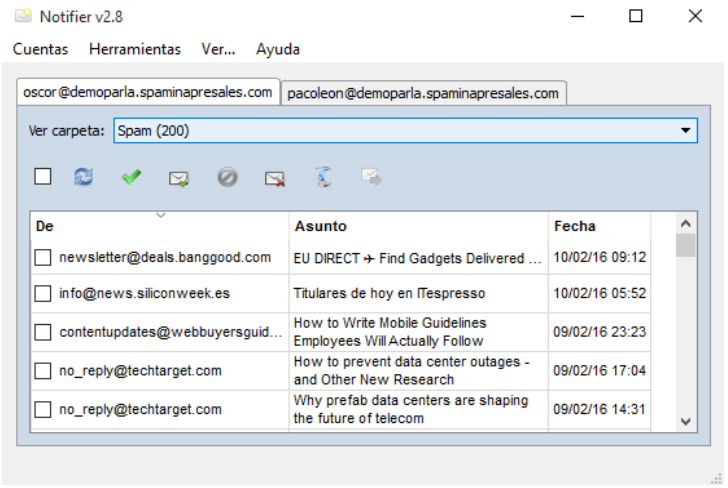


Imagen. - Desktop Notifier

3.1.10. INTEGRACIÓN CON OUTLOOK

Por medio del Add-in de Outlook [4], el usuario puede modificar sus preferencias de filtrado directamente desde su cliente de escritorio Microsoft Outlook™, permitiendo definir su nivel de filtrado, listas blancas y listas negras personales, así como decidir sobre ciertos criterios de filtrado como las notificaciones de virus, avisos de servidor, etc. Esto permite a los usuarios poder interactuar con su solución de seguridad de filtrado de correo directamente desde el mismo gestor que utilizan para acceder a su correo corporativo.

4 Outlook 2007 / 2010 / 2013 / 2016.

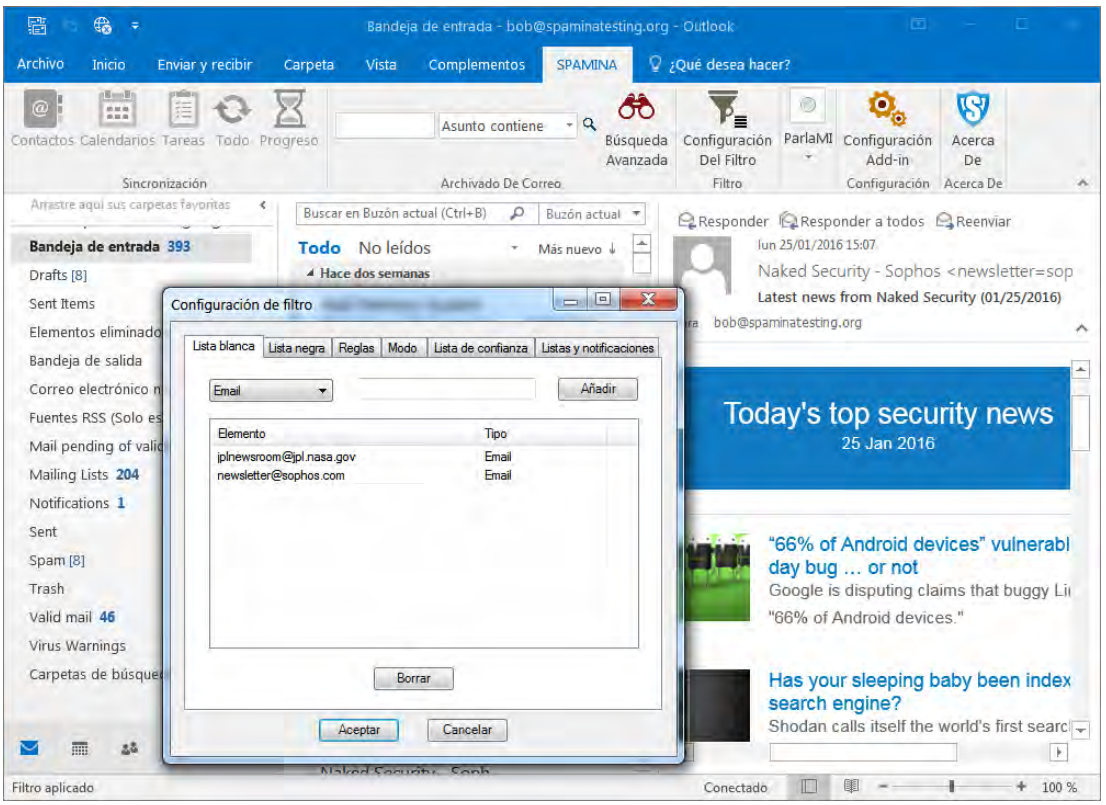


Imagen. – Add-In de CEF para **Microsoft Outlook ™**

3.1.11. LICENCIAMIENTO

La solución Cloud Email Firewall se licencia por usuario al que se le brinda la protección de correo entrante y saliente. Una licencia de Cloud Email Firewall incluye las siguientes características técnicas para cada usuario licenciado:

- Protección de correo entrante y saliente para el usuario.
- Filtrado de correo saliente.
- Motores antimalware (2).
- Continuidad de negocio, incluyendo:
  - Backup de correo entrante (5 días).
  - Encolado de correo entrante (4 días).
  - Interfaz webmail de emergencia.
- 5 direcciones de correo alternativas (alias), incluidas en la licencia sin coste adicional. Direcciones de correo alternativas consumirán una licencia adicional cada una a partir de la 5ª.

En caso de requerir la licencia adicional 'Advanced Threat Protection', se puede licenciar para toda la organización, dominios o usuarios específicos.

3.2. CLOUD EMAIL ARCHIVING

Es una solución de archivado y administración segura del correo electrónico, desarrollada para proporcionar un almacenamiento libre de posibles modificaciones de los correos y otorgando acceso inmediato a los correos ayudando a cumplir tanto normativas internas de las empresas como legales.

El correo electrónico es una herramienta estratégica para las organizaciones que debe ser protegida. Existen regulaciones legales que indican que el correo electrónico debe ser almacenado durante cierto tiempo y un sistema de archivo de correos ayuda a reducir problemas de almacenamiento en el servidor final de correo que facilita el acceso a la información a través de búsquedas ágiles y dirigidas.

El archivado del correo electrónico debe cumplir con una serie de requisitos clave, incluyendo la disposición legal, cumplimiento normativo y la garantía de tener siempre los emails originales de la organización y que sean accesibles en el momento.

Un servicio de archivado de correo electrónico debe cumplir todos estos requisitos y, además, facilitar que los departamentos de TI puedan reducir tanto costes como complejidad en la gestión de grandes volúmenes de datos, tanto en los sistemas administrados como en los sistemas que están fuera del control directo del TI.

Cloud Email Archiving guarda y mantiene los correos originales de la empresa hasta 10 años, para su búsqueda y recuperación inmediata ante requerimientos legales y consultas. Los usuarios y administradores tienen acceso directo a la búsqueda de una forma sencilla e intuitiva, desde su panel de control.

ARCHIVADO Y CUMPLIMIENTO NORMATIVAS

El archivado del correo electrónico debe cumplir con una serie de requisitos clave, incluyendo la disposición legal, cumplimiento normativo y la optimización del almacenamiento del correo electrónico dentro de las organizaciones. Para estar preparados para reclamaciones de ámbito legal y cambios en las leyes, las empresas deben conocer donde se encuentran almacenados los datos al mismo tiempo que deben ser capaces de reunir datos, buscar y recupéralos en un breve espacio de tiempo. Las empresas también deben tener la capacidad de hacer que se cumplan las políticas con los requisitos legales específicos de cada país y que se ajusten a los criterios corporativos de cada organización. Cuando se realiza inadecuadamente, la exposición a los riesgos legales y de incumplimiento normativo puede convertirse en un asunto grave para las organizaciones. Esto puede llevar a elevadas multas, sentencias condenatorias y reputación dañada.

Un servicio de archivado de correo electrónico debe cumplir todos estos requisitos además facilitar que los departamentos de TI puedan reducir tanto costes como complejidad en la gestión de grandes volúmenes de datos, tanto en los sistemas administrados como en los sistemas que están fuera del control directo del TI. Cloud Email Archiving integra un almacén centralizado de búsqueda que proporciona a los usuarios finales un acceso a la información almacenada histórica que aporta una solución integral a todas las necesidades corporativas.

AUDITORIA Y CUMPLIMIENTO LEGAL

Cloud Email Archiving proporciona una herramienta integral de auditoría y cumplimiento legal para las empresas. Con un nivel de acceso jerárquico basado en roles, ofrece a administradores y a auditores, todos los registros de acceso de actividad y además garantiza que los emails no son modificables mediante la firma de su cabecera y la recuperación intacta.

El archivado del correo electrónico garantiza el cumplimiento normativo de regulaciones europeas e internacionales sobre protección y tratamiento de los datos personales y de los servicios digitales en la nube, como son LOPD (España), PCI, DSS, HIPAA, FINRA, Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP de México), LEY 25.326. Protección de los Datos Personales (ARGENTINA), Ley estatutaria 1581 de 2012 y Decreto 1377 (COLOMBIA), y otras otras de ámbito legal. Cloud Email Archiving conserva los correos electrónicos protegidos para posibles futuros litigios legales, investigación interna o conflicto laboral.

CONSOLA DE ADMINITRADOR Y USUARIO

- Consola Administrador: SPAMINA ofrece una consola unificada que permitir a los administradores supervisar de forma global el archivado del email, facilitando un control de distintos dominios, la posibilidad de ejecutar auditorias y profundizar en la información a nivel de usuario de forma instantánea. El administrador podrá ver una imagen segmentada o completa del repositorio de Email y hacer seguimiento de cualquier correo accediendo al archivo global

- Consola de Usuario: Los usuarios necesitan acceso rápido y sencillo a correos electrónicos independientemente de que sean recientes o con varios años de antigüedad. Cloud Email Archiving ofrece a los usuarios una consola que no requiere aprendizaje alguno y proporciona buscador avanzado con múltiples opciones de filtrado sobre los correos electrónicos archivados.

FÁCIL DE USAR CON RESULTADOS INSTANTÁNEOS

Con una interfaz muy intuitiva en las búsquedas, configuración de las políticas, informes de tráfico y la gestión, Cloud Email Archiving destaca de forma considerable por no necesitar de ninguna curva de aprendizaje permitiendo que los administradores queden totalmente liberados en el uso diario de los usuarios. Cloud Email Archiving ha sido desarrollado para proporcionar una búsqueda en tiempo real a través de toda la organización, para poder dar una respuesta inmediata a cualquier petición se optó por el rediseño integral de la arquitectura de archivado lo cual ha sentado las bases para una operativa extremadamente optimizada y escalable.

3.2.1. CARACTERISTICAS CLAVE

Cloud Email Archiving es una solución que proporciona todos los medios necesarios para capturar, indexar, almacenar, buscar y recuperar rápidamente el correo entrante, saliente e interno de su organización, así como los archivos adjuntos de dichos correos.

Cloud Email Archiving proporciona a la empresa las siguientes funcionalidades clave:

- Privacidad de datos. El servicio de archivado de correos Cloud Email Archiving ofrecido desde la nube de Spamina cumple con la exigente normativa de la Unión Europea en materia de protección de datos, ayudando a su empresa a mantener la máxima seguridad. El almacenado de correos electrónicos se realiza únicamente en Centros de Proceso de Datos dónde la legislación establecida garantiza la privacidad de datos de nuestros clientes.

- Salvaguarda y cumplimiento legal. La legislación en algunos países establece los correos electrónicos como una fuente de datos que debe conservarse durante diferentes períodos de tiempo en el caso de que tal información sea requerida en un tribunal de justicia.
- Archivado inmutable del correo entrante, saliente e interno de su organización por un periodo de hasta 10 años.
- Búsqueda y localización de correos en el archivo utilizando distintos criterios, incluyendo información contenida dentro de archivos adjuntos.
- Almacenamiento de correo con espacio virtualmente ilimitado [5].
- Auditoría de acciones: Registro de acciones realizadas sobre el archivo tanto por administradores como por los usuarios finales de su organización.
- Importación de correos desde repositorios de correo en formato estándar.
- Exportación de correos del archivo en formatos estándar que preservan la integridad del correo, incluyendo sus cabeceras (MBOX, EML).
- Interacción con gran variedad de servidores estándar [6].
- Informes de uso del archivo y dashboard de actividad.
- Integración con Outlook para la realización de búsquedas [7].

3.2.2. BENEFICIOS

- Puede ser contratado junto a otros servicios de Spamina o de forma independiente.
- Almacenamiento de todo el correo de su organización, entrante saliente e interno.
- Ayuda al cumplimiento de normativas legales e internas de su organización.
- Permite el acceso y recuperación de correos antiguos, a aquellos que hayan sido eliminados por los usuarios de sus respectivos buzones e incluso a correos de buzones que ya no existan en su organización siempre y cuando se hubiera tenido el servicio de archivado activo con anterioridad.
- Reducción de problemas de almacenamiento en el servidor final de correo.
- Permite a su organización auditar y presentar ante un posible contencioso legal los correos electrónicos de los empleados o proveedores.
- Permite a administradores y organizaciones auditar las acciones realizadas sobre los correos del archivo.
- Presentación de estadísticas de uso, volumen de correo archivado y otra información de interés para los administradores.
- Crecimiento virtualmente ilimitado del servicio de archivado de correo para su organización.
- Búsquedas complejas que permite tanto a los administradores como usuarios finales la creación filtros de búsqueda dirigidas, combinando operadores lógicos (AND, OR) en varios grupos de condiciones.
- Capacidad para reconocer los destinatarios en copia oculta en sistemas de intercambio [8].

[5] El almacenamiento del servicio CEA está sujeto a una cláusula de uso justo del servicio y comprende un máximo de 5 GB de almacenamiento por usuario final y año de servicio.

[6] Pueden ser requeridas funcionalidades de Journaling en el servidor de correo del cliente.

[7] Requiere la instalación de un Add-in, disponible para Outlook 2007 / 2010 / 2013 / 2016.

[8] Se reconoce correctamente destinatarios en copia oculta en la importación de correos desde repositorios estándar, no en el flujo de correo entrante / saliente.

- Facilidad de integración, siendo transparente la implantación si el servicio de archivado se contrata como un módulo adicional al servicio de protección de correo CEF [9] o junto con el buzón seguro en la nube Parla Mailbox [10].

3.2.3. ADMINISTRACION

- Portal único para la administración de la solución, integrado junto con el resto de consolas de gestión de los productos de Spamina.
- Conexión segura para administradores y usuarios.
- Configuración por empresa y dominio del conector IMAP para el archivado de correo desde buzones de Journaling.
- Auditoria de accesos y actividad por parte del administrador.
- Auditoría de acciones que informa sobre las actividades y acciones de los usuarios finales del servicio: Log-in, búsquedas, vistas de datos o cambios, exportaciones y mucha más información que se registra y es auditable.
- Los usuarios de Parla Mailbox que contraen el servicio de Cloud Email Archiving pueden recuperar correos del archivo directamente en una carpeta de su buzón.
- Acceso HTTPS/SSL y tráfico cifrado TLS.

3.2.4. FUNCIONAMIENTO DEL ARCHIVADO Y RECUPERACION DE CORREOS

Cloud Email Archiving es una solución que incluye todos los medios necesarios para capturar, indexar, almacenar, buscar y recuperar rápidamente el correo entrante, saliente e interno de su organización, así como sus respectivos archivos adjuntos. El funcionamiento puede resumirse en los siguientes puntos:

- El correo entrante, saliente e interno, es indexado y almacenado en Cloud Email Archiving de Spamina. El indexado se realiza por múltiples campos, incluyendo el contenido de mensajes adjuntos.
- En caso de que se tenga contratado Cloud Email Firewall o Parla Mailbox, el correo entrante a la empresa será filtrado por Cloud Email Firewall, y posteriormente se almacenará una copia de cada correo válido en el archivo. No se almacenará el correo clasificado como Spam.

[9] El archivado de correo interno de la organización cuando se contrata el servicio CEF requiere de la configuración de buzones de Journaling en Microsoft Exchange ™.

[10] La integración de CEA con el servicio de buzón en la nube es completamente transparente y no requiere de configuraciones adicionales en la infraestructura del cliente para poder realizar el archivado de correo entrante, saliente e interno de la organización.

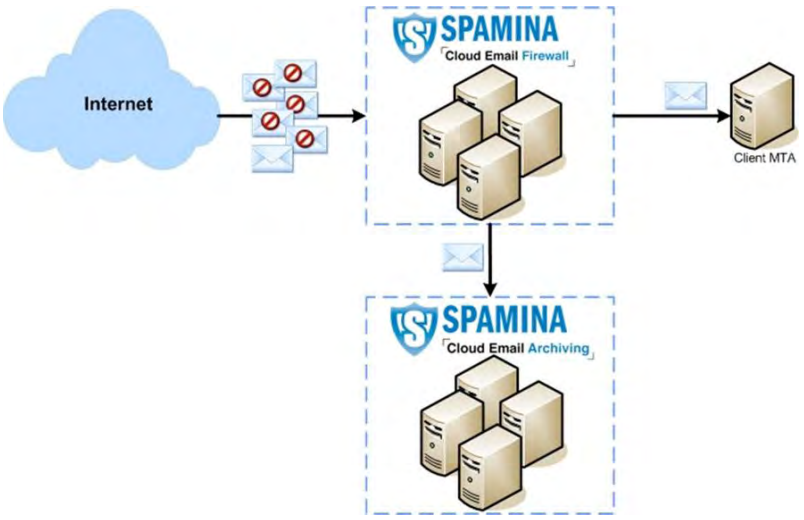


Imagen. – Integración de archivado de correo entrante del servicio CEA con CEF

- En caso de que se tenga contratado Cloud Email Firewall, el correo saliente de la empresa será filtrado por Cloud Email Firewall y posteriormente se almacenará una copia de cada correo válido en el archivo. No se almacenarán correos salientes que hubieran sido rechazados por de filtrado saliente de CEF.

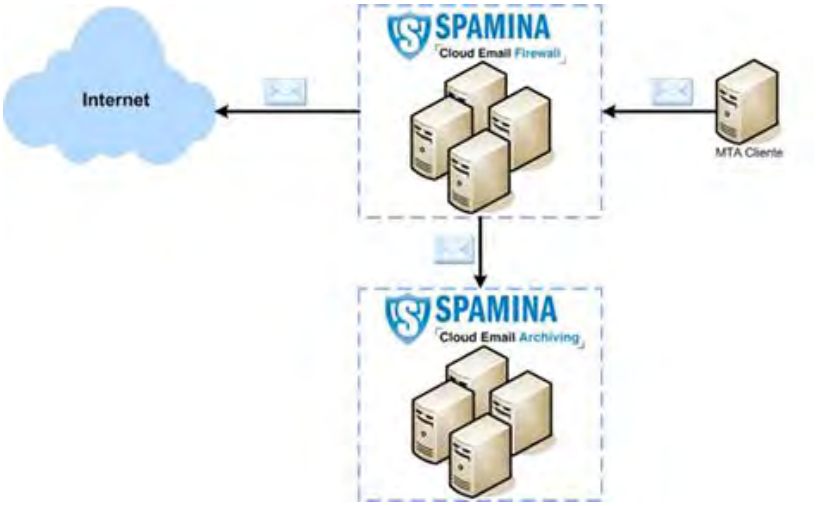


Imagen. – Integración de archivado de correo saliente del servicio CEA con CEF

- Tanto si se quiere archivar correo interno de la empresa como si se hubiera contratado el servicio de archivado sin Cloud Email Firewall o Parla Mailbox, se puede realizar el archivado de estos correos utilizando un buzón de Journaling en el servidor Microsoft Exchange ™ de correo de la empresa que contrata el servicio de archivado.

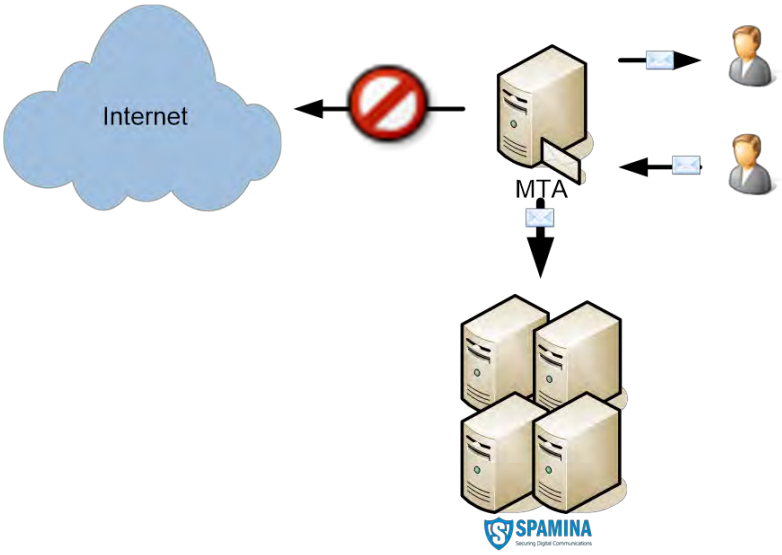


Imagen. – Integración de archivado de correo para correo interno

- Una vez archivado el correo, el periodo máximo de retención de ese correo será de 10 años, trascurrido ese tiempo el correo será eliminado del sistema de archivo.
- Tanto administradores como usuarios finales pueden realizar búsquedas en el archivo utilizando la consola de gestión unificada de los productos de Spamina.
- Los usuarios finales del servicio que utilicen Microsoft Outlook ™ como cliente de correo pueden realizar búsquedas y recuperar los correos utilizando el add-in de Spamina [11].
- Permite realizar consultas por diversos criterios (rangos de fechas de envío y recepción, remitentes, destinatarios, asunto, contenido de los correos y contenido de los adjuntos de los correos). Asimismo, los resultados obtenidos pueden ser exportados o reenviados a una cuenta de correo indicada por el administrador o los usuarios finales.

3.2.5. AUDITORIA DE ACCIONES

Debido al cumplimiento de normativas, su organización puede requerir dejar registro de todas las acciones de revisión de datos y configuración que se realizan en la plataforma. Esto es de especial importancia cuando los administradores tienen acceso a una herramienta tan sensible como es un sistema de archivado de toda la comunicación por correo de su corporación como puede ser Cloud Email Archiving.

Toda acción realizada sobre el archivo por los administradores o usuarios finales de la solución queda reflejada en el log de auditoría, que es posteriormente consultable por los administradores de la solución. El log de auditoría de Spamina permite localizar los distintos tipos de acciones realizados sobre el sistema de archivado:

- Búsquedas en el sistema de archivo.

11 Outlook 2007 / 2010 / 2013 / 2016

- Reenvío de mensajes.
- Descarga de adjuntos.
- Visualización de mensajes en el archivo.

3.2.6. INTEGRACION CON OUTLOOK

Por medio del Add-in de Outlook [10], el usuario puede realizar consultas a su correo archivado y gestionar los resultados obtenidos desde ese cliente de correo.

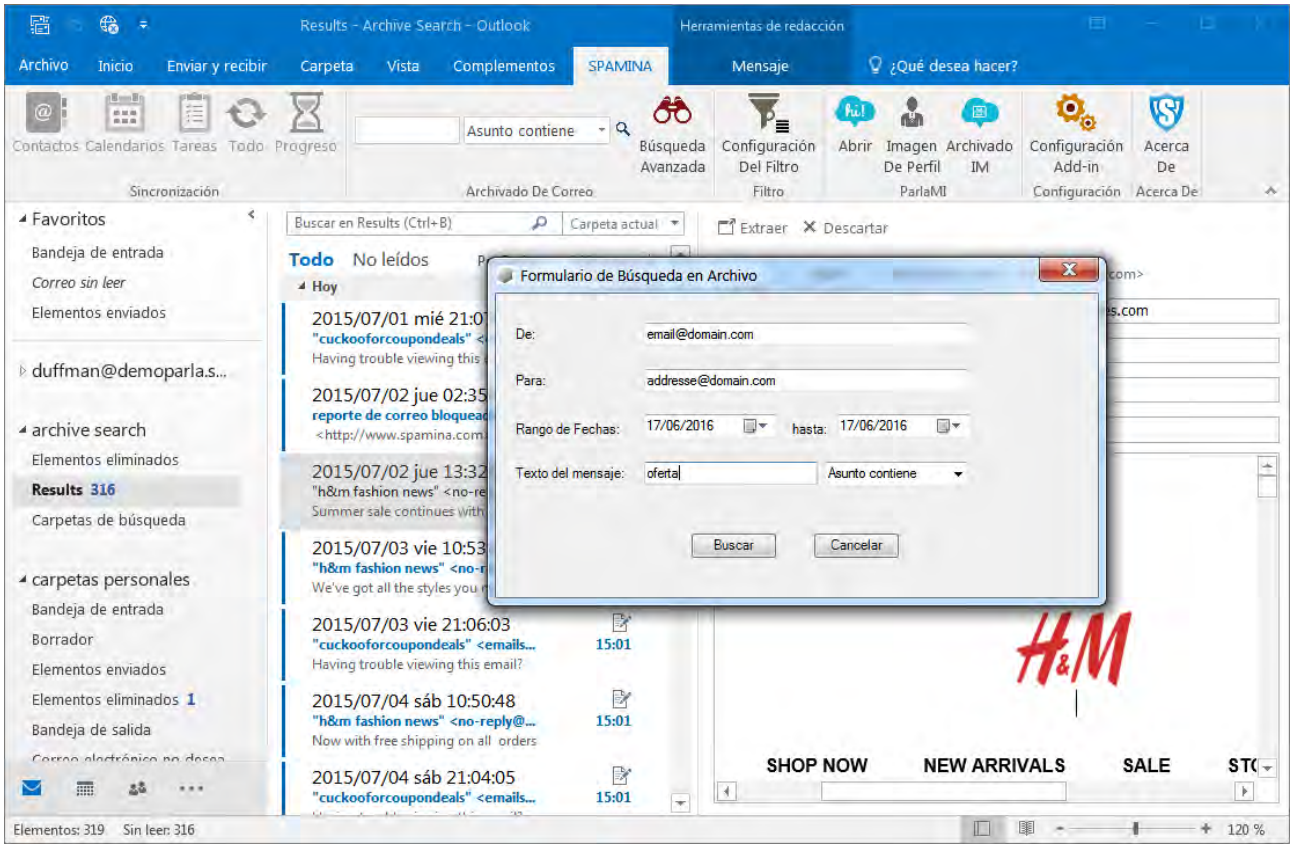


Imagen. – Add-**In de CEA para Microsoft Outlook ™**

El usuario final puede realizar búsquedas y recuperar correos desde su archivo directamente utilizando el cliente de correo Microsoft Outlook ™ sin necesidad de entrar en consolas de gestión de la plataforma.

3.2.7. LICENCIAMIENTO

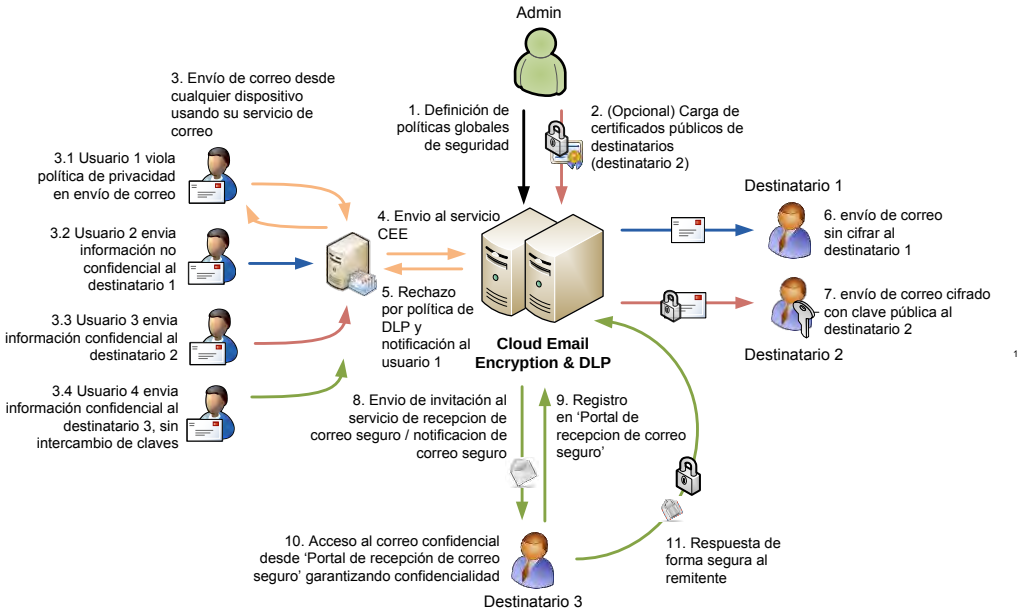
La solución Cloud Email Archiving se licencia por usuario de la organización del que se quiere archivar su correo. Una licencia de Cloud Email Archiving incluye las siguientes características técnicas para cada usuario licenciado:

- Archivado de correo entrante, saliente e interno.
- 5 direcciones de correo alternativas (alias), incluidas en la licencia sin coste adicional. Direcciones de correo alternativas consumirán una licencia adicional cada una a partir de la 5ª dirección de correo alternativa.

- Espacio de almacenamiento virtualmente ilimitado [12]

Existe la posibilidad de importar datos que el cliente ya tuviera en formatos estándar al sistema de archivado. Dicho proceso de ingestión de datos se realizará off-line por parte de Spamina y está sujeto a costes adicionales.

Por otra parte, si el cliente quiere finalizar el servicio con Spamina, podrá solicitar la exportación de su archivo. Este proceso será realizado off-line por parte de Spamina y está sujeto a costes adicionales.



[12] Cada licencia tiene asociada una cláusula de uso justo del servicio que incluye 5GB por usuario y año de servicio de archivado.

4. PARLA SECURE CLOUD EMAIL

Parla es una plataforma segura de comunicación para empresas basada en la nube, ideal tanto para empresas pequeñas como organizaciones grandes hasta con decenas de miles de cuentas gracias a su sistema de aprovisionamiento escalable. Parla proporciona un entorno de correo electrónico, mensajería instantánea y de colaboración totalmente integrado con las capas de seguridad que protegen a los empleados del spam, malware y otras posibles amenazas externas.

Parla funciona en cualquier ordenador o dispositivo móvil con conexión de datos; ya sea en la oficina, en una reunión o viajando su correo electrónico estará siempre disponible. Al correo electrónico ofrecido por Parla mailbox se puede acceder con los clientes locales como Outlook, desde cualquier dispositivo móvil (iOS, Android y Windows Mobile) así como a través de cualquier navegador. La plataforma de Webmail permite gestionar el correo electrónico, calendario, administrar documentos, tareas, compartir cuentas de correo entre usuarios. Parla usa la tecnología Cloud Email Firewall de Spamina que permiten identificar los patrones de Spam a tiempo real y bloquear su entrada, dejando almacenado cualquier tipo de malware en la nube de Spamina.

Parla es un ecosistema de productos que incluye:

- Parla Mailbox: Correo electrónico seguro en la nube con capacidad del buzón de hasta 30GB, con capa de seguridad integrada.
- ParlaMI: La mensajería instantánea segura para empresas. Sobre este servicio se ofrece también:
- IM Archiving: Archivado de mensajería instantánea.
- IM Firewall: Capa extra de seguridad para la protección frente a malware y URLS maliciosas.
- Mobile Device Management: Gestión de dispositivos móviles.
- Cloud Email Archiving: Integración con el servicio de archivado de correo.
- Cloud Email Encyption: Integración con servicio de cifrado de email.

Tipos de Usuarios

Parla Secure Cloud Email	Parla 2	Parla 10	Parla 30
Tamaño de Buzón	2 Gb	10 Gb	30 Gb
Webmail	✓	✓	✓
Contactos	✓	✓	✓
Calendario	✓	✓	✓
Tareas	✓	✓	✓
Notas	✓	✓	✓
Marcadores	✓	✓	✓
Soporte IMAP/S POP3	✓	✓	✓

Parla	Parla 2	Parla 10	Parla 30
Smartphone /Tablet Sync (iOS, Android, BB, Windows mobile)	✓	✓	✓
Gestión de Filtrado de Correo Saliente	✓	✓	✓
Cloud Email Firewall (Antispam, Anti*malware*, Antiphshing..)	✓	✓	✓
Compartición de Archivos en la nube	✓	✓	✓
Mensajería Instantánea (ParlaMI)	✓	✓	✓
Gestión de Dispositivos Móviles,MDM (Opcional)	✓	✓	✓
Integración Outlook (contactos, calendarios, tareas)		✓	✓

4.1. PARLA MAILBOX

Parla Mailbox ofrece un servicio de correo electrónico corporativo basado en la nube con hasta 30GB de almacenamiento. La plataforma Webmail permite gestionar el correo electrónico desde cualquier ordenador o dispositivo móvil, conexión directa con calendario, administrar documentos, tareas, compartir documentos.

Los usuarios de Parla Mailbox pueden acceder a su correo con los clientes locales como Outlook (2007, 2010, 2013 y 2016), desde cualquier dispositivo móvil (iOS, Android y Windows Phone), a través de cualquier navegador o utilizando cualquier otro cliente de correo estándar gracias al amplio abanico de protocolos estándar soportados: POP3, IMAP, SMTP, CalDAV, CardDAV, ActiveSync, etc.

Parla Mailbox está disponible en versión de 2GB, 10GB y 30GB.

4.1.1. CARACTERISTICAS CLAVE

Parla Mailbox funciona en cualquier ordenador o dispositivo móvil con conexión de datos, permitiendo además de seguir trabajando incluso cuando está desconectado. Estará siempre disponible ya sea en la oficina, en una reunión o viajando su correo electrónico.

A continuación se expone un resumen de las características clave principales de Parla Mailbox:

- Privacidad de datos. El servicio de correo electrónico en nube Parla Mailbox ofrecido desde la nube de Spamina cumple con la exigente normativa de la Unión Europea en materia de protección de datos, ayudando a su empresa a mantener la máxima seguridad. El almacenado de correos electrónicos se realiza únicamente en Centros de Proceso de Datos dónde la legislación establecida garantiza la privacidad de datos de nuestros clientes.

- Incluye el Sistema de seguridad integrado Cloud Email Firewall (CEF) para correo entrante y saliente: Incluyendo filtros de conexión, antivirus, antispam y anti-*malware*, y análisis con patrones heurísticos & bayesianos y propios Spamina (SFF® v2.0).
- Calendarios, contactos, tareas, notas, gestor de ficheros y entorno de colaboración incorporados en el buzón, permitiendo a los usuarios de su organización el acceso a estos elementos desde cualquier lugar y dispositivo.
- Add-in Outlook: integración con Outlook 2007/2010/2013/2016.
- Solución de mensajería instantánea segura y video conferencia: Parla Mailbox incluye ParlaMI, una solución de mensajería segura para la empresa, que incluye aplicación para moviles IOS y Android.
- Integración nativa con Apple IOS, Windows Phone o Android: Sincronice el correo, calendarios, contactos y tareas en cualquier Smartphone mediante el protocolo ActiveSync.
- Sincronización con clientes de correo estándar: Parla Mailbox soporta un amplio abanico de protocolos (POP3 / IMAP / iCal / CalDAV / CardDAV, SyncML) aportando compatibilidad con cualquier cliente de correo estándar.
- Motor de políticas para cumplimiento de normativas y control del correo entrante y saliente.
- Informes y seguimiento del correo entrante y saliente de su organización a través de la consola unificada de seguridad de la plataforma Parla.
- Sincronización con Active Directory mediante un agente PUSH, posibilitando la sincronización de contraseñas para Single Sign On.
- Ampliación del buzón y la mensajería con otros servicios adicionales, como Cloud Email Archiving, Cloud Email Encryption, IM Archiving, IM Firewall y Mobile Device Management, tanto para todos los buzones de su organización como para usuarios individuales.

4.1.2. WEBMAIL

Parla Mailbox proporciona una completa interfaz webmail que hace innecesario el despliegue de clientes de correo en los usuarios finales de su organización:

La interfaz Webmail de Parla Mailbox incluye las siguientes funcionalidades:

- Vista optimizada para dispositivos con pantalla reducida: Smartphone, Ipad / Tablet.
- Vista de Escritorio con AJAX dinámico.
- Completamente integrado con la consola de administración de Cloud Email Security.
- Interfaz tipo Drag & Drop.
- Correo electrónico completo, con entorno de colaboración de archivos, tareas, además de muchas características adicionales.

La potente interfaz webmail de Parla Mailbox incluye las siguientes funcionalidades:

Calendarios:

- Posibilidad de compartir Calendarios con otros miembros de Parla Mailbox
- Acceso remoto a Calendarios
- Soporta CalDAV & iTip / iCalendar
- Visualización del estado de los asistentes (disponible/ocupado)
- Sincronización de calendarios over-the-air con dispositivos móviles

Contactos:

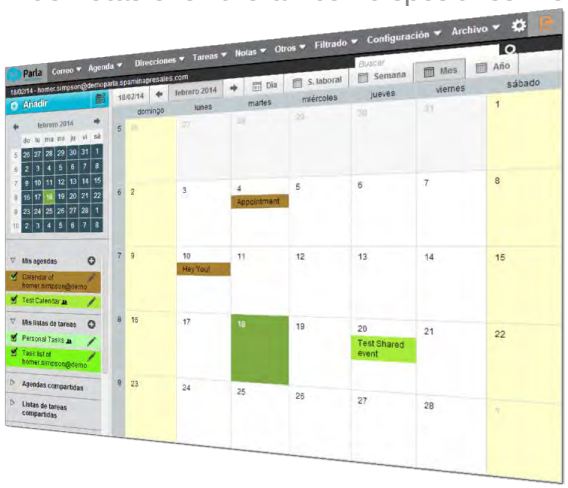
- Soporta importación y exportación de CSV, TSV & vCard
- Listas de distribución
- Posibilidad de compartir contactos
- Compatibilidad con CardDAV
- Búsquedas en libreta global de direcciones de su organización
- Asistente de búsqueda de contactos duplicados
- Sincronización de contactos over-the-air con dispositivos móviles

Tareas:

- Soporta importación/exportación CSV / iCalendar
- Visualización por estados
- Asignación de tareas a otros usuarios de la organización y seguimiento de progreso
- Búsqueda avanzada de tareas
- Posibilidad de compartir tareas
- Sincronización de tareas over-the-air con dispositivos móviles

Notas:

- Soporta importación CSV y vNote.
- Soporte exportación CSV y PDF
- Posibilidad de compartir notas
- Búsqueda por título y contenido en las notas
- Sincronización de notas over-the-air con dispositivos móviles



4.1.3. CALENDARIO, CONTACTOS Y ENTORNO COLABORATIVO

Parla Mailbox permite a los usuarios de su organización administrar fácilmente los contactos y múltiples libretas de direcciones con otros usuarios, crear eventos repetidos en el calendario, establecer etiquetas y compartir calendarios, crear y compartir notas con otros usuarios, comprobar la disponibilidad de usuarios de cara a convocatorias de reunión e incluso compartir un buzón o carpetas concretas de un buzón con otros usuarios. Todo ello desde la interfaz Webmail incluida en Parla o mediante Microsoft Outlook™ [13].

Parla Mailbox permite establecer distintos privilegios de acceso cuando se comparten los elementos. De esta forma, se pueden otorgar permisos de visualización, lectura o escritura sobre calendarios, libretas de direcciones, buzones o carpetas dentro de un buzón, así como notas.

[13] Add-In de Outlook disponible para 2007 / 2010 / 2013 y 2016.

Para facilitar la tarea de administración, se incluye el concepto de grupos. De esta forma los administradores pueden compartir fácilmente cualquier recurso perteneciente a algún buzón de la organización con extensas áreas o grupos de usuarios dentro de la organización.

4.2. INTEGRACION CON CLIENTES DE COREO ESTANDAR

Parla funciona en cualquier ordenador o dispositivo móvil con conexión de datos y además de permitir seguir trabajando incluso cuando no se está desconectado utilizando una gran variedad de clientes de correo. Ya sea en la oficina, en una reunión o viajando su correo electrónico estará siempre disponible. Al correo electrónico se puede acceder con los clientes locales como Outlook, así como los dispositivos iOS y Android. Además, los empleados pueden iniciar sesión en nuestra completa plataforma de Webmail donde podrá gestionar el correo electrónico, colaboración, administrar documentos y realizar muchas más funciones.

Spamina Mailbox soporta una gran variedad de protocolos que le permiten interactuar con el buzón de correo en la nube y sincronizar todos los elementos. Entre los protocolos de comunicación que soporta Spamina Mailbox se encuentran:

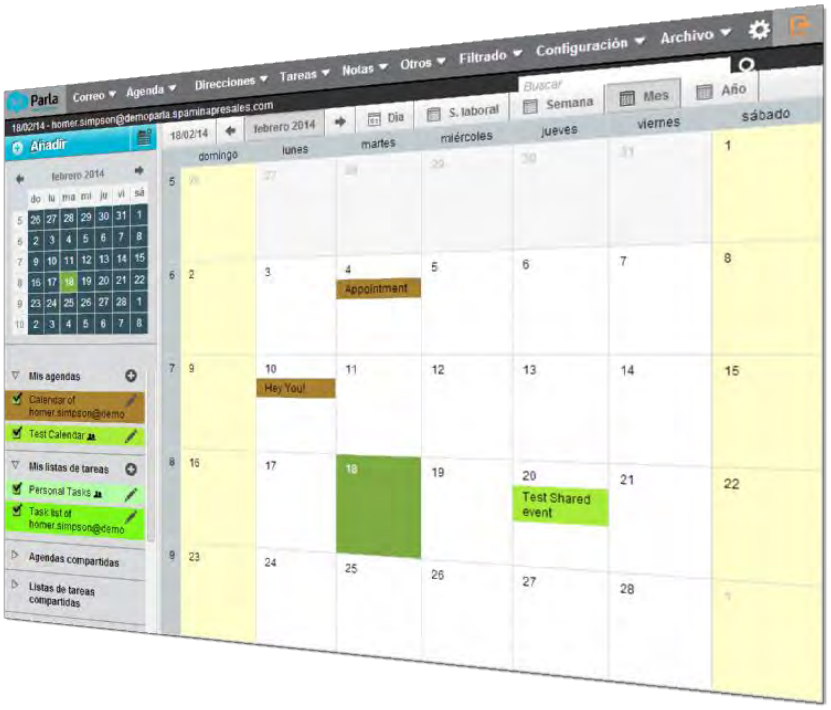
- POP3 y POP3/S
- IMAP e IMAP/S
- SMTP y SMTPS
- ActiveSync
- CalDAV
- CardDAV

4.3. CALENDARIO, CONTACTOS Y ENTORNO COLABORATIVO

Administre fácilmente sus contactos, comparta la libreta de direcciones con otros usuarios, cree la repetición de eventos en el calendario, establezca etiquetas y comparta calendarios, cree y comparta notas, compruebe el estado disponible / ocupado de los usuarios y gestione libreta de direcciones, administrador de tareas y el módulo de notas.

Manténgase organizado y al día con el calendario, reciba recordatorios de los eventos, tenga una visión rápida y sencilla de sus reuniones con nuestra interfaz fácil de usar. Adjunte archivos o documentos a su evento y así tendrá el material adecuado para cuando su reunión comience y fácilmente invite a otros miembros a futuras reuniones.

Compartir el calendario hace que sea mucho más fácil encontrar tiempo con la gente que trabaja y ayuda a los empleados a ser más productivos eliminando barreras de organización



La potente interfaz webmail de Parla Mailbox incluye las siguientes funcionalidades:

Calendarios:

- Posibilidad de compartir Calendarios con otros miembros de Parla Mailbox
- Acceso remoto a Calendarios
- Soporta CalDAV & iTip / iCalendar
- Visualización del estado de los asistentes (disponible/ocupado)
- Sincronización de calendarios over-the-air con dispositivos móviles

Contactos:

- Soporta importación y exportación de CSV, TSV & vCard
- Listas de distribución
- Posibilidad de compartir contactos
- Compatibilidad con CardDAV
- Búsquedas en libreta global de direcciones de su organización
- Asistente de búsqueda de contactos duplicados
- Sincronización de contactos over-the-air con dispositivos móviles

Tareas:

- Soporta importación/exportación CSV / iCalendar
- Visualización por estados

- Asignación de tareas a otros usuarios de la organización y seguimiento de progreso
- Búsqueda avanzada de tareas
- Posibilidad de compartir tareas
- Sincronización de tareas over-the-air con dispositivos móviles

Notas:

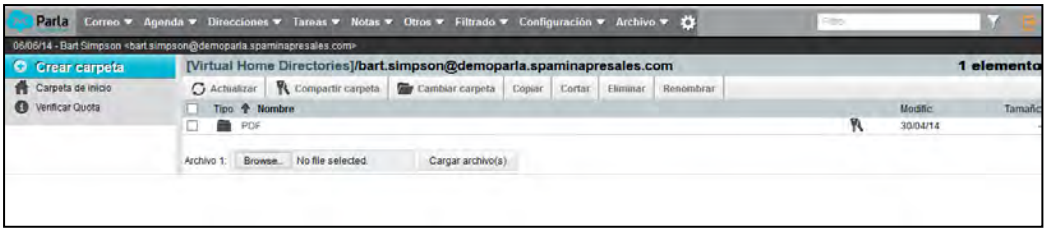
- Soporta importación CSV y vNote.
- Soporte exportación CSV y PDF
- Posibilidad de compartir notas
- Búsqueda por título y contenido en las notas
- Sincronización de notas over-the-air con dispositivos móviles

Compartición de Buzones:

- Posibilidad de compartir carpetas dentro de nuestro buzón, con otros usuarios del mismo dominio
- Acceso remoto a carpetas de otros usuarios
- Tres niveles de acceso personalizables por usuario: Leer, Insertar y Enviar
- Visualización de las carpetas o buzones desde el cliente de correo (Outlook, Thunderbird,...)
- Sincronización con Outlook, permitiendo trabajar con ellas igual que desde el webmail

4.4. GESTOR DE ARCHIVOS

Un gestor de documentos integrado de Parla que elimina la necesidad de tener herramientas de gestión de documentos por separado. Agiliza el proceso de compartir archivos por email, reduce el uso de la red corporativa y ahorra espacio de almacenamiento, a las compañías.



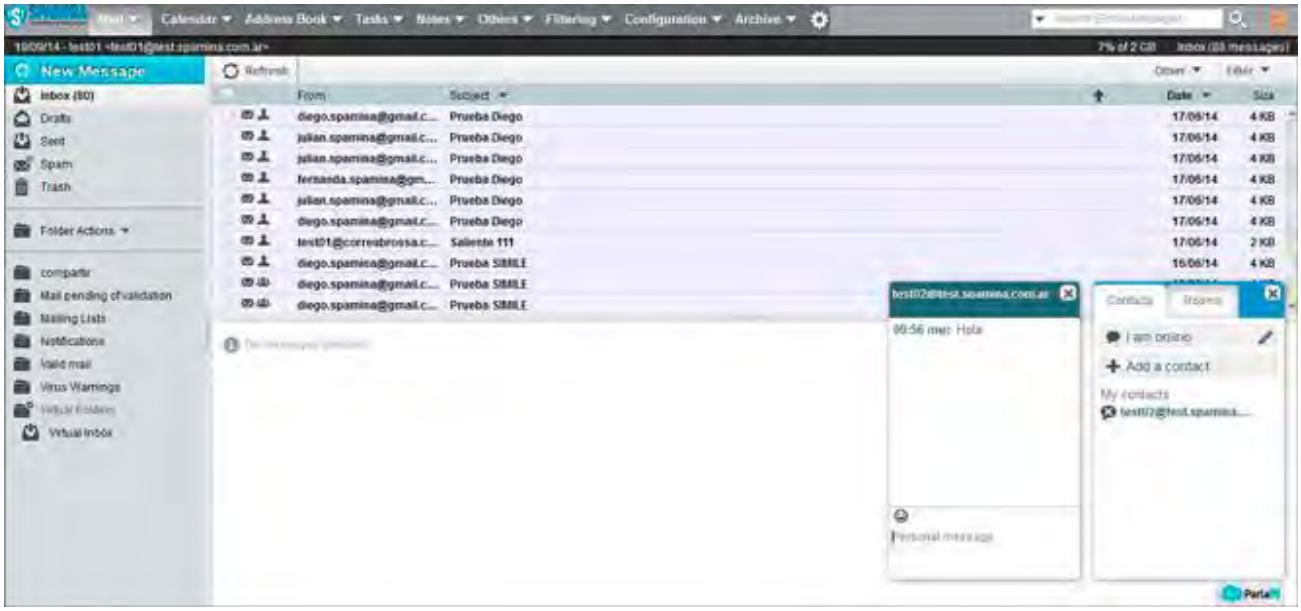
Con el gestor de archivos se pueden compartir carpetas entre usuarios y cargar varios archivos de cualquier tipo con un solo paso desde el escritorio. El gestor de archivos identificará cada tipo de archivo función del tipo de archivo subido, y proporcionará automáticamente un icono asociado en función del tipo de archivo.

4.5. SERVICIO DE MENSAJERIA INSTANTANEA (ParlaMI)

Los usuarios de Parla Mailbox disponen de un servicio de mensajería instantánea, denominado ParlaMI, que permite la comunicación en tiempo real entre miembros individuales, grupos privados, con usuarios externos o entre distintos dominios siempre que alguno sea usuario del servicio de correo seguro en la nube Parla. Todas estas comunicaciones de ParlaMI están protegidas para garantizar la seguridad en las comunicaciones.

Cuando un usuario de Parla comienza una sesión en la interfaz webmail, automáticamente aparece en su pantalla una pestaña que le permite acceder al servicio de chat, sin tener que salir de la aplicación del correo electrónico. Las conversaciones entre usuarios de Parla, siguen el mismo protocolo de seguridad que los correos electrónicos, y pueden ser archivadas y almacenadas en la nube de Spamina mediante la contratación de la licencia adicional *IM Archiving*.

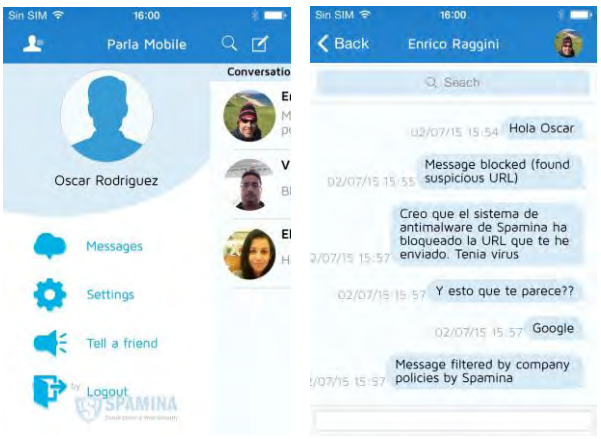
Con ParlaMI se consigue optimizar el uso del correo electrónico dentro de las organizaciones, así como favorecer la comunicación interdepartamental, siempre desde un entorno seguro y gestionable por el administrador, bajo la tecnología de Spamina.



4.5.1. APLICACIÓN PARLAMI PARA DISPOSITIVOS MOVILES (APP)

Spamina ParlaMI puede ser utilizado desde dispositivos móviles IOS y Android mediante la descarga de una App.

Esta integración permite a los usuarios mantener conversaciones individuales o grupales con el resto de usuarios de la organización cualquiera que sea su localización. De esta manera, se hace innecesario en la empresa permitir el uso de aplicaciones no corporativas para la mensajería instantánea de los empleados, devolviendo el control al departamento de IT sobre este tipo de comunicaciones corporativas.



La App permite guardar un histórico de los últimos 500 mensajes. Para poder acceder al histórico completo de mensajes será necesario contratar la licencia adicional IM Archiving para el usuario.

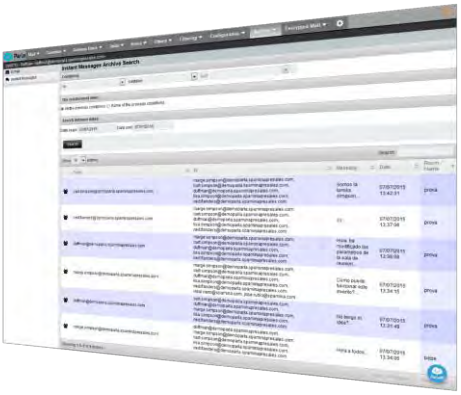
4.5.2. SERVICIO DE ARCHIVADO DE PARLAMI (IM ARCHIVING)

ParlaMI admite una licencia adicional que permite a la empresa guardar una copia de toda la mensajería instantánea realizada por sus usuarios. Tanto administradores como usuarios podrán consultar con posterioridad los mensajes archivados en el sistema.

El servicio de archivado de mensajería instantánea se encuentra integrado en todas las consolas de los usuarios:

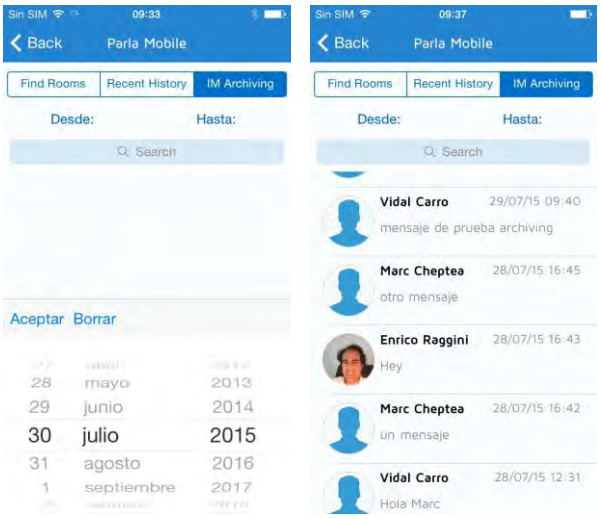
Integracion en la interfaz Parla Webmail

Cuando un usuario tiene asignadas licencias de IM Archiving, en su interfaz Webmail de parla podrá acceder a las búsquedas de los mensajes instantáneos que haya recibido o enviado, teniendo a su disposición un histórico de todas sus comunicaciones:



Integracion ParlaMI App

Cuando un usuario tiene asignadas licencias de IM Archiving podrá acceder a todo su histórico de conversaciones desde su propio dispositivo móvil, así como hacer búsquedas dirigidas que le permita localizar rápidamente las conversaciones que busque el usuario.



4.5.3. SERVICIO DE FILTRADO DE PARLAMI (IM FIREWALL)

Los usuarios de Parla Mailbox disponen de un servicio de mensajería instantánea, denominado ParlaMI, que permite la comunicación en tiempo real entre miembros individuales, grupos privados, con usuarios externos o entre distintos dominios siempre que alguno sea usuario del servicio de correo seguro en la nube Parla. Todas estas comunicaciones de ParlaMI están protegidas para garantizar la seguridad en las comunicaciones.

4.6. INTEGRACION CON OUTLOOK

Parla ofrece total compatibilidad con Microsoft Outlook, Apple Mail y otros clientes de correo POP / IMAP / SMTP, etc. Una vez integrada la nube de Spamina Parla con Microsoft Outlook, se activa una sincronización bidireccional en tiempo real de correos, contactos, tareas y calendarios.

Los empleados que disfrutan trabajando con Outlook como su cliente de email, no notarán ninguna diferencia al comprobar su correo electrónico, compartir sus calendarios o la gestión de sus tareas.

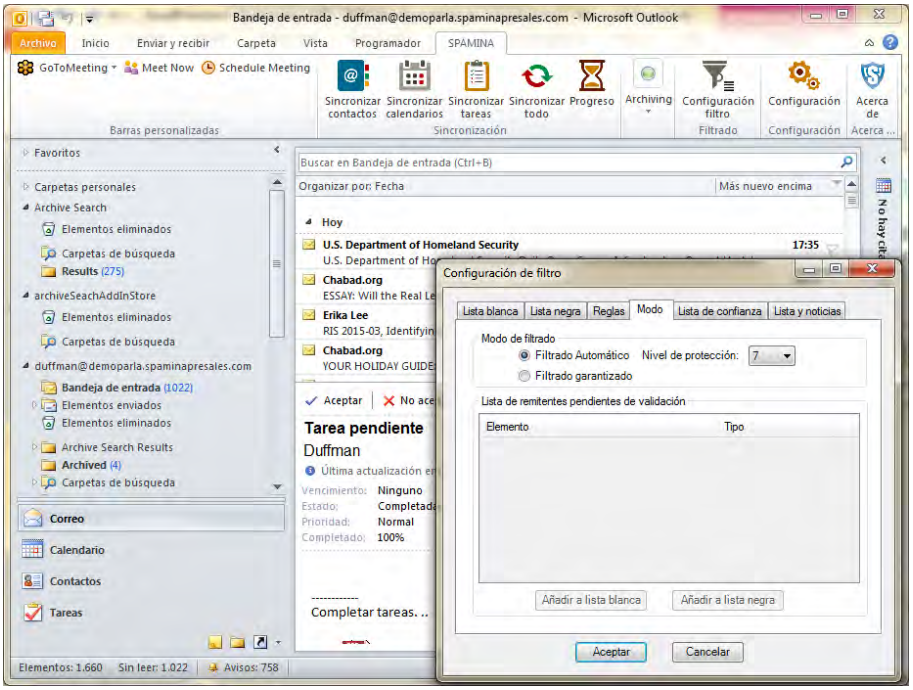
Parla añade a su compatibilidad con todos los clientes de correo, la posibilidad de integrarse directamente en la interface de Outlook, disponible para las versiones 2007/2010/2013/2016.

Para los usuarios de PARLA10 y PARLA30, se activa una sincronización bidireccional de correos, contactos, tareas y calendarios, desde Webmail a Outlook y viceversa. Los empleados que disfrutan trabajando con Outlook como su cliente de email, no notarán ninguna diferencia al comprobar su correo electrónico o gestionar de sus tareas.

Para los usuarios de PARLA2, se activa la sincronización bidireccional del correo pero no incluye la sincronización de contactos, tareas y calendarios.

Esta nueva versión permite la configuración de filtrado de datos CEF para todos los tipos de buzón (listas blancas y negras, reglas, modo de Y además:

- Instalación desatendida / silencio
- Posibilidad de personalizar por terceros (característica de marca blanca)
- Ajuste de los Intervalos de sincronización para evitar bloqueos durante búsquedas.
- Integración para Cloud Email Archiving.



4.7. INTEGRACION DE PARLA MAILBOX CON CLOUD EMAIL FIREWALL

El objetivo principal de Parla Mailbox es proporcionar a las empresas de correo electrónico seguro. El Spam sigue siendo una amenaza grave para el correo electrónico corporativo debido a que continua siendo un negocio muy rentable para los spammers, por esa razón las organizaciones exigen una protección total en la gestión del spam. Parla Mailbox incluye Cloud Email Firewall sin coste adicional, que usa tecnologías de detección patentadas para analizar billones de correos electrónicos cada día que permiten identificar los patrones de Spam a tiempo real y bloquear su entrada, eliminando cualquier tipo de *malware*, y liberando las bandejas de entrada de los buzones de correo no deseado, reteniéndolo hasta 28 días en sus correspondientes carpetas de Spam dentro del buzón.

El filtrado de Email está diseñado para la detección de mensajes de spam, *phising*, *malware* y virus usando patrones y clasificaciones avanzadas que se procesan en los centros de datos de Spamina detectando los ataques en tiempo real. Para conseguir una seguridad integral previniendo la entrada de virus, Cloud Email Firewall integra varios niveles de filtros antivirus por defecto así como la opción de añadir otras capas de filtrado como un tercer motor Antivirus Premium (también incluído con el módulo ATP) o el módulo completo de Advanced Threat Protection, mediante la contratación de licencias adicional por cada usuario/dominio o por compañía.

4.8. RESUMEN DE CARACTERISTICAS PARLA MAILBOX

La siguiente tabla resume todas las características de Parla Mailbox

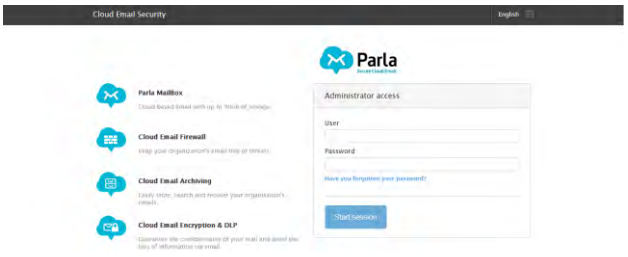
Mensajería
Buzones de correo de 1GB, 2GB, 10GB o 30GB de capacidad
Transferencia de datos ilimitada
Potente interface Webmail basada en AJAX:
✓ Opciones de seguridad de Cloud Email Firewall plenamente integradas
✓ Visualización de mensajes por conversaciones
✓ Visualización adaptada a dispositivos móviles (iPad & Tablet)
✓ Funcionalidades avanzadas de busqueda
✓ Funcionalidad Drag & Drop
✓ Multiples libretas personales y libreta global de contactos
✓ Manejo de multiples agendas simultaneamente
✓ Comprobación de estado de asistentes a reuniones (disponible / ocupado)
✓ Visualización de tareas por estados
✓ Búsqueda avanzada de tareas y notas
✓ Almacenamiento y administración de Bookmarks
✓ Visor de Archivos integrado
Acceso a correos clasificados como Spam directamente desde el buzón de correo
Servicio de correo basado en la nube: No requiere la instalación de hardware dedicado
Soporte de listas de distribución corporativas
Servicio de Mensajería Instantánea, **ParlaMI**

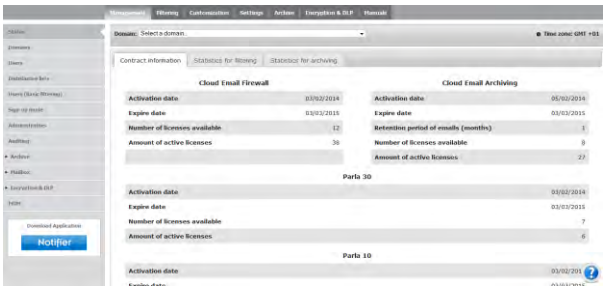
Mensajería
Herramientas de colaboración
Compartición de elementos del buzón de correo:
Agendas
Libretas de direcciones
Tareas
Notas
Archivos
Compatibilidad e Integración
Nuevo: Integración nativa con Outlook
Nuevo: Integración con la solución para la Gestión de Dispositivos Móviles (MDM)
Nuevo: Integración con la solución de Encriptación y Prevención de Fuga de Datos (CEE & DLP)
Sincronización de correo, agendas, contactos y notas con smartphones (iPhone, Android y Window Mobile).
Integración con Outlook mediante conector de sincronización para agendas, contactos, tareas y notas
Sincronización nativa de agendas, contactos, tareas y notas en Outlook 2007/2016 mediante ActiveSync
Sincronización de correo con cualquier cliente estándar mediante POP3 / IMAP / SMTP
Sincronización de contactos y calendarios mediante CalDAV / CardDAV
Importación/Exportación de agendas mediante CalDAV & iTip / iCalendar
Importación/Exportación de contactos mediante CSV, TSV & vCard
Importación de notas mediante CSV/vNotes
Importación de marcadores desde Firefox/Internet Explorer
Integración con Cloud Email Archiving (CEA)
Seguridad
Nuevo: Envío y recepción de correos encriptados gracias a Cloud Email Encryption (opcional)
Nuevo: Spamina Fingerprint Filtering (SFF) para la detección y gestión de correos de envíos masivos
Servicio de correo libre de Spam (servicio de seguridad Cloud Email Firewall completamente integrado en el buzón)

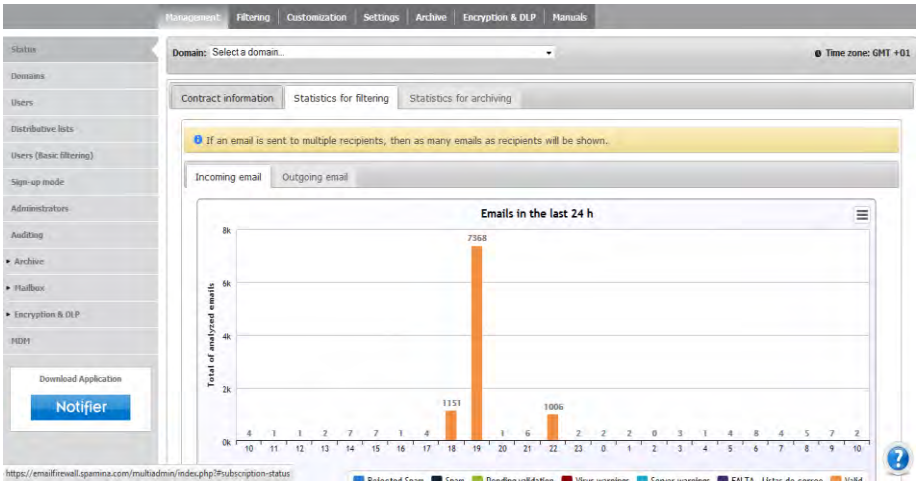
Mensajería
Protección contra *malware*, virus, phishing y demás amenazas
Filtrado multicapa con compatibilidad IPv6
Filtrado de correo entrante y saliente e interno.
Libre de *Prism Data Collection*
Email Archiving (opcional)
Gestión
Dashboard de actividad de correo
Potente motor de informes
Visualización de información de correos entrantes y salientes procesados
Log de auditoría de cambios de configuración
Migración
Herramienta de migración de correo desde servidor Microsoft Exchange
Soporte
Servicio técnico 24x7 Opcional

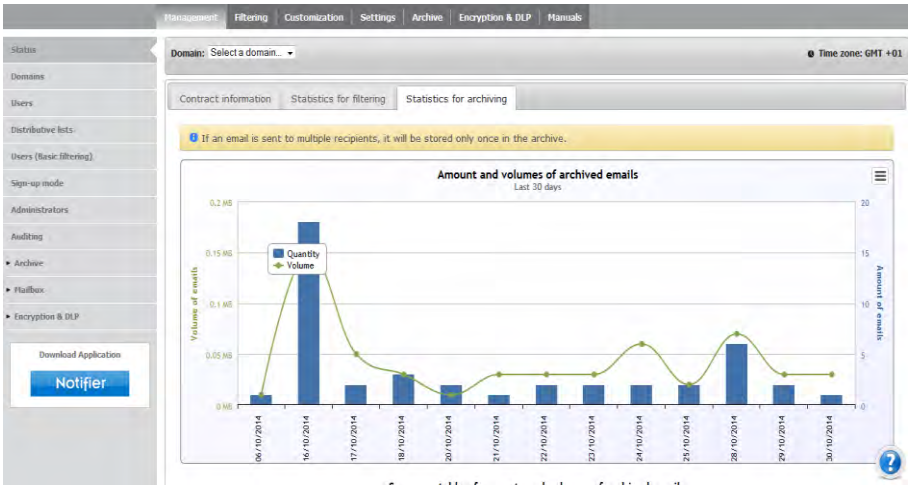
5. CONSOLA UNIFICADA DE ADMINISTRACION

La nueva consola unificada permite a los administradores gestionar todos los productos desde una consola unificada. El Buzón Parla, el Spamina Cloud Email Firewall, Cloud Email Archiving, Cloud Email Encryption y DLP se puede acceder fácilmente desde una única consola de gestión basada en web.









6. PROCEDIMIENTOS DE SOPORTE

Dependiendo del tipo de soporte contratado cada cliente disfrutará de la asistencia de nuestros técnicos y servicios de soporte en dos modalidades:

- Soporte Básico 10x5: está incluido en todos los productos de SPAMINA ofrece asistencia telefónica y por email continuadamente desde las 9:00 hasta las 19:00 los días laborables (España).

- Soporte Premium 24x7: para aquellos clientes que por sus características especiales o criticidad en su negocio necesiten asistencia en cualquier momento, estará disponible este servicio de soporte telefónico fuera del horario estándar básico. Para disfrutar de este servicio es necesario indicarlo así en el contrato inicial.

El programa de Soporte al cliente cuenta con tres áreas básicas:

- El Centro de Gestión de Servicios (CGS): se trata de un help-desk que canalizará cualquier incidencia o requerimiento del cliente.

- Centro de Gestión Avanzado (CGA): compuesto por personal con alto conocimiento técnico en Integración de Sistemas y Aplicaciones.

- Centro de Monitorización SPAMINA (CMS): forman parte de los Centros CGA.

6.1. CENTRO DE GESTIÓN DE SERVICIOS (CGS)

El CGS ofrece un punto de contacto técnico centralizado para clientes en general y está ubicado en Barcelona. Su principal misión es la asistencia diaria a clientes a través de su *Help-Desk*, que atiende consultas de primer nivel y canaliza al departamento correspondiente las posibles incidencias en el servicio. En este departamento se abren estudian los tickets de incidencias o *trouble tickets*, que permiten detallar la calidad del servicio ofrecido a los clientes y mantener un histórico de los problemas encontrados.

Cuando un cliente de SPAMINA se pone en contacto con el CGS para informar de alguna incidencia, éste se encarga de registrarla y de ponerse en contacto con el departamento técnico apropiado para que procedan a la resolución de la misma.

En resumen, el CGS se encarga de:

- El registro de incidencias.

- Resolución de dudas o incidencias simples.

- La asignación de la incidencia al departamento apropiado.

A lo largo de todo este proceso, el CGS dispondrá de información del estado de cualquier incidencia del cliente, pudiendo actuar como punto de contacto inmediato, siendo ésta su principal responsabilidad.

Uno de los compromisos de calidad del CGS es escalar todos los problemas críticos al interlocutor apropiado antes de una hora.

6.2. CENTRO DE GESTIÓN AVANZADO (CGA)

El CGA está ubicado en las oficinas de Spamina en Girona (Esp) y Tandil (Arg), operando 24 horas al día / 365 días del año. Se trata de un departamento de gestión de incidencias centralizado para atender todas las actividades relativas al servicio y poder responder de manera eficaz y totalmente organizada.

Este departamento cuenta con los expertos necesarios para el mantenimiento del servicio.

El CGA utiliza una plataforma de monitorización de aplicaciones basada en la plataforma OpenSource Nagios. En caso de que el cliente lo solicite, se realiza la instalación de agentes en cada uno de los servidores y aplicaciones para la detección de fallos críticos y de rendimiento.

El CGA además recoge incidencias de servicio a través de:

- CGS, principalmente a través de aplicaciones de trouble-ticketing que permiten hacer un sencillo seguimiento de las incidencias en horario laboral.
- CMS, a través de las herramientas de monitorización sobre nuestra plataforma Cloud, permitiendo anticiparse a la mayoría de incidencias HW o degradación del servicio antes de que el usuario lo perciba.
- Directamente del cliente, en aquellos casos en que, por sus requerimientos de atención o complejidad de diseño, precisen atención directa e inmediata y mediante la contratación del soporte 24x7.

Nuestro objetivo es garantizar la máxima disponibilidad y rendimiento de todos los equipos que integran el servicio.

Cuando un cliente de SPAMINA se pone en contacto con el CGA para informar de alguna incidencia, éste se encarga de registrarla y gestionarla, siendo responsable de la correcta evolución de su resolución en los tiempos y modos comprometidos. En cualquier fase de la resolución del problema, poseerá información detallada y actuará como coordinador técnico con cualquier área de soporte involucrada en posibles problemas de escalabilidad. Su misión es ponerse en contacto con el departamento apropiado y realizar un seguimiento efectivo de la incidencia hasta su resolución.

A lo largo de todo este proceso, el CGA, es el principal responsable de la resolución de incidencias. Además, será el responsable de mantener al cliente constantemente informado sobre los progresos realizados hasta la resolución final de la incidencia.

El CGA cuenta con personal técnico cualificado que permite ofrecer soporte y mantenimiento de alto nivel, así como capacidad e información para la implementación de cambios en los servicios suministrados.

El personal del CGA trabaja estrechamente con los desarrolladores de software y fabricantes de hardware, pudiendo requerir en ciertos casos su presencia para resolver u optimizar el funcionamiento de una aplicación o equipo.

Las principales funciones del CGA son:

- Asistencia Telefónica: el CGA proporciona soporte "*on-line*" para cualquier consulta orientada a la identificación de problemas, cambios de configuración en sus equipos, integración o implementación de nuevos servicios.
- Monitorización y Gestión Remota de los servicios del cliente: Spamina dispone, en sus oficinas en Girona, de distintas Plataformas de Gestión a través de las cuales se efectúa un seguimiento preventivo (en el caso del servicio Cloud en los CPDs de Spamina) y correctivo de los servicios Cloud contratados.
- Asistencia "in situ": el CGA se ocupa de la diagnosis y resolución del problema en el caso de Software, y de la sustitución del componente averiado y restitución del servicio en el caso de Hardware.

6.3. NIVELES DE RESPONSABILIDAD

SPAMINA trabajará conjuntamente con el personal designado por parte del cliente para diseñar y acordar los documentos de control necesarios y los procesos para la gestión de incidencias.

6.4. RESOLUCIÓN DE INCIDENCIAS

Las incidencias se gestionan siguiendo códigos de "gravedad" estándar especificados en la tabla siguiente. Éstos marcan la importancia y el impacto de una incidencia sobre los usuarios de la red.

Gravedad	Importancia
Crítico	La incidencia impide a los usuarios acceder al servicio. La incidencia impide la entrega de correo. La incidencia supone un funcionamiento y rendimiento de red seriamente degradado.
No Crítico	La incidencia produce problemas operacionales de forma intermitente. La incidencia no produce ningún tipo de problema a los usuarios en el ámbito operacional.

Tabla 1. Códigos de "gravedad" estándar

6.5. TIEMPOS DE RESPUESTA Y RESOLUCIÓN

Gravedad	Tiempo máximo de respuesta
Crítico	< 1 hora (24x7)
No Crítico	< 2 hora (10x5)

Es importante diferenciar entre tiempo de respuesta y tiempo de resolución:

- Tiempo de Respuesta: tiempo transcurrido desde la notificación de una incidencia por parte del cliente y el inicio de su resolución por parte del personal técnico del CGA.
- Tiempo de Resolución: tiempo transcurrido desde la notificación de la incidencia por parte del cliente hasta la verificación de servicio restablecido por parte del CGA, una vez cerrada la incidencia. En el caso de instalaciones dedicadas, no se contabilizará el tiempo necesario para resolver incidencias no asociadas directamente con el producto (Hardware, infraestructuras del cliente o terceros, etc.).

6.6. PROCEDIMIENTO OPERATIVO EN CASO DE INCIDENCIA

SPAMINA ha establecido una serie de procedimientos para la resolución de incidencias.

El procedimiento operativo a seguir en caso de surgir alguna incidencia en el servicio es el siguiente:

- Notificación de la incidencia por parte del cliente vía e-mail o llamada telefónica al CGS en horario laboral o al CGA fuera del horario laboral.
- Vía telefónica: el CGS o el CGA pedirá los datos necesarios para abrir la incidencia.
- Vía email: el cliente facilitará sus datos en el correo donde se describa el problema detectado.

Los datos necesarios que se pedirán son:

- Nombre completo.
- Teléfono de contacto.
- Email de contacto.

En el caso de no obtener estos datos no se podrá iniciar el tratamiento de la incidencia.

- Recogida de la incidencia directamente por los operadores del CGA a través de las estaciones de monitorización del centro de gestión CMS si se da el caso. Se notificará al cliente, telefónicamente o mediante un e-mail, los datos de contacto indicado en este documento.

- El personal de CGS asignará y proporcionará al cliente un número de control por equipo averiado o incidencia de servicio. Este número tendrá la finalidad de identificar la incidencia y servirá como referencia para posibles consultas sobre el estado de su solución.

- A continuación, el personal especializado del CGA de SPAMINA realizará una intervención para diagnosticar la incidencia o problema.

- Una vez detectada la problemática, SPAMINA procederá a la resolución de la incidencia. En este punto, puede ser necesario solicitar la asistencia de una tercera empresa o del fabricante del hardware.

- Una vez comprobado el correcto funcionamiento, siempre bajo autorización del cliente, se procederá a cerrar la incidencia.

7. CONSIDERACIONES DE LOS MODOS DE DESPLIEGUE

7.1. DESPLIEGUE DEL SERVICIO EN PUBLIC CLOUD

Los servicios descritos con anterioridad referentes a Cloud Email Firewall (CEF) con Spamina PARLA pueden ofrecerse desde la infraestructura de nube pública. Las ventajas de optar por este tipo de despliegue son:

- Despliegue inmediato del servicio.
- No es necesario despliegue de equipamiento en el cliente final.
- Todas las funcionalidades descritas anteriormente estarán disponibles.
- El tiempo de despliegue del servicio será inmediato si se opta por un despliegue en la infraestructura pública de Spamina.

8. PROPUESTA TÉCNICA

8.1. BENEFICIOS DE LA SOLUCIÓN

Soluciones Cloud de Spamina:

- Solución transparente:
  - No ralentiza la máquina del usuario
  - Sin instalación de software adicional.
- Solución escalable, que responde tanto a las necesidades actuales como a las futuras previsibles.
- Actualización de las versiones dedicadas del producto previo acuerdo con el de cliente (*)
- La versión del producto en modo Cloud está totalmente gestionada por SPAMINA, una gestión de la plataforma:
  - Actualización totalmente transparente, para los usuarios.
  - Mantenimiento 24x7.
- Centro de atención al cliente, que actúa como punto de contacto para todos los aspectos relacionados con el servicio.

(*) Es necesario acceso remoto para realizar actualizaciones de producto.

Cloud Email Firewall:

- Eficiencia asegurada:
  - Hasta un 100% en detección de spam (modo garantizado).
  - Hasta un 99,8% en detección de spam (modo automático).
- Optimización de recursos:
  - Eliminar el spam del correo supondrá que su utilización de Internet sea inferior permitiendo que aumente la agilidad del resto de aplicaciones Web.
  - Los servidores de correo del cliente utilizarán menos disco y CPU al procesar menor cantidad de correo
  - El personal de IT podrá dedicar su tiempo a más tareas que eliminar Virus y
  - *Malware* de los usuarios.
  - Mayor productividad del usuario.
  - Actualización automática de filtros antispam y antivirus.
  - Los productos de seguridad del correo electrónico de SPAMINA ofrecen:
  - Máximo Control
  - Panel de Control Administrador de la plataforma
  - Panel de Control Usuario final
  - Notificador SPAMINA para usuarios avanzados
  - Email diario con el correo retenido para todas los buzones que lo requieran
- Estadísticas de uso

Spamina PARLA:

- Filtrado Multicapa
  - Filtrado Multicapa (conexión, antivirus y contenido) basado en tecnologías de reconocimiento de amenazas.
  - Correo 99,9% libre de amenazas.

- Gestor de ficheros integrado.

- Elimina la necesidad de tener herramientas de gestión de documentos por separado y agiliza el proceso de compartir archivos usando la herramienta corporativa de correo.

- Integración con dispositivos móviles:
  - Parla se integra nativamente con aplicaciones de correo, contactos y calendarios en cualquier iPhone, ActiveSync. iPad, Android, Windows Mobile o Tablet utilizando el protocolo.

- Integración con Outlook:
  - Parla ofrece total compatibilidad con Microsoft Outlook, Apple Mail y otros clientes de correo POP3 / IMAP / iCal / CalDAV / CardDAV.

- Disponible en diferentes modalidades de provisión (Public, Private y Hybrid).
- Adaptable a cualquier tipo de organización / MSPs / ISPs.
- Solución basada en arquitectura distribuida y escalable (SDA).
- Plataforma adaptable a futuras necesidades de su organización.
  - Gestión de las políticas del uso del correo electrónico de las empresas. Control del correo entrante y saliente.
  - Cumplimiento de normativas de la organización mediante políticas.
  - Trazabilidad de los correos entrantes y salientes de su organización.
  - Herramientas de gestión del flujo de correo que permiten tener visibilidad

- Solución completa de externalización de correo.
  - Acceso al correo seguro independientemente de la ubicación y del dispositivo (Portátil, dispositivos móviles, etc).
  - Interfaces de gestión disponibles para los diferentes perfiles Administrador de empresa, administrador de dominio y usuario final)
- Granularidad de gestión de la plataforma e integración de la seguridad en la interfaz Webmail de los usuarios finales.

8.2. DESPLIEGUE DEL SERVICIO EN PUBLIC CLOUD

Los servicios descritos con anterioridad referentes a Cloud Email Firewall (CEF) con Spamina PARLA pueden ofrecerse desde la infraestructura de nube pública. Las ventajas de optar por este tipo de despliegue son:

- Despliegue inmediato del servicio.
- No es necesario despliegue de equipamiento en el cliente final.
- Todas las funcionalidades descritas disponibles.
- El tiempo de despliegue del servicio será inmediato si se opta por un despliegue en la infraestructura pública de Spamina.
- Spamina ofrece un servicio en su Cloud seguro y protegido, que cumple con las normativas más exigentes sobre privacidad y protección de los datos del cliente.

9. OFERTA ECONÓMICA

9.1. PROPUESTA DE CORREO SEGURO

PRODUCTO	NUMERO DE PARTE	CANTIDAD	PERIODO	PRECIO UNITARIO	DESCUENTO	IMPORTE
Cloud Email Firewall (CEF) 1 Year 250-500 seats	CEF_SPSESF10 0500	500	1 AÑO	$ 16.34	40%	$ 4,902.00
Cloud Email Firewall (CEF) 1 Year 501-1000 seats	CEF_SPSESF10 1000	1000	1 AÑO	$ 14.74	40%	$ 8,844.00
Cloud Email Firewall (CEF) 1 Year 1001-3000 seats	CEF_SPSESF10 3000	3000	1 AÑO	$ 13.78	40%	$ 24,804.00
Cloud Email Firewall (CEF) 1 Year 3001-10000 seats	CEF_SPSESF11 0000	5000	1 AÑO	$ 10.79	40%	$ 32,370.00
ADVANCED THREAT PROTECTION 1 YEAR	ATTP10001	1	1 AÑO	$ 12.00	40%	$ 7.20
Cloud Email Archiving (CEA) 1 Year until 10 Years	CEA_SPSESA30 0000	1	1 AÑO	$ 39.00	40%	$ 23.40
Cloud Email Encryption & DLP (CEE) 1 Year 0-100000 seats	CEE_SPSESE10 0500	1	1 AÑO	$ 25.00	40%	$ 15.00
Parla - 1 year - 2GB Mailbox Size + CEF included	Parla10002	1	1 AÑO	$ 17.10	40%	$ 10.26
Parla - 1 year - 10GB Mailbox Size + CEF Included	Parla10010	1	1 AÑO	$ 28.44	40%	$ 17.06
Parla - 1 year - 30GB Mailbox Size + CEF Included	Parla10030	1	1 AÑO	$ 57.00	40%	$ 34.20

CONDICIONES COMERCIALES

MONEDA : DOLARES AMERICANOS(USD)
PRECIOS : ESTOS PRECIOS YA CONTIENEN I.V.A.
***PRECIOS SUJETOS A CAMBIO SIN PREVIO AVISO
VIGENCIA : 20 DIAS NATURALES, CONTADOS A PARTIR DE LA FECHA DE ESTA PROPUESTA
PAGO : **DENTRO DE LOS SIGUIENTES 5 DÍAS NATURALES, DE HABERSE COLOCADO LA ORDEN DE COMPRA**
ENTREGA : DENTRO DE LOS SIGUIENTES 5 DÍAS NATURALES, DE HABERSE COMPROBADO EL PAGO TOTAL

NOTAS:

1.- PARA CUALQUIER ACLARACIÓN, FAVOR DE COMUNICARSE CON SU REPRESENTANTE DE VENTAS.
2.- UNA VEZ COLOCADA LA ORDEN DE COMPRA, **NO SE ACEPTAN CANCELACIONES**
3.- CUALQUIER SERVICIO ADICIONAL A LO COTIZADO EN LA PRESENTE PROPUESTA, **GENERARA UN COSTO ADICIONAL**
4.- PARLA 2GB, 10GB y 30GB CONTIENE LA SEGURIDAD INTEGRADA DE CLOUD EMAIL FIREWALL (CEF), **SIN COSTO ADICIONAL**
5.- PARLA 2GB NO SOPORTA EL PLUGIN PARA OUTLOOK, POR LO QUE LAS SIGUIENTES FUNCIONALIDADES **NO SE ENCUENTRAN HABILITADAS**:
   - NO CUENTA CON LA FUNCIONALIDAD DE CHAT SEGURO PARLA-MI
   - NO SINCRONIZA CON SMARTPHONE EN OUTLOOK
5.- **ATP** SE DEPLEGARA EN UN ENTORNO **HYBRID CLOUD**

10. GARANTÍAS LEGALES Y CONFIDENCIALIDAD

El certificado desarrollado por Xnovo Legal & Web Solutions, reconoce que SPAMINA cumple los requisitos legales de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) de España.

Nº Certificado 0510102

Este certificado se otorga tras un riguroso análisis Legal, practicado por Xnovo a SPAMINA, garantizando la ADECUACIÓN del Sitio, así como lo referente a:

- Condiciones de Contratación.
- Protección de Datos.
- Propiedad Intelectual.
- Demás aspectos regulados por dicha Ley.

SPAMINA, en cumplimiento a los preceptos legales en materia de Protección de Datos Personales recogidos en la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal" (LOPD); y en los Reales Decretos que la desarrollan, informa que se compromete con el respeto a los datos de carácter personal e intimidad del usuario. El tratamiento de datos de carácter personal será recogido en un fichero automatizado, cuyo responsable es Aegis Security, S.L., debidamente inscrito ante la AEPD.

11. TERMINOS Y CONDICIONES DEL SERVICIO

Identificación

- Titular: AEGIS SECURITY S.L. (en adelante, Spamina)
- Domicilio social: Calle Arte 15 28033 Madrid, España
- CIF: B-63952485
- Registro Público: Inscrita en el Registro Mercantil de Madrid Tomo 32495, Folio 48, Hoja M-586010, inscripción 2ª.
- E-mail: info@spamina.com

Ambas partes, Spamina y el cliente (que serán comúnmente designados como las "Partes" y cada uno de ellos, indistinta e individualmente, como "Parte"), están interesadas en suscribir el presente acuerdo aceptando los términos establecidos en las siguientes,

CLAUSULAS

Objeto

Por medio del presente Acuerdo, las Partes convienen las condiciones que regirán la prestación de servicios por Spamina al Cliente.

Spamina y el Cliente convienen que, en el marco de sus relaciones contractuales, serán aplicables dos tipos de condiciones: por una parte, las condiciones de carácter general, que son de aplicación y tienen plena eficacia en relación con todos los servicios proveídos por Spamina (en adelante, las "Condiciones Generales"); y, por otra parte, las condiciones particulares, que son de aplicación respecto a determinados servicios (en adelante, las "Condiciones Particulares"). Desde la firma del presente Acuerdo, tanto las Condiciones Generales como las Condiciones Particulares serán vinculantes para ambas Partes y ello, sin perjuicio de su aplicación conjunta con las condiciones de contratación pactadas entre Spamina y el Cliente en el momento de la aceptación de la oferta de servicio.

En todo caso, Spamina se reserva el derecho a modificar unilateralmente las citadas condiciones, a condición de que: i) la modificación introducida no afecte sustancialmente las condiciones esenciales del presente Acuerdo; ii) la modificación en cuestión sea expresamente comunicada al Cliente mediante su remisión al Administrador del sistema vía correo electrónico; y, iii) cualquier modificación quede reflejada en todo momento en la página a la que se accede por medio del enlace http://es.spamina.com/es/datos/terminos.html

La aceptación de las Condiciones Generales y de las Condiciones Particulares por parte del Cliente será requisito esencial para la prestación del servicio contratado a Spamina.

Información previa

Los contratos celebrados por vía telemática serán vinculantes en sus propios términos y producirán todos sus efectos, siempre que concurra el consentimiento mutuo de ambas Partes.

A estos efectos, se entenderá que el seguimiento de todas las fases del proceso de activación y configuración del servicio y el abono de la cantidad económica correspondiente por el Cliente, determinan: i) que se ha prestado el consentimiento requerido para la contratación; ii) que el Cliente reconoce que las características del producto o servicio contratado se ajustan a sus necesidades; y, iii) que el Cliente ha sido informado adecuadamente por parte de Spamina.

Spamina se reserva el derecho a realizar, cuando lo estime oportuno, cambios comercialmente razonables en las presentes condiciones. En caso de que Spamina lleve a cabo cualquier modificación de las condiciones que regulan el servicio, informará al Cliente con una antelación mínima de treinta (30) días con anterioridad a la entrada en vigor de la referida modificación. Si la eventual modificación afectase a alguno de los elementos esenciales del Acuerdo y el Cliente no la aceptare, éste podrá rescindir unilateralmente el contrato.

El proceso de activación del servicio comenzará mediante la remisión al Administrador designado por parte del Cliente de un correo electrónico junto con su usuario y contraseña de acceso, donde figurarán las presentes condiciones que, en todo caso, deberán ser aceptadas para poder continuar con el uso de los servicios proveídos por Spamina.

La aceptación de las condiciones por el Cliente se realizará mediante el marcado de la casilla correspondiente y en ningún caso posible continuar con el proceso de uso y activación de la plataforma si, previamente, no ha marcado la citada casilla con la aceptación de las condiciones, siendo ésta una condición indispensable para la ejecución del Acuerdo entre las partes.

Tras la aceptación, Spamina almacenará en un fichero histórico los datos del Cliente, el día y hora de la aceptación de las condiciones de registro vigentes en este momento con el fin de acreditar la conformidad del Cliente.

En todo caso, el documento resultante de la aceptación por parte del Administrador del sistema será debidamente archivado, quedando asociado tanto a la dirección IP, como al momento exacto en el que se realizó la aceptación.

Una vez validado en el sistema, el Administrador procederá a activar los diferentes usuarios dependientes, debiendo el primero remitirles la información de autenticación en el sistema, sin perjuicio de las configuraciones que sean realizadas por parte del Administrador. Esta medida, unida al resto de medidas tecnológicas del propio servicio y las que aplica internamente Spamina, garantizan la seguridad e integridad de todos sus accesos al servicio y la información asociada al mismo. Estos datos, una vez generados serán responsabilidad única y exclusivamente del usuario final y en su caso del Cliente de Spamina.

En cualquier caso, la contraseña de acceso facilitada podrá ser modificada por el Cliente en cuestión, siendo así el único que conozca los datos de acceso.

Servicio de atención al usuario y servicio técnico

Spamina pone a disposición del Cliente un servicio de atención al usuario y asistencia técnica que reunirá las siguientes características:

El servicio de atención al usuario será prestado telefónicamente, a través de correo electrónico y por medio del portal de soporte al que se accede por el siguiente enlace (http://es.spamina.com/es/soporte.php).

El servicio de atención al usuario será prestado en el horario indicado en la referida página, pudiendo, no obstante, Spamina modificar dichos horarios, en función de los cambios horarios y de las necesidades técnicas y comerciales de Spamina.

El servicio de atención al usuario será exclusivamente prestado en castellano e inglés, sin perjuicio de que Spamina pueda poner a disposición del Cliente otros idiomas, de conformidad con lo expresamente pactado entre las Partes.

Con el fin de dotar al sistema de la máxima seguridad posible y mejorar la calidad del servicio, Spamina se reserva el derecho a grabar las

conversaciones telefónicas mantenidas en el marco del servicio de atención al usuario.

El Cliente y el usuario final consienten que sus respectivas conversaciones telefónicas con Spamina puedan ser grabadas con el objeto de mejorar la calidad de los servicios y la seguridad en la prestación de los mismos.

Obligaciones del Cliente

El Cliente mediante la aceptación de las presentes condiciones garantiza que:

- No utilizará el servicio o cualquiera de los elementos que lo integren para desarrollar operaciones de tiempo compartido.
- No se convertirá en proveedor de servicios de aplicaciones software en la medida en que los mismos posibiliten el acceso de terceros al servicio contratado o a cualquiera de sus componentes, a través de operaciones de alquiler, servicios administrativos o cualesquiera otros de análoga consideración.
- No someterá los servidores, accesos o cualesquiera de sus elementos, a actividades que conduzcan, directa o indirectamente a la descompilación de su software, implicando la realización de operaciones de naturaleza inversa a las que permitieron su construcción u operaciones que constituyan o, puedan constituir, operaciones de ingeniera regresiva o inversa, descompilación o desensamblado.
  En ningún caso, el Cliente y todas las personas relacionadas con el mismo, podrán acceder al código fuente del servicio de Cloud.
- No utilizará el servicio como sistema de gestión e intercambio de información y/o documentación ilegal, contraria a la moral, al orden público, a los derechos de autor y/o de propiedad industrial.
- Ostenta capacidad suficiente para poder llevar a cabo la aceptación de las presentes condiciones.
- No someter los servicios a cargas de trabajo que desestabilicen los mismos, incluyendo ataques de denegación de servicios (DoS) o situaciones semejantes.

  En caso de detectarse este tipo de situaciones acontecerá una situación de emergencia, de modo que el nivel de servicio acordado entre las Partes no será de aplicación. Si tras la reanudación del servicio se reiterase esta circunstancia, se procederá a la baja del servicio sin derecho a devolución de cantidad alguna, por considerar uso abusivo del producto o servicio contratado.

- No utilizar el servicio con fines ilícitos (entre otros, spam, mail bombing, phising, escrow fraud, scam 419, pharming, difusión de virus, o cualquier otro tipo de actividad realizada con ánimo saboteador, fraudulento o delictivo, etc.), para intercambiar información ilegal o para evadir el cumplimiento de obligaciones legales en el estado de origen o destino de la comunicación.
- No llevar a cabo actos de ingeniería inversa, toma de requisitos y demás actividades encaminadas a desarrollar un servicio online semejante al proveído por Spamina, considerándose esta actividad como un acto de competencia desleal que vulnera los derechos de propiedad intelectual e industrial que Spamina ostenta sobre los servicios de Cloud ofertados.
- No traducir, adaptar, mejorar, transformar, corregir o introducir cualquier modificación en el servicio, o en cualquiera de los elementos que los integran, no pudiendo en ningún caso incorporar el servicio a otros softwares propios o de terceros.
- No retirar, suprimir, alterar, manipular, ni modificar en modo alguno aquellas notas, leyendas, indicaciones o símbolos que Spamina, como legítimo titular de los derechos, incorpore a sus propiedades en materia de propiedad intelectual o industrial (como, por ejemplo, copyright, ©, ® y TM, etc.).
- Se compromete a abonar las cantidades económicas pactadas por virtud del presente Acuerdo en tiempo y forma.
- Poner en conocimiento de Spamina cualquier hecho o situación que pudiera poner en riesgo la seguridad en el acceso por parte de usuarios autorizados.

Nivel de servicio y garantías

El Cliente y Spamina se comprometen a cumplir íntegramente los términos reflejados en el Acuerdo y a respetar la normativa vigente, debiendo las Partes actuar lealmente y de buena fe durante toda la vigencia de su relación contractual.

Spamina está comprometida con el correcto funcionamiento del servicio y los sistemas asociados al mismo, así como con los más altos niveles de calidad, seguridad y disponibilidad.

Spamina se compromete a proporcionar al Cliente el nivel de servicio expresamente acordado entre las Partes y, en defecto de acuerdo entre las Partes sobre el nivel de servicio, Spamina se obliga a proporcionar al Cliente el nivel dispuesto en las presentes condiciones.

En este sentido, Spamina garantiza al Cliente la provisión de un nivel de servicio adecuado que le permita su pleno disfrute, que estará disponible durante las 24 horas al día, los 7 días de la semana y con un nivel de disponibilidad de las comunicaciones equivalente al 99,86% del tiempo. Ello, sin perjuicio de la ocurrencia de situaciones que conlleven la interrupción temporal del servicio, servicios de mantenimiento programados o puntuales, así como como guerras, desastres naturales, huelga, cierre patronal, fuego, no disponibilidad del proveedor de alojamiento y la existencia de circunstancias imprevisibles o de circunstancias previsibles pero inevitables.

Sin perjuicio de lo anterior, Spamina pone a disposición del Cliente la posibilidad de pactar un nivel de servicio expresamente adaptado a sus necesidades. Por consiguiente, el nivel de servicio podrá verse ampliado y especificado previo acuerdo entre las Partes, debiendo éstas, en todo caso, proceder a la firma del correspondiente contrato por el que se determine la disponibilidad, el nivel de servicio garantizado y las penalizaciones aplicables. No obstante, Spamina se reserva el derecho a interrumpir el servicio contratado en función de los mantenimientos programados, reparaciones técnicas, así como para la mejora de los propios servicios. En tal caso, Spamina se compromete a notificar al Cliente este tipo de actividades con una antelación mínima de cuarenta y ocho (48) horas.

Para cumplir con los niveles de servicio previamente citados, Spamina cuenta con sistemas redundantes en alta disponibilidad y disaster recovery en alta disponibilidad. Sin perjuicio de ello, Spamina no puede garantizar absolutamente la disponibilidad de todos los servicios, en tanto éstos dependen de la conectividad y disponibilidad de terceros proveedores, tales como la red eléctrica o red de datos. No obstante, lo anterior, a título informativo, Spamina cuenta con acuerdos con dichos proveedores que garantizan niveles de servicio superiores o, en su caso, idénticos a los descritos en las presentes condiciones.

Asimismo, Spamina garantiza que toda la información necesaria para restaurar el servicio alojada en los servidores asociados al servicio, -incluidas las bases de datos-, son sometidas, al menos, a un proceso de copia de seguridad, siendo en cualquier caso alojada dicha copia en un dispositivo hardware diferente al principal y ello con vistas a posibilitar la recuperación de datos.

En caso de terminación del Acuerdo por la causa que fuere, Spamina se compromete a poner a disposición del Cliente, en el plazo máximo de treinta (30) días laborables, toda la información y documentación alojada en el al momento de la solicitud de la misma y este servicio podrá tener un coste adicional para el Cliente en función del volumen de información

que sea necesario recuperar. La puesta a disposición del Cliente de la documentación se realizará en un formato interoperable LDAP (ldiff) y/o MySQL (sql), o formatos exportables por estos.

En conexión con ello, Spamina se halla exenta de toda responsabilidad en caso de que el sistema empleado a posteriori por el Cliente no cumpla con los estándares mencionados en el párrafo anterior, y en ningún caso Spamina tendrá la obligación de intervenir en labores de implementación e integración posteriores que fueran necesarias para el correcto funcionamiento de la información en otros servidores.

Responsabilidades

Spamina no asumirá ningún tipo de responsabilidad derivada del incumplimiento de las presentes condiciones, a excepción de aquella responsabilidad directamente asociada con el servicio propiamente dicho.

En todo caso, la responsabilidad que pudiera corresponder a Spamina por el incumplimiento reiterado de sus obligaciones, no podrá superar la cantidad total abonada por el Cliente durante el año en curso y en cualquier caso la del último pago efectuado. Las Partes acuerdan que queda excluida cualquier reclamación de daño por lucro cesante.

No obstante lo anterior, si Spamina incumpliera los compromisos asumidos en las presentes condiciones o en las condiciones específicas que, en su caso fueren aplicables a cada producto contratado, y dicho incumplimiento consistiera en la prestación de un servicio ineficiente durante periodos intermitentes o no continuados, la responsabilidad de Spamina se limitará a la devolución de las cantidades económicas abonadas por el producto o servicio durante los períodos de interrupción efectivamente constatados.

Del mismo modo, Spamina no asume ninguna responsabilidad, ya sea directa o indirecta, derivada del mal uso que los Clientes o usuarios puedan hacer del servicio de Cloud o de cualquiera de los contenidos que se encuentren alojados en los servidores contratados.

De conformidad con lo dispuesto en el artículo 16 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y de Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, Spamina en ningún caso podrá ser considerada como responsable de los contenidos alojados, siendo única y exclusivamente responsable el Cliente o usuario que, en su caso, haya remitido los contenidos a los servidores de Spamina.

Sobre la base de ello, Spamina no asume ningún tipo de responsabilidad en relación con:

- El contenido alojado en los productos contratados y la información transmitida y almacenada en sus servidores, de los que será responsable el Cliente o usuario.
- La veracidad de la información alojada y/o intercambiada por los Clientes y/o los usuarios.
- Los errores producidos por los proveedores de acceso.
- La contaminación por virus en sus equipos, cuya protección incumbe al Cliente y/o usuario.
- Las intrusiones de terceros en los productos contratados por el Cliente, aunque Spamina haya establecido medidas razonables de protección.
- La configuración defectuosa por parte del Cliente y/o usuario.
- Los deterioros de equipos (terminales del usuario) o su mal uso (responsabilidad del usuario).
- La vulneración de los derechos de propiedad intelectual o industrial, o de cualesquiera otros derechos o intereses legítimos que puedan derivarse de la utilización del producto contratado por el Cliente.
- Aquellas actuaciones que sean exclusivamente imputables al Cliente y/o usuario, incluyendo los daños directos o indirectos que el Cliente y/o usuario pudiera ocasionar a terceros.

Condiciones Particulares aplicables a los servicios cloud spamina

El filtrado de email de Spamina está diseñado para proteger el servidor de correo de spam, virus, spoofing, phising y spyware. El referido filtrado almacena el spam y malware en la nube de Spamina, liberando al servidor de correo electrónico y reduciendo el uso de ancho de banda en la red corporativa del usuario y ello, sin necesidad de que el usuario utilice algún hardware adicional.

En cuanto al correo entrante que se clasifique como spam, en el servicio proporcionado por Spamina, se incluye de serie un servicio de backup de correo válido entrante de 5 días y de 28 días. En dicho servicio también se incluye de serie el módulo de Cloud Email Continuity, que se activa en caso de caída del servidor de correo y que garantiza al usuario: i) la entrega de los correos electrónicos recibidos durante los 4 últimos días desde la caída; y, ii) el acceso vía webmail.

Las características técnicas del servicio que, en todo caso, Spamina garantizará durante la vigencia de la relación contractual entre ésta y el Cliente, son:

- Filtrado Multicapa para correo entrante y saliente (incluye filtrado de conexión, antivirus, antispam y antimalware).
- Dashboard Visión dinámica del estado del sistema y la actividad de filtrado para distintos periodos de tiempo.
- Auditoría de acciones.
- Motor de gestión de informes (reportes pre-definidos).
- Funciones de cuarentena centralizada (acciones masivas sobre correos desde listados de logs).
- Información detallada sobre las clasificaciones y filtros aplicados.
- Posibilidad de uso en modo Public y Private Cloud.
- Solución perimetral basada en una arquitectura distribuida y escalable (SDA).
- API basado en WebServices para interoperabilidad con aplicaciones de terceros.
- Gestión de las políticas de uso del correo electrónico.
- Almacenamiento configurable para correos entrantes Spam y Válidos.
- Motor de reglas para correo entrante y saliente.
- Varios niveles de perfil (administrador de empresa, administrador de dominio y usuario final).
- Múltiples administradores de empresa y dominio.
- Compatibilidad con IPv6.

Todo Cliente que contrate los servicios de Spamina, contará con la información necesaria para que éste o los usuarios autorizados por el mismo puedan acceder a dichos servicios. En esta información se detallará el link de acceso al panel de administración, configuración de los usuarios, empresas, idiomas, integración de LDAP (en su caso), informes de actividad del tráfico de correo electrónico y dominio, gestión de cuarentenas, actualizaciones y otros elementos necesarios para la adecuada configuración y uso del servicio.

Respecto a la seguridad del servicio, Spamina utiliza antivirus perimetral, sistemas de antispam, sistemas antiphishing, antimalware y antispoofing, así como sistemas de protección contra ataques de directorio, tales como Delay o GreyListing.

El sistema de filtrado automático es integrable en las principales plataformas existentes en el mercado destinadas a la Gestión del Correo electrónico y que realizan un archivado completo del correo entrante y de los correos incluidos en "*cuarentena*". Sin perjuicio de ello, el Cliente, con anterioridad a la contratación del servicio, debe confirmar con nuestro departamento técnico si éste es compatible con su sistema de correo electrónico.

El sistema de monitorización de correo electrónico ofrecido por Spamina es un servicio 24x7x365 con soporte técnico 10x5, que posibilita la continuidad del servicio.

En aras de salvaguardar la estabilidad y la seguridad del servicio, Spamina se reserva el derecho a suspender o bloquear, temporalmente o de forma indefinida, el dominio o dominios que se vean afectados en caso de que alguno de estos supere los límites, capacidad de análisis y filtrado medio indicados a continuación.

A estos efectos y salvo indicación en contrario, se entenderá que ha sido superada la capacidad de filtrado y análisis medio por dominio, cuando la media del dominio supere los 250 correos electrónicos recibidos al día (por cuenta de correo), cuando el consumo total en Mb supere la cantidad de 50 Mb/día (por cuenta de correo), o cuando se detecte la remisión de más de 1.000 correos electrónicos en el plazo de 60 minutos (por cuenta de correo), entendiéndose en tal caso que el Cliente, o los usuarios por él autorizados, pudieran estar realizando acciones de envíos correos electrónicos masivos. No obstante, por acuerdo expreso entre las Partes, se podrán establecer limitaciones específicas y adecuadas a las características concretas de la entidad que sea.

El Cliente tendrá derecho a usar 5 alias gratuitos por cada buzón de correo contratado.

Spamina se reserva el derecho a limitar el número de usuarios básicos contratados por el Cliente, no pudiendo superar este tipo de usuarios más del 5% del total de licencias contratadas. Una vez alcanzado el número máximo, en caso de que el Cliente desee añadir usuarios adicionales, éste únicamente podrá añadir usuarios avanzados.

El servicio de alojamiento se encuentra limitado a la cantidad de 256 Mb por cada cuenta de usuario y dicha capacidad podrá ser ampliada a través de la contratación de servicios adicionales ofrecidos por Spamina.

De conformidad con lo anteriormente indicado, el servicio de filtrado de correo electrónico de Spamina incorpora un sistema de copias de seguridad de serie que garantiza al Cliente la posibilidad de recuperar el correo electrónico recibido durante los últimos 5 días para el correo regular y durante los últimos 28 días para el correo spam. Sin perjuicio de ello, para ofrecer la máxima seguridad y garantías a sus Clientes, Spamina pone a su disposición un servicio adicional de archivado del correo electrónico que garantiza la posibilidad de recuperar todos los correos electrónicos enviados y recibidos desde cada una de las cuentas activadas.

Spamina ofrece a los Clientes un servicio de archivado seguro, permanente y automatizado de todos los buzones de correo electrónico seleccionados por el administrador del sistema. En caso de no haber seleccionado los buzones donde deberá ser aplicado, Spamina no estará obligada a suministrar dicho servicio.

El servicio de archivado únicamente será activado cuando el Cliente, de forma expresa, lo haya contratado y abonado, no siendo un servicio incluido por defecto en los servicios básicos de Spamina. Este servicio sólo será activado sobre aquellas cuentas de correo electrónico que específicamente sean designadas por el Cliente, no siendo aplicable por defecto en el resto de cuentas de correo electrónico del Cliente.

Spamina informa al Cliente que quedará una copia de cada uno de los correos recibidos o enviados, de tal forma que el Cliente siempre contará con una copia remota, de fácil acceso e íntegra de su buzón de correo electrónico, garantizándole el acceso remoto al contenido de su buzón desde cualquier punto.

Asimismo, en atención a las características del servicio, el Cliente y/o usuario podrán exportar o reenviar todos los correos electrónicos sobre los que se ha realizado la copia de seguridad.

Con el fin de garantizar la seguridad de los sistemas locales del Cliente y de cada uno de los usuarios dependientes de éste, Spamina únicamente almacenará una copia de aquel correo electrónico que cumpla con los niveles de seguridad determinados en la configuración del Cliente. En conexión con ello, Spamina no se responsabiliza en caso de que el sistema no guarde una copia de seguridad de dicho correo electrónico, por no cumplir éste con los niveles de seguridad expresamente indicados por parte del Cliente en el momento de la configuración del servicio.

Del mismo modo, Spamina no garantiza que aquellos correos electrónicos que contengan ficheros con un tamaño superior a 10 Mb sean efectivamente accesibles desde el archivo realizado, quedando reservada a Spamina la posibilidad de almacenar únicamente el texto del correo electrónico en cuestión y no los ficheros adjuntos.

En esta línea, Spamina informa al Cliente que el servicio de archivado de correo electrónico en ningún caso podrá almacenar más de 5Gb, por cuenta de correo electrónico y por año. En caso de que una cuenta alcanzara el tamaño máximo indicado, Spamina queda expresamente facultada para eliminar del servicio de archivado los correos electrónicos más antiguos hasta alcanzar el espacio necesario para el correcto funcionamiento del servicio.

De igual forma, Spamina pone a disposición del Cliente un completo servicio de cifrado de la información intercambiada a través de sus sistemas.

El servicio DLP únicamente será activado cuando el Cliente, efectivamente haya contratado y abonado el servicio en cuestión, no siendo un servicio incluido por defecto en los servicios básicos de Spamina.

Este servicio únicamente será activado sobre aquellas cuentas de correo electrónico que específicamente sean designadas por parte del Cliente, no siendo aplicable por defecto en el resto de cuentas de correo electrónico del cliente.

Spamina garantiza al Cliente que este servicio emplea algoritmos de cifrados basados en infraestructuras PKI de probada y reconocida seguridad, permitiendo la plena integridad y confidencialidad de la información intercambiada a través de los sistemas de correo electrónico.

Spamina garantiza que toda la información alojada en los sistemas será accesible desde cualquier dispositivo, tanto fijo, como móvil, siempre que el Cliente y/o usuario introduzca la clave privada de acceso, siendo esta un requisito indispensable para descifrar el contenido.

Spamina ostenta todos los derechos, títulos e intereses sobre el servicio objeto del presente Acuerdo y sobre todos sus módulos, modificaciones, actualizaciones y sobre cualquier elemento y/o funcionalidad que fuera desarrollada en relación con el mismo.

Propiedad industrial e intelectual

Spamina está altamente comprometida con la protección de los derechos en materia de propiedad intelectual e industrial. Por este motivo, Spamina manifiesta lo siguiente:

Spamina es la legítima propietaria de la totalidad de los derechos de propiedad intelectual existentes sobre el servicio y en relación con el mismo, no existe ninguna disputa legal con carácter previo a la firma del presente Acuerdo. A estos efectos, pertenecen a Spamina todos los derechos de autor, propiedad intelectual, y/o industrial, estando facultada para explotar el servicio, sin restricción de naturaleza alguna, referida a medios de difusión o modalidades de explotación.

La estructura, características, códigos, métodos de trabajo, sistemas de

información e intercambio de la misma, herramientas de desarrollo, know-how, metodologías, procesos, tecnologías o algoritmos que constituyan y/o puedan estar relacionados con el servicio de Cloud, son propiedad exclusiva de Spamina y no pueden ser objeto de ulterior modificación, copia, alteración, reproducción, adaptación o traducción por el Cliente o los usuarios, sin que exista el previo consentimiento expreso por parte de Spamina.

Asimismo, todos los manuales de uso, textos, dibujos gráficos, bases de datos y resto de materiales asociados al servicio, son propiedad de Spamina, sin que puedan ser objeto de ulterior modificación, copia, alteración, reproducción, adaptación o traducción por parte del Cliente o los usuarios.

La puesta a disposición del Cliente o de los usuarios por él autorizados del servicio de Cloud o, el mero acceso a este servicio por parte de ellos, en ningún caso implica la cesión de su titularidad, ni la concesión de algún derecho de uso a su favor, a excepción de aquellos expresamente indicados en este Acuerdo. En todo caso, cuando nada se indicare en el presente Acuerdo, los derechos se entenderán reservados a favor de Spamina.

Todos los contenidos e informaciones facilitados por el Cliente y alojados en los servidores de Spamina pertenecen al Cliente y Spamina se limita a ser un mero prestador de servicios que se encarga del almacenamiento de datos, sin que en ningún caso le pertenezca derecho de propiedad intelectual sobre dichos contenidos. Por ende, en relación con dichos contenidos e informaciones, serán exclusivamente el Cliente y el personal designado por éste los únicos que tienen la capacidad para explotarlos.

Condiciones temporales

El servicio de Cloud tendrá una duración determinada y concretada por virtud de acuerdo entre las Partes. En caso de que las Partes no hubieran acordado una duración expresa, el servicio tendrá una duración de 12 meses desde el día de la firma del presente Acuerdo.

La baja en la prestación del servicio se producirá en el día indicado por el Cliente, siempre que su petición se formule con una antelación mínima de 90 días con anterioridad al día efectivo de baja.

Llegado el término, el sistema avisará automáticamente, con al menos 30 días de antelación, sobre la necesidad de renovar el servicio. En caso de no renovación, el servicio será dado de baja automáticamente a las 00.00 del día siguiente a la finalización del plazo de prestación del servicio (12 meses o en su caso, el plazo expresamente acordado entre las Partes).

Cesión y subcontratación

Las cuentas de los Clientes registrados son completamente personales e intransferibles. De esta forma, el Cliente no podrá ceder, subcontratar, ni disponer los derechos y obligaciones derivados de este Acuerdo a favor de un tercero, sin la autorización previa y por escrito de parte de Spamina.

En caso de que el Cliente haya recabado la autorización expresa de Spamina para llevar a cabo la cesión o subcontratación de la cuenta a un tercero, el Cliente responderá, junto a este tercero, de forma solidaria frente a Spamina en relación con los derechos y obligaciones dimanantes del presente Acuerdo que, en su caso, fueran incumplidos por el tercero en cuestión.

Confidencialidad, seguridad y protección de datos

Spamina, en su calidad de proveedor de servicios de comunicaciones electrónicas y alojamiento de información, garantiza al Cliente que toda la información intercambiada o alojada a través de los sistemas de Spamina será considerada confidencial. Por ende, a esta información le serán aplicadas las medidas de seguridad adecuadas para lograr su máxima protección durante la vigencia de la relación contractual entre las Partes. Asimismo, Spamina se compromete a que esta obligación de confidencialidad persista, con carácter indefinido, tras la terminación de la relación contractual entre las Partes.

Spamina manifiesta que los servidores empleados para la provisión del servicio se encuentran bajo su efectivo control, encontrándose ubicados en el territorio de la Unión Europea o, en su caso, en países cuyos niveles de seguridad y protección son equiparables a los requeridos por la normativa comunitaria.

Asimismo, Spamina garantiza al Cliente que el tratamiento de la información y de los datos personales se realizará de conformidad con las directrices siguientes:

- Que Spamina tratará la información facilitada conforme a las instrucciones del Cliente.
- Que Spamina tratará la información a los solos efectos de la correcta prestación de los servicios.
- Que Spamina no los comunicará, ni siquiera para su conservación, a terceros.
- Que, tras el cese en la prestación de los servicios, Spamina procederá a su desactivación y pondrá a disposición del Cliente en formato electrónico toda la información y ficheros disponibles en la plataforma en el momento de la solicitud.

Spamina manifiesta que el tratamiento de datos personales se realizará con pleno sometimiento a las medidas de seguridad establecidas por la normativa española en materia de protección de datos. En todo caso, Spamina realizará sus mejores esfuerzos para implementar las medidas técnicas y organizativas que sean necesarias para lograr la máxima seguridad de los datos de carácter personal, evitando su alteración, pérdida, tratamiento y acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que estén expuestos.

De conformidad con lo dispuesto en la normativa española y comunitaria en materia de protección de datos, Spamina informa al Cliente que, en aras de garantizar una mayor calidad, disponibilidad y nivel del servicio, Spamina ha procedido a contratar los servicios de alojamiento de servidores a las compañías Fhios Smart Knowledge, S.L., con CIF B-64720782 y domicilio social en Ávila, 52 5º 3ª, 08018, y Barcelona y a Claranet S.A.U, con CIF A-61129086, con domicilio social en la calle Juan Gris, 10-18, planta 4, Torres Cerdà (08014), Barcelona y a estos efectos, se ha procedido con las referidas compañías a la firma de los correspondientes contratos de prestación de servicios, acuerdos de nivel de servicios, revisiones y auditorías de cumplimiento de las obligaciones legalmente dispuestas por la normativa de protección de datos.

Suspensión

Las Partes acuerdan que, en caso de impago por parte del Cliente, los servicios contratados a Spamina serán suspendidos de forma automática. El caso de suspensión, el Cliente dispondrá de un plazo de 30 días para abonar a Spamina los importes debidos.

En caso de que el Cliente no abonare a Spamina las cantidades económicas pendientes en el plazo indicado de 30 días, Spamina procederá a la suspensión automática de todos los servicios sobre los que exista alguna cantidad debida por el Cliente y esta suspensión devendrá efectiva al día siguiente tras el cumplimiento del plazo de los 30 días. La duración de esta suspensión se prolongará hasta el día en que el Cliente abone a Spamina la totalidad de importes adeudados.

Si las Partes hubieran acordado que el pago se realice mensualmente, Spamina seguirá facturando durante los meses siguientes al momento de

la suspensión. En caso de que el pago se hubiera pactado por períodos anuales, tras la suspensión, Spamina seguirá cobrando los importes mensualmente, subsistiendo en todo caso la obligación del Cliente de abonar todos los importes que se le vayan facturando hasta alcanzar el pago de la cuantía total acordada.

En caso de que el Cliente al que se le hubiera suspendido el servicio por falta de pago, siguiera incumpliendo su obligación de pago durante un plazo superior a los 30 días, este incumplimiento será considerado como incumplimiento esencial del Acuerdo y por ende, Spamina podrá rescindirlo sin que corresponda al Cliente derecho indemnizatorio alguno.

Resolución anticipada del Acuerdo

Ambas Partes pueden suspender la vigencia del presente Acuerdo, o en su caso, rescindirlo en caso de que se verifique alguna de las circunstancias siguientes:

- Cualquier Parte incumpliere, de forma esencial, las condiciones contenidas en el Acuerdo y no subsanare dicho incumplimiento en el plazo de 30 días contados a partir de la a notificación escrita de la otra Parte instándole a subsanar.
- Cualquier Parte cesara sus operaciones empresariales o se viera sometida a procedimientos de insolvencia y dichos procedimientos no se desestimarán en un plazo inferior a 90 días (** previsión nula según la ley española*).
- Cualquier Parte incumpliere, de forma esencial, lo dispuesto en este Acuerdo más de 2 veces.

En caso de resolución anticipada, se producirán los siguientes efectos:

- La cesión de derechos por cualquier Parte a la otra cesará con efecto inmediato (a menos que se disponga de otro modo en este apartado)
- Spamina proporcionará al Cliente acceso a los datos generados en relación con el mismo, dándole la posibilidad de exportarlos en un formato interoperable y estándar en el mercado, durante un periodo de tiempo comercialmente razonable y ello, sin perjuicio del derecho de Spamina a facturarle por la prestación del referido servicio.
- Transcurrido un período como máximo de treinta días, Spamina eliminará los datos del Cliente mediante la supresión de re direccionamientos que hagan referencia a estos datos en los servidores activos de Spamina y los irá sobrescribiendo conforme transcurra el tiempo, de suerte que la recuperación de dicha información devendrá imposible.
- Ambas Partes realizarán esfuerzos comercialmente razonables para devolver o destruir cualquier información confidencial perteneciente a la otra Parte, si ésta lo solicitara.

En caso de resolución anticipada del presente Acuerdo, Spamina se reserva el derecho a facturar al Cliente la cantidad no abonada restante hasta la culminación del compromiso anual asumido para con el Cliente.

En caso de que el Acuerdo sea resuelto anticipadamente por el Cliente por causas imputables, directa o indirectamente, a éste, a usuarios autorizados, o a terceros ajenos al Acuerdo, el Cliente reconoce que Spamina no tendrá obligación de devolver cantidad económica alguna que en su caso se le hubiera anticipado. Ello, sin perjuicio del derecho de Spamina a reclamar al Cliente los daños y perjuicios que la resolución anticipada hubiera podido causarle.

En caso de que el Acuerdo sea resuelto unilateralmente por el Cliente, sin que exista alguna justa causa para ello, el Cliente se compromete a abonar a Spamina, en concepto de indemnización, las cantidades pendientes hasta el cumplimiento del plazo de prestación del servicio acordado entre las Partes.

Legislación aplicable y fuero

Para toda cuestión litigiosa o conflicto que se derive del presente Acuerdo, será aplicable la ley española. Ambas Partes, con renuncia expresa a su fuero propio, se someten a la jurisdicción y competencia de los Juzgados y Tribunales de la ciudad de Madrid.

Gartner Cool Vendor Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
The Gartner Cool Vendor Logo is a trademark and service mar kif Gartner, Inc., and/or its affiliates, and is used here in with permission. All rights reserved.

Gartner, Inc., Cool Vendors in Spain, 2016, Luis Anavitarte | Federico De Silva | Monica Basso | Angela McIntyre | Lawrence Pingree | Adam Preset, 26 April 2016.