Anexo 1
Descripción General de Servicios

LOS SERVICIOS Y/O NIVELES DE SERVICIO QUE RECOGEN LOS ANEXOS 2 Y 3 MÁS ABAJO Y QUE EL CLIENTE NO HAYA ENCARGADO EN LA SECCIÓN B DEL CONTRATO NO SERÁN APLICABLES A ESE CLIENTE.

1. Definitions

1.1. En el Contrato, incluidos sus Anexos, las siguientes palabras tendrán, a menos que el contexto requiera claramente lo contrario, los siguientes significados:

«Correo Electrónico»	es todo mensaje SMTP enviado o recibido a través del Servicio;
«Correo Masivo»	es un grupo de más de cinco mil (5.000) mensajes electrónicos con un contexto esencialmente similar enviados o recibidos en una única operación o en una serie de operaciones relacionadas entre sí;
«Horario Laboral Habitual»	es el horario comprendido entre las 08.30 y 17.30 horas del Reino Unido, de lunes a viernes, sin contar los días festivos reconocidos en Inglaterra;
«Miembro»	se refiere al Cliente y a las organizaciones con las que el Cliente crea redes cifradas mediante el uso del Servicio de Cifrado de Límites;
«Paquete de Servicios Indisociable»	es un paquete de Servicios tal y como se establece en el Apartado B, «Servicio y Costes», que está sujeto a las disposiciones de la Cláusula 4.7;
«Proxy Abierto»	alude a un servidor proxy configurado de tal manera que permite a terceros desconocidos o desautorizados a acceder, guardar o reenviar DNS, páginas web u otros datos;
«Retransmisión Abierta»	es un servidor de correo electrónico configurado para recibir mensajes electrónicos de un tercero desconocido o no autorizado y reenviar dicho mensaje a uno o varios destinatarios que no son usuarios del sistema de correo electrónico al que está conectado dicho servidor de correo electrónico. Retransmisión Abierta también puede nombrarse como «retransmisión de spam» o «retransmisión pública»";
«Spam (correo basura)»	es el correo electrónico comercial no solicitado;
«Torre»	es un clúster de servidores de correo electrónico de carga equilibrada;
«Usuario»	se refiere a una persona, buzón de correo o máquina que utilice el Servicio; y
«Virus»	es un elemento de un código de programa, entre otros un elemento auto replicador, que suele (aunque no siempre) estar disfrazado de otra cosa y que desencadena unos hechos inesperados y normalmente no deseados por la víctima y que está diseñado de tal manera que pueda infectar otros sistemas informáticos.

2. Introducción

2.1 Symantec es un proveedor de servicios gestionados especializado en seguridad web, Correo Electrónico y de mensajería instantánea a nivel de Internet.

2.2 El Servicio está gestionado las veinticuatro (24) horas del día y los siete (7) días de la semana por el Centro de Operaciones Global de Symantec. El Servicio se controla para la disponibilidad de los equipos capacidad del servicio y utilización de los recursos de la red.

2.3. Si Symantec fuera incapaz de entregar el Correo Electrónico al servidor de correo de un Cliente, Symantec almacenará el correo entrante del Cliente hasta un máximo de siete (7) días pendiente de entrega.

2.4. El Servicio está disponible para Clientes que están conectados de forma permanente a Internet con una dirección IP fija. No puede suministrarse a Clientes cuyos sistemas están conectados a Internet mediante conexión de acceso telefónico o líneas ISDN, o aquellos cuya dirección IP esté asignada de modo dinámico.

2.5. Para todo el correo entrante, se determina la reputación del IP del remitente. El Correo Electrónico que se envíe desde una fuente de dudosa reputación (del tipo a la de los remitentes de spam) se ralentizará para minimizar el impacto sobre la capacidad de la red.

2.6. El Cliente debe configurar los servidores de correo electrónico para limitar la cantidad de destinatarios a menos de 500 por cada conexión SMTP saliente. Un destinatario es una dirección individual de correo electrónico. Un grupo de correo electrónico puede contener uno o varios destinatarios. Si un correo electrónico entrante o saliente incluye más de 500 destinatarios en una conexión SMTP, Symantec procesará los primeros 500 destinatarios y enviará un código de respuesta de SMTP al servidor de correo electrónico remitente para solicitarle a dicho servidor que vuelva a enviar el correo electrónico a los destinatarios restantes.

3. Mantenimiento Previsto

3.1. Para los fines de esta Cláusula 2, el «Mantenimiento Previsto» se refiere a los periodos de mantenimiento respecto de los cuales el Cliente habrá recibido notificación previa con siete (7) días de antelación por parte de Symantec y que puede provocar trastornos en el Servicio debido a la ausencia de disponibilidad de las Torres. El Mantenimiento Previsto no durará más de ocho (8) horas por mes natural y, en ningún caso, tendrá lugar entre las 8.00 y las 16.00 horas (en la zona horaria en la que se encuentre la Torre).

3.2. Siempre que sea posible, el Mantenimiento Previsto se llevará a cabo sin que esto afecte al Servicio. Esto puede conseguirse ejecutando el Mantenimiento Previsto en los periodos conocidos de tráfico lento y llevándolo a cabo en una parte, no en toda, de la red en un momento determinado. Durante los periodos de Mantenimiento Previsto, el tráfico se redireccionará a secciones de la red que no estén sometidas al mantenimiento para reducir los trastornos del Servicio.

3.3. Cuando sea necesario un mantenimiento de emergencia y esto pueda afectar al Servicio, Symantec intentará por todos los medios informar a las partes afectadas y fijará un mensaje de alerta en ClientNet a la mayor brevedad, y, en cualquier caso, dentro de la primera (1ª) hora desde el comienzo del mantenimiento de emergencia.

4. ClientNet

4.1. ClientNet es una herramienta de gestión, de informes y de configuración basada en Internet que es parte integral del Servicio de Symantec. ClientNet, que se pone a disposición del Cliente a través de un registro protegido con una contraseña segura que no debe revelarse a ningún tercero, le ofrece al Cliente la posibilidad de acceder a los datos y estadísticas sobre el uso que hace del Servicio, y ofrece prestaciones de configuración y gestión.

5. Servicio Técnico

5.1. Symantec, durante las veinticuatro (24) horas del día, los siete (7) días de la semana:

a) proporciona servicio técnico al Cliente para los problemas que surjan con el Servicio; y
b) interactúa con el Cliente para resolver dichos problemas.

6. Atención al Cliente

6.1. Symantec ofrece un servicio de atención al Cliente durante el horario laboral habitual para:

a) recibir y procesar órdenes para el suministro del Servicio;
b) recibir y procesar peticiones para efectuar modificaciones sobre los aspectos operativos del Servicio; y
c) responder a las consultas sobre facturas y recibos.

6.2. A menos que se estipule lo contrario en la Descripción del Servicio pertinente, tras recibir una solicitud debidamente cumplimentada y preparada para su ejecución, el departamento de Global Provisioning de Symantec trabará para comenzar a suministrar el Servicio en un plazo de veintisiete (27) horas laborables habituales, teniendo en cuenta que ya se hayan completado todas las fases de diligencia técnica necesaria.

7. Paquetes de servicio indisociables

7.1 La tabla siguiente muestra los Paquetes de Servicio Indisociables que pueden seleccionarse en el Apartado B, «Servicio y Costes»:

Nombre del Paquete de Servicio no Indisociables actual	**Servicios componentes (Servicio componente anterior)**	**Nombre del Paquete de Servicio no Indisociables anterior**
Symantec MessageLabs Email Protect.cloud	Email AV, Email AS	MessageLabs Email Protect
Symantec MessageLabs Email Control.cloud	Email IC, Email CC	MessageLabs Email Control
Symantec MessageLabs Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC	MessageLabs Email Safeguard (or MessageLabs Email Protect & Control)
Symantec MessageLabs Web v2 Protect & Control.cloud	Web v2 Protect, Web v2 URL	MessageLabs Web Protect & Control
Not Offered	(Email AV, Email AS, Web AVASv2)	MessageLabs Email Protect & Web Protect
Not Offered	(Email AV, Email IC, Email AS, Email CC, Web AVASv2)	MessageLabs Email Protect & Control & Web Protect
Not Offered	(Email AV, Email AS, Web AVASv2, Web URLv2)	MessageLabs Email Protect & Web Protect & Control
Symantec MessageLabs Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web v2 Protect, Web v2 URL (Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2)	MessageLabs Email & Web Safeguard (or MessageLabs Email & Web Protect & Control)
Symantec MessageLabs 2 Email Services Bundle	2 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 2 Email Services Bundle
Symantec MessageLabs 3 Email Services Bundle	3 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 3 Email Services Bundle
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving (P))	MessageLabs Email Protect & Control & Archiving (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Lite (P))	MessageLabs Email Protect & Control & Archiving Lite (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Premium(P))	MessageLabs Email Protect & Control & Archiving Premium(P)
Symantec MessageLabs Security Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2, IMS	MessageLabs Security Safeguard
Symantec MessageLabs Complete Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud **(Para los clientes que adquirieron servicios antes del 1 de octubre de 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud)	MessageLabs Complete Email Safeguard
Symantec MessageLabs Complete Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL **(Para los clientes que adquirieron servicios antes del 1 de octubre de 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL)	MessageLabs Complete Email & Web Safeguard
Symantec MessageLabs Ultimate Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL, IMS **(Para los clientes que adquirieron servicios antes del 1 de octubre de 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud,	MessageLabs Ultimate Safeguard

	Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL, IMS)	
Symantec Enterprise Vault.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud	MessageLabs Email Archiving L or Email Archiving.cloud (L)
Symantec Enterprise Vault Enhanced.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec EnterpriseVault Mailbox Continuity.cloud	Messagelabs Email Enhanced Archive L or Email Enhanced Archiving.cloud (L)

8. Nombres del servicio anterior

8.1 Para los clientes que adquirieron servicios antes del 1 de junio de 2011, los nombres de los servicios en este documento se indican mediante una nomenclatura diferente a la de los nombres originales de los servicios anteriores. El siguiente cuadro muestra los términos anteriores correspondientes a la nomenclatura revisada a fin de que los clientes puedan determinar qué secciones del documento se aplican a los servicios adquiridos con la nomenclatura anterior.

Nombre del Servicio anterior	Nombre del Servicio actual
MessageLabs Email Anti-Virus	Symantec MessageLabs Email Anti-Virus.cloud
MessageLabs Email Image Control	Symantec MessageLabs Email Image Control.cloud
MessageLabs Email Anti-Spam	Symantec MessageLabs Email Anti-Spam.cloud
MessageLabs Email Content Control	Symantec MessageLabs Email Content Control.cloud
MessageLabs Boundary Encryption	Symantec MessageLabs Email Boundary Encryption.cloud
MessageLabs Web Anti-Spyware and Anti-Virus Service v2	Symantec MessageLabs Web v2 Protect.cloud
MessageLabs Web URL Service v2	Symantec MessageLabs Web v2 URL.cloud
MessageLabs Email Archiving P	Symantec MessageLabs Email Archiving.cloud (P)
MessageLabs Enterprise Instant Messenger (EIM)	Symantec MessageLabs EIM.cloud
MessageLabs EIM Connect	Symantec MessageLabs EIM Connect.cloud
MessageLabs EIM Communicate	Symantec MessageLabs EIM Communicate.cloud
MessageLabs Policy Based Encryption	Symantec MessageLabs Policy Based Encryption.cloud
MessageLabs Email Continuity (EC), or Symantec MessageLabs Email Continuity.cloud (D)	Symantec Email Continuity.cloud (EC)
Schemus Tool	Schemus Tool
MessageLabs Instant Messaging Security Service (IMS)	Symantec MessageLabs Instant Messaging Security.cloud
MessageLabs Email Archiving D, or Symantec MessageLabs Email Archiving.cloud (D)	Symantec Email Continuity Archive.cloud
MessageLabs Email Archiving Lite D, or Symantec MessageLabs Email Archiving.cloud Lite (D)	Symantec Email Continuity Archive Lite.cloud
MessageLabs Volume Mail	Symantec MessageLabs Volume Mail
Hosted Endpoint Protection	Symantec Endpoint Protection.cloud
MessageLabs Personal Archive L or Symantec MessageLabs Email Personal Archiving.cloud (L)	Symantec Enterprise Vault Personal.cloud
MessageLabs Email Discovery Archive L, or Symantec MessageLabs Email Discovery Archiving.cloud (L)	Symantec Enterprise Vault Discovery.cloud
MessageLabs Personal Archive L for BlackBerry®, or Symantec MessageLabs Personal Archive for BlackBerry®.cloud (L)	Symantec Enterprise Vault.cloud Blackberry Option
MessageLabs Email Archiving Premiium L , or Symantec MessageLabs Email Premium Archiving.cloud (L)	AdvisorMail on Symantec.cloud™
MessageLabs Email Archiving IM Premium L, or Symantec MessageLabs Email Premium Archiving.cloud for IM (L)	AdvisorMail IM Option on Symantec.cloud™
MessageLabs Email Archiving Bloomberg Message Premium L, or Symantec MessageLabs Premium Archiving.cloud for Bloomberg	AdvisorMail Bloomberg Option on Symantec.cloud™
MessageLabs Email Archive Import Service L, or Symantec MessageLabs Email Archiving.cloud (L) Import	Symantec Enterprise Vault.cloud Data Import Option
MessageLabs Email Continuity L, or Symantec MessageLabs Email Continuity.cloud (L)	Symantec Enterprise Vault Mailbox Continuity.cloud
MessageLabs User Roaming Agent Service (“Smart Connect”)	Symantec MessageLabs Web v2 Smart Connect.cloud

Anexo 2
Descripción de Servicios

Apéndice 1 – Servicio Symantec MessageLabs Email Anti-Virus.cloud (Anti-Virus para Correo Electrónico)

1. Aspectos Generales

1.1. El Servicio Symantec MessageLabs Email Anti-Virus.cloud («Email AV») es un Servicio de Symantec que analiza la existencia de virus en el correo electrónico en el entorno de Internet. El correo entrante y saliente del Cliente, así como todos los documentos adjuntos, macros y archivos ejecutables, pasa por Email AV mediante el uso de configuración de registros DNS y MX.

1.2. El correo y los adjuntos los analizan una serie de múltiples productos antivirus líderes en el sector, entre los que se incluye Skeptic™, el sistema heurístico de análisis propio de Symantec.

2. Mensajes de Alerta

2.1. Si se encuentran virus en el correo entrante del Cliente o en los adjuntos, y si el Cliente así lo ha seleccionado, se enviará una alerta automática al remitente y al destinatario mediante una notificación. En el caso del correo saliente del Cliente, el Servicio se lo notificará únicamente al remitente y no al destinatario. En ambos casos también pueden enviarse notificaciones al administrador de correo. El correo infectado se redirecciona a un servidor seguro y queda pendiente de destrucción automática tras el plazo de siete (7) días, siempre que no haya sido enviado como virus de emisión de correo masivo, en cuyo caso se destruye inmediatamente.

2.2. En caso de una fuga trascendental de un nuevo virus, se fijará un mensaje de alerta en ClientNet.

3. Configuración

3.1. ClientNet puede utilizarse para personalizar textos de título, liberar los Correos Electrónicos infectados con virus y establecer tamaños máximos de correo.

4. Liberación de un Correo Electrónico infectado con virus

4.1. Cuando se constate que un Correo Electrónico infectado con virus pueda liberarse, éste podrá ser liberado del servidor seguro usando ClientNet. El Correo Electrónico se liberará bien a la primera dirección de la lista original de destinatarios, bien a una dirección específica notificada previamente a Symantec y registrada por Symantec en ClientNet (Nota: estas direcciones pueden ser grupos de direcciones de Correo Electrónico o alias, en cuyo caso el Correo Electrónico será liberado a todas las direcciones del grupo o alias). De forma opcional, Symantec puede liberar el Correo Electrónico infectado a una dirección alternativa tras recibir el Formulario adecuado de Autorización para la Liberación. Symantec únicamente actuará a petición autorizada por el Cliente para redireccionar el Correo Electrónico infectado por virus. Symantec no devolverá los Correos Electrónicos infectados por virus al remitente, ni los reenviará a terceros. Ciertos Correos Electrónicos infectados con virus enviados al Cliente no podrán liberarse debido a que contienen virus que son especialmente infecciosos o nocivos, en cuyo caso se exponen en ClientNet como susceptibles de liberación.

5. Términos y Condiciones de Email AV

5.1. En caso de solicitar la liberación de un Correo Electrónico infectado con virus, Symantec lo liberará en un plazo de ocho (8) horas laborables habituales tras recepción de la petición de liberación debidamente autorizada.

Apéndice 2
Servicio Symantec MessageLabs Email Image Control.cloud
(Control de Imagen para Correo Electrónico)

1. Aspectos Generales

1.1. El Servicio Symantec MessageLabs Email Image Control.cloud («Email IC») es un Servicio de control de imagen de Symantec en el entorno de Internet diseñado para detectar imágenes pornográficas dentro de archivos de imágenes.

2. Descripción del Servicio

2.1. El correo entrante y saliente del Cliente se puede analizar mediante un Análisis de Composición de la Imagen (Image Composition Analysis o ICA), que detecta imágenes pornográficas dentro de archivos de imágenes adjuntos al Correo Electrónico.

2.2. Si se sospecha que el correo entrante o saliente del Cliente puede contener imágenes pornográficas, se tomará una serie de medidas en función de las opciones de configuración seleccionadas por el Cliente.

3. Configuración

3.1. Tras recibir una solicitud totalmente cumplimentada y aceptada, Symantec se encargará de que el servicio Email IC esté disponible para el Cliente. En principio, Email IC estará habilitado para cada dominio del Cliente, y el Cliente es responsable de establecer las opciones de configuración de Email IC, mediante el uso de ClientNet, para cada dominio en función de las necesidades del Cliente.

3.2. Existen unas opciones para especificar el nivel de sensibilidad de detección del filtro ICA. Dicha sensibilidad puede establecerse en Alta, Media o Baja; aunque estas opciones son especialmente subjetivas, en el nivel de sensibilidad Alta se sospechará la existencia de un mayor número de imágenes pornográficas que en el nivel de sensibilidad Baja.

3.3. Existen unas opciones para definir las medidas que deben tomarse al detectar una imagen sospechosa. Dichas opciones pueden establecerse de manera independiente para el correo entrante y saliente, y deberían establecerse de forma compatible con la política de uso de equipos informativos existente y aceptable del Cliente (o su equivalente). Estas opciones son:

3.3.1. registrar el Correo Electrónico sospechoso (proporciona estadísticas que pueden verse vía ClientNet);

3.3.2. etiquetar el Correo Electrónico sospechoso dentro de la cabecera (sólo para correo entrante);

3.3.3. copiar el Correo Electrónico sospechoso a una dirección de Correo Electrónico predefinida;

3.3.4. redireccionar el Correo Electrónico sospechoso a una dirección de Correo Electrónico predefinida;

3.3.5. eliminar el Correo Electrónico sospechoso;

3.3.6. etiquetar el Correo Electrónico sospechoso en la línea del asunto.

3.4. Cuando el Cliente haya identificado remitentes o destinatarios de Correo Electrónico de confianza para la administración de Email IC, el Correo Electrónico de dichos remitentes y destinatarios no se analizará con Email IC.

4. Informe

4.1. Si las opciones elegidas en la Cláusula 3.3 de este Apéndice son redireccionar o eliminar el Correo Electrónico que contenga imágenes sospechosas de pornografía, al remitente se le enviará una alerta automática. Si el Correo Electrónico llega al Cliente también se enviará una alerta al destinatario elegido. El Cliente puede activar y desactivar dichas alertas automáticas mediante ClientNet.

4.2. A través de ClientNet se facilitan informes sobre la eficacia de Email IC en donde se muestran las estadísticas sobre la cantidad de correo entrante y saliente sospechoso de contener imágenes pornográficas. ClientNet puede configurarse para generar informes que se envíen por Correo Electrónico al Cliente de forma semanal o mensual.

5. Términos y Condiciones de Email IC

5.1. NINGÚN PROGRAMA DE DETECCIÓN DE IMÁGENES PORNOGRÁFICAS PUEDE GARANTIZAR UNA DETECCIÓN DEL 100%, POR LO QUE SYMANTEC PUEDE NO ACEPTAR RESPONSABILIDAD ALGUNA POR DAÑOS Y PERJUICIOS NI POR PÉRDIDAS RESULTANTES DE FORMA DIRECTA O INDIRECTA DE CUALQUIER FALLO DEL SERVICIO AL DETECTAR IMÁGENES PORNOGRÁFICAS O AL IDENTIFICAR DE FORMA ERRÓNEA UNA IMAGEN SOSPECHOSA DE SER PORNOGRÁFICA Y QUE PRUEBE POSTERIORMENTE NO SER TAL COSA.

5.2. Puede que no resulte posible analizar los adjuntos cuyo contenido esté bajo el control directo del remitente (por ejemplo, archivos adjuntos cifrados y/o protegidos con contraseña).

5.3. Email IC puede analizar imágenes pornográficas dentro de documentos de algunas versiones de Word, Excel, PowerPoint y pdf, pero no en otros documentos.

5.4. Symantec hace hincapié en que la configuración de Email IC está totalmente bajo el control del Cliente. Email IC está pensado únicamente para permitir que el Cliente lleve a cabo una política de uso de equipos informáticos aceptable, instaurada de forma eficaz y existente (o un equivalente). En algunos países puede ser necesario el consentimiento de los individuos. Symantec aconseja al Cliente que siempre compruebe la legislación local antes de hacer uso de Email IC. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de Email IC. El Cliente reconoce que la definición de lo que constituye o no una imagen pornográfica es subjetiva, y debe tenerlo en cuenta a la hora de configurar el Servicio.

5.5. Si el Cliente libera o solicita la liberación de un Correo Electrónico infectado con virus, el Correo Electrónico liberado no será analizado con Email IC antes de su liberación.

.

Apéndice 3
Servicio Symantec MessageLabs Email Anti-Spam.cloud (Anti Spam para Correo Electrónico)

1. Aspectos Generales

1.1. El Servicio Symantec MessageLabs Email Anti-Spam.cloud («Email AS») es un Servicio Anti Spam para Correo Electrónico en el entorno de Internet diseñado para proteger al Cliente del Correo Electrónico no solicitado o no deseado.

2. Descripción del Servicio

2.1. El correo entrante del Cliente se podrá analizar mediante un número de distintos métodos de detección para determinar si se trata o no de Spam. Si se sospecha que un Correo Electrónico es Spam, se emprenderá una de dichas acciones en función de las opciones de configuración seleccionadas por el Cliente en la Cláusula 3.2 que figura más adelante.

2.2. El Cliente puede elaborar una lista de remitentes privados autorizados y, también pueden hacerlo los Usuarios si el Cliente ha activado las opciones para los Usuarios. Si este método de detección está activado y se recibe un Correo Electrónico entrante enviado desde un dominio que figura en la lista de remitentes autorizados, automáticamente pasará por encima de cualquier otro método de detección de Spam seleccionado.

2.3. El Cliente puede elaborar una lista de remitentes privados bloqueados, y, también pueden hacerlo los Usuarios si el Cliente ha activado las opciones para los Usuarios. Si está seleccionado este método de detección y se recibe un Correo Electrónico entrante enviado desde un dominio que figura en la lista de remitentes bloqueados, se emprenderá una acción tal y como se define en las opciones de configuración de la Cláusula 3.2 que figura más adelante.

2.4. Pueden utilizarse también varias listas de remitentes públicos bloqueados; si uno de estos métodos de detección está seleccionado y se recibe un Correo Electrónico entrante enviado desde un dominio que figura en alguna lista de remitentes públicos bloqueados, se emprenderá una acción tal y como se define en la opción de configuración de la Cláusula 3.2 que figura más adelante.

2.5. Si el Correo Electrónico no se ha eliminado como resultado de su bloqueo tal y como se ha mencionado anteriormente, y el sistema de firma está seleccionado y como resultado de la detección del Correo Electrónico como Spam debería emprenderse una acción aún más severa que la que ya está seleccionada como resultado de la detección de la lista de remitentes bloqueados, el Correo Electrónico entrante del Cliente se analizará mediante el sistema de firma. Si se detecta un Correo Electrónico como Spam meditante este método, se emprenderá una acción tal y como se define en las opciones de configuración de la Cláusula 3.2 que figura más adelante. Dicha acción sustituirá a cualquier otra acción menos severa que hubiera estado seleccionada previamente en cualquiera de los métodos de listas de remitentes bloqueados.

2.6. Si el Correo Electrónico no se ha eliminado como resultado de los procesos anteriores y está seleccionada la opción de detección heurística, y la acción que debería haberse emprendido como resultado de la detección del Correo Electrónico como Spam tal y como está configurado por el Cliente es más severa que la que está actualmente seleccionada como resultado de una detección por los procesos anteriores, el Correo Electrónico entrante del Cliente se analizará mediante un análisis heurístico. Si se detecta heurísticamente un Correo Electrónico entrante como Spam, se emprenderá una acción definida en las configuraciones de la Cláusula 3.2 que figura más adelante. Dicha acción sustituirá a cualquier otra acción menos severa que hubiera estado seleccionada previamente por alguno de los métodos anteriores.

2.7. Las listas de remitentes bloqueados o autorizados facilitadas por Symantec únicamente se ofrecen a modo de ejemplo.

3. Configuración

3.1. Tras recibir una solicitud totalmente cumplimentada y aceptada, Symantec se encargará de que el servicio Email AS esté disponible para el Cliente. En principio, Email AS estará habilitado para cada dominio del Cliente. EL CLIENTE RECONOCE QUE EMAIL AS SE LE FACILITARÁ DE CONFORMIDAD CON LAS CONFIGURACIONES POR DEFECTO DE SYMANTEC APLICADAS DESDE EL PRINCIPIO; DE IGUAL MODO, RECONOCE QUE ES RESPONSABILIDAD EXCLUSIVA DEL CLIENTE LA CONFIGURACIÓN DE EMAIL AS A TRAVÉS DE CLIENTNET EN FUNCIÓN DE SUS PROPIAS NECESIDADES. Las configuraciones por defecto aplicadas para Email AS incluyen las siguientes acciones:

3.1.1 Bloqueo y eliminación de Correo Electrónico; o
3.1.2 Cuarentena de Correo electrónico; y
3.1.3 Uso de una lista aceptada de remitentes para direcciones IP, dominios y direcciones de correo electrónico; y
3.1.4 Uso de detección de Spam previsto (Skeptic).

3.2. Existen unas opciones para definir las medidas que deben tomarse al detectar un Correo Electrónico sospechoso de ser Spam. Dichas opciones que figuran a continuación pueden seleccionarse para cada método disponible de detección:

3.2.1. etiquetar el Correo Electrónico sospechoso dentro de la cabecera;

3.2.2. etiquetar el Correo Electrónico sospechoso en la línea del asunto.

3.2.3. redireccionar el Correo Electrónico sospechoso a una dirección de Correo Electrónico predefinida (que deberá estar dentro de un dominio analizado por el Servicio);

3.2.4. eliminar el Correo Electrónico sospechoso;

3.2.5. Spam Quarantine (Spam en Cuarentena).

4. Descripción del Servicio Spam Quarantine (Spam en Cuarentena)

4.1. Si el Cliente configura Spam Quarantine para un dominio, la cuenta de Cuarentena de Spam de cada Usuario se instalará automáticamente la primera vez que Email AS identifique un Correo Electrónico sospechoso de ser Spam, y el Usuario recibirá automáticamente una notificación.

4.2. El Usuario puede acceder a Spam Quarantine mediante la interfaz Spam Manager (Gestor de Spam).

4.3. El Spam sospechoso puede almacenarse un máximo de catorce (14) días después de los cuales se eliminará automáticamente. El Cliente puede ampliar el periodo de almacenamiento a más de catorce (14) días mediante pago de una cuota adicional que se calcula en función del número de días por Usuario ("Symantec MessageLabs Extended Spam Quarantine").

4.4. Si Spam Quarantine no es capaz de aceptar el Correo Electrónico, el Spam sospechoso se etiquetará y se enviará al destinatario.

5. Configuración de Spam Quarantine

5.1. El Cliente configura Spam Quarantine a través de ClientNet.

5.2. Las notificaciones del Usuario enviadas por defecto están definidas en el punto 5.2.1 siguiente. El Usuario podrá seleccionar de forma puntual la siguientes opciones de notificación:

5.2.1. Notificaciones diarias;

5.2.2. Notificaciones a diversas frecuencias;

5.2.3. Ninguna recepción de notificaciones.

5.3. Las siguientes opciones de liberación están disponibles mediante Spam Manager:

5.3.1. Eliminación del Correo Electrónico;

5.3.2. Liberación del Correo Electrónico a las direcciones de los destinatarios originales;

5.3.3. Revisión del texto del Correo Electrónico.

5.4. Para poder utilizar Spam Quarantine el Cliente debe contar con una Lista de Validación registrada en Symantec. La Lista de Validación comprende todas las direcciones válidas de Correo Electrónico utilizadas por el Cliente. Cualquier dirección de destinatario que no figure en la Lista de Validación se considerará inválida y el Correo Electrónico no se enviará a dicha dirección.

5.5. Mediante ClientNet el Cliente puede controlar otros aspectos de Spam Manager: (a) política de notificación automática o manual; (b) configuración de resumen de notificaciones; (c) configuraciones de idiomas; (d) Configuraciones para Usuarios; (e) programación de Correos Electrónicos con alias y (f) Usuarios especializados (por ejemplo, Administradores de Cuarentena).

5.6. El Cliente podrá designar grupos de direcciones de correo electrónico para poner en cuarentena mensajes indeseados (Spam Quarentine) englobándolos todos en una única dirección a nombre de un alias, siendo esta dirección accesible a personas autorizadas. El número máximo de direcciones de correo que se pueden englobar en una única dirección se sitúa en cincuenta (50). Symantec se reserva el derecho de eliminar el grupo de cuentas del Cliente en el caso de que se supere el número máximo de direcciones vinculadas al alias.

6. Informe

6.1. A través de ClientNet se puede acceder al informe sobre la eficacia de Email AS. ClientNet puede configurarse para generar informes que se enviarán al Cliente por Correo Electrónico de forma semanal o mensual.

7. Términos y Condiciones de Email AS

7.1. NINGÚN PROGRAMA ANTI SPAM PUEDE GARANTIZAR UNA DETECCIÓN DEL 100%, POR LO QUE SYMANTEC NO ACEPTARÁ RESPONSABILIDAD ALGUNA POR DAÑOS Y PERJUICIOS NI POR PÉRDIDAS RESULTANTES DE FORMA DIRECTA O INDIRECTA DE CUALQUIER FALLO DEL SERVICIO AL DETECTAR SPAM O AL IDENTIFICAR DE FORMA ERRÓNEA UN CORREO ELECTRÓNICO SOSPECHOSO DE SER SPAM Y QUE PRUEBE POSTERIORMENTE NO SER TAL COSA.

7.2 Symantec hace hincapié en que la configuración de Email AS está totalmente bajo el control del Cliente. Symantec aconseja al Cliente que cuente con una política de uso de equipos informáticos aceptable (o su equivalente). En ciertos países puede ser necesaria la obtención del consentimiento de los individuos, por lo que Symantec aconseja consultar siempre la legislación local antes de hacer uso de Email AS. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de Email AS.

Apéndice 4
Servicio Symantec MessageLabs Email Content Control.cloud
(Control del Contenido para Correo Electrónico)

1. Aspectos Generales

1.1. El Symantec MessageLabs Email Content Control.cloud («Email CC») es el Servicio de control de contenido de Symantec diseñado para permitir que el Cliente configure su propia regla basada en una estrategia de filtrado en consonancia con su política de uso de los equipos informáticos aceptable (o su equivalente) respecto del Correo Electrónico.

2. Descripción del Servicio

2.1. Email CC permite que el Cliente cree una compilación de reglas en función de las cuales se filtre el correo entrante y saliente de conformidad con el presente Apéndice 4. Una regla es una instrucción configurada por el Cliente que se usa para identificar un formato especial de mensaje/adjunto o de contenido que tiene aparejado un tipo de medida que deberá tomarse en relación con el Correo Electrónico.

3. Configuración

3.1. Tras recibir una solicitud totalmente cumplimentada y aceptada, Symantec hará que el servicio Email CC esté disponible para cada dominio aplicable del Cliente. El Cliente es responsable de establecer las opciones de configuración de Email CC, mediante el uso de ClientNet, para cada dominio en función de las necesidades del Cliente.

3.2. El Cliente puede configurar las reglas 'por dominio', 'por grupo' o de forma 'individual'.

3.3. Los cambios que efectúe el Cliente en las reglas estarán en vigor en un plazo de 24 horas tras la ejecución del cambio.

3.4. Existen unas opciones para definir las medidas que deben tomarse al detectar un Correo Electrónico sospechoso. Dichas opciones pueden establecerse de manera independiente para el correo entrante y saliente, y deberían establecerse de forma compatible con la política de uso de equipos informativos existente y aceptable del Cliente (o su equivalente). Estas opciones son:

3.4.1. Bloqueo y eliminación del Correo Electrónico sospechoso;

3.4.2. Etiquetado (si es entrante) y redirección del Correo Electrónico sospechoso a un administrador especificado;

3.4.3. Etiquetado (si es entrante) y copia del Correo Electrónico sospechoso a un administrador especificado;

3.4.4. Etiquetado (si es entrante) en el encabezado del Correo Electrónico sospechoso;

3.4.5. Compresión de los archivos adjuntos al Correo Electrónico;

3.4.6. Registro únicamente para las estadísticas de ClientNet;

3.4.7. Etiquetado en la línea de asunto.

4. Informe

4.1. A través de ClientNet el Cliente puede acceder a los resultados de sus reglas mediante resúmenes diarios, semanales, mensuales o anuales organizados tanto por regla como por Usuario.

4.2. Los Informes que contienen registros de actividad del Servicio pueden generarse de forma semanal o mensual y enviarse por Correo Electrónico al Cliente cuando éste lo solicite.

4.3. Meditante ClientNet el Cliente puede activar y desactivar las notificaciones configuradas por el Cliente en función de cada regla.

5. Ayuda de Content Control

5.1. La ayuda incluye un paseo por la interfaz de Email CC con una descripción del Servicio y una sesión de Preguntas Frecuentes.

6. Comodines

6.1. Email CC trabaja con un acoplamiento exacto de las reglas configuradas del Cliente. Como excepción específica, no obstante, los comodines permiten que el Cliente configure Email CC mediante ClientNet para identificar ciertas fórmulas alfanuméricas que siguen un patrón específico (como números de la Seguridad Social, números de Seguros Sociales Nacionales e información sobre tarjetas de crédito).

7. Términos y Condiciones de Content Control

7.1. La lista sugerida de palabras y ejemplos de normas facilitados por Symantec contienen palabras que pueden resultar ofensivas.

7.2. El Cliente acepta y acuerda que Symantec podrá compilar y publicar listas de palabras predeterminadas que contengan palabras obtenidas de las listas de palabras elaboradas por los Clientes.

7.3. El Cliente reconoce que si Email CC se utiliza junto con la medida de cuarentena del Servicio de Anti-Spam para Correo Electrónico, esto puede tener como resultado que el Spam sospechoso se ponga en cuarentena antes de ser filtrado por Email CC.

7.4. Email CC puede analizar el contenido de documentos de algunas versiones de Word, Excel, PowerPoint y pdf, pero no en otros documentos.

7.5. Symantec hace hincapié en que la configuración de Email CC está totalmente bajo el control del Cliente y que la exactitud de dicha configuración determinará la exactitud del Servicio de Email CC, por lo que Symantec puede no aceptar responsabilidad alguna por daños y perjuicios ni por pérdidas resultantes de forma directa o indirecta de cualquier fallo del servicio al detectar o identificar de forma errónea un Correo Electrónico con contenido sospechoso y que pruebe posteriormente no ser tal cosa.

7.6. Symantec aconseja al Cliente que cuente con una política de uso de equipos informáticos aceptable (o su equivalente) para controlar el uso del correo electrónico por parte de sus Usuarios, y que toda regla plantilla facilitada por Symantec apoye dicha política. En ciertos países puede ser necesaria la obtención del consentimiento de los individuos, y Symantec aconseja consultar siempre la legislación local antes de hacer uso de Email CC. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de Email CC.

Apéndice 5
Servicio Symantec MessageLabs Email Boundary Encryption.cloud (Cifrado de Límites)

1. Aspectos Generales

1.1. El Servicio Symantec MessageLabs Email Boundary Encryption.cloud («BE») ofrece unos canales de comunicación cifrada que permiten que el Cliente forme una red de Correo Electrónico privada y segura (SPEN) con organizaciones socias designadas («SPEN Partners» o «Socios SPEN»). Esta configuración se conoce como cifrado « Obligado» o «Enforced».

1.2. Asimismo, el Cliente podrá recibir correo electrónico cifrado enviado de forma oportunista desde organizaciones con servidores de correo compatibles con TLS para los que no existe cifrado Obligado con el Cliente si dichas organizaciones cuentan con servidores de correo compatibles con TLS. Esta configuración se conoce como cifrado «Oportunista».

1.3. Si el Cliente ha contratado el BE pero no ha identificado a ningún miembro de SPEN (red privada segura de correo electrónico), el Cliente puede recibir mensajes entrantes en TLS oportunista, y enviar mensajes electrónicos oportunistas salientes cifrados a organizaciones que no son miembros de SPEN.

1.4. El Cliente debe asimismo configurar sus servidores de correo electrónico para el modelo de conexión segura ("Secure Connection") de BE, en cuyo caso:

1.4.1 El intercambio de e-mails entre Symantec y los servidores de correo de la conexión segura del Cliente se llevará a cabo con codificación de seguridad TLS. Los reenvíos se llevarán a cabo en formato codificado o no codificado según (i) el Cliente haya pedido concretamente que se cumpla TLS y (ii) la capacidad del servidor del destinatario para recibir e-mails en TLS Oportunista.

1.4.2 **EL CLIENTE RECONOCE QUE EN CASO DE QUE NO SE APLIQUE EL MODELO DE CONEXIÓN SEGURA A UN SERVIDOR DE CORREO EN PARTICULAR, EL CORREO DE ENTRADA Y DE SALIDA DEL CLIENTE QUE SE ORIGINE O SE RECIBA EN ESE SERVIDOR DE CORREO NO CONTARÁ CON LA SEGURIDAD DE LA CODIFICACIÓN TLS. EL CLIENTE RECONOCE, POR TANTO, QUE NO DEBE ENVIAR NI RECIBIR DATOS CONFIDENCIALES POR MEDIO DE DICHOS SERVIDORES DE CORREO Y QUE SI LO HACE EL RIESGO CORRE POR SU CUENTA.**

1.5 En el supuesto de que el Cliente utilice BE junto con el servicio PBE, Symantec recomienda como práctica óptima que el Cliente implemente el modelo de conexión segura de BE en todos sus servidores de correo.

1.6 **BE NO PUEDE FUNCIONAR DE FORMA AUTÓNOMA, SÓLO FUNCIONA CUANDO SE USA JUNTO CON UNO DE LOS SIGUIENTES SERVICIOS: E-MAIL AV, E-MAIL AS, E-MAIL IC Ó E-MAIL CC**.

2. Aprovisionamiento y facturación

2.1. Symantec comenzará a cobrar por BE a partir de la fecha en que confirme que la red del cliente cuenta con capacidad técnica para admitir BE ("Fecha de aprobación técnica").

2.2 La cláusula 6.2 de Anexo 1 no es válida para BE. Symantec pretende aprovisionar los pedidos y las solicitudes de cambio de BE en un plazo de cuatro semanas a partir de la Fecha de aprobación técnica, siempre y cuando el cliente haya cumplido con la diligencia debida.

2.3 En la eventualidad de que Symantec tenga que asignar recursos técnicos adicionales para prestar el servicio BE debido a que el Cliente no ha cumplido los requisitos, Symantec se reserva el derecho a cobrar comisiones adicionales a razón de €1500 el día por persona.

2. Configuración

2.1. El Cliente definirá los Socios SPEN con los que desea comunicarse de forma segura por dominio. Los Socios SPEN podrán ser clientes o no de BE, no obstante, Symantec no será compatible directamente con Socios SPEN. Las organizaciones que no sean Socios SPEN podrán recibir correo electrónico a través de TLS Saliente Oportunista, tal y como se describe anteriormente en la Cláusula 1 siembre que sus servidores de correo sean compatibles con la recepción de correo cifrado.

2.2. BE está basado en el SMTP sobre TLS estándar (Simple Mail Transfer Protocol over Transport Layer Security o protocolo simple de transferencia de correo electrónico sobre seguridad de la capa de transporte) («STARTTLS»).

2.3. Tanto el servidor de correo del Cliente como del Socio SPEN debe ser compatible con STARTTLS para permitir el uso de BE.

2.4. BE es compatible con las Torres seleccionadas a través de las cuales se envía todo el Correo Electrónico STARTTLS. Por consiguiente, el Cliente designa cuáles de sus dominios utilizarán BE.

2.5. Cuando se utilice BE junto con la aplicación del sistema de firma de Email AS, Symantec aconseja que el Cliente incluya en su una lista de remitentes autorizados para Email AS todos los dominios de sus socios SPEN. Si no se aplica esta buena práctica recomendada, el Cliente admite y acepta que en determinadas circunstancias que impliquen la imposibilidad del sistema local de firma el Correo Electrónico puede ser redireccionado a un sistema de firma remoto a través de una red pública.

3. Certificados y Autenticación

3.1. Cuando el Cliente origina una conexión STARTTLS, el servidor de correo que acepta debe facilitar su certificado para su autenticación. Si el servidor de correo que acepta desea autenticar el Servicio, Symantec le facilitará su certificado de cliente para la autenticación. Si el servidor de correo que acepta no puede autenticar, el Correo Electrónico le será devuelto al Cliente.

3.2. Cuando un servidor de correo externo origine una conexión STARTTLS, el Servicio facilitará su certificado de servidor para su autenticación, pero no insistirá en que el servidor de correo externo facilite su certificado de cliente para su autenticación.

3.3. La validación de todo certificado se basa en la Autoridad de Certificación que ha firmado el certificado. Para cada certificado emitido por un servidor de correo remoto como parte de una conexión STARTTLS, el Servicio validará que una Autoridad de Certificación reconocida ha firmado el certificado. Si un certificado no puede ser validado frente a una Autoridad de Certificación reconocida, la conexión se abandonará y el Correo Electrónico se le devolverá al remitente.

4. Términos y Condiciones del Cifrado

4.1. Symantec no asumirá ninguna responsabilidad por el incumplimiento por parte del Cliente o de un tercero (entre los que se incluye todo Socio SPEN) del cumplimiento de sus obligaciones respecto de los certificados de registro o por lo oportuno o la exactitud de dicha información.

4.2. BE está pensado para ser utilizado únicamente para permitir que el Cliente llevar a cabo una política existente, ejecutada de forma eficaz, de uso de equipos informáticos aceptable (o su equivalente). El uso de los Servicios de cifrado en ciertos países puede estar sujeto a una legislación. Se aconseja al Cliente que consulte siempre la legislación local antes de hacer uso del Servicio BE. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de BE.

Apéndice 6
Servicio Symantec MessageLabs Web v2 Protect.cloud
(Anti Spyware en la web y Anti virus V2)

1. Aspectos Generales

1.1. Una vez que los cambios de configuración pertinentes se han ejecutado, se envían electrónicamente las solicitudes de páginas Web y adjuntos a través del Servicio Symantec MessageLabs Web v2 Protect.cloud («Web v2 Protect») y se examinan digitalmente en busca de virus.

2. Descripción del Servicio

2.1. Las solicitudes externas de HTTP y FTP sobre HTTP, incluidos los adjuntos, macros o archivos ejecutables se redireccionan a través de Web v2 Protect.

3. Configuración

3.1. Las opciones de configuración que exigen dirigir este tráfico externo a través de Web v2 Protect las efectúa y las mantiene el Cliente y dependen de la infraestructura técnica del Cliente. El Cliente debe garantizar que el tráfico interno HTTP/FTP sobre HTTP (por ejemplo a la red corporativa) no se dirija a través de Web v2 Protect. Cuando el Cliente cuente con servicios de Internet que ordenen una conexión directa en lugar de a través de un proxy, será responsabilidad del Cliente hacer todos los cambios necesarios en su propia infraestructura para facilitar esta situación.

3.2. El acceso a Web v2 Protect está restringido mediante Scanning IP, es decir, las direcciones IP desde las que se origina el tráfico web del Cliente. Scanning IP también se utiliza para identificar al Cliente y seleccionar de forma dinámica las configuraciones específicas del Cliente.

3.3. Web v2 Protect analizará los elementos pertinentes de la página web y los adjuntos a ella que puedan contener virus, códigos dañinos, spyware o adware. Puede que no sea posible analizar ciertas páginas web, contenidos o adjuntos (por ejemplo, cuando están protegidos por contraseñas). Los adjuntos identificados específicamente como no analizables no se bloquearán. El tráfico transmitido y cifrado (como el de los medios de comunicación transmitidos y/o HTTPS/SSL) no puede analizarse y pasará a través de Web v2 Protect sin ser analizado.

3.4. Roaming User Support es una función optativa que amplía el servicio Web v2 Protect a Usuarios que no tengan acceso a una red empresarial (por ejemplo, un Usuario que trabaja en casa). El Cliente deberá instalar un archivo PAC en el PC del Usuario para dirigirlo al portal de Internet de Symantec cuando se pone en marcha el explorador. Para obtener acceso al portal de Internet, el Usuario deberá contar con un nombre de usuario y contraseña. El archivo PAC se puede bajar de ClientNet en forma de plantilla para que el Cliente haga las modificaciones necesarias.

4. Alertas

4.1. Si la página web o los adjuntos de un Cliente resultan contener un elemento identificado como un virus, spyware o adware, el acceso a esa página web o adjunto quedará denegado y al usuario de Internet se le aparecerá una página web de alerta automática. En casos aislados, y cuando uno o más elementos del contenido solicitado esté bloqueado, puede no ser posible mostrar la página web de alerta, y la página de alerta puede sustituir al contenido del elemento solicitado, pero el acceso a la página o al adjunto infectados seguirá estando denegado.

4.2. Hay un apartado dentro de las páginas web de alerta automática que los Clientes pueden personalizar a través de ClientNet.

5. Informes

5.1. A través de ClientNet se accede a los informes sobre la eficacia de Web v2 Protect.

5.2. Para activar los informes por Usuario o por grupo, el Cliente deberá instalar el programa pertinente (el «Client Site Proxy» o proxy del sitio del Cliente) de conformidad con las directrices de instalación. El uso del Client Site Proxy está sujeto al Acuerdo de Licencia del Usuario Final que se facilita con el Client Site Proxy.

5.3. El Cliente reconoce que los datos procedentes de los informes detallados de ClientNet se guardan solamente por un plazo máximo de cuarenta (40) días y no estarán a disposición del Cliente una vez vencido ese plazo. Los datos resumidos de ClientNet están disponibles por un periodo máximo de doce (12) meses.

5.4. El Cliente podrá solicitar la ampliación del plazo de los informes detallados de ClientNet hasta un máximo de seis (6) meses suscribiendo el servicio WSS Enhanced Data Retention

6. Términos y Condiciones Generales

6.1. NINGÚN PROGRAMA DE ANÁLISIS PUEDE GARANTIZAR UNA DETECCIÓN DEL 100%, POR LO QUE SYMANTEC NO ACEPTARÁ RESPONSABILIDAD ALGUNA POR DAÑOS Y PERJUICIOS NI POR PÉRDIDAS RESULTANTES DE FORMA DIRECTA O INDIRECTA DE CUALQUIER FALLO DE WEB v2 PROTECT AL DETECTAR VIRUS, CÓDIGO MALICIOSO, SPYWARE O ADWARE.

6.2. Symantec hace hincapié en que la configuración de Web v2 Protect está totalmente bajo el control del Cliente. Web v2 Protect está pensado únicamente para permitir que el Cliente lleve a cabo una política de uso de equipos informáticos aceptable, instaurada de forma eficaz y existente (o un equivalente). En algunos países puede ser necesario el consentimiento de los individuos. Symantec aconseja al Cliente que siempre compruebe la legislación local antes de hacer uso de Web v2 Protect. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de Web v2 Protect.

6.3 El tráfico web del Cliente, cuando éste utiliza Web v2 Protect, no podrá exceder la cantidad de treinta megabytes (30 MB) por Usuario al día (calculado como la media por Usuario del Número de Uso Registrado del Cliente respecto de Web v2 Protect). En la eventualidad de que se sobrepase dicho límite, Symantec se reserva el derecho a:

6.3.1 no prestar el Servicio o suspender Web v2 Protect total o parcialmente de inmediato mientras no se remedie la situación; o bien

6.3.2 cobrar al Cliente por más Usuarios de tal modo que la cuota refleje el tráfico real del web usado por el Cliente y expedir más facturas y/o modificar las facturas siguientes para cubrir el aumento registrado en la utilización del Servicio de forma prorrateada durante el tiempo que quede del periodo de facturación en curso.

Apéndice 7
Servicio Symantec MessageLabs Web v2 URL.cloud
(Filtro de URL Web v2)

1. Aspectos Generales

1.1. Una vez que los cambios de configuración pertinentes se han ejecutado, se envían electrónicamente las solicitudes de páginas Web y adjuntos a través del Servicio Symantec MessageLabs Web v2 URL.cloud («Web v2 URL») y se examinan digitalmente.

2. Descripción del Servicio

2.1. Las solicitudes de HTTP y FTP sobre HTTP externas, incluidos los adjuntos, macros o archivos ejecutables, se redireccionan a través de Web v2 URL.

3. Configuración

3.1. Las opciones de configuración que exigen dirigir este tráfico externo a través de Web v2 URL las efectúa y las mantiene el Cliente y dependen de la infraestructura técnica del Cliente. El Cliente debe garantizar que el tráfico interno HTTP/FTP sobre HTTP (por ejemplo a la intranet corporativa) no se dirija a través de Web v2 URL. Cuando el Cliente cuente con servicios de Internet que ordenen una conexión directa en lugar de a través de un proxy, será responsabilidad del Cliente hacer todos los cambios necesarios en su propia infraestructura para facilitar esta situación.

3.2. El acceso a Web v2 URL está restringido a través de Scanning IP, es decir, las direcciones IP desde las que se origina el tráfico web del Cliente. Scanning IP también se utiliza para identificar al Cliente y seleccionar de forma dinámica las configuraciones específicas del Cliente.

3.3. El Cliente puede configurar Web v2 URL para crear reglas de política de restricción de acceso a través de ClientNet (basado tanto en categorías como en tipos de contenido) y desplegar dichas reglas en momentos determinados para Usuarios o grupos específicos mediante el uso del Client Site Proxy descrito en la Cláusula 5.1.

3.4. EL CLIENTE RECONOCE QUE Web v2 URL SE LE FACILITARÁ DE CONFORMIDAD CON LAS CONFIGURACIONES POR DEFECTO DE SYMANTEC APLICADAS DESDE EL PRINCIPIO; DE IGUAL MODO, RECONOCE QUE ES RESPONSABILIDAD EXCLUSIVA DEL CLIENTE LA CONFIGURACIÓN DE Web v2 URL A TRAVÉS DE CLIENTNET EN FUNCIÓN DE SUS PROPIAS NECESIDADES. Las configuraciones por defecto comprenden una función de «Bloqueo y Registro» para las siguientes Categorías de URL:
3.4.1 Adultos / Sexo Explícito; y
3.4.2 Spyware; y
3.4.3 URL de Spam; y
3.4.4 Actividades Delictivas.
3.5. Roaming User Support es una función optativa que amplía el servicio Web v2 URL a Usuarios que no tengan acceso a una red empresarial (por ejemplo, un Usuario que trabaja en casa). El Cliente deberá instalar un archivo PAC en el PC del Usuario para dirigirlo al portal de Internet de Symantec cuando se pone en marcha el explorador. Para obtener acceso al portal de Internet, el Usuario deberá contar con un nombre de usuario y contraseña. El archivo PAC se puede bajar de ClientNet en forma de plantilla para que el Cliente haga las modificaciones necesarias.

4. Alertas

4.1. Si un Usuario solicita una página web o adjuntos en los que se aplique una política de restricción de acceso, el acceso a dicha página web o adjunto será denegado, y al Usuario se le aparecerá una página web de alerta automática. En casos aislados, y cuando uno o más elementos del contenido solicitado está bloqueado, puede no ser posible mostrar la página web de alerta, y la página de alerta puede sustituir al contenido del elemento solicitado, pero el acceso a la página seguirá estando denegado.

4.2. Hay un apartado dentro de las páginas web de alerta automática que los Clientes pueden personalizar a través de ClientNet.

5. Informes

5.1. A través de ClientNet se accede a los informes sobre los resultados de las reglas de la política de restricción de acceso creadas en virtud de la Cláusula 3.3 anterior.

5.2. Para activar los informes y administración por Usuario o por grupo, el Cliente deberá instalar el programa pertinente (el «Client Site Proxy» o proxy del sitio del Cliente) de conformidad con las directrices de instalación. El uso del Client Site Proxy está sujeto al Acuerdo de Licencia del Usuario Final que se facilita con el Client Site Proxy.

5.3 El Cliente reconoce que los datos procedentes de los informes detallados de ClientNet se guardan solamente por un plazo máximo de cuarenta (40) días y no estarán a disposición del Cliente una vez cumplido ese plazo. Los datos resumidos de ClientNet están disponibles por un periodo máximo de doce (12) meses.

5.4 El Cliente podrá solicitar la ampliación del plazo de los informes detallados de ClientNet hasta un máximo de seis (6) meses suscribiendo el servicio WSS Enhanced Data Retention.

6. Términos y Condiciones Generales

6.1 NINGÚN PROGRAMA DE FILTRADO PUEDE GARANTIZAR UNA DETECCIÓN DEL 100%, POR LO QUE SYMANTEC NO ACEPTARÁ RESPONSABILIDAD ALGUNA POR DAÑOS Y PERJUICIOS NI POR PÉRDIDAS RESULTANTES DE FORMA DIRECTA O INDIRECTA DE CUALQUIER FALLO DE Web v2 URL AL DETECTAR URL O CONTENIDO BLOQUEADOS

6.2. Symantec hace hincapié en que la configuración de está totalmente bajo el control del Cliente. Web v2 URL está pensado únicamente para permitir que el Cliente lleve a cabo una política de uso de equipos informáticos aceptable, instaurada de forma eficaz y existente (o un equivalente). En algunos países puede ser necesario el consentimiento de los individuos. Symantec aconseja al Cliente que siempre compruebe la legislación local antes de hacer uso de Web v2 URL. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de Web v2 URL.

6.3 El tráfico web del Cliente, cuando éste utiliza Web v2 URL, no podrá exceder la cantidad de treinta megabytes (30 MB) por Usuario al día (calculado como la media por Usuario del Número de Uso Registrado del Cliente respecto de Web v2 URL). En la eventualidad de que se sobrepase dicho límite, Symantec se reserva el derecho a:

6.3.1 no prestar el Servicio o suspender Web v2 URL total o parcialmente de inmediato mientras no se remedie la situación; o bien
6.3.2 cobrar al Cliente por más Usuarios de tal modo que la cuota refleje el tráfico real del web usado por el Cliente y expedir más facturas y/o modificar las facturas siguientes para cubrir el aumento registrado en la utilización del Servicio de forma prorrateada durante el tiempo que quede del periodo de facturación en curso.

Apéndice 8
Servicio Symantec MessageLabs Email Archiving.cloud (P)

1. Visión global del servicio

1.1 El Servicio Symantec MessageLabs Email Archiving.cloud (P), el Symantec MessageLabs Email Archiving.cloud Lite (P) y el Servicio Symantec MessageLabs Email Archiving.cloud Premium (P) (en conjunto el "Servicio de Archivado (P)") son servicios gestionados híbridos para el archivado, almacenamiento y recuperación de mensajes electrónicos.

1.2 Para Clientes con *500 Usuarios o número inferior,* el Servicio *Symantec MessageLabs Email Archiving.cloud Lite (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3 más abajo;
(ii) Un periodo de retención de 3 años;
(iii) Máximo almacenamiento de 3 GB por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

Para clientes con *más de 500 Usuarios*, el Servicio *Symantec MessageLabs Email Archiving.cloud Lite (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3;
(ii) Un periodo de retención de 3 años;
(iii) Almacenamiento máximo de 1,5 GB por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

1.3 Para Clientes con *500 Usuarios o número inferior,* el Servicio *Symantec MessageLabs Email Archiving.cloud (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3;
(ii) Un periodo de retención de 10 años;
(iii) Máximo almacenamiento de 10 GB (por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

Para clientes con *más de 500 Usuarios*, el Servicio *Symantec MessageLabs Email Archiving.cloud (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3;
(ii) Periodo de retención ilimitado;
(iii) Almacenamiento máximo de 6 GB por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

1.4 Para clientes con *500 Usuarios o número inferior*, el Servicio *Symantec MessageLabs Email Archiving.cloud Premium (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3;
(ii) Las prestaciones especiales (premium) que recoge la cláusula 4 más abajo;
(iii) Un periodo de retención de 10 años;
(iv) Almacenamiento máximo de 10GB por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

Para clientes con *más de 500 Usuarios*, el Servicio *Symantec MessageLabs Email Archiving.cloud Premium (P)* comprende las siguientes prestaciones:

(i) Las prestaciones normales que recoge la cláusula 3;
(ii) Las prestaciones especiales (*premium*) que recoge la cláusula 4;
(iii) Un periodo ilimitado de retención;
(iv) Almacenamiento máximo de 6 GB por Usuario (calculado como la media por Usuario tomando el número total de Usuarios).

1.5 El Cliente debe configurar la función de *journaling* – registro por diario – de Exchange para depositar una copia de los e-mailes internos y externos en un buzón local del servidor Exchange. El o los dispositivos que residan detrás del firewall dentro de la red empresarial del cliente (los "*Dispositivos de Archivado*") pueden entonces emplearse para sacar datos del buzón para su presentación al Servicio de Archivado (P). Los e-mailes depositados en el buzón de *journaling* no se eliminan mientras no se haya confirmado su almacenamiento en el Servicio de Archivado (P).

1.6 Symantec vigilará el uso real del Servicio de Archivado (P) por parte del cliente, de tal modo que si en la práctica el almacenamiento supera la capacidad contratada, el cliente deberá adquirir un bloque adicional de almacenamiento a la tarifa vigente que tenga Symantec. Symantec pasará facturas adicionales y/o hará ajustes prorrateados a las facturas subsiguientes para cubrir los cargos del almacenamiento adicional de forma prorrateada durante el resto del periodo de facturación actual.

1.7 El cliente reconoce y acepta que un e-mail no puede ser eliminado tras ser archivado mientras no se haya cumplido el periodo de retención correspondiente. Lo que quiere decir es que no es posible eliminar mensajes individuales de una forma selectiva.

2. Activación del servicio

2.1 El Cliente deberá rellenar el formulario de solicitud de servicios de Symantec con precisión.

2.2 El Cliente deberá contratar Dispositivo(s) de Archivado para poder utilizar el Servicio de Archivado (P). Los Dispositivos de Archivado adquiridos (y la documentación correspondiente) serán enviados al Cliente para su instalación y configuración. El Cliente se hará cargo de fletes, impuestos, seguros y cargos del Dispositivo de Archivado.

2.3 Symantec se pondrá en contacto con el Cliente para concertar la llamada inicial al cliente.

2.4 Las medidas indicadas en el documento de configuración de cliente de Symantec ("Client Setup Document") deben ser realizadas por el cliente antes de la llamada inicial. Las medidas comprenden las siguientes, pero no están limitadas a ellas:

2.4.1 Abrir una nueva cuenta de directorio activo de usario;
2.4.2 Abrir grupos adicionales de directorios activos;
2.4.3 Añadir usuarios a los grupos de Exchange;
2.4.4 Configurar Firewall (si procede);
2.4.5 Habilitar Microsoft Exchange Journaling (no más de 48 horas antes de instalar el Dispositivo de Archivado);
2.4.6 Instalar Dispositivo de Archivado (debe estar en rack y encendido);
2.4.7 Asegurarse de que todos los buzones para archivar estén habilitados para recibir correo (*mail enabled*);
2.4.8 Configurar acceso remoto para Symantec.

Si el Cliente necesita ayuda con las medidas expuestas, puede llamar a Atención al Cliente de Symantec.

2.5 La llamada inicial al cliente se realizará por medio de WebEx. En esta llamada las partes realizarán las siguientes acciones:

2.5.1 Comprobar que todas las medidas indicadas en el Documento de Instalación de Cliente hayan sido cumplidas;
2.5.2 Instalar el software de archivado y otros programas siguiendo lo expuesto en el Documento de Procedimientos de Instalación de Archivado de Symantec;
2.5.3 Revisar la configuración del directorio activo;
2.5.4 Activar el servicio;
2.5.5 Comprobar la accesibilidad a la interfaz de usuario;
2.5.6 Verificar el proceso de archivado (sitio-a-sitio);
2.5.7 Generar copias de las claves de cifrado de acuerdo con el documento de procedimientos de backup de claves de Symantec (*Key Backup Procedures Document)*.

2.6 Tras la llamada inicial al cliente, éste dispone de una sesión de formación gratuita que comprende sesiones centradas en: (i) Informática, (ii) Normativa, (iii) Supervisión, (iv) Usuario final.

2.7 Una segunda llamada se realiza aproximadamente una (1) semana después de la fecha de activación del servicio. Una vez que se haya comprobado que todo funciona satisfactoriamente, el Cliente contará con los procedimientos estándar de apoyo en el caso de que necesite más asistencia.

3. Prestaciones estándar

3.1 *Resolución de direcciones y lista de distribución/Ampliación del grupo*. Las direcciones de buzones que Exchange marque como direcciones internas serán resueltas al buzón del Usuario correspondiente. Por cada lista de distribución referenciada como recipiente del mensaje, se capturará una lista de las personas que a la sazón estén dadas de alta como metadatos adicionales sobre el mensaje electrónico.

3.2 *Índice de todo el texto*. El Dispositivo de Archivado es capaz de extraer el contenido textual de diversas clases de adjunto como también campos comunes del mensaje creando un índice de todo el texto para facilitar la función de búsqueda con el Servicio de Archivado (P).

3.3 *Cifrado.* Los contenidos y el índice de datos de mensaje (salvo campos como fechas y otra información que no identifica a la persona) se cifran con tecnologías estándar en función de una clave de cifrado particular para cada cliente, siendo el Cliente en cuestión el único que está en posesión de ella. El Cliente es el único que tiene todas las contraseñas, claves de cifrado y valores

de configuración. En consecuencia, el Cliente debe asegurarse de que todas estén guardadas en plica o en un sitio seguro. Symantec no aceptará responsabilidad por la pérdida de contraseñas, claves de cifrado o valores de configuración. El Cliente reconoce que la pérdida de contraseñas y claves de cifrado implica la no accesibilidad al archivo.

3.4 *Normativa de retención*. El Cliente puede definir y actualizar la normativa de retención por medio de la interfaz de usuario. Cada criterio de retención puede incorporar elementos como las personas involucradas, palabras clave o frases en el contenido y tipo de archivos adjuntos. A medida que se archiva cada mensaje, éste es evaluado cotejándolo con los criterios vigentes de retención. Si un mensaje cumple más de un criterio de retención, se aplica el periodo más prolongado. Si el mensaje no cumple ningún criterio particular de retención, se aplica el periodo de retención predeterminado.

3.5 *Etiquetas de información (metadatos)*. El Cliente puede definir y actualizar etiquetas de información (InfoTags) por medio de la interfaz de usuario. Cada etiqueta puede incorporar elementos como las personas involucradas, palabras clave o frases en el contenido, y la clase de archivos adjuntos. A medida que se archiva cada mensaje, éste es evaluado cotejándolo con una serie de etiquetas activas y se lo señala con cada etiqueta aplicable.

3.6 *Seguimiento de criterios*. Los cambios de normativa de retención y supervisión se guardan en el sistema de una forma inalterable con fines de consulta. El Cliente puede generar archivos en formato PDF de los criterios actuales o anteriores por medio de la interfaz de usuario.

3.7 *Seguimiento Histórico de Usuarios*. Cada noche se introduce al sistema una lista de todos los usuarios que tienen un buzón dentro de Exchange a fin de mantener una lista corriente de todos los buzones que hayan existido desde la implantación del Servicio de Archivado (P). Esta información puede ser utilizada para crear normativas y tener un referente de los Usuarios que hayan sido eliminados del Directorio Activo, como también para proporcionar a otros usuarios acceso a los mensajes de ex empleados.

3.8 *Indicador de adjuntos*. El Cliente puede habilitar la funcionalidad que sirve para sustituir el contenido de adjuntos dentro del sistema de correo del cliente ("Mailbox Data" o datos de buzón) con un indicador que señala la copia correcta dentro del archivo. El Cliente puede definir y actualizar los criterios para introducir indicadores con reglas distintas por cada grupo de buzones, de acuerdo con la antigüedad y tamaño del mensaje, como también con la carpeta en la que éste se encuentra. Para facilitar la restauración automática del adjunto inicial del archivo cuando los Usuarios reenvían mensajes, el cliente puede instalar el formulario de personalización del Indicador de Adjuntos (Attachment Stubbing) a su Biblioteca de Formularios de Organización (Organization Forms Library) (una carpeta pública especial del servidor Exchange). Entonces Outlook instala automáticamente el formulario de personalización del servidor. Para facilitar el acceso para recuperar adjuntos fuera de la red del Cliente, éste puede instalar el Archive Proxy (OWA) en sus servidores Exchange. El indicador solamente se añadirá a los datos de buzón que hayan sido previamente archivados. El Cliente puede habilitar una opción para almacenar una copia de los adjuntos que no hayan sido archivados anteriormente para facilitar la sustitución con indicadores de los adjuntos en el buzón. El Cliente puede fijar criterios de retención buzón por buzón para determinar el tiempo durante el cuál los adjuntos almacenados serán retenidos. En el supuesto de que no fije un plazo, la normativa predeterminada de retención será de aplicación a esos adjuntos. Los adjuntos almacenados según este proceso no se pueden encontrar con la función de búsqueda dentro del archivo.

3.9 *Acceso al usuario final*. El Cliente puede optar por ofrecer a usuarios individuales acceso a la función de búsqueda en el archivo, ya sea dentro de la interfaz de usuario de la web, o directamente dentro de Outlook.

3.10 *Acceso a revelación obligatoria*. El Cliente puede hacer búsquedas en el archivo dentro de la interfaz de usuario. El Cliente puede crear un "legal hold" que es un repositorio de mensajes pertinentes a un asunto determinado. El Cliente puede llevar a cabo una búsqueda dentro de ese repositorio de mensajes "legal hold" de la misma manera que puede hacer otras búsquedas en el archivo activo.

3.11 *"Legal Holds" ad hoc*. El Cliente puede utilizar la interfaz de usuario de fijar normativas para definir y actualizar "legal holds" con fines determinados. El "legal hold" puede considerar factores como las personas involucradas, palabras clave o frases en el contenido, y la clase de archivos adjuntos. A medida que se archiva cada mensaje, éste es evaluado cotejándolo con los "legal holds" activos a la sazón. El mensaje se vincula a cada "legal hold" cuyos criterios cumple. Para pasar datos archivados existentes a un "legal hold" especial, el Cliente puede ejecutar una búsqueda empleando los criterios del caso, copiar los resultados en una carpeta, y a continuación copiar el contenido de la carpeta al repositorio "legal hold". Cada "legal hold" ad hoc tiene un periodo indefinido de retención - los mensajes en un "legal hold" ad hoc determinado son guardados hasta que deje de ser de aplicación la razón de ese "legal hold".

3.12 *"Legal holds" en torno a personas*. El cliente puede utilizar la interfaz de usuario de fijar normativas para definir y actualizar "legal holds" en torno a personas. Cada "legal hold" sobre personas define un grupo de usuarios. A medida que se archiva cada mensaje, si éste tiene algo que ver con una persona cuyo nombre aparece en la lista de un "hold", se vincula a ese "hold". El sistema, por otra parte, captura automáticamente mensajes que pertenecen a usuarios a los que se refiere a la sazón el "hold", creando una nueva copia de los mensajes para guardarla en ese "hold". Cuando se eliminan usuarios de un "legal hold" de personas, los mensajes que pertenecen exclusivamente a los usuarios que han desaparecido de las listas desaparecen también del "hold". Los mensajes para los usuarios actuales que están en un "hold" permanecen hasta que la razón para la existencia del "hold" desaparezca.

3.13 *Exportación de datos*. Los mensajes del archivo activo o del "legal hold" pueden ser exportados a archivos PST. El sistema creará entonces archivos PST múltiples si fuese necesario debido al tamaño de los archivos.

3.14 *Informes*. El Cliente dispone de informes sobre el tamaño y crecimiento del archivo dentro de la interfaz de usuario para su visualización en formato HTML o para su exportación a archivos PDF o CSV (datos únicamente).

3.15 *Huella (audit trail)*. Las búsquedas, la visualización de mensajes, la exportación, recuperación y supervisión dejan huellas. Las huellas pueden ser visualizadas como una propiedad de un mensaje determinado. Un visualizador de huellas de todos los mensajes permite su visualización en función de criterios como la clase de actividad realizada, la persona que llevó a cabo dicha actividad y/o la fecha de esa actividad.

3.16 *Integración al Directorio Activo*. El acceso al archivo se gestiona añadiendo usuarios (o grupos existentes de usuarios) a un set de grupos de seguridad previamente definidos dentro del Directorio Activo. Cada uno de estos grupos tiene una serie de privilegios propios. Un usuario puede llevar a cabo diversos papeles en virtud de que está en varios de esos grupos de seguridad. La autenticación se lleva a cabo directamente frente al Directorio Activo. Los usuarios entran en el Directorio Activo utilizando su nombre de usuario y contraseña usuales, y si sus cuentas han sido deshabilitadas pierden derecho de acceso al archivo. Los grupos del Directorio Activo pueden ser referenciados por diversos aspectos distintos del sistema para facilitar las tareas de administración de elementos como pueden ser criterios o normativas. Un proceso de sincronización ejecutado cada noche sirve para capturar los cambios registrados en la membresía del grupo.

3.17 *Gestión de retención y eliminación*. El Servicio de Archivado (P) clasificará los mensajes y les asignará una fecha objetivo de eliminación, o bien registrará el mes en el que fue archivado el mensaje para su retención indefinida, en función de la normativa de retención formulada por el Cliente por medio de la interfaz de usuario. Las fechas objetivo de eliminación se designan para principios de cada mes. Cuando llegue la fecha objetivo de eliminación, el usuario o usuarios autorizados del cliente pueden aprobar formalmente la eliminación de todos los mensajes vinculados a esa fecha. Para mensajes archivados por un periodo indefinido de retención, el usuario o usuarios autorizados del Cliente pueden aprobar formalmente la eliminación de todos los mensajes que fueron archivados en un mes en particular. El Cliente reconoce y acepta que los datos designados para eliminación no pueden ser restaurados de forma legible por el ser humano en ningún medio de almacenamiento (incluidos los backups sin excepción).

4. Prestaciones especiales o *premium*

Las siguientes prestaciones forman parte del Servicio *Symantec MessageLabs Email Archiving.cloud Premium (P)* únicamente:

4.1 *Supervisión.*

4.1.1 *Selección automática para examen de supervisión.* El cliente puede definir y actualizar normativas por medio de la interfaz de usuario y puede añadir mensajes a una cola de mensajes a examinar. Cada normativa puede incorporar las personas involucradas, frases o palabras clave en el contenido, y tipos de archivos. Por otra parte, se pueden configurar normativas de muestreo aleatorio para usuarios determinados.
4.1.2 Examen de supervisión. El Cliente puede asignar a examinadores derechos de acceso para que puedan leer mensajes añadidos a la cola de mensajes a examinar para que los marquen como aceptables o no.
4.2 *Archivado Bloomberg*
4.2.1 El Servicio Symantec MessageLabs Email Archiving.cloud Premium (P) emplea las prestaciones del login del servicio Bloomberg Professional que registra los e-mail y conversaciones por mensaje instantáneo en archivos XML que se suben cada noche al sitio Bloomberg FTP.
4.2.2 Si el Cliente está dado de alta en el servicio Bloomberg Professional, el Dispositivo de Archivado puede ser utilizado para recuperar copias de esos archivos XML del sitio FTP para su conversión a mensajes en formato HTML y proceder a su archivado.
4.2.3 Tiene compatibilidad con el formato FIRM pero no con ACCOUNT o con el formato de extracto histórico de los logins de Bloomberg.
4.2.4 La integración de archivado Bloomberg no elimina el contenido del sitio Bloomberg FTP, pero hace un seguimiento de los archivos que han sido procesados. En vista de que Bloomberg elimina contenidos de su sitio FTP frecuentemente, y el proceso de integración de archivado Bloomberg elimina las copias que ha hecho en los Dispositivos de Archivado, el Cliente debe comprobar constantemente que la integración de archivado está funcionando y que no se eliminen archivos antes de que el proceso de integración de archivado Bloomberg haya sido capaz de recuperarlos y procesarlos.
4.2.5 Se utiliza una lista de identificadores Bloomberg FIRM para reconocer qué usuarios referenciados en el XML son empleados internos. El proceso de integración Bloomberg proporciona una interfaz de mapeado con base en la web que permite a un administrador vincular cada una de las cuentas de usuario Bloomberg a las cuentas de usuario del Directorio Activo correspondiente. A medida que los archivos XML son procesados, si un mensaje referencia a un usuario interno que todavía no ha sido mapeado, se añaden las direcciones a la lista de direcciones que no han sido mapeadas y no se procesa el mensaje. Con el mapeado de esas direcciones por un administrador, se iniciará un reprocesamiento de los mensajes vinculados. Las direcciones empresariales resueltas de e-mail se utilizan como remitentes/recipientes del mensaje.
4.2.6 Un bloque de información dentro del cuerpo del mensaje proporciona información adicional sobre las direcciones reales/nombres a visualizar de las personas involucradas en el mensaje/conversación, incluidos los datos de la cuenta Bloomberg del usuario.

5. Importación de datos heredados
5.1 El Cliente puede importar datos heredados al Servicio de Archivado (P) previo pago de una tarifa que se cobra en función de la cantidad de datos a importar. En la eventualidad de que la cantidad real de datos heredados supere la cantidad de datos importados abonada, Symantec se reserva el derecho a cobrar la tarifa vigente a la sazón por esos datos adicionales
5.2 En la eventualidad de que el Cliente opte por usar el software de otra empresa independiente para facilitar la importación de datos al archivo, el Cliente reconoce y acepta que Symantec no es responsable del software de esa empresa, y que el Cliente corre con el gasto y el riesgo de utilizar ese software.

6. Finalización del servicio
6.1 Tras la finalización del servicio Archiving.cloud (P), Symantec eliminará los datos del cliente de los archivos de almacenamiento. Antes de la finalización, el cliente puede extraer los datos que se encuentran en el archivo de almacenamiento, o puede solicitar que el tercero designado por Symantec transfiera los datos archivados al cliente en formato de archivo PST, de acuerdo con la Cláusula 6.2 a continuación.
6.2 Si el cliente solicita que el tercero designado por Symantec transfiera los datos archivados después de la finalización:
6.2.1 El cliente debe establecer un acuerdo directo con el tercero designado. Symantec no formará parte de dicho acuerdo.
6.2.2 Como los datos se almacenan en un formato cifrado, el cliente deberá proporcionar al tercero una clave de cifrado para descifrar el correo electrónico en un formato libre.
6.2.3 El cliente será responsable de los costes de transferencia. Los costes se pactarán en el acuerdo con el tercero. Los costes dependen de: (i) la cantidad de datos, (ii) el formato/medio de transferencia, (iii) los costes de configuración del proceso de transferencia, (iv) el tiempo y los materiales utilizados para llevar a cabo la transferencia.
6.2.4 Symantec se reserva el derecho a cobrar las tarifas de almacenamiento vigentes en ese momento en caso de que los datos no se exporten ni se eliminen del archivo de almacenamiento en la fecha efectiva de finalización.

7. Términos y condiciones del servicio
7.1 Symantec, a su solo albedrío, tendrá derecho a resolver el contrato de Servicio de Archivado (P) de inmediato sin previo aviso y tomar las medidas defensivas que considere necesario en los siguientes casos:
7.1.1 Si se lo ordena un tribunal judicial u otra autoridad competente;
7.1.2 En la eventualidad de que el Servicio de Archivado (P) o la red sean objeto de ataque;
7.1.3 En la eventualidad de que el Cliente o cualquiera de sus usuarios contravenga la cláusula 7.3 más abajo, Normativa de Uso Aceptable.
7.2 El Cliente será responsable de asegurar que cada uno de sus Usuarios esté informado y cumpla la cláusula 7.3, Normativa de Uso Aceptable.
7.3 *Normativa de Uso Aceptable*. Los usuarios no deben en ninguna circunstancia llevar a cabo, intentar llevar a cabo, ni instigar o secundar ninguna acción que pueda poner en peligro el Servicio de Archivado (P), ni deliberada, ni negligente, ni inocentemente. Esto incluye, pero no se limita a:
7.3.1 Intentar quebrar un service host o red;
7.3.2 Ataques tipo “Denegación de servicio” o “Inundación” contra un service host o red;
7.3.3 Todo intento de soslayar la autenticación de usuario o la seguridad de un service host o red;
7.3.4 El uso derrochador del Servicio de Archivado (P);
7.3.5 La creación, transmisión, almacenamiento o publicación de cualquier clase de virus, de programas destructivos o datos defectuosos;
7.3.6 Cualquier otro acto capaz de afectar adversamente el Servicio de Archivado (P) o su funcionamiento.
7.4 NINGÚN SERVICIO DE ARCHIVADO DE E-MAIL PUEDE GARANTIZAR UNA EXACTITUD DEL 100% POR LO QUE SYMANTEC NO ACEPTARÁ NINGUNA RESPONSABILIDAD EN CASO DE DAÑOS O PÉRDIDA QUE RESULTE A CONSECUENCIA DIRECTA O INDIRECTA DE UN FALLO EN EL SERVICIO SALVO EN LA MEDIDA CONTEMPLADA EXPRESAMENTE EN EL CONTRATO DE NIVEL DE SERVICIOS.
7.5 El Cliente reconoce que los e-mail pueden contener información que identifique a una persona y que el archivado de mensajes electrónicos puede en consecuencia constituir el procesamiento de datos personales. Por otra parte, el Cliente reconoce que el Servicio de Archivado (P) es un servicio configurable y que el Cliente es el único responsable de la configuración del Servicio de Archivado (P) de acuerdo con la normativa de uso aceptable de computadoras (o equivalente) del Cliente y las normas y leyes vigentes. Las plantillas suministradas por Symantec sirven simplemente de guía para que el Cliente sea capaz de crear sus propias normativas personalizadas y otras plantillas. En consecuencia, Symantec recomienda al Cliente consultar siempre la legislación local con anterioridad a la instalación del Servicio de Archivado (P) y a asegurarse de que la empresa y sus empleados son conscientes de y cumplen las responsabilidades que tienen de acuerdo con lo dispuesto en la legislación sobre la privacidad y la protección de datos y/o los reglamentos en relación con la utilización por parte del Cliente del Servicio de Archivado (P). En algunos países puede ser necesario obtener autorización de miembros del personal antes de poder usar el Servicio de Archivado (P). Symantec no aceptará responsabilidad civil ni penal en el caso de que el Cliente incurra en irregularidades en la operación del Servicio de Archivado (P).

El Cliente debe tener esto en cuenta a la hora de configurar el Servicio de Archivado (P).

7.6 El Cliente tiene la obligación de seleccionar la ubicación del centro de archivado de datos cuando envíe su pedido, calculándose los cargos según el centro seleccionado. EN LA EVENTUALIDAD DE QUE SE OPTE POR UN CENTRO DE ARCHIVADO EN LOS ESTADOS UNIDOS DE AMÉRICA, EL CLIENTE SE COMPROMETE A TOMAR TODAS LAS MEDIDAS NECESARIAS PARA (I) INFORMAR A SUS EMPLEADOS, AGENTES Y CONTRATISTAS, COMO TAMBIÉN A TERCEROS QUE UTILICEN EL SISTEMA DE COMUNICACIONES QUE SE VALE DEL SERVICIO DE ARCHIVADO (P) DEL HECHO DE QUE TODA INFORMACIÓN, INCLUIDA SIN EXCEPCIÓN TODA INFORMACIÓN QUE IDENTIFIQUE A UNA PERSONA, PUEDE SER PROCESADA EN LOS ESTADOS UNIDOS DE AMÉRICA; Y (II) OBTENER LA AUTORIZACIÓN DE DICHOS EMPLEADOS, AGENTES, CONTRATISTAS Y TERCEROS PARA ESE PROCESAMIENTO CON ANTERIORIDAD A LA OPERACIÓN DEL SERVICIO DE ARCHIVADO (P) POR PARTE DEL CLIENTE.

7.7 El Cliente reconoce y acepta que (i) los servicios de escaneo de Symantec (E-mail AV, E-mail AS, E-mail IC y E-mail CC) no escanean todos los mensajes que entran en el archivo y (ii) que los servicios de escaneo de Symantec (E-mail AV, E-mail AS, E-mail IC y E-mail CC) no escanean los mensajes electrónicos que salen del archivo para su reinstauración en el buzón de un usuario. En consecuencia, Symantec no aceptará responsabilidad de virus, spam, imágenes y otro contenido inapropiado que contengan los mensajes electrónicos reinstaurados. Por otra parte, el Contrato de Nivel de Servicio no será de aplicación a los e-mailes reinstaurados.

8. Licencia de Software

8.1 Los siguientes términos y condiciones se aplicarán a los programas instalados en el Dispositivo del Archivado (en lo sucesivo, el «Programa»):

8.1.1 El Cliente reconoce y acuerda que en todo momento, entre el Cliente y Symantec, Symantec y/o sus proveedores serán los propietarios del Programa. El presente Contrato otorga al Cliente una licencia limitada y no exclusiva para usar el Programa en relación con el Servicio de Archivado (P) descrito en el presente Apéndice, y no servirá para la venta de dicho Programa o de cualquier otra propiedad intelectual. Symantec y sus proveedores se reservan todos los derechos que no sean otorgados expresamente de conformidad con el presente Contrato.

8.1.2 El Cliente podrá usar una copia del Programa con un Dispositivo de Archivado. Para el objeto del presente Contrato, «usar» significa ejecutar, activar, mostrar y almacenar el Programa durante el periodo de duración del suministro del Servicio de Archivado (P) al Cliente.

8.1.3 El Programa está protegido por las leyes de copyright canadienses y estadounidenses, así como por los tratados internacionales. El Cliente no podrá arrendar ni alquilar el Programa ni copiar la documentación que acompaña al Programa. El Cliente no podrá copiar, descomponer, descompilar o decodificar o intentar crear el código fuente del Programa.

8.1.4 El Cliente acuerda que el incumplimiento de dichas disposiciones tendrá como resultado un daño irreparable a Symantec y sus proveedores, y por tanto acuerda que Symantec y/o sus proveedores podrán llevar a cabo de forma directa este apartado, entre lo que se incluye (entre otros) hacerlo mediante una ejecución específica o medidas cautelares además de todas las reparaciones a las que dicha parte pudiera tener derecho por ley o equidad.

8.1.5 Toda la tecnología, programas, documentación y procesos utilizados por Symantec para facilitar el Servicio de Archivado (P) son de propiedad exclusiva de Symantec o sus proveedores.

Apéndice 9 – Servicio Symantec MessageLabs EIM.cloud (mensajería instantánea corporativa)

1. Descripción del Servicio

1.1 El Servicio Symantec MessageLabs EIM.cloud («EIM» o Servicio de mensajería instantánea corporativa) es un Servicio gestionado que permite control administrativo, almacenaje centralizado y gestión del dominio de los mensajes instantáneos.

1.2 A excepción de MSI y de las versiones de Java, el cliente de EIM (el «POD») se instala en la estación de trabajo de cada Usuario. Todos los casos permiten que el Usuario se conecte de forma segura a la plataforma de EIM y utilice EIM. El POD tiene la funcionalidad siguiente:

(a) Intercambio de documentos;
(b) Conversaciones seguras de mensajes instantáneos;
(c) Interoperabilidad con las redes de mensajería instantánea pública (sólo con el paquete CONNECT).

1.3 La herramienta de administración de EIM, una consola basada en Internet, permite a los administradores definidos controlar su estructura de dominio y su base de usuarios.

2. Características del Servicio EIM

Características del Servicio – Symantec MessageLabs EIM Communicate.cloud ("COMMUNICATE")

(i) Intercambio de archivos integrado (100 mb de capacidad por Usuario);
(ii) Solución de copia de seguridad de escritorio;
(iii) Capacidad para intercambiar información con Usuarios de EIM que estén conectados o no;
(iv) Listas de control de acceso;
(v) Comunicaciones seguras, de 168-bit 3DES SSL cifradas POD a POD;
(vi) Consola de administración basada en Internet;
(vii) Interfaz de opciones de usuario exhaustivas;
(viii) Detección y seguimiento avanzado de presencia ;
(ix) Ayuda para una gran variedad de servidores proxy;
(x) Posibilidades de túnel HTTP;
(xi) Notificaciones de alerta para archivos nuevos;
(xii) Sistema de archivos en función de los objetos con capacidad de búsqueda extensa.

Características del Servicio – Symantec MessageLabs EIM Connect.cloud ("CONNECT")

Todas las características del paquete COMMUNICATE se aplicarán además de las siguientes:

(i) Servicios de Mensajería Instantánea interoperable (AOL, MSN, Yahoo!);
(ii) Envío de SMS (2 mensajes por Usuario o «Cuota de Usuario»);
(iii) Capacidades de registro de Mensajería Instantánea.

Características del Servicio – COLLABORATE

Todas las características del paquete CONNECT se aplicarán además de las siguientes:

(i) Integración con WebEx;
(ii) Integración con Salesforce.com.

3. Responsabilidad sobre el Número/Contraseña de Cuenta.

3.1 El Cliente es responsable de todo el uso de la administración del sitio web, ya esté autorizado o no por el Cliente, y el Cliente es responsable asimismo de mantener la confidencialidad del registro y las contraseñas de la cuenta del Cliente. El Cliente acuerda notificar a Symantec de forma inmediata en caso de un uso no autorizado de la cuenta del Cliente.

4. Responsabilidad por el Contenido de las Comunicaciones en la Cuenta del Cliente.

4.1 Symantec no efectúa garantía alguna explícita o implícita relativa al suministro del Servicio EIM, a excepción de lo estipulado en el presente Contrato. Symantec no garantiza una detección del 100% de virus o spam, y por tanto no aceptará responsabilidad alguna por daños y perjuicios ni por pérdidas resultantes de forma directa o indirecta de cualquier fallo de EIM al detectar virus o spam o al identificar de forma errónea un mensaje sospechoso de tener virus o ser spam y que pruebe posteriormente no ser tal cosa.

4.2 Symantec no efectúa garantía alguna explícita o implícita relativa a la capacidad de EIM, o la capacidad de EIM para retener todos los datos.

4.3 Symantec hace hincapié en que la configuración de EIM está totalmente bajo el control del Cliente. En algunos países puede ser necesario el consentimiento de los individuos. Symantec aconseja al Cliente que siempre compruebe la legislación local antes de hacer uso de EIM. Symantec no aceptará responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de EIM.

5. Obligaciones

5.1 El Cliente acuerda que no:

5.1.1 transmitirá o almacenará mediante el POD o EIM ningún dato, texto, vídeo, audio, programa y otro contenido que sea ilegal;

5.1.2 transmitirá o almacenará mediante el POD o EIM ningún contenido que infrinja cualquier patente, marca, copyright, derechos de publicidad u otro tipo de derecho de propiedad intelectual;

5.1.3 transmitirá o almacenará ningún contenido que viole las leyes locales, estatales, nacionales o internacionales aplicables y que puedan dar lugar a responsabilidad civil o penal;

5.1.4 transmitirá o almacenará ningún contenido no solicitado de tipo promocional, material publicitario, spam, *spim* (o correo basura a través de sistemas de mensajería instantánea), cartas en cadena u otro tipo de material de captación;

5.1.5 usar el POD o EIM para difundir, transmitir o emitir públicamente un contenido distinto del relativo a los fines de las comunicaciones de la sociedad;

5.1.6 usar el POD o EIM para transmitir de forma intencionada contenido que incluya virus, gusanos, *cancelbot*, bomba de tiempo, troyanos, *sniffer* u otros códigos diseñados para obtener información sobre otros usuarios o interrumpir la funcionalidad o capacidad de cualquier programa informático, base de datos, EIM o cualquier otro *host* de Internet; o

5.1.7 disfrazarse de la identidad del Usuario POD mediante falsificación, imitación de encabezados, uso de retransmisores de terceros, u oscurecer de algún modo el origen del contenido transmitido, entre lo que se incluye la usurpación de alguna personalidad o entidad.

6. Interoperabilidad

6.1 El Cliente recibirá la funcionalidad de interoperabilidad de conformidad con la Cláusula 2 anterior (ver paquete CONNECT más arriba). Symantec no efectúa garantía alguna sobre la capacidad de EIM para interoperar con cualquier proveedor de Mensajería Instantánea, entre lo que se incluye AOL, MSN y Yahoo!.

7. Almacenamiento de Datos Sólo en EE. UU.

7.1 SE DESTACA AL CLIENTE EL HECHO DE QUE TODOS LOS MENSAJES QUEDARÁN ALMANCENADOS EN LOS ESTADOS UNIDOS, Y SYMANTEC NO PODRÁN ACEPTAR RESPONSABILIDAD ALGUNA RESPECTO DE CUALQUIER INCUMPLIMIENTO DE LA LEGISLACIÓN O NORMATIVAS EN VIGOR. EL CLIENTE ACEPTA QUE LA CONFIGURACIÓN Y EL USO DE EIM ESTÁ COMPLETAMENTE BAJO SU CONTROL Y PROPIO CRITERIO. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de EIM. El Cliente debe tener en cuenta lo anterior a la hora de configurar EIM.

8. Registro y cumplimiento

8.1 El cliente puede escoger registrar la mensajería instantánea que pase a través del servicio EIM, lo que está sujeto al pago de los cargos correspondientes por la funcionalidad del registro.

8.2 Symantec envía archivos de registro al cliente a diario para que éste pueda almacenarlos en un archivo de almacenamiento compatible si lo desea.

8.3 Symantec conserva el registro por un periodo de tres (3) años, tras lo cual, los elimina de manera permanente. El representante autorizado del cliente puede solicitar por escrito (i) una copia de los registros o (ii) su eliminación en cualquier momento antes de que transcurra el periodo de retención de tres (3) años.

8.4 Se le advierte al cliente que la consola de administración le permite deshabilitar los registros por grupo o subgrupo en

cualquier momento y, por lo tanto, es posible que éstos no ofrezcan un registro completo del uso del servicio EIM.
8.5 Symantec puede notificar por escrito su intención de suspender el aprovisionamiento y la asistencia del servicio EIM con seis (6) meses de antelación. Al término del periodo de notificación, el servicio EIM se dará por finalizado.
8.6 Una vez finalizado el servicio EIM, el cliente puede solicitar la devolución o la eliminación de sus registros. Si el cliente no manifiesta su elección en un plazo de (90) posteriores a la finalización, Symantec eliminará los registros de manera permanente.
8.7 El cliente reconoce y acepta que, en virtud de las normativas de SEC, Symantec no puede actuar como tercero descargador en ningún caso.

9. Licencia de software

9.1 Otorgamiento de licencia

Con arreglo a las condiciones del presente contrato, Symantec otorga al usuario el derecho intransferible y no exclusivo de instalar y utilizar el software para el servicio EIM únicamente para las actividades empresariales internas del usuario ("Software" se refiere a cada programa de software para el servicio EIM en formato código objeto licenciado por Symantec y cuya utilización se regirá por las condiciones contractuales, y comprende, sin limitación, las nuevas versiones o actualizaciones que se distribuyan con arreglo a lo dispuesto en virtud de este contrato).
Todos los derechos de propiedad intelectual sobre el Software son propiedad de Symantec (y/o de sus proveedores). Symantec no vende el Software, sino que lo licencia. El usuario reconoce que el Software y toda la información relacionada con el mismo, incluidas, sin limitación, las actualizaciones, son propiedad de Symantec y sus suministradores. El cliente será totalmente responsable de que cada usuario final cumpla las condiciones contractuales y deberá responder de cada incumplimiento. El usuario deberá notificar inmediatamente a Symantec del uso desautorizado o violación de las condiciones de esta licencia.

9.2. Limitaciones en cuanto a copias y utilización

El usuario está autorizado a descargar e instalar el Software con arreglo a las siguientes condiciones:
9.2.1. El usuario no está autorizado a descargar o instalar el Software para un número mayor de usuarios finales que el número de licencias de usuario final otorgadas al cliente ("usuario final" para estos efectos es el ordenador en el que se instala el Software).
9.2.2. El usuario está autorizado para copiar el Software según justifiquen las circunstancias con fines de backup, archivaje o recuperación tras un fallo catastrófico. La documentación impresa puede ser reproducida por el usuario para su utilización interna únicamente ("Documentación" son las guías de Symantec para el usuario y/o los manuales de funcionamiento del Software incluido en la descarga del mismo.).
9.2.3 El usuario no está autorizado ni deberá permitir que terceros: (i) descompilen, desensamblen o apliquen ingeniería inversa al Software, salvo en la medida expresamente contemplada por la legislación vigente, sin la previa autorización escrita de Symantec; (ii) suprimir una identificación del producto o aviso de derechos de propiedad; (iii) alquilar, prestar o utilizar el Software para su utilización en aplicaciones de tiempo compartida o por oficinas de servicios (*service bureau):* (iv) modificar, traducir, adaptar o crear derivados del Software, o (v) en general utilizar o copiar el Software de una forma que nos esté expresamente contemplada en esta licencia.

9.3. Traspaso de derechos

El usuario no está facultado a traspasar, ceder o delegar la licencia de Software al amparo de este contrato sin la previa autorización escrita de Symantec. Todo traspaso, cesión o delegación de derechos en contravención de lo expuesto anteriormente no tendrá ningún efecto.

9.4. Garantía limitada y advertencia

9.4.1 Symantec garantiza que tras su descarga el Software cumplirá todas las funciones que contempla la documentación vigente de Symantec.
9.4.2 Esta garantía no será de aplicación en los siguientes supuestos: (i) el Software no se utiliza de acuerdo con este contrato o la documentación; (ii) el Software en todo o en parte ha sido modificado por una entidad ajena a Symantec; o (iii) la causa de que el Software no funcione bien se debe al equipo del usuario o software de terceros.
9.4.3 CON ARREGLO A LA PRESENTE GARANTÍA, SYMANTEC SE COMPROMETE ÚNICAMENTE A REEMPLAZAR EL SOFTWARE DEFECTUOSO SEGÚN DISPONIBILIDAD. SYMANTEC NO GARANTIZA QUE EL SOFTWARE FUNCIONARÁ SIN INTERRUPCIÓN O SIN ERRORES. SYMANTEC ADVIERTE EXPRESAMENTE QUE NO OFRECE NINGUNA CLASE DE GARANTÍA EXPRESA, IMPLÍCITA O DE OTRA FORMA, EN LO QUE SE REFIERE A LA APTITUD DEL SOFTWARE PARA EL COMERCIO O EL CONSUMO, CALIDAD SATISFACTORIA, IDONEIDAD PARA UN FIN EN PARTICULAR, NI GARANTÍA DE OTRA ÍNDOLE.

9.5. Extinción

Una vez extinguido el servicio EIM o el contrato, cesará de inmediato el derecho del usuario a utilizar el Software que se le otorga en esta licencia. El usuario deberá devolver a Symantec o destruir los ejemplares del Software y la documentación.

Apéndice 10
Symantec MessageLabs Policy Based Encryption.cloud
(Cifrado basado en normas propias)

1. Descripción del servicio

1.1 El Servicio Symantec MessageLabs Policy Based Encryption.cloud ("PBE") de Symantec ofrece la capacidad para enviar y recibir correo electrónico cifrado de acuerdo con las normas de seguridad que el cliente determine para proteger sus mensajes electrónicos.

1.2 A fin de valerse de PBE, el cliente debe suscribirse además a los siguientes servicios:

- **Symantec MessageLabs Email Boundary Encryption.cloud ("BE**"), sistema de cifrado según se explica en el anexo 2, apéndice 5; y
- **Symantec MessageLabs Email Content Control.cloud ("Email CC")**, según se explica en al anexo 2, apéndice 4.

1.3 PBE proporciona las siguientes funciones:

- Capacidad para utilizar Email CC para definir las normas de cifrado para el correo electrónico saliente;
- Transmisión cifrada del correo electrónico hasta la bandeja de entrada del destinatario;
- El destinatario abre el correo electrónico cifrado por medio de un portal seguro de Internet;
- El destinatario puede entrar en el portal seguro para enviar su contestación en un formato cifrado.

2. Características del PBE

2.1 PBE ofrece al Cliente la capacidad para enviar correo electrónico cifrado directamente a la bandeja de entrada del destinatario sin necesidad de que éste tenga que descargar ningún programa.

2.2 El Cliente puede configurar el método de codificación para que sea Push o Pull. Para Symantec MessageLabs Policy Based Encryption.cloud (Z) ("PBE Z"), la regla Email CC decide entre Push o Pull. Para Symantec MessageLabs Policy Based Encryption.cloud (E) ("PBE E"), el método de codificación predeterminado es Pull, que el destinatario puede cambiar a Push bajando la funcionalidad Secure Reader dentro de su portal seguro de Internet.

2.2.1 La variante "PBE Push" del servicio PBE se encarga de enviar al destinatario una notificación de e-mail con el mensaje originario incluido en la misma en un adjunto cifrado. Tras el registro inicial online, el destinatario puede ver el mensaje descifrado utilizando una aplicación Java de sobremesa.

2.2.2 La variante "PBE Pull" del servicio PBE se encarga de enviar al destinatario una notificación de e-mail. El destinatario puede ver el mensaje descifrado online iniciando una sesión segura SSL en su explorador tras hacer el login en un portal seguro de la web y de introducir su contraseña.

2.3 PBE también permite al destinatario entrar en un portal seguro de la web y responder a un mensaje cifrado en formato igualmente cifrado.

2.4 El Cliente puede determinar la imagen o aspecto del portal que sus destinatarios utilicen para leer sus mensajes cifrados (puede por ejemplo incorporar el logotipo de su empresa y números de apoyo).

2.5 El destinatario de un mensaje cifrado puede enviar un mensaje totalmente nuevo a cualquiera de los Usuarios de PBE del Cliente.

2.6 En el supuesto de que el Cliente esté abonado a PBE E, hay disponible un Plug-In de terceros para Outlook que añade un icono de codificación a la barra de herramientas de Outlook del destinatario. El Cliente reconoce que Symantec no aceptará responsabilidad alguna por el software de terceros.

2.7 En el supuesto de que el cliente esté abonado a PBE E, el destinatario puede escoger el idioma de su portal seguro de Internet y de los e-mails de notificación siempre que figure en la lista de idiomas disponibles.

3. Prestación del servicio, facturación y cambios en el servicio

3.1 Symantec comenzará a cobrar por PBE a partir de la fecha en que confirme que la red del cliente cuenta con capacidad técnica para admitir PBE ("Fecha de aprobación técnica").

3.2 La cláusula 6.2 de Anexo 1 no es válida para PBE. Symantec pretende aprovisionar los pedidos y las solicitudes de cambio de PBE en un plazo de cuatro semanas a partir de la Fecha de aprobación técnica, siempre y cuando el cliente haya cumplido con la diligencia debida.

3.3 El Cliente se compromete a suministrar los recursos, información y autorizaciones necesarios, según corresponda, y a activar o corregir sus servicios de correo DNS para conectividad a PBE.

3.4 El Cliente puede cambiar la imagen de marca de su portal dos veces al año como máximo.

4. Configuración

4.1 El Cliente se responsabiliza de la configuración de PBE con arreglo a sus propios criterios. El Cliente deberá configurar su PBE por medio de ClientNet haciendo una selección de las opciones que ofrece el servicio Email CC.

4.2 Symantec hace hincapié en el hecho de que la configuración del PBE está totalmente bajo el control del Cliente y que la precisión del PBE depende enteramente de la precisión de la configuración. En consecuencia, Symantec no aceptará ninguna responsabilidad por pérdidas, daños o perjuicios que resulten directa o indirectamente de que PBE no haya cumplido los criterios de cifrado del Cliente.

5. Parámetros del servicio

5.1 El servicio PBE tiene las siguientes limitaciones:

5.1.1 En el supuesto de que el Cliente esté abonado a PBE Z, el número de mensajes electrónicos seguros que el Cliente puede enviar en un mes cualquiera no debe exceder la suma de 300 veces la utilización registrada para el PBE. En el supuesto de que el Cliente esté abonado a PBE E, el número de mensajes electrónicos seguros que el Cliente puede enviar en un mes cualquiera no debe exceder la suma de 480 veces la utilización registrada para el PBE. En el envío de un solo mensaje a una multiplicidad de destinatarios, cada dirección contará como un mensaje electrónico seguro. En la eventualidad de que el Cliente envíe un número mayor que la cantidad permitida de mensajes seguros en un mes cualquiera, Symantec incrementará la tasa de utilización registrada. En este caso, Symantec, a su libre albedrío, enviará facturas adicionales y/o hará los ajustes necesarios en las facturas subsiguientes en lo que queda del periodo de facturación para cobrar, pro-rata, el uso adicional.

5.1.2 Los mensajes electrónicos enviados por el PBE Z se verán limitados a un tamaño máximo de cincuenta megabytes (50 MB) por mensaje, comprimido. Los mensajes electrónicos cuya ruta pasa por PBE E deben conformarse a un límite máximo de cincuenta megabytes (50 MB) por mensaje tras su cifrado.

5.1.3 El Nivel de Servicio de Latencia de Correo Electrónico que recoge el Contrato de Nivel de Servicios no será de aplicación al PBE.

5.1.4 El número mínimo de Usuarios para PBE Z es 50. El pedido inicial y los subsiguientes para PBE Z deben ser para bloques de 50 Usuarios como mínimo con incrementos de 10 Usuarios cuando el pedido cumpla el requisito mínimo de 50 Usuarios.

5.1.5 **EL PBE SOLAMENTE FUNCIONA EN CONJUNTO CON LOS SERVICIOS BE Y EMAIL CC. NO ES UN SERVICIO AUTÓNOMO. CADA USUARIO DE PBE DEBE SER TAMBIÉN USUARIO DE EMAIL CC.**

6. Condiciones

6.1 EL CLIENTE SABE Y ACEPTA QUE EL USO Y CONTROL DE PBE ESTÁ ENTERAMENTE A SU DISPOSICIÓN. PBE tiene por objeto capacitar al Cliente para ejecutar una política de uso de equipos informáticos aceptable (o su equivalente) que ya ha sido implantada. El empleo de servicios de cifrado en ciertos países puede estar regulado por las leyes. Se recomienda al Cliente consultar siempre cuáles son las normas vigentes con anterioridad a la instalación de PBE. Symantec no aceptará ninguna responsabilidad civil ni penal en la eventualidad de que el Cliente haya contravenido alguna norma a consecuencia de haber utilizado PBE.

Apéndice 11
Symantec Email Continuity.cloud ("EC")
[Continuidad de mensajes electrónicos]

1. Visión general de EC

1.1 Symantec Email Continuity.cloud (EC) es un sistema de respaldo para el envío de mensajes electrónicos en entornos Microsoft Exchange y Lotus Notes. EC sirve para sincronizar información fundamental del sistema y del usuario, incluidos, sin límite, el directorio de e-mail y contactos personales. El Cliente puede asimismo configurar EC para que pueda utilizarse con aparatos BlackBerry® con reenvió inalámbrico por medio de BlackBerry® Web Client o de BlackBerry® Internet Service, y una experiencia integrada de Outlook para usuarios de Outlook 2003 modalidad caché o de Outlook 2007 modalidad caché tras la instalación de una extensión de Outlook.

1.2. *Compatibilidad:* es compatible con Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Versión 6, Lotus Notes Versión 7.

1.3 *Compatibilidad con Outlook Extension*: es compatible con las versiones Microsoft Outlook 2003, modalidad caché; Microsoft Outlook 2007, modalidad caché.

1.4 El cliente es responsable de proporcionar y mantener el hardware y el software necesarios (como se indica en el formulario de aprovisionamiento).

2. Explicación del servicio EC

2.1. *Activación*. El Cliente puede solicitar por teléfono al equipo de apoyo de Symantec la activación de EC o por medio del portal Email Management Services ("EMS"). Tras la activación de EC el Cliente recibirá alertas por SMS enviados a los móviles y a los e-mails previamente asignados. Entonces EC empezará a recibir y ordenar mensajes entrantes de e-mail, para filtrarlos (con arreglo a lo dispuesto en la cláusula 3.4) de conformidad con cualquier otro servicio de Symantec al que esté suscrito el Cliente (p. ej., el servicio de e-mail AV), para enviarlos a las casillas de Usuario correspondientes. EC proporciona almacenamiento y retención de mensajes electrónicos enviados y recibidos durante la activación del servicio hasta un máximo de treinta (30) días después de la desactivación a fin de permitir al Cliente integrar esos mensajes a su sistema principal de correo electrónico si así lo desea.

2.2 *Retención.* El Cliente será responsable de designar a los Usuarios con cobertura del servicio EC, así como también indicar el tiempo de retención para cada Usuario. Los mensajes electrónicos retenidos serán suprimidos cuando se cumpla el primero de los siguientes plazos: (a) el plazo de retención designado para el Usuario del caso, o (b) vigencia de EC. El Cliente tiene la obligación de adquirir suficiente espacio de almacenamiento teniendo en cuenta el tipo de retención requerida de conformidad con lo estipulado en la cláusula 4.1 más abajo.

2.3 *Gestor de autenticación.* El Cliente podrá ampliar sus políticas de seguridad para Autenticación de Directorio Activo de tal modo que abarquen EC, permitiendo a los Usuarios hacer el login en sus correos EC con su contraseña para Windows. De esta forma se elimina la necesidad de tener una contraseña diferente para EC. La autenticación de Windows exige tener disponible un controlador de dominios Windows accesible por el Gestor de Autenticación que sea capaz de autenticar a los Usuarios que intentan abrir correos EC cuando se lleva a cabo la activación de EC. Compatibilidad: es compatible con las versiones Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007.

2.4 El número mínimo de Usuarios de EC que el Cliente puede contratar será lo mayor entre (a) el mismo que el número de buzones de e-mail en la organización Microsoft Exchange del Cliente o bien (b) diez (10).

3. Configuración

3.1 *Activación parcial*: En el caso de ciertos sistemas/versiones de e-mail (los entornos Microsoft Exchange 2000, 2003 y 2007), EC puede ser activado para subgrupos del entorno del Cliente (uno o varios individuos, servidores y/o ubicaciones) en la modalidad "Activación Parcial", a fin de superar la no disponibilidad de e-mail por fallos más localizados.

3.2 *Activación*: La suscripción EC da derecho al Cliente a realizar veinticuatro (24) activaciones al año, cada una con una duración máxima de doce (12) horas consecutivas ("Activaciones Incluidas"). (Por ejemplo, una sola activación de seis (6) horas de duración contaría como una (1) activación y una sola activación con una duración de diecinueve (19) horas contaría como dos (2) activaciones). En la eventualidad de que el Cliente haya agotado su cuota de activaciones – es decir, el número de Activaciones Incluidas -, podrá suscribir un número adicional de activaciones (cada una de hasta doce (12) horas consecutivas) abonando la tarifa de Symantec vigente a la sazón.

3.3 Ensayos del sistema: Los Ensayos del Sistema constan de (a) un (1) ensayo trimestral del EC de todos los Usuarios, prueba que durará un máximo de cuatro (4) horas, y (b) de los entornos Microsoft Exchange 2000, Microsoft Exchange 2003 ó Microsoft Exchange 2007, ensayo parcial ilimitado de hasta un diez (10) por ciento de Usuarios. El Cliente debe fijar las fechas para dichas pruebas junto con Symantec con un mínimo de siete (7) días hábiles de antelación a la fecha deseada.

3.4 **EL CLIENTE RECONOCE Y ACEPTA QUE CUANDO EL CLIENTE ESTÁ EN ESTADO ACTIVADO, Y PROCEDE A ENVIAR MENSAJES ELECTRÓNICOS A, O RECIBIRLOS DE, OTRA ORGANIZACIÓN QUE TAMBIÉN ESTÁ EN ESTADO ACTIVADO, ESOS MENSAJES NO SERÁN OBJETO DE ESCANEO POR PARTE DE LOS SERVICIOS DE SYMANTEC QUE EL CLIENTE SUSCRIBA.**

3.5 En el supuesto de que el Cliente utilice Email AV, Email AS, Email CC y/o Email IC Services, Symantec puede configurar la ruta de reserva ("failover routing") para los e-mails del Cliente al entorno EC dentro de ClientNet. La ruta de reserva se utiliza cuando el servicio EC ha sido activado.

3.6 **EN EL SUPUESTO DE QUE EL CLIENTE NO UTILICE EMAIL AV, EMAIL AS, EMAIL CC O EMAIL IC, EL CLIENTE TIENE EL DEBER DE CONFIGURAR Y PROBAR LA RUTA DE RESERVA PARA LOS E-MAILS DEL CLIENTE AL ENTORNO EC. LA CONFIGURACIÓN DEBE OBSERVAR LAS INSTRUCCIONES DE SYMANTEC DURANTE EL PROCESO DE ABASTECIMIENTO Y DEBEN CUMPLIRSE TAMBIÉN POSTERIORMENTE. EL CLIENTE RECONOCE QUE EN LA EVENTUALIDAD DE QUE NO CONFIGURE NI MANTENGA LAS RUTAS DE RESERVA, LOS E-MAILS NO PUEDEN SER DIRIGIDOS A EC.**

4. Opciones

4.1 *Symantec Email Continuity.cloud Storage Option*.

4.1.1 El cliente tiene la obligación de alquilar suficiente espacio de almacenamiento para fines de retención.

4.1.2 En el caso de que el Cliente esté dado de alta en Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email and Web Safeguard.cloud o Symantec MessageLabs Ultimate Safeguard.cloud, dichos paquetes comprenden un máximo de 0,7 GB de almacenamiento anual de email por Usuario para los servicios combinados de Symantec Email Continuity.cloud y Symantec Email Continuity Archive.cloud. Si el Cliente necesita más capacidad de almacenamiento que la permitida, deberá contratar suficiente capacidad de almacenamiento para el Servicio conforme a la tarifa de Symantec que esté vigente a la sazón.

4.1.3 En el caso de que el Cliente no esté dado de alta en uno de los paquetes indicados en 4.1.2, el precio por Usuario no comprende almacenamiento, por lo que el Cliente deberá contratar suficiente capacidad de almacenamiento para el Servicio conforme a la tarifa de Symantec que esté vigente a la sazón.

4.1.4 En el caso de que el Cliente tenga que contratar almacenamiento adicional, Symantec pasará las facturas adicionales del caso y/o hará los ajustes necesarios a las facturas posteriores para cubrir el precio del almacenamiento adicional de una forma prorrateada durante el resto del periodo de facturación en curso.

4.2 *Symantec Email Continuity.cloud Wireless Option (Inalámbrico).*

4.2.1 En el caso de que el Cliente esté suscrito al servicio Symantec Email Continuity.cloud Wireless Option, los administradores del sistema podrán estipular ciertos dispositivos BlackBerry® gestionados por los servidores corporativos BlackBerry® Enterprise Servers (BES) de RIM. Cuando se active EC, los dispositivos BlackBerry® estipulados seguirán enviando y recibiendo mensajes electrónicos comunicándose con el portal EMS por medio de un canal seguro abierto por el servidor BES.

4.2.2. Compatibilidad: es compatible con las versiones Microsoft Exchange 2000, Microsoft Exchange 2003 y Microsoft Exchange 2007; BlackBerry® Enterprise Server versión 4.0 (o posterior); BlackBerry® Handheld Devices firmware versión 4.1 (o posterior).

5. Condiciones para la contratación de EC

5.1 NINGÚN SERVICIO DE EMAIL CONTINUITY PUEDE GARANTIZAR UNA SINCRONIZACIÓN DEL 100% POR LO QUE SYMANTEC NO ACEPTARÁ RESPONSABILIDAD DE DAÑOS Y PERJUICIOS QUE RESULTEN DIRECTA O INDIRECTAMENTE DEL HECHO DE QUE EC NO HAYAN PODIDO SINCRONIZAR SISTEMAS DE E-MAIL.

5.2 Symantec hace hincapié en que la configuración de EC está totalmente bajo el control del Cliente. Symantec aconseja al Cliente que cuente con una política de uso de equipos informáticos aceptable (o su equivalente). En ciertos países puede ser necesaria la obtención del consentimiento de los individuos, por lo que Symantec aconseja consultar siempre la legislación local antes de hacer uso de EC. Symantec puede no aceptar responsabilidad alguna respecto de obligaciones civiles o penales en las que pueda haber incurrido el Cliente como resultado de la operación de EC.

6. Licencia de software de EC

6.1 Otorgamiento de licencia

Con arreglo a las condiciones del presente contrato, Symantec otorga al usuario el derecho intransferible y no exclusivo de instalar y utilizar el software para el servicio EC únicamente para las actividades empresariales internas del usuario ("Software" se refiere a cada programa de software para el servicio EC en formato código objeto licenciado por Symantec y cuya utilización se regirá por las condiciones contractuales, y comprende, sin limitación, las nuevas versiones o actualizaciones que se distribuyan con arreglo a lo dispuesto en virtud de este contrato).

Todos los derechos de propiedad intelectual sobre el Software son propiedad de Symantec (y/o de sus proveedores). Symantec no vende el Software, sino que lo licencia. El usuario reconoce que el Software y toda la información relacionada con el mismo, incluidas, sin limitación, las actualizaciones, son propiedad de Symantec y sus suministradores. El cliente será totalmente responsable de que cada usuario final cumpla las condiciones contractuales y deberá responder de cada incumplimiento. El usuario deberá notificar inmediatamente a Symantec del uso desautorizado o violación de las condiciones de esta licencia.

6.2. Limitaciones en cuanto a copias y utilización

El usuario está autorizado a descargar e instalar el Software con arreglo a las siguientes condiciones:

6.2.1. El usuario no está autorizado a descargar o instalar el Software para un número mayor de usuarios finales que el número de licencias de usuario final otorgadas al cliente ("usuario final" para estos efectos es el ordenador en el que se instala el Software).

6.2.2. El usuario está autorizado para copiar el Software según justifiquen las circunstancias con fines de backup, archivaje o recuperación tras un fallo catastrófico. La documentación impresa puede ser reproducida por el usuario para su utilización interna únicamente ("Documentación" son las guías de Symantec para el usuario y/o los manuales de funcionamiento del Software incluido en la descarga del mismo.).

6.2.3 El usuario no está autorizado ni deberá permitir que terceros: (i) descompilen, desensamblen o apliquen ingeniería inversa al Software, salvo en la medida expresamente contemplada por la legislación vigente, sin la previa autorización escrita de Symantec; (ii) suprimir una identificación del producto o aviso de derechos de propiedad; (iii) alquilar, prestar o utilizar el Software para su utilización en aplicaciones de tiempo compartida o por oficinas de servicios (*service bureau):* (iv) modificar, traducir, adaptar o crear derivados del Software, o (v) en general utilizar o copiar el Software de una forma que nos esté expresamente contemplada en esta licencia.

6.3. Traspaso de derechos

El usuario no está facultado a traspasar, ceder o delegar la licencia de Software al amparo de este contrato sin la previa autorización escrita de Symantec. Todo traspaso, cesión o delegación de derechos en contravención de lo expuesto anteriormente no tendrá ningún efecto.

6.4. Garantía limitada y advertencia

6.4.1 Symantec garantiza que tras su descarga el Software cumplirá todas las funciones que contempla la documentación vigente de Symantec.

6.4.2 Esta garantía no será de aplicación en los siguientes supuestos: (i) el Software no se utiliza de acuerdo con este contrato o la documentación; (ii) el Software en todo o en parte ha sido modificado por una entidad ajena a Symantec; o (iii) la causa de que el Software no funcione bien se debe al equipo del usuario o software de terceros.

6.4.3 CON ARREGLO A LA PRESENTE GARANTÍA, SYMANTEC SE COMPROMETE ÚNICAMENTE A REEMPLAZAR EL SOFTWARE DEFECTUOSO SEGÚN DISPONIBILIDAD. SYMANTEC NO GARANTIZA QUE EL SOFTWARE FUNCIONARÁ SIN INTERRUPCIÓN O SIN ERRORES. SYMANTEC ADVIERTE EXPRESAMENTE QUE NO OFRECE NINGUNA CLASE DE GARANTÍA EXPRESA, IMPLÍCITA O DE OTRA FORMA, EN LO QUE SE REFIERE A LA APTITUD DEL SOFTWARE PARA EL COMERCIO O EL CONSUMO, CALIDAD SATISFACTORIA, IDONEIDAD PARA UN FIN EN PARTICULAR, NI GARANTÍA DE OTRA ÍNDOLE.

6.5. Extinción

Una vez extinguido el Servicio EC o el contrato, cesará de inmediato el derecho del usuario a utilizar el Software que se le otorga en esta licencia. El usuario deberá devolver a Symantec o destruir los ejemplares del Software y la documentación.

Apéndice 12
Schemus Tool

1.1 Schemus Tool es un software que sincroniza los datos del servidor de directorio del Cliente con los servicios de Symantec en los que el Cliente está dado de alta.
1.2 El Cliente está autorizado para utilizar Schemus Tool por Schemus Limited en virtud de una licencia propia de usuario final otorgada por dicha empresa ("Third Party EULA" o LUF de terceros).
1.3 El Cliente reconoce y acepta que el acceso y empleo de Schemus Tool depende de que el Cliente acepte y cumpla los términos y condiciones de la LUF de Terceros (solicite una copia a Symantec).
1.4 Schemus Tool es una tecnología controlada sujeta a las leyes y normas de importación y exportación, particularmente a los controles de exportación indicados en la sección "General" del Contrato. **EL CLIENTE RECONOCE Y ACEPTA QUE TENDRÁ QUE FIRMAR UNA DECLARACIÓN DE FIEL CUMPLIMIENTO (SOLICITE COPIA A SYMANTEC) (I) CON ANTERIORIDAD A LA DESCARGA DEL SOFTWARE, (II) CON ANTERIORIDAD A LA EMISIÓN DE LA CLAVE DE LICENCIA Y (III) POSTERIORMENTE CADA AÑO A SOLICITUD DE SYMANTEC**.
1.5 Symantec no ofrece ninguna garantía adicional (ni expresa ni implícitamente, legal o no) respecto de Schemus Tool. En la eventualidad de fallos relacionados con Schemus Tool, Symantec tomará las medidas comercialmente razonables para determinar la causa del problema y si corresponde, remitirá el problema a Schemus Limited.
1.6 La responsabilidad máxima de Symantec frente al Cliente respecto de Schemus Tool se verá limitada a una suma equivalente a la abonada por el Cliente por Schemus Tool, ó a 350 €, según cuál sea superior.

Apéndice 13
Symantec MessageLabs Instant Messaging Security.cloud (IMS)

1 Visión global

1.1 El cliente debe sincronizar el directorio de usuarios con Symantec para crear una lista de los nombres de usuario de Active Directory y los nombres de usuario de mensajes instantáneos correspondientes dentro de ClientNet. Un "usuario interno" es un usuario de mensajes instantáneos públicos y admitidos que se conecta a IMS desde la dirección IP de un cliente, un usuario de Microsoft Lync que se conecta a IMS desde el servidor perimetral de un cliente o un usuario roaming que se conecta a IMS con el dominio SIP de un cliente. Un "usuario externo" es cualquiera que no cumple los criterios antes mencionados.

1.2 El cliente debe cambiar la configuración de acuerdo con la guía de implementación pertinente, que se puede encontrar en SymHelp.

1.3 Una vez que IMS se configura de acuerdo con las cláusulas 1.1 y 1.2, los mensajes instantáneos que pasan de los usuarios internos a los usuarios externos, y viceversa, se dirigen mediante IMS para que sean analizados por productos líderes, incluido Skeptic™, el propio análisis heurístico de Symantec.

1.4 IMS solo puede analizar ciertas versiones de clientes de mensajes instantáneos públicos. Si desea obtener una lista de las últimas versiones admitidas, solicítela al equipo de asistencia. El cliente reconoce y acepta que Symantec puede actualizar y cambiar esta lista de forma regular sin aviso.

1.5 Si un mensaje instantáneo **entrante**:

1.5.1 se considera infectado con un virus u otro código malicioso, será bloqueado;

1.5.2 contiene una URL de una página web donde se ha detectado un virus u otro código malicioso, el acceso a dicha página web será denegado.

1.6 IMS también proporciona una funcionalidad básica antiphishing, que bloquea los mensajes instantáneos **entrantes** que se consideran ataques de phishing.

1.7 IMS puede analizar archivos adjuntos en busca de códigos maliciosos.

1.8 IMS no puede analizar ciertos mensajes instantáneos cifrados.

2. Control de contenido IMS

2.1 IMS permite al Cliente configurar su propia estrategia para filtrar el contenido de mensajes entrantes y salientes en función de reglas.

2.2 El Cliente es el responsable de ejecutar las opciones de configuración de acuerdo con su normativa sobre el uso aceptable de computadoras (o equivalente) por medio de ClientNet. Las reglas se pueden configurar para individuos o grupos. Los cambios que efectúe el Cliente en las reglas entrarán en vigor dentro de un plazo de cuatro (4) horas.

2.3 Hay opciones disponibles para determinar las medidas a tomar tras la detección de un contenido controlado en un MI. Estas opciones se desglosan en ClientNet y en la última versión de la Guía para Administradores.

2.4 El Cliente puede comprobar el resultado de las reglas adoptadas por medio de ClientNet en forma de resúmenes diarios, semanales, mensuales y anuales ordenados según regla y usuario.

2.5 IMS puede analizar nombres de archivos adjuntos, pero no puede analizar su contenido.

3 Diarios y almacenamiento

3.1 En el caso de que el Cliente haya habilitado la funcionalidad de diario (*logging*), Symantec compilará cada día diarios de los escaneos de MI realizados ese día. Cada diario indicará la fecha y hora, contenido y nombre de los archivos transferidos. Los archivos que no pasen al Cliente serán almacenados durante un plazo de treinta y un (31) días, cumplido el cual serán destruidos.

3.2 El cliente también puede configurar IMS para que envíe una copia de cada mensaje instantáneo a una dirección de correo electrónico.

4 Notificaciones

4.1 El Cliente puede configurar IMS para que éste envíe automáticamente las siguientes notificaciones:

4.1.1 al remitente y a la persona a la que esté dirigida el mensaje en la eventualidad de que éste sea bloqueado por considerarse que contiene un Virus, o que constituye un ataque de phishing, o que tiene un contenido controlado; o

4.1.2 al recipiente si el acceso a una dirección web es denegado por considerarse que esta contiene un virus o elementos maliciosos.

4.2 El Cliente puede activar, personalizar y desactivar la función de notificaciones por medio de ClientNet.

5 Asistencia para mensajes instantáneos CC

5.1 Las funciones de apoyo comprenden un paseo guiado por la interfaz de IMS CC que comprende una descripción del servicio y una sesión de preguntas y respuestas. (No incluye ayuda con la configuración de regla o análisis de la efectividad de las reglas).

6 Términos y condiciones de IMS

6.1 Las listas de palabras controladas y plantillas propuestas de reglas que proporciona Symantec contienen palabras que pueden considerarse ofensivas.

6.2 El Cliente reconoce y acepta que Symantec puede compilar y publicar listas de palabras predeterminadas utilizando palabras sacadas de las listas personalizadas de palabras del Cliente.

6.3 El Cliente reconoce que los mensajes instantáneos pueden contener información que permita identificar a personas y que el registro y la intercepción de MI puede por tanto constituir el procesamiento de datos personales. Por otra parte, el Cliente reconoce que IMS es un servicio configurable y que el Cliente es el único responsable de configurar IMS de acuerdo con la normativa de uso aceptable de computadoras (o equivalente) del Cliente y las normas y leyes vigentes. En consecuencia, Symantec recomienda al Cliente consultar siempre la legislación local con anterioridad a la instalación de IMS y a asegurarse de que la empresa y sus empleados son conscientes de, y cumplen las responsabilidades que tienen de acuerdo con lo dispuesto en, la legislación sobre la privacidad y la protección de datos y/o los reglamentos en relación con la utilización por parte del Cliente de IMS. En algunos países puede ser necesario obtener autorización de miembros del personal para poder proceder a la intercepción y registro de mensajes instantáneos. Como mínimo, el Cliente procederá a adoptar, con el mínimo de adaptación para personalizarla, la notificación predeterminada de Symantec para IMS para quienes utilicen cualquier sistema de comunicaciones que se valga de IMS, que (i) indica que las comunicaciones transmitidas por medio de ese sistema serán registradas e interceptadas, (ii) indica los fines de dicho registro e intercepción, y (iii) obtiene la autorización previa del usuario a dicho registro e intercepción. El Cliente podrá traducir pero no modificar de otra forma las estipulaciones de (i), (ii) y (iii) dentro de la personalización de la notificación predeterminada respecto de IMS. Symantec no aceptará responsabilidad civil ni penal en el caso de que el Cliente incurra en irregularidades en la operación de IMS. El Cliente eximirá de toda responsabilidad a Symantec frente a demandas de sus empleados, terceros y/o entes gubernamentales relativas a la intercepción o registro de mensajes instantáneos por Symantec o por el incumplimiento de leyes y/o normas por parte del Cliente.

6.4 **CABE HACER NOTAR AL CLIENTE EL HECHO DE QUE LOS MENSAJES INSTANTÁNEOS QUE PASEN POR IMS PUEDEN SER ESCANEADOS Y GUARDADOS EN EQUIPO SITUADO EN LOS ESTADOS UNIDOS DE AMÉRICA. EN CONSECUENCIA, EL CLIENTE SE COMPROMETE A TOMAR LAS MEDIDAS NECESARIAS PARA (I) INFORMAR A SUS EMPLEADOS, AGENTES Y CONTRATISTAS, COMO TAMBIÉN A TERCEROS QUE UTILICEN EL SISTEMA DE COMUNICACIONES QUE SE VALEN DE IMS, DEL HECHO DE QUE TODA INFORMACIÓN, INCLUIDA SIN EXCEPCIÓN TODA INFORMACIÓN QUE POSIBLEMENTE IDENTIFIQUE A UNA PERSONA, PUEDE SER PROCESADA EN LOS ESTADOS UNIDOS DE AMÉRICA; Y (II) OBTENER LA AUTORIZACIÓN DE DICHOS EMPLEADOS, AGENTES, CONTRATISTAS Y TERCEROS PARA ESE PROCESAMIENTO CON ANTERIORIDAD A, O A LA VEZ QUE, LA OPERACIÓN DE IMS POR PARTE DEL CLIENTE. POR OTRA PARTE, LOS DATOS PERSONALES QUE EL CLIENTE PROPORCIONE A SYMANTEC PUEDEN SER TRANSFERIDOS A FILIALES DE SYMANTEC Y/O A SUBCONTRATISTAS QUE ACTÚAN DE PARTE DE SYMANTEC. DICHAS FILIALES O SUBCONTRATISTAS PUEDEN ESTAR RADICADOS EN LOS EE.UU. O EN OTROS PAÍSES QUE PUEDEN TENER LEGISLACIÓN VIGENTE EN MATERIA DE PROTECCIÓN DE**

DATOS MENOS EFECTIVA QUE EN LA REGIÓN EN LA QUE EL CLIENTE ESTÁ RADICADO, EN CUYO CASO SYMANTEC HABRÁ TOMADO MEDIDAS PARA QUE LOS DATOS RECOGIDOS, EN CASO DE SER TRANSFERIDOS, TENGAN UN NIVEL ADECUADO DE PROTECCIÓN. EL CLIENTE SE COMPROMETE A TOMAR LAS MEDIDAS NECESARIAS PARA (I) INFORMAR A SUS EMPLEADOS, AGENTES Y CONTRATISTAS, COMO TAMBIÉN A TERCEROS, CUYOS DATOS PERSONALES EL CLIENTE PROPORCIONA A SYMANTEC, DEL HECHO DE QUE SUS DATOS PUEDEN SER PROCESADOS EN ESOS PAÍSES; Y (II) OBTENER LA AUTORIZACIÓN DE DICHOS EMPLEADOS, AGENTES, CONTRATISTAS Y TERCEROS PARA DICHO PROCESAMIENTO. SYMANTEC NO ACEPTARÁ NINGUNA RESPONSABILIDAD POR EL INCUMPLIMIENTO DE LA LEGISLACIÓN O NORMAS APLICABLES.

6.5 NINGÚN SOFTWARE O SERVICIO PUEDEN GARANTIZAR UNA TASA DE DETECCIÓN DE MI DEL 100%. EN CONSECUENCIA, SYMANTEC NO ACEPTARÁ RESPONSABILIDAD POR DAÑOS O PERJUICIOS QUE RESULTEN DIRECTA O INDIRECTAMENTE DE NO HABER DETECTADO CORREO BASURA (SPAM), VIRUS, ATAQUES DE PHISHING, CÓDIGOS MALICIOSOS, URL BLOQUEADAS O CONTENIDOS CONTROLADOS, O POR LA IDENTIFICACIÓN ERRÓNEA POR IMS DE MI QUE CONTIENE CORREO BASURA, VIRUS, ATAQUES DE PHISHING, CÓDIGOS MALICIOSOS, URL BLOQUEADAS O CONTENIDOS CONTROLADOS. Por otra parte, la configuración de las reglas que gobiernan el control de contenido de IMS está a cargo del Cliente totalmente, y la exactitud de la configuración afectará la exactitud de IMS.

Apéndice 14
Symantec Email Continuity Archive.cloud y
Symantec Email Continuity Archive Lite.cloud

1. Visión global

1. Los Servicios Symantec Email Continuity Archive.cloud y Symantec Email Continuity Archive Lite.cloud son sistemas hospedados de almacenamiento de mensajes electrónicos que permiten a los administradores de sistema del Cliente fijar normativas determinadas de retención de e-mail para el almacenamiento histórico del correo electrónico de un grupo determinado de buzones.

2. Obligaciones del Cliente

2.1 El Cliente tiene las siguientes responsabilidades en relación con el Servicio:
2.1.1 Proporcionar y mantener el hardware y software necesarios (conforme a lo que indique el formulario de prestación del Servicio);
2.1.2 Asegurarse de que haya disponible un recurso técnico especializado con derechos administrativos para la prestación del Servicio;
2.1.3 Designar qué Usuarios tienen derecho a recibir el Servicio y el periodo indicado de retención por cada usuario;
2.1.4 Designar y proteger privilegios de acceso al archivo a través de la interfaz de cliente;
2.1.5 Fijar y gestionar la normativa de retención de datos archivados;
2.1.6 Llevar a cabo búsquedas para recuperar datos archivados.
2.2 En la eventualidad de que el Cliente no haya tomado las medidas necesarias para prestar el Servicio dentro de un plazo de treinta (30) días a partir de la fecha del pedido del Cliente, Symantec tendrá derecho a empezar a cobrar por el Servicio.

3. Prestaciones

3.1 El *Servicio Symantec Email Continuity Archive.cloud* comprende las siguientes prestaciones:
3.1.1 *Captura y almacenamiento de E-mail* el e-mail es capturado cuando llega al entorno primario del Cliente y se transfiere a un archivo de mensajes electrónicos para su indexación y almacenamiento. El mensaje electrónico es cifrado y guardado en el Servicio. La normativa de retención de mensajes puede ser fijada para que los usuarios determinen qué mensajes serán eliminados del Servicio.
3.1.2 *Recuperación* – ofrece la capacidad para restaurar mensajes electrónicos para los almacenes de mensajes del Exchange del Cliente a partir del archivo de mensajes electrónicos.
3.1.3 *Revelación electrónica (E-discovery)* – ofrece a los administradores de sistema del Cliente la capacidad de nombrar "Examinadores" (Reviewers) a ciertos Usuarios, otorgándoles la capacidad para examinar los mensajes electrónicos de buzones ajenos para efectos de revelación electrónica y otros. Los Examinadores pueden crear un archivo de revelaciones para guardar los resultados de una búsqueda por los buzones de los usuarios. El archivo de revelaciones puede ser exportado a un buzón único.
3.1.4 *Autenticación de Windows* – permite a un Cliente que utiliza Microsoft Exchange 2000, Microsoft Exchange 2003 y/o Microsoft Exchange 2007 extender los criterios de seguridad del Cliente para la autenticación de Microsoft Active Directory a Usuarios del Servicio permitiendo que los Usuarios hagan el login en el Servicio utilizando su contraseña para Active Directory.
3.1.5 *Archivo de Usuario Final* – permite a los Usuarios que forman parte de una normativa de retención acceder a su archivo personal que contiene los e-mails de su buzón por medio de una interfaz de web. Los administradores de e-mail del Cliente pueden también precisar si los usuarios pueden o no reenviar mensajes electrónicos de su archivo personal.
3.1.6 *Gestión de almacenamiento* – el administrador de sistema del Cliente puede definir la normativa para la gestión de almacenamiento que gobernará el movimiento de adjuntos de los almacenes de mensajes de Exchange del cliente al Servicio con el fin de reducir la capacidad de almacenamiento necesaria.
3.2 El *Servicio Symantec Email Continuity Archive Lite.cloud* comprende las siguientes prestaciones (según la explicación expuesta de cada una):
3.2.1 *Captura y almacenamiento de e-mail*
3.2.2 *Recuperación*
3.2.3 *E-Discovery*
3.2.4 *Autenticación de Windows*
El servicio Symantec Email Continuity Archive Lite.cloud no comprende las prestaciones de archivo de usuario final o gestión de almacenamiento. El Cliente podrá elevar el nivel de prestaciones con la inclusión del servicio Archivo de usuario final dándose de alta en *Symantec Email Continuity Archive Lite.cloud End User Pack* (Paquete de Usuario Final de Email Continuity Archive Lite).
3.3 *Importaciones* – el Cliente puede importar al Servicio datos heredados de archivos pst bajando y utilizando una herramienta de importación previo pago de una cuota de importación en función de la cantidad de datos a importar. En la eventualidad de que la cantidad real de datos heredados exceda la cantidad de datos importados correspondiente a la tarifa pagada, Symantec se reserva el derecho a cobrar por la capacidad adicional conforme a las tarifas vigentes a la sazón.

4. Storage D

4.1 El cliente tiene la obligación de alquilar suficiente espacio de almacenamiento para fines de retención.
4.2 En el caso de que el Cliente esté dado de alta en Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email and Web Safeguard.cloud o Symantec MessageLabs Ultimate Safeguard.cloud, dichos paquetes comprenden un máximo de 0,7 GB de almacenamiento anual de email por Usuario para los servicios combinados de Symantec MessageLabs Email Continuity.cloud (D) y Symantec MessageLabs Email Archiving.cloud (D). Si el Cliente necesita más capacidad de almacenamiento que la permitida, deberá contratar suficiente capacidad de almacenamiento para el Servicio conforme a la tarifa de Symantec que esté vigente a la sazón.
4.3 En el caso de que el Cliente no esté dado de alta en uno de los paquetes indicados en 4.2, el precio por Usuario no comprende almacenamiento, por lo que el Cliente deberá contratar suficiente capacidad de almacenamiento para el Servicio conforme a la tarifa de Symantec que esté vigente a la sazón.
4.4 En el caso de que el Cliente tenga que contratar almacenamiento adicional, Symantec pasará las facturas adicionales del caso y/o hará los ajustes necesarios a las facturas posteriores para cubrir el precio del almacenamiento adicional de una forma prorrateada durante el resto del periodo de facturación en curso.

5. Términos y condiciones

5.1 NINGÚN SERVICIO DE ARCHIVADO DE E-MAIL PUEDE GARANTIZAR UNA EXACTITUD DEL 100% POR LO QUE SYMANTEC NO ACEPTARÁ NINGUNA RESPONSABILIDAD EN CASO DE DAÑOS O PÉRDIDA QUE RESULTE A CONSECUENCIA DIRECTA O INDIRECTA DE UN FALLO EN EL SERVICIO SALVO EN LA MEDIDA CONTEMPLADA EXPRESAMENTE EN EL CONTRATO DE NIVEL DE SERVICIOS.
5.2 Symantec no aceptará responsabilidad por la incapacidad para prestar los Servicios expuestos en este documento que se deba a (a) la incapacidad de Symantec de aplicar sus prácticas normales para la instalación y gestión del Servicio al Cliente, (b) la incapacidad por parte del Cliente de observar las directrices de Symantec expuestas en el manual de usuario o en el formulario de prestación de servicio, o (c) la incapacidad del Cliente para activar o utilizar el Servicio.
5.3 Symantec pone de relieve que la configuración y utilización del Servicio están completamente bajo el control del Cliente. Symantec recomienda que el Cliente adopte una normativa para el uso aceptable de computadoras (o su equivalente). Cabe la posibilidad de que en algunos países sea necesario obtener autorización de miembros del personal. Symantec recomienda al Cliente consultar siempre la legislación local con anterioridad a la instalación del servicio. Symantec no aceptará responsabilidad civil ni penal en el caso de que el Cliente incurra en irregularidades en la operación del servicio.
5.4 EL CLIENTE RECONOCE Y ACEPTA QUE TODO O PARTE DEL SERVICIO PUEDE SER EJECUTADO EN LOS ESTADOS UNIDOS DE AMÉRICA Y QUE EL CLIENTE ES RESPONSABLE DE OBTENER LAS AUTORIZACIONES Y APROBACIONES CORRESPONDIENTES PARA EFECTUAR LA TRANSFERENCIA DE DATOS. EL CLIENTE RECONOCE Y ACEPTA, ASIMISMO, QUE SYMANTEC NO ACEPTARÁ RESPONSABILIDAD DE POSIBLES INCUMPLIMIENTOS DE LA LEGISLACIÓN O NORMAS APLICABLES.

5.5 El Cliente reconoce y acepta que (i) los servicios de escaneo de Symantec (E-mail AV, E-mail AS, E-mail IC y E-mail CC) no escanean todos los mensajes que entran en el archivo y (ii) que los servicios de escaneo de Symantec (E-mail AV, E-mail AS, E-mail IC y E-mail CC) no escanean los mensajes electrónicos que salen del archivo para su reinstauración en el buzón de un usuario. En consecuencia, Symantec no aceptará responsabilidad de virus, spam, imágenes y otro contenido inapropiado que contengan los mensajes electrónicos reinstaurados. Por otra parte, el Contrato de Nivel de Servicio no será de aplicación a los e-mailes reinstaurados.
5.6 El cliente reconoce y acepta que, en virtud de las normativas de SEC, Symantec no puede actuar como tercero descargador en ningún caso.

6. Licencia de software

6.1 Otorgamiento de licencia

Con arreglo a las condiciones del presente contrato, Symantec otorga al usuario el derecho intransferible y no exclusivo de instalar y utilizar el software para el servicio Symantec Email Continuity Archive.cloud y Symantec Email Continuity Archive Lite.cloud únicamente para las actividades empresariales internas del usuario ("Software" se refiere a cada programa de software para el servicio Symantec Email Continuity Archive.cloud y Symantec Email Continuity Archive Lite.cloud en formato código objeto licenciado por Symantec y cuya utilización se regirá por las condiciones contractuales, y comprende, sin limitación, las nuevas versiones o actualizaciones que se distribuyan con arreglo a lo dispuesto en virtud de este contrato). Todos los derechos de propiedad intelectual sobre el Software son propiedad de Symantec (y/o de sus proveedores). Symantec no vende el Software, sino que lo licencia. El usuario reconoce que el Software y toda la información relacionada con el mismo, incluidas, sin limitación, las actualizaciones, son propiedad de Symantec y sus suministradores. El cliente será totalmente responsable de que cada usuario final cumpla las condiciones contractuales y deberá responder de cada incumplimiento. El usuario deberá notificar inmediatamente a Symantec del uso desautorizado o violación de las condiciones de esta licencia.

6.2. Limitaciones en cuanto a copias y utilización

El usuario está autorizado a descargar e instalar el Software con arreglo a las siguientes condiciones:
6.2.1. El usuario no está autorizado a descargar o instalar el Software para un número mayor de usuarios finales que el número de licencias de usuario final otorgadas al cliente ("usuario final" para estos efectos es el ordenador en el que se instala el Software).
6.2.2. El usuario está autorizado para copiar el Software según justifiquen las circunstancias con fines de backup, archivaje o recuperación tras un fallo catastrófico. La documentación impresa puede ser reproducida por el usuario para su utilización interna únicamente ("Documentación" son las guías de Symantec para el usuario y/o los manuales de funcionamiento del Software incluido en la descarga del mismo.).
6.2.3 El usuario no está autorizado ni deberá permitir que terceros: (i) descompilen, desensamblen o apliquen ingeniería inversa al Software, salvo en la medida expresamente contemplada por la legislación vigente, sin la previa autorización escrita de Symantec; (ii) suprimir una identificación del producto o aviso de derechos de propiedad; (iii) alquilar, prestar o utilizar el Software para su utilización en aplicaciones de tiempo compartida o por oficinas de servicios (*service bureau):* (iv) modificar, traducir, adaptar o crear derivados del Software, o (v) en general utilizar o copiar el Software de una forma que nos esté expresamente contemplada en esta licencia.

6.3. Traspaso de derechos

El usuario no está facultado a traspasar, ceder o delegar la licencia de Software al amparo de este contrato sin la previa autorización escrita de Symantec. Todo traspaso, cesión o delegación de derechos en contravención de lo expuesto anteriormente no tendrá ningún efecto.

6.4. Garantía limitada y advertencia

6.4.1 Symantec garantiza que tras su descarga el Software cumplirá todas las funciones que contempla la documentación vigente de Symantec.
6.4.2 Esta garantía no será de aplicación en los siguientes supuestos: (i) el Software no se utiliza de acuerdo con este contrato o la documentación; (ii) el Software en todo o en parte ha sido modificado por una entidad ajena a Symantec; o (iii) la causa de que el Software no funcione bien se debe al equipo del usuario o software de terceros.
6.4.3 CON ARREGLO A LA PRESENTE GARANTÍA, SYMANTEC SE COMPROMETE ÚNICAMENTE A REEMPLAZAR EL SOFTWARE DEFECTUOSO SEGÚN DISPONIBILIDAD. SYMANTEC NO GARANTIZA QUE EL SOFTWARE FUNCIONARÁ SIN INTERRUPCIÓN O SIN ERRORES. SYMANTEC ADVIERTE EXPRESAMENTE QUE NO OFRECE NINGUNA CLASE DE GARANTÍA EXPRESA, IMPLÍCITA O DE OTRA FORMA, EN LO QUE SE REFIERE A LA APTITUD DEL SOFTWARE PARA EL COMERCIO O EL CONSUMO, CALIDAD SATISFACTORIA, IDONEIDAD PARA UN FIN EN PARTICULAR, NI GARANTÍA DE OTRA ÍNDOLE.

6.5. Extinción

Una vez extinguido el Servicio Symantec Email Continuity Archive.cloud y Symantec Email Continuity Archive Lite.cloud o el contrato, cesará de inmediato el derecho del usuario a utilizar el Software que se le otorga en esta licencia. El usuario deberá devolver a Symantec o destruir los ejemplares del Software y la documentación.

7. Finalización del servicio y extracción de datos

7.1 Tras la finalización de los servicios Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud, Symantec eliminará los datos del cliente del archivo de almacenamiento.

7.2 El cliente puede extraer sus datos del archivo de almacenamiento en cualquier momento antes de la finalización.

Apéndice 15
Symantec MessageLabs Volume Mail Service
[Servicio de correo de elevado volumen]

1. En la eventualidad de que el Cliente esté suscrito al servicio de correo de elevado volumen, el Cliente podrá enviar y recibir correo de elevado volumen conforme a las siguientes condiciones:

1.1 Solamente formarán parte del servicio de correo de elevado volumen las personas que opten expresamente por recibir este servicio. A solicitud de Symantec, y conforme a la legislación vigente, el Cliente deberá proporcionar constancia escrita de dicha elección.

1.2 Un correo de alto volumen, adjuntos incluidos, no deberá exceder los 500 kilobytes.

1.3 La casilla de "Destinatarios" en cada correo de elevado volumen no debe contener más de quinientas (500) direcciones como máximo.

1.4 El Cliente deberá contar con un sistema de gestión de lista efectivo que sea capaz de eliminar con prontitud direcciones inválidas y mensajes de cancelación de la suscripción.

1.5 El Cliente deberá tener contratado el servicio Symantec MessageLabs Email Anti-Virus.cloud para su correo normal.

1.6 El correo de elevado volumen del Cliente deberá proceder de, o estar dirigido a, un dominio que no sea el de su correo normal para que el correo de elevado volumen apunte a una Torre de Control especialmente equipada.

1.7 El banner predeterminado de correo de salida deberá indicar al destinatario que el correo de elevado volumen se ha sometido a control de virus, pero no mostrará el logotipo de Symantec.

1.8 En la eventualidad de que el Cliente se haya dado de alta en las bandas F ó G del servicio de correo de elevado volumen en la sección B "Servicios y tarifas", el Cliente deberá recibir o enviar correo de elevado volumen en lotes de un máximo de 250.000 destinatarios al día.

1.9 El Cliente reconoce y acepta que el envío de correo de elevado volumen probablemente tenga unos efectos variables en el flujo de tráfico. Dichos efectos son ajenos a la voluntad de Symantec y por esta razón los niveles de servicio que recoge el Contrato de Niveles de Servicio no será de aplicación al correo de elevado volumen.

1.10 Si en cualquier momento (i) los sistemas de correo del Cliente pasan a formar parte de la lista negra, o bien (ii) los sistemas de Symantec pasan a formar parte de la lista negra por culpa del Cliente debido al envío de correo spam, , o bien (iii) el Cliente incumple alguna de sus obligaciones que recoge este anexo, Symantec deberá notificar al Cliente reservándose el derecho a dejar de prestar, suspender o terminar los Servicios a su albedrío total o parcialmente y de inmediato.

1.11 Cada banda de servicio de correo de elevado volumen tiene una cuota máxima de destinatarios permitidos cada mes. Dichas cuotas no son ni transferibles ni acumulativas y por lo tanto el número de destinatarios no aprovechado un mes determinado no puede transferirse a meses subsiguientes.

1.12 El Cliente deberá notificar a Symantec en la eventualidad de que el número de destinatarios mensuales sobrepase el número permitido correspondiente a la banda del Cliente para que Symantec cobre la cuota de la banda que corresponda conforme a la tarifa vigente a la sazón. Symantec tambien observará el uso efectivo de correo de elevado volumen del Cliente y si el numero de recipientes por mes es mayor que el permitido por la banda de servicio del Cliente, Symantec aumentará las cargas según sus tarifas vigentes. Symantec, a su discreción, pasará facturas adicionales y/o ajustará las facturas trimestrales subsiguientes para cobrar esos incrementos.

Apéndice 16
Symantec Enterprise Vault.cloud

1. Descripción general

Symantec EV.cloud es el nombre colectivo de una cantidad de servicios de archivado (como se describe en las Cláusulas 1.1 a 1.10 inclusive, a continuación) a los que el cliente puede suscribirse. Todos los servicios de la gama Symantec EV.cloud son compatibles con las versiones aprobadas de los servidores Exchange y los servicios alojados de Exchange de las instalaciones.

1.2 La información a continuación se aplica a los servicios Symantec Enterprise Vault Personal.cloud y Symantec Enterprise Vault Discovery.cloud:

1.2.1 El tamaño máximo de correo electrónico que pueden asimilar los servicios Symantec Enterprise Vault Personal.cloud y Symantec Enterprise Vault Discovery.cloud es de 50 MB.

1.2.2 La información a continuación se aplica a los servicios Symantec Enterprise Vault Personal.cloud y Symantec Enterprise Vault Discovery.cloud:

1.2.3 Los clientes pueden responder o reenviar directamente mensajes contenidos en el archivo de almacenamiento creado por cualquiera de los servicios, lo que permite al cliente crear archivos de copia de seguridad regularmente en caso de que se produzca un fallo en el correo electrónico del cliente.

1.2.4 Ninguno de los servicios reemplaza la necesidad del cliente de realizar una copia de seguridad local del servidor de correo electrónico. En caso de que el cliente necesite volver a crear el servidor de correo, debe hacerlo a partir de los datos gestionados de forma local en lugar de datos de los archivos de almacenamiento.

1.1. Symantec Enterprise Vault Personal.cloud

El servicio Symantec Enterprise Vault Personal.cloud es el servicio de archivado basado en Internet de Symantec. Está diseñado para ofrecer a los usuarios individuales del cliente acceso a sus propios archivos del correo electrónico personal directamente de Microsoft Outlook o Outlook Web Access (cuando sea compatible) para encontrar o restaurar correos electrónicos perdidos o eliminados.

1.1.1 Los correos electrónicos entrantes y salientes del cliente, incluidos los archivos adjuntos, se capturan en un repositorio online que permite realizar búsquedas ("Personal Archive"), de forma que los usuarios puedan encontrar correos electrónicos eliminados o perdidos.

1.1.2 Además, los usuarios pueden acceder al Personal Archive desde Microsoft Outlook, Outlook Web Access (cuando sea compatible), IBM Lotus Notes, dispositivos BlackBerry® y mediante un sitio web seguro basado en navegador.

1.1.3 Los usuarios disponen de dos formas de buscar correos electrónicos y archivos adjuntos específicos en el Personal Archive: búsqueda rápida y búsqueda avanzada. La opción Búsqueda avanzada ofrece a los usuarios la capacidad de personalizar sus búsquedas en función de diferentes criterios, como palabra clave en el mensaje, de, para, asunto, fecha y tipo de archivo adjunto.

1.1.4 Si la opción está habilitada, los usuarios pueden redactar, responder y reenviar mensajes directamente desde Personal Archive, al igual que en Outlook o Notes.

1.1.5 Los usuarios pueden crear búsquedas personalizadas en función de diferentes criterios (por ejemplo, intervalo de fechas, remitente del correo electrónico, tipo de archivo adjunto, etc.) y, luego, guardarlas para reutilizarlas según sea necesario.

1.1.6 La transferencia del correo electrónico antiguo del cliente al Personal Archive y la eliminación de los archivos locales ayuda a recuperar espacio en los servidores de correo electrónico y las unidades compartidas del cliente.

1.1.7 El Personal Archive del cliente puede utilizarse para recuperar correos electrónicos antiguos en caso de robo o pérdida de un equipo de escritorio o portátil.

1.1.8 Los clientes pueden incluir archivos PST en Personal Archive, y se permite mantener la estructura de carpetas después de la inclusión.

1.2. Symantec Enterprise Vault Discovery.cloud

El servicio Symantec Enterprise Vault Discovery.cloud es el servicio de archivado basado en Internet de Symantec. Está diseñado para acelerar las solicitudes de detección legal (e-discovery), aplicar las políticas de uso del correo electrónico y ayudar a mitigar la pérdida de datos. Symantec Enterprise Vault Discovery.cloud ayuda a los clientes a mantener el correo electrónico relacionado con demandas judiciales o retenciones legales, y a proteger las comunicaciones de acceso restringido entre abogado y cliente.

1.2.1 Symantec Enterprise Vault Discovery.cloud almacena e indexa correos electrónicos, archivos adjuntos y mensajes de BlackBerry® (texto SMS, PIN a PIN, registro de llamada) en un repositorio online centralizado.

1.2.2 Los clientes pueden colocar retenciones legales en comunicaciones específicas (en función de criterios de búsqueda) para ayudar a evitar que el personal del cliente o las políticas de eliminación automática eliminen accidentalmente correos electrónicos relevantes para el caso. Los administradores y los revisores pueden marcar las comunicaciones confidenciales entre abogado y cliente y excluirlas de las solicitudes de detección electrónica.

1.2.3 El registro de búsqueda de Symantec Enterprise Vault Discovery.cloud captura las actividades de los revisores para permitir a los administradores realizar las revisiones apropiadas.

1.2.4 Los administradores pueden agrupar usuarios en función de criterios personalizados. Luego, los revisores pueden realizar búsquedas en estos grupos.

1.2.5 Los clientes pueden buscar en el contenido de correos electrónicos y archivos adjuntos almacenados con varios criterios de búsqueda, como de, para, fecha, asunto, cuerpo del mensaje, archivos adjuntos del mensaje y otras propiedades del mensaje.

1.2.6 Los revisores del cliente pueden navegar con eficacia por los resultados de las búsquedas, identificar términos de búsqueda resaltados y etiquetar correos electrónicos potencialmente dañinos a fin de permitir la fácil recuperación para una mayor revisión.

1.2.7 Los clientes pueden etiquetar correos electrónicos relacionados con un caso específico o un asunto legal y, luego, exportarlos a una solución de gestión de casos de otro fabricante u otra aplicación para una mayor revisión y análisis.

1.2.8 Los revisores del cliente pueden crear y guardar búsquedas personalizadas de correo electrónico en función de políticas de correo electrónico del cliente y reutilizarlas según sea necesario.

1.2.9 Los revisores del cliente pueden configurar alertas de políticas para recibir notificaciones cuando un correo electrónico reúne los criterios de "Búsqueda guardada" (por ejemplo, contiene palabras o frases específicas).

1.3. Symantec Enterprise Vault.cloud BlackBerry® Option

El servicio Symantec Enterprise Vault.cloud BlackBerry® Option es el servicio basado en Internet de Symantec. Está diseñado para permitir a los usuarios individuales del cliente buscar correos electrónicos, archivos adjuntos, SMS, mensajes de PIN a PIN y archivos de registro de llamadas archivados, y acceder a ellos mediante sus dispositivos BlackBerry®. Los usuarios pueden buscar y restaurar correos electrónicos perdidos o eliminados y continuar utilizando su dispositivo BlackBerry® para redactar, responder y enviar mensajes en tiempo real, incluso durante una interrupción del servidor principal de correo electrónico del cliente. El servicio Symantec Enterprise Vault.cloud BlackBerry® Option es un servicio complementario opcional del servicio Symantec Enterprise Vault Personal.cloud.

1.3.1 Los administradores pueden implementar el servicio Symantec Enterprise Vault.cloud BlackBerry® Option para usuarios desde BlackBerry® Enterprise Server (BES) mediante BlackBerry® Desktop Manager.

1.3.2 Los usuarios pueden iniciar sesión en el Symantec Enterprise Vault.cloud BlackBerry® Option haciendo clic en el icono que aparece en la pantalla principal del dispositivo.

1.3.3 Al hacer clic en la aplicación, se muestra una pantalla de inicio durante tres segundos y, luego, el usuario debe introducir sus credenciales.

1.3.4 Una vez que el usuario inicia sesión correctamente, es dirigido a la pantalla principal (es decir, a la pantalla de Vista de la lista) del Personal Archive.

1.3.5 Desde la pantalla de Vista de la lista (Buzón), los usuarios pueden realizar diferentes funciones, como: redactar mensajes nuevos, responder o reenviar correos electrónicos y realizar búsquedas simples o avanzadas.

1.3.6 Los usuarios pueden encontrar correos electrónicos antiguos, perdidos o eliminados con funciones de búsqueda simple o avanzada de todos los mensajes y archivos de registro de llamadas almacenados en su Personal Archive y, luego, restaurar estos mensajes en su bandeja de entrada.
1.3.7 Los usuarios pueden introducir texto en el cuadro de búsqueda y pulsar el icono de búsqueda para iniciar la búsqueda. Los resultados de búsqueda pueden filtrarse por "Fecha", "De" y "Para".
1.3.8 El usuario puede usar su Personal Archive para redactar, responder y enviar mensajes, incluso si la plataforma principal de correo electrónico del cliente (por ejemplo, Microsoft Exchange) no está disponible.

1.4 AdvisorMail on Symantec.cloud™
El servicio AdvisorMail on Symantec.cloud™ ("AdvisorMail") es el servicio de archivado de correo electrónico basado en Internet de Symantec que logra acelerar el proceso de comprobación del correo electrónico exigido por algunos requisitos normativos. El servicio de AdvisorMail archiva los correos electrónicos en un único repositorio. Los mensajes se autoanalizan y se marcan según las políticas específicas del cliente. Los mensajes o los archivos adjuntos que contengan palabras claves o frases específicas pueden ser revisados por profesionales de cumplimiento para la aplicación de políticas.
1.4.1 AdvisorMail captura automáticamente los mensajes enviados y recibidos sin la intervención del cliente y los transmite de manera segura a diferentes centros de datos para su retención, mediante el cifrado de TLS o VPN.
1.4.2 Las herramientas de administración y elaboración de informes de AdvisorMail incluyen modos previos o posteriores a la revisión, muestras aleatorias, reglas personalizables para dominios o direcciones de correo electrónico e informes de resumen específicos.
1.4.3 AdvisorMail ofrece dos niveles de permiso distintos para la revisión del correo electrónico: administrador (acceso completo) y auditor (derechos de supervisión para buzones seleccionados).
1.4.4 AdvisorMail ofrece una cantidad de herramientas para racionalizar el proceso de supervisión, incluida la marca automática de correos electrónicos sospechosos para que el auditor los revise.
1.4.5 Los clientes puede preseleccionar su carpeta de inicio (por ejemplo, posterior a la revisión), el intervalo de fechas y la vista de los mensajes (por ejemplo, vista de lista o fragmento).
1.4.6 Los clientes pueden usar la función Siguiente clic para ir a la siguiente infracción en los mensajes de correo electrónico y archivos adjuntos con un solo clic. Las acciones del botón secundario del ratón les permiten elegir los comandos simplemente haciendo clic con el botón secundario del ratón (por ejemplo, agregar palabras clave al diccionario).
1.4.7 La función de supervisión por niveles de AdvisorMail permite a los clientes distribuir un diccionario corporativo (lista de frases y palabras clave de infracción) a las oficinas remotas con un solo comando.
1.4.8 El editor de lista blanca de AdvisorMail permite a los clientes crear una lista blanca de palabras clave y frases que se encuentran habitualmente en las renuncias de responsabilidad (por ejemplo, las renuncias de responsabilidad legales que aparecen en los pies de página de los correos electrónicos) para reducir la cantidad de falsos positivos de las infracciones de cumplimiento.
1.4.9 AdvisorMail permite a los clientes agregar direcciones de correo electrónico, trasladar usuarios a otras oficinas, modificar reglas y revisar diferentes correos electrónicos.
1.4.10 El registro de búsqueda de AdvisorMail captura las actividades de auditoría de los revisores de la empresa, lo que ayuda a los administradores a cumplir con los requisitos de cumplimiento.
1.4.11 Los auditores pueden agregar notas a los mensajes según sea necesario.

1.5 AdvisorMail IM Option on Symantec.cloud™
AdvisorMail IM Option on Symantec.cloud™ es el servicio de archivo basado en Internet de Symantec para las plataformas de mensajes instantáneos compatibles. Los mensajes instantáneos se capturan, se almacenan y se indexan en AdvisorMail y, después, se supervisan según las políticas de cumplimiento específicas del cliente. Luego, los profesionales de cumplimiento pueden revisar los mensajes instantáneos que contengan palabras claves o frases específicas para la aplicación de políticas. El servicio AdvisorMail IM Option on Symantec.cloud™ es un servicio complementario opcional de AdvisorMail.
1.5.1 El servicio AdvisorMail IM Option on Symantec.cloud™ funciona con clientes y redes de MI compatibles que, actualmente, incluyen redes de MI públicas, como AOL, MSN, Yahoo y Google Talk, y redes privadas (Reuters) y clientes de MI empresariales (Microsoft Office Communicator, Lotus Sametime y Jabber).
1.5.2 Los mensajes instantáneos se indexan y se copian en su formato original a soportes donde pueden buscarse fácilmente.
1.5.3 El cliente puede buscar y recuperar conversaciones de mensajería instantánea específica en función de diferentes criterios de búsqueda, como intervalo de fechas, palabra clave o frase y remitente/destinatario.
1.5.3 Para fines de auditoría, se conserva un historial de registro.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™
El servicio AdvisorMail Bloomberg Option on Symantec.cloud™ es el servicio de archivado basado en Internet de Symantec para Instant Bloomberg (mensajes instantáneos) y el correo electrónico de Bloomberg. Los mensajes de Bloomberg se capturan, se almacenan y se indexan en AdvisorMail y, después, se supervisan según las políticas específicas de la empresa. Luego, los profesionales de cumplimiento pueden revisar los mensajes de Bloomberg que contienen frases o palabras clave especificadas. El servicio AdvisorMail Bloomberg Option on Symantec.cloud™ es un servicio complementario opcional de AdvisorMail.
1.6.1 El servicio AdvisorMail Bloomberg Option on Symantec.cloud™ captura Instant Bloomberg y correos electrónicos de Bloomberg en AdvisorMail, en su formato propietario.
1.6.2 Los mensajes de Bloomberg se indexan y se copian en su formato original a soportes de almacenamiento, donde pueden buscarse fácilmente.
1.6.3 El cliente puede buscar y recuperar mensajes de Bloomberg específicos en función de diferentes criterios de búsqueda, como intervalo de fechas, palabra clave o frase y remitente/destinatario.
1.6.4 Para fines de auditoría, se conserva un historial de registro.

1.7 Reservado

1.8 Symantec Enterprise Vault.cloud Data Import Option
El Symantec Enterprise Vault.cloud Data Import Option es el servicio basado en Internet de Symantec. Está diseñado para migrar y procesar datos existentes de correos electrónicos anteriores en el repositorio de archivos del cliente. El servicio de importación permite al cliente realizar búsquedas en el archivo de correo electrónico (por ejemplo, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud y AdvisorMail) e incluir correos electrónicos anteriores procesados y nuevos flujos de correo electrónico.
1.8.1 El Symantec Enterprise Vault.cloud Data Import Option requiere que el cliente envíe datos de correo electrónico por correo seguro o S-FTP en formato de archivo PST o EML.
1.8.2 El cliente puede extraer los datos de forma manual y proporcionarlos en formato PST o EML, o usar los servicios profesionales de Symantec para la extracción automatizada desde repositorios admitidos.
1.8.3 Con la ayuda del cliente, el servicio Symantec Enterprise Vault.cloud Data Import Option asigna la titularidad a cada mensaje encontrado. Los mensajes que no pueden ser asignados directamente a una persona específica se archivan en un buzón "catchall" (que abarca todo) dentro del archivo de almacenamiento del correo electrónico.
1.8.4 Toda la actividad de migración puede registrarse y auditarse para brindar integridad a los registros de correo electrónico del cliente y mantener la "cadena de custodia".
1.8.5 El servicio Symantec Enterprise Vault.cloud Data Import Option implica la participación activa del cliente en la planificación, análisis y ejecución de un plan de procesamiento con mínimas interrupciones para la empresa.

1.8.6 El tamaño máximo de correo electrónico que puede asimilar el servicio es de 40 MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud

SI SYMANTEC NO PUEDE ESTABLECER UNA CONEXIÓN SMTP CON EL CLIENTE, LOS CORREOS ELECTRÓNICOS DEL CLIENTE SE DIRIGIRÁN AL SERVICIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD EN NOMBRE DEL CLIENTE ("EVENTO DE CONTINUIDAD"). PARA EVITAR DUDAS: (I) SI EL FIREWALL DEL CLIENTE ACTÚA COMO PROXY Y RESPONDE EN NOMBRE DEL SERVIDOR DE CORREO, O (II) SI EL SERVIDOR DE CORREO DEL CLIENTE EMITE CUALQUIER RESPUESTA (INCLUIDOS CÓDIGOS DE ERROR SIN LIMITACIÓN), ESTO CONSTITUIRÁ UNA CONEXIÓN SMTP Y NO SERÁ UN EVENTO DE CONTINUIDAD.

1.9.1 Durante un evento de continuidad, los usuarios individuales del cliente pueden acceder a su correo electrónico a través de una carpeta en Microsoft Outlook® o una interfaz de usuario basada en Web. El usuario puede: (i) ver hasta noventa (90) días de correos electrónicos históricos, incluidos los nuevos correos electrónicos enviados y recibidos durante el evento de continuidad, (ii) crear, responder y reenviar correos electrónicos, y (iii) usar herramientas comunes de correo electrónico como la corrección ortográfica, inserción de archivos adjuntos y formato enriquecido.

1.9.2 Si el cliente está suscrito únicamente a Symantec Enterprise Vault Mailbox Continuity.cloud, los correos electrónicos de continuidad se almacenarán en dicho servicio por un periodo de noventa (90) días. Si el cliente adquirió un servicio de archivo adicional en virtud del presente Apéndice 17, los correos electrónicos de continuidad se mantendrán de acuerdo con el periodo de retención seleccionado por el cliente en dicho servicio.

1.9.3 Los correos electrónicos de continuidad se entregarán al servidor principal de correo electrónico del cliente en el momento en que dicho servidor comience nuevamente a aceptar correos electrónicos, con la excepción de que no se entregará ningún correo electrónico que haya estado en cola durante más de siete (7) días y, en su lugar, el cliente deberá recuperar los correos electrónicos de los archivos de continuidad que se describen en la Cláusula 1.9.2 anterior.

1.9.4 El servicio Symantec Enterprise Vault Mailbox Continuity.cloud utiliza una conexión de seguridad de capa de transporte (TLS) ad-hoc, en lugar de aplicada, cuando envía los correos electrónicos. La TLS es un protocolo de seguridad mejorado diseñado para proteger y cifrar el correo electrónico durante el transporte a través de Internet. **TODOS LOS CLIENTES DE LOS SERVICIOS BOUNDARY ENCRYPTION Y POLICY BASED ENCRYPTION QUE TAMBIÉN SELECCIONEN EL SERVICIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD RECONOCEN Y ACEPTAN QUE SE INTENTARÁ UNA CONEXIÓN TLS, PERO ES POSIBLE QUE NO SE REALICE Y, POR CONSIGUIENTE, ES POSIBLE QUE DICHOS CORREOS ELECTRÓNICOS NO SE CIFREN. EN CONSECUENCIA, EL CLIENTE RECONOCE QUE NO DEBERÁ ENVIAR O RECIBIR INFORMACIÓN CONFIDENCIAL A TRAVÉS DEL SERVICIO SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD O EL CLIENTE LO HACE A SU CUENTA Y RIESGO.**

1.9.5 Obligaciones de Symantec Enterprise Vault Mailbox Continuity.cloud

El servicio Symantec Enterprise Vault Mailbox Continuity.cloud sólo entrega correos electrónicos a un único servidor designado por dominio especificado y "por enrutamiento de usuario", por lo que los clientes aceptan este aspecto del servicio. El cliente acepta configurar el servicio Symantec Enterprise Vault Mailbox Continuity.cloud como una ruta de entrega de conmutación por error con la interfaz de ClientNet e informar a Symantec acerca de la ubicación de entrega (nombre del correo o dirección IP) por dominio de sus servidores de correo al inicio de este servicio. El cliente reconoce y acepta que tiene la obligación permanente de poner al corriente a Symantec sobre cualquier cambio en dicha ubicación de entrega mientras dure el servicio de Symantec Enterprise Vault Mailbox Continuity.cloud. El cliente reconoce que si no logra realizar dichas configuraciones o proporcionar a Symantec dicha información de entrega, repercutirá negativamente en la funcionalidad del servicio Symantec Enterprise Vault Mailbox Continuity.cloud.

1.10 Symantec Enterprise Vault.cloud Folder Sync Option

1.10.1 Symantec Enterprise Vault.cloud Folder Sync Option es un servicio complementario al servicio de Symantec Enterprise Vault Personal.cloud que sólo se describe en la Sección 1.1 de este Apéndice. El servicio Symantec Enterprise Vault.cloud Folder Sync Option permite a los clientes ver correos electrónicos en el servicio Symantec Enterprise Vault Personal.cloud de forma similar a cómo se organiza el correo electrónico en las carpeta de Outlook del cliente. Symantec Enterprise Vault.cloud Folder Sync Option permite a los administradores sincronizar las estructuras de carpeta de Outlook del cliente dentro de Symantec Enterprise Vault Personal.cloud. Los clientes mueven los mensajes de correo electrónico entre carpetas de Outlook y crean y trasladan las carpetas de Outlook. Posteriormente, el servicio de sincronización replica la estructura de las carpetas dentro de Symantec Enterprise Vault Personal.cloud.

1.10.2 Los administradores implementan Symantec Enterprise Vault.cloud Folder Sync Option para el cliente a través de un servicio local que realiza un seguimiento de las carpetas y los movimientos por elemento.

1.10.3 Después de la sincronización inicial, Symantec Enterprise Vault.cloud Folder Sync Option proporciona una sincronización incremental entre las carpetas de Outlook y Symantec Enterprise Vault Personal.cloud.

1.10.4 La sincronización incremental se puede programar una vez por semana, por día o por hora, según lo determine el cliente.

1.10.5 El cliente puede filtrar los resultados de una búsqueda de archivo mediante la función de "filtrado", seleccionando una carpeta de la lista que se devuelve en los filtros de búsqueda.

El servicio sólo es compatible con las plataformas de Microsoft Exchange Server 2003, 2007 o 2010.

2. Términos adicionales.

2.1 Symantec enfatiza que la configuración y el uso del servicio se encuentra completamente bajo control del cliente. Symantec recomienda que el cliente disponga de una política de uso del equipo aceptable (o su equivalente). En determinados países, es posible que se requiera el consentimiento del personal individual. Symantec recomienda al cliente que siempre compruebe la legislación local antes de la implementación del servicio. Symantec no será responsable, ni civil ni penalmente, por ninguna consecuencia que pueda sufrir el cliente como resultado de la operación del servicio.

2.2 **EL CLIENTE RECONOCE Y ACEPTA QUE EL SERVICIO, EN PARTE O EN SU TOTALIDAD, PUEDE REALIZARSE EN LOS ESTADOS UNIDOS DE NORTEAMÉRICA Y QUE ÉL ES EL RESPONSABLE DE OBTENER TODOS LOS CONSENTIMIENTOS Y LAS APROBACIONES NECESARIAS PARA EFECTUAR LA TRANSFERENCIA DE DATOS. ASIMISMO, EL CLIENTE RECONOCE Y ACEPTA QUE SYMANTEC NO PUEDE ACEPTAR NINGUNA RESPONSABILIDAD POR EL INCUMPLIMIENTO CORRESPONDIENTE DE LA LEGISLACIÓN O LAS REGULACIONES APLICABLES.**

2.3 El cliente acepta y reconoce que (i) los servicios de análisis de Symantec (Email AV, Email AS, Email IC y Email CC) no analizan todos los correos electrónicos que inicialmente ingresan en el archivo de almacenamiento y que (ii) los servicios de análisis de Symantec (Email AV, Email AS, Email IC y Email CC) no analizan los correos electrónicos que se envían desde el archivo para su reestablecimiento al buzón de un usuario. En consecuencia, Symantec no puede ser responsable por ningún virus, spam o imágenes y contenido inadecuado que dichos correos electrónicos reestablecidos puedan contener. Asimismo, el acuerdo de nivel de servicio no se aplicará a dichos correos electrónicos reestablecidos.

2.4 Sujeto a los términos y condiciones de este acuerdo, Symantec otorga al cliente el derecho no exclusivo e intransferible de instalar y utilizar cualquier software perteneciente a los servicios previamente mencionados, que se aplican únicamente para las operaciones empresariales internas del cliente. Todos los derechos de propiedad intelectual de este software son y serán propiedad de Symantec (y/o sus

proveedores). El Software se otorga con licencia de Symantec, no se vende. El cliente reconoce que el software y toda la información relacionada, incluidas, entre otras, las actualizaciones, son propiedad de Symantec y sus proveedores. Los clientes serán completamente responsables por el cumplimiento o el incumplimiento de cada usuario de los términos de este acuerdo. Los clientes deberán notificar de inmediato a Symantec todo uso no autorizado o infracción de los términos de esta licencia.

2.5 El cliente reconoce y acepta que, en virtud de las normativas de SEC, Symantec no puede actuar como tercero descargador en ningún caso.

2.6 Todos los datos del cliente que Symantec o sus distribuidores terceros almacenen o archiven en virtud de este documento son propiedad exclusiva del cliente ("Datos del cliente"), y nada en el presente confiere a Symantec o a sus distribuidores ningún derecho legal o equitativo, título o interés en relación con los datos del cliente.

2.7 Los datos del cliente se almacenarán o archivarán durante el plazo del servicio, y por un periodo de ciento veinte (120) días después del la finalización del servicio, o ciento veinte (120) días después de la fecha de finalización si el servicio finaliza antes del plazo de vencimiento (colectivamente, el "Periodo de retención posterior a la finalización"). Durante o antes del periodo de retención posterior a la finalización, el cliente deberá enviar una notificación escrita sobre su elección para que Symantec: (i) elimine los datos del cliente de forma gratuita (a menos que la ley o una orden judicial lo prohíba), o (ii) proporcione una copia sin conexión en formato PST a través de un disco duro según los índices de Symantec vigentes en ese momento y a un índice que no sea superior a dos (2) terabytes por mes hasta que todos los datos del cliente se devuelvan al cliente. En caso de que el cliente no desee proporcionar instrucciones escritas a Symantec, según lo indicado en el párrafo anterior, Symantec deberá eliminar los datos del cliente (a menos que la ley o una orden judicial lo prohíba) cuando caduque el periodo de retención posterior a la finalización.

Apéndice 17: Symantec Endpoint Protection.cloud
(Protección gestionada para puntos finales)

1. Descripción general

1.1 Para poder recibir el servicio Symantec Endpoint Protection.cloud Service, el cliente debe instalar un agente en los ordenadores de los usuarios finales y asignar políticas adecuadas para utilizar el Servicio. El portal de administración de Symantec Endpoint Protection.cloud es un portal para administradores que se utiliza para gestionar equipos, políticas, alertas e informes ("Portal de gestión").

1.2 Es posible que el cliente tenga que realizar algunos cambios básicos en el firewall para permitir que el agente se comunique y funcione con la infraestructura de Symantec Hosted Services.

1.3 Una vez que se haya configurado el servicio de acuerdo con las cláusulas 1.1 y 1.2, el Portal de gestión se usa para gestionar a los agentes.

1.4 Symantec publicará una lista de sistemas operativos de equipos compatibles con el agente y navegadores compatibles con el Portal de gestión. El cliente reconoce y acepta que Symantec puede actualizar y cambiar esta lista de forma regular sin aviso.

1.5 El agente en el equipo:

1.5.1 Protegerá el equipo contra malware detectado de acuerdo con los métodos conocidos según el servicio.

1.5.2 Bloqueará en el equipo los ataques de programas maliciosos conocidos de la red.

1.5.3 Hará lo posible por proporcionar funcionalidad antiphishing en los navegadores compatibles, la cual bloqueará los ataques de phishing estimados.

2. Portal de gestión

2.1 El Portal de gestión permite que el cliente configure su propia seguridad basada en políticas para los agentes.

2.2 El cliente es responsable de la implementación de las opciones de configuración de acuerdo con la política de uso aceptable de equipos del cliente (o similar) a través del Portal de gestión. Las políticas se configuran en el grupo de equipos.

2.3 Los cambios efectuados en la política se podrán ver de inmediato en el Portal de gestión, y se organizan para ser trasladados a los agentes. La configuración efectiva de políticas en los agentes individuales puede consultarse en el Portal de gestión o en el agente que se ejecuta en el equipo del usuario final.

3. Registros e informes

3.1 Todos los registros e informes efectuados por el agente se almacenan; pueden consultarse y descargarse desde el Portal de gestión por doce (12) meses; trascurrido ese periodo, los registros se eliminan.

4. Notificaciones

4.1 El cliente puede configurar el servicio Symantec Endpoint Protection.cloud Service para que envíe una notificación automática a los destinatarios de correo electrónico configurados según la regla de alertas, que puede configurarse en el Portal de gestión.

4.2 El cliente puede crear, eliminar y personalizar las notificaciones con el Portal de gestión.

5. Asistencia

5.1 La asistencia incluye:

5.1.1 Procedimientos guiados del Portal de gestión incluyendo una descripción del servicio y una sesión de preguntas y respuestas. (Esto no incluye asistencia en la configuración de políticas ni análisis de la efectividad de las políticas);

5.1.2 Guía del administrador;

5.1.3. Guía del usuario.

6. Symantec Endpoint Protection.cloud Data Privacy

6.1 El cliente reconoce que los registros pueden contener información de caracter personal y que el procesamiento y la intercepción de los registros pueden, por lo tanto, abarcar el proceso de datos personales. Además, el cliente reconoce que Symantec Endpoint Protection.cloud es un servicio que puede configurarse y que el cliente es el único responsable de configurarlo de acuerdo con la política de uso informático aceptable del cliente (o similar) y todas las leyes y normas aplicables. Por consiguiente, Symantec advierte al cliente que siempre debe revisar la legislación local antes de implementar el servicio Hosted Endpoint Protection, asegurándose de ésta cumpla todas las responsabilidades en lo que respecta a las leyes y/o normas de protección y privacidad de datos, y que los empleados las conozcan y las cumplan al utilizar el servicio Hosted Endpoint Protection. En determinados países, es posible que sea necesario obtener el consentimiento del personal individual antes de la intercepción y el registro. El Cliente debe instalar cualquier agente de Symantec Endpoint Protection.cloud con una personalización mínima y razonable. El Cliente acuerda que los dispositivos cubiertos por el servicio Symantec Endpoint Protection.cloud (i) registran información relacionada con el funcionamiento del servicio Hosted Endpoint Protection, (ii) que la información será transmitida a MessaLabs con el fin de proporcionar información de gestión e informar al Cliente y que (iii) el Cliente consiente tal registro y transmisión.

7. Configuración

7.1 Si el cliente adquirió el servicio a través de un distribuidor de Symantec, el cliente autoriza expresamente a dicho distribuidor de Symantec a (i) realizar cambios en la configuración del servicio con el objetivo de lograr una óptima funcionalidad del servicio y (ii) presentar tickets de asistencia en nombre del cliente.

Apéndice 18: Symantec MessageLabs Web v2 Smart Connect.cloud ("Smart Connect.cloud")

1. **Descripción general**

1.1. Una vez que se ha instalado el agente de usuario móvil y se han realizado los cambios de configuración pertinentes, las solicitudes de páginas web y archivos adjuntos se dirigen de manera electrónica al Servicio Symantec MessageLabs Web v2 URL.cloud ("Web v2 URL") y al Servicio Symantec MessageLabs Web v2 Protect.cloud ("Web v2 Protect") a través del agente de usuario y, a continuación, se examinan digitalmente.

2. **Descripción del servicio**

2.1. Cuando el usuario se conecta a Internet en los países "en servicio" designados, las solicitudes de HTTP y FTP por HTTP externas del cliente, incluyendo todos los archivos adjuntos, las macros o los programas ejecutables, son dirigidas a través de las ofertas de servicio de Web v2 URL y Web v2 Protect.

3. **Configuración**

3.1. La realización y el mantenimiento de los parámetros de configuración necesarios para dirigir este tráfico web externo al software de agente de usuario móvil, así como el tráfico de reenvío de salida a los servicios Web v2 URL y Web v2 Protect, son tareas del cliente y dependen de la infraestructura técnica de éste. El cliente debe instalar un archivo PAC en el equipo del usuario para que, en el momento de iniciarse el navegador, éste apunte hacia el agente móvil de Symantec. El cliente puede descargar un archivo PAC en ClientNet y modificarlo. El cliente debe asegurarse de que el tráfico interno HTTP/FTP por HTTP (por ejemplo, a la intranet corporativa) no se dirija al software de agente móvil.

3.2. El acceso a Web v2 URL y Web v2 Protect está restringido a sistemas autorizados que contienen una versión válida del software de agente móvil, así como a usuarios autorizados que se activan para estos servicios en ClientNet. El agente móvil del software y la información del usuario autorizado se utilizan para identificar al cliente y seleccionar dinámicamente la configuración específica del cliente.

3.3. Se aplicarán las mismas políticas para el servicio Web v2 URL y el mismo análisis de contenido para el servicio Web v2 Protect que cuando los usuarios utilizan el servicio de agente móvil, así como cuando se conecten a través de una ubicación de red configurada, es decir, la LAN corporativa.

3.4. El cliente reconoce que el agente móvil contará con la configuración predeterminada de Symantec aplicada desde el comienzo, la cual incluye el uso de maneras razonables para dirigir el tráfico web del usuario hacia un punto de acceso de infraestructura de servicio "óptimo". Este enrutamiento se basa en un conocimiento de la ubicación del usuario móvil de acuerdo con la dirección IP y el uso de una base de datos de ubicación geográfica de otro fabricante para identificar cuál es el país probable desde el cual se conecta el usuario. Symantec dirigirá los usuarios con la designación de país adecuada hacia lo que se considera el punto de acceso de servicio óptimo para el país especificado. Esto se llevará a cabo independientemente de cualquier evaluación de rendimiento probable para la conexión individual del usuario final y sólo para esos países en donde se considere que Symantec ha sido capaz de ofrecer un nivel de servicio aceptable.

Para cualquier otro país fuera de los países de servicio aceptable, el cliente reconoce que Symantec no estará en condiciones de proporcionar las capacidades de los servicios Web v2 URL o Web v2 Protect. En estas situaciones, en las que se determina que el usuario final se encuentra en un país "sin servicio", el agente móvil seguirá abierto, lo cual significa que el usuario final podrá conectarse a Internet sin disfrutar de los beneficios de las ofertas de servicio de Symantec, disponibles en los países de servicio aceptable.

EL CLIENTE RECONOCE Y ACEPTA QUE EL TRÁFICO WEB DEL USUARIO PUEDE DIRIGIRSE A INFRAESTRUCTURAS UBICADAS EN ZONAS GEOGRÁFICAS FUERA DE LA U.E. PARA SU PROCESAMIENTO CONFORME A ESTA CLÁUSULA 3.4. EL CLIENTE ES EL RESPONSABLE DE OBTENER TODOS LOS CONSENTIMIENTOS Y LAS APROBACIONES NECESARIAS PARA EFECTUAR LA TRANSFERENCIA DE DICHO TRÁFICO WEB. ASIMISMO, EL CLIENTE RECONOCE Y ACEPTA QUE SYMANTEC NO PUEDE ACEPTAR NINGUNA RESPONSABILIDAD POR EL INCUMPLIMIENTO CORRESPONDIENTE DE LA LEGISLACIÓN O LAS REGULACIONES APLICABLES.

4. **Términos de exportación adicionales para Smart Connect.cloud**

4.1 El cliente o partner no deberá llevar a cabo, ni permitir que un tercero lo haga, la venta, reventa, exportación, reexportación, transferencia, desviación, eliminación, divulgación ni otro tipo de tratamiento relacionado con la Tecnología Controlada, directa o indirectamente en cualquiera de los siguientes países: Afganistán, Angola, Armenia, Azerbaiyán, Bosnia y Herzegovina, Birmania, Burundi, China, Cuba, República Democrática del Congo, Eritrea, Etiopía, Irán, Irak, Corea del Norte, Liberia, Libia, Nigeria, Ruanda, Sierra Leona, Somalia, Sudán, Siria, Tanzania, Uganda y Zimbabue.

4.2 El cliente o partner no transferirá el agente móvil web a ningún otra empresa ni persona que no sea un empleado del cliente o partner, con las siguientes excepciones: (i) El cliente o partner puede transferir o habilitar la descarga del agente móvil web por parte de sus subcontratistas terceros para su uso en nombre del cliente o partner, y/o (ii) el cliente o partner puede transferir o habilitar la descarga del agente móvil web por parte de sus clientes finales terceros a quienes revende el servicio de Symantec, siempre que el cliente o partner hagan llegar a los terceros las obligaciones de esta Cláusula.

Apéndice 19: Symantec Backup Exec.cloud

1. Descripción general

1.1 Symantec Backup Exec.cloud es un servicio de recuperación y copias de seguridad online. Este servicio protege los datos críticos de los clientes transmitiéndolos automáticamente a centros de datos de Symantec. Los datos se cifran durante la transmisión y cuando están almacenados.

1.2 Para poder recibir el servicio Symantec Backup Exec.cloud, el cliente debe instalar un agente en los equipos correspondientes de los usuarios finales y asignar políticas adecuadas para utilizar el servicio. El portal de gestión ("Portal de gestión") de Symantec.cloud es un portal para administradores que se utiliza para gestionar equipos, políticas, alertas e informes.

1.3 Es posible que el cliente tenga que realizar algunos cambios básicos en el firewall para permitir que el agente se comunique y funcione con la infraestructura de Symantec.cloud.

1.4 Una vez que se haya configurado el servicio de acuerdo con las cláusulas 1.2 y 1.3, el Portal de gestión se empleará para gestionar los agentes.

1.5 Symantec publicará una lista de sistemas operativos compatibles para el uso y la instalación del agente, y navegadores compatibles para el uso del Portal de gestión. El cliente reconoce y acepta que Symantec puede actualizar y cambiar esta lista de forma regular sin aviso.

1.6 El agente instalado en el equipo correspondiente del usuario final debe realizar una copia de seguridad de los datos en los centros de datos de Symantec según los archivos y las carpetas que se han seleccionado mediante el Portal de gestión.

2. Portal de gestión

2.1. El Portal de gestión permite al cliente configurar el servicio Symantec Backup Exec.cloud según las políticas y los requisitos del cliente.

2.2. El cliente es responsable de la implementación de las opciones de configuración de acuerdo con la política de uso aceptable de equipos del cliente (o similar) mediante el Portal de gestión. Las políticas se configuran en el grupo de equipos.

2.3. Los cambios efectuados en la política se pueden ver de inmediato en el Portal de gestión y en la configuración del usuario final, y se organizan para ser trasladados a los agentes cuando los puntos finales están online y disponibles. La configuración efectiva de políticas de los agentes individuales puede consultarse en el Portal de gestión.

3. Registros e informes

3.1. Todos los registros e informes generados por el agente se almacenan en el Portal de gestión durante doce (12) meses, y pueden consultarse y descargarse desde allí. Una vez transcurrido ese período, los registros se eliminan.

4. Notificaciones

4.1. El cliente puede configurar el servicio Symantec Backup Exec.cloud para que envíe una notificación automática a los destinatarios de correo electrónico configurados según alertas predeterminadas, que pueden ser establecidas por el cliente en el Portal de gestión.

4.2. El cliente puede crear, eliminar y personalizar las notificaciones con el Portal de gestión.

5. Asistencia

5.1. La asistencia incluye:

5.1.1. Orientación telefónica sobre el Portal de gestión, incluyendo una descripción del servicio y una sesión de preguntas y respuestas. (Esto no incluye asistencia para establecer políticas ni análisis de la efectividad de las políticas).

5.1.2. Acceso a la guía del administrador y la guía del usuario; ambas pueden obtenerse en el Portal de gestión.

6. Términos adicionales

6.1. Todos los datos del cliente ("Datos del cliente") que Symantec o sus proveedores almacenen o archiven en virtud de este documento son propiedad exclusiva del cliente, y nada en el presente confiere a Symantec o a sus proveedores ningún derecho legal o equitativo, título o interés en relación con los datos del cliente.

6.2. El cliente es el único responsable de su conducta en relación con el servicio Symantec Backup Exec.cloud, incluido el control sobre el contenido de cualquier dato del cliente almacenado en el servicio Backup Exec.cloud. El cliente acepta específicamente que no usará el servicio Backup Exec.cloud:

6.2.1. en infracción de las leyes o regulaciones, incluidos, entre otros, la limitación, la carga, la transmisión, el almacenamiento o la copia de seguridad de alguna otra manera de cualquier contenido obsceno, indecente o pornográfico;

6.2.2. de manera alguna que infrinja los derechos de propiedad intelectual de terceros; o

6.2.3. para transmitir materiales que contengan virus u otros archivos o códigos informáticos dañinos, como troyanos, gusanos o bombas de tiempo.

6.3. El cliente puede cargar o almacenar los Datos del cliente, o realizar copias de seguridad de alguna otra manera de ellos, hasta la cantidad total de almacenamiento o cuota asignada ("Almacenamiento máximo") que el cliente ha comprado a Symantec. En caso de que el cliente se exceda del Almacenamiento máximo, Symantec se reserva el derecho a restringir la capacidad del cliente de realizar copias de seguridad de los datos hasta que el cliente reduzca el uso del almacenamiento o se suscriba a un plan de almacenamiento con cuotas superiores.

6.4. El cliente puede acceder a los Datos del cliente durante el plazo de vigencia. Al vencer o finalizar el plazo de vigencia, el cliente ya no podrá acceder a los Datos del cliente. No obstante, Symantec seguirá almacenando y manteniendo los Datos del cliente ("Datos almacenados") durante un período de sesenta (60) días a partir de la fecha de vencimiento o finalización del plazo de vigencia ("Período de retención posterior a la finalización"). Durante el Período de retención posterior a la finalización, el cliente podrá elegir renovar el plazo de vigencia y pagar los costes correspondientes, que le permitirán acceder a los Datos almacenados nuevamente. Al vencer el Período de retención posterior a la finalización, Symantec eliminará los Datos del cliente, y ni el cliente ni Symantec podrán acceder a ellos en caso de que el cliente no renueve el servicio.

6.5. **EL CLIENTE RECONOCE Y ACEPTA QUE EL SERVICIO, EN PARTE O EN SU TOTALIDAD, PUEDE REALIZARSE EN LOS ESTADOS UNIDOS DE AMÉRICA Y/O EN OTRAS JURISDICCIONES DONDE SYMANTEC ESTÁ PRESENTE. EL CLIENTE ES RESPONSABLE DE OBTENER TODOS LOS CONSENTIMIENTOS Y LAS APROBACIONES NECESARIOS (SI HAY) PARA EFECTUAR LA TRANSFERENCIA DE DATOS DEL CLIENTE FUERA DE LOS ESTADOS UNIDOS, LA UNIÓN EUROPEA Y/U OTROS PAÍSES. ASIMISMO, EL CLIENTE RECONOCE Y ACEPTA QUE SYMANTEC NO SERÁ RESPONSABLE ANTE EL CLIENTE POR EL INCUMPLIMIENTO DE NINGUNA LEGISLACIÓN O REGULACIÓN APLICABLE EN RELACIÓN CON TAL TRANSFERENCIA DE DATOS.**

Anexo 3
Contrato de Nivel de Servicio

1. Definiciones

1.1. Los siguientes términos tendrán los siguientes significados para los fines del presente Contrato de Nivel de Servicio:
«**Solicitud de Reembolso**» se refiere a la notificación que el Cliente debe enviar a Symantec por correo electrónico a support.cloud@symantec.com con el asunto «Credit Request» (Solicitud de Reembolso) (a menos que Symantec notifique lo contrario);
«**Clúster de Torres Designadas**» se refiere a dos (2) o más Torres, distribuidas en un mínimo de dos (2) ubicaciones, designadas para suministrar el Servicio al Cliente;
«Falso Positivo de Virus en Correo Electrónico» se refiere a un Correo Electrónico válido que se ha marcado/capturado de forma incorrecta como un correo que contiene un Virus;
«**Servicios de Correo Electrónico**» se refiere a los Servicios de Email AV, Email AS, Email IC, Email CC, Cifrado basado en normas propias (Policy Based Encryption) y a los Servicios de Cifrado de Límites (Boundary Encryption);
«Virus Conocidos» se refiere a un Virus para el que, en el momento de recepción de su contenido por parte de Symantec: (i) ya existe una firma disponible públicamente para un mínimo de una (1) hora para la configuración por parte un escáner comercial de un tercero y utilizado por Symantec; o (ii) se incluye en la lista «Wild List» que se encuentra en http://www.wildlist.org y está identificado como «In the wild» o activos por un mínimo de dos participantes de la lista *Wild List*.
«Rastreador de Symantec» es una herramienta de Symantec a través de la que se mide la Disponibilidad del Servicio y la Latencia;
«**Factura Mensual**» se refiere a la factura mensual por los Servicios, tal y como se estipula en el Contrato;
«**Nivel de Servicio**» se refiere a los parámetros del Servicio definidos en el presente Contrato de Nivel de Servicio;
«Falso Negativo de Spam» se refiere a un correo electrónico Spam que no se ha identificado como Spam;
«Falso Positivo de Spam» se refiere a un Correo Electrónico válido marcado/capturado de forma incorrecta como Spam;
«Configuración Recomendada para el Spam» se refiere a las directrices de configuración de buenas prácticas de Symantec para Email AS;
«Torre» se refiere a un número de servidores de carga equilibrada;
«Servicios Web» se refiere a los Servicios Web v2 Protect y Web v2 URL en conjunto.

2. Aspectos Generales

2.1. En caso de que el Cliente crea que tiene derecho a algún tipo de reparación de conformidad con este Contrato de Nivel de Servicio, el Cliente deberá enviar una Solicitud de Reembolso en un plazo de diez (10) días laborables tras finalizar el mes natural en cuestión. El Cliente reconoce que los registros únicamente se mantienen un número limitado de días y, por tanto, cualquier Solicitud de Reembolso enviada fuera del plazo estipulado se considerará nula.
2.2. Todas las Solicitudes de Reembolso deberán ser verificadas por Symantec de conformidad con las disposiciones aplicables del presente Contrato de Nivel de Servicio.
2.3. El presente Contrato de Nivel de Servicio no operará: (i) durante los periodos de Mantenimiento Previsto o mantenimiento de emergencia, periodos de no-disponibilidad debidos a causas de fuerza mayor o actos u omisiones tanto del Cliente como de un tercero; (ii) durante todo periodo de suspensión del Servicio por parte de Symantec de conformidad con el Contrato; (iii) en caso de que el Cliente esté incumpliendo el Contrato (incluidos, entre otros, si el cliente tiene facturas vencidas); (iv) respecto a los correos electrónicos que no hayan pasado por el Servicio (incluyendo si el cliente no ha bloqueado su router para dirigir el tráfico de correo electrónico a Symantec); ni (v) en relación con los correos electrónicos entrantes o salientes enviados inicialmente a Symantec con más de 500 destinatarios por cada sesión de SMTP.
2.4. Las reparaciones establecidas en el presente Contrato de Nivel de Servicio serán reparaciones exclusivas y propias del Cliente, ya se expresen mediante contrato, extracontractualmente (entre lo que se incluye la negligencia) o de cualquier otra forma respecto de los niveles del Servicio.
2.5. La responsabilidad máxima acumulable de Symantec en virtud del presente Contrato de Nivel de Servicio en cualquier mes natural no será superior al cien por cien (100%) de la Factura Mensual pagadera por parte del Cliente por el Servicio afectado.
2.6 En el supuesto de que el Servicio afectado forme parte de una Paquete de Servicios Indisociable:
a) a los efectos de calcular los créditos de servicio, la Factura Mensual del Servicio afectado se calculará tomando la cuota total pagadera por la Paquete de Servicios Indisociable y dividiéndola por el número de Servicios constituyentes que abarca esa paquete; y
b) si el Cliente rescinde el Servicio afectado con arreglo a este Contrato de Nivel de Servicio, la nueva cuota pagadera por el Paquete de Servicios Indisociable será calculada tomando el total de la Factura Mensual originaria pagadera por la Paquete de Servicios Indisociable, dividida por el número de Servicios constituyentes originario que comprendía la paquete, y multiplicando el resultado por el número de Servicios constituyentes restantes que comprende dicha paquete.
2.7 Los Niveles de Servicio para Servicios de Correo Electrónico no son de aplicación al Servicio EC. En consecuencia, los Niveles de Servicio para Servicios de Correo Electrónico contemplados en las cláusulas 3 a 5 inclusive abajo se verán suspendidos durante cualquier periodo en el que el Servicio EC esté en estado activo.

3. Disponibilidad del Servicio 100%

3.1 Este Nivel de Servicio de Disponibilidad del Servicio operará únicamente si el Cliente utiliza uno o más Servicios Web o Servicios de Correo Electrónico.
3.2 En relación con los Servicios de Correo Electrónico, el nivel de disponibilidad se refiere a la capacidad para iniciar una sesión de SMTP en el puerto 25 del Clúster de Torres Designadas determinada por el Rastreador de Symantec. Este Nivel de Servicio será de aplicación únicamente si el Clúster de Torres Designadas es capaz de:
3.2.1 recibir el Correo Electrónico entrante del Cliente desde registros MX correctamente configurados en nombre del dominio del Cliente durante las 24 horas, los 7 días; y
3.2.2 aceptar el Correo Electrónico saliente del Cliente desde un *host* SMTP del Cliente correctamente configurado en nombre del dominio (o los dominios) del Cliente durante las 24 horas y los 7 días.
3.3 En relación con los Servicios Web, el nivel de disponibilidad se refiere a la capacidad de los Servicios Web de aceptar los pedidos de salida al web del Cliente y solamente serán de aplicación si los dispositivos de hospedaje y de portal del Cliente o sus proxys están configurados correctamente para funcionar 24x7.
3.4 Si en cualquier mes natural la Disponibilidad del Servicio Web o de Correo Electrónico es inferior al cien por cien (100%), el Cliente puede tener derecho al siguiente porcentaje de reembolso:

Porcentaje sobre la Disponibilidad del Servicio por mes natural	Porcentaje del reembolso de la Factura Mensual
<100% pero >=99,0%	25
<99,0% pero >=98,0%	50
<98,0%	100 y cancelación del Servicio afectado según criterio del Cliente

3.5 En caso de que la Disponibilidad del Servicio Web o de Correo Electrónico caiga por debajo del noventa y ocho por ciento (98%) en cualquier mes natural, el Cliente estará autorizado a cancelar el Servicio afectado y a recibir un reembolso prorrateado de las facturas pagadas con antelación y que pertenezcan al Servicio afectado durante el periodo posterior a la cancelación.

4. Entrega del Correo Electrónico al 100%

4.1 El presente Nivel de Servicio de Entrega de Correo Electrónico operará únicamente si el Cliente utiliza uno o más Servicios de Correo Electrónico
4.2 Symantec entregará el 100% de todo el Correo Electrónico enviado a o desde el Cliente sujeto a lo siguiente:
4.2.1 el Correo Electrónico deberá haberlo recibido el Clúster de Torres Designadas; y

4.2.2 el Correo Electrónico no debe tener Virus, Spam u otros contenidos que pueden provocar el bloqueo de los Servicios de Correo Electrónico.
4.3 Sujeto a las Cláusulas 4.1 y 4.2 anteriores, en caso de que Symantec incumpla la entrega de un Correo Electrónico para o desde el Cliente y el Cliente no esté incumpliendo los términos del Contrato, el Cliente estará autorizado a rescindir el Servicio de Email en un plazo de treinta (30) días previa notificación por escrito.

5. Latencia del Correo Electrónico – 60 Segundos

5.1. Previo cumplimiento de lo dispuesto a tenor de la cláusula 5.2, el presente Nivel de Servicio de Latencia de Correo Electrónico operará únicamente en caso de que el Cliente utilice uno o más Servicios de Correo Electrónico.
5.2. Este Nivel de Servicio de Latencia de Correo Electrónico **no** será de aplicación al Servicio Policy Based Encryption.
5.3. En el supuesto de que en un mes natural cualquiera la media del tiempo que tarda un Correo Electrónico enviado cada 5 minutos (determinado por el Rastreador de Symantec) en ir y volver a la Torre de Emails dentro del Clúster de Torres Designadas del Cliente es superior a los tiempos indicados en la tabla que aparece al pie, el Cliente tendrá derecho a solicitar el descuento que recoge dicha tabla:

Tiempo medio de traslado del 100% (en minutos y segundos)	Porcentaje de reembolso de la Factura Mensual
> 1 min pero <= 1min 30 seg	25
> 1min 30 seg pero <= 2 min	50
> 2 min pero <= 2mins 30 seg	75
> 2 min 30 seg	100

5.4. Este Nivel de Servicio de Latencia no operará:
5.4.1. Si el usuario no ha proporcionado a Symantec una lista concreta de direcciones de correo electrónico para recibir el Servicio (la "Lista de Validación") y es víctima de un ataque de denegación de servicio;
5.4.2. En los retrasos provocados por un bucle de corro desde o para los sistemas del Cliente.

6. Latencia Web – 0,1 Segundos

6.1 El presente Nivel de Servicios de Latencia Web operará únicamente en caso de que el Cliente utilice uno o más Servicios Web.
6.2. En el supuesto que la media del tiempo de escaneo del contenido de web, desde el instante de su recibo por Symantec hasta el instante del intento de transmisión de dicho contenido, calculado a lo largo de un mes natural sea inferior al 100% de lo indicado en la tabla al pie, el Cliente podrá enviar una Solicitud de Reembolso:

Porcentaje medio del análisis del contenido Web en 100 milisegundos	Porcentaje de reembolso de la Factura Mensual
< 100% pero >= 99%	25
< 99% pero >= 98%	50
< 98% pero >= 97%	75
< 97%	100 y cancelación del Servicio afectado según criterio del Cliente

6.3 El presente Nivel de Servicio de Latencia Web se aplicará únicamente a los objetos de 1MB o menos.

7. Spam – Falsos Positivos 0,0003%

7.1. El presente Nivel de Servicio de Falsos Positivos de Spam se aplicará únicamente si el Cliente utiliza el Servicio Antispam para Correo Electrónico y aplica las Configuraciones Recomendadas por Symantec para Spam.
7.2. Cuando el índice de capturas de Falsos Positivos supera el 0,0003% de todo el tráfico de correo electrónico del Cliente en cualquier mes natural, el Cliente tiene derecho a recibir un reembolso de conformidad con la tabla siguiente:

Porcentaje del índice de captura de Falsos Positivos durante el mes natural	Porcentaje del reembolso de la Factura Mensual
>0,0003 pero <= 0,003	25
>0,003 pero <= 0,03	50
>0,03 pero <= 0,3	75
>0,3	100

7.3. Los siguientes Correos Electrónicos no constituirán Correos Electrónicos Falsos Positivos para los fines del presente Nivel de Servicio:
7.3.1. Los Correos Electrónicos que no constituyen Correo Electrónico propiamente empresarial;
7.3.2. Los Correos Electrónicos que contengan más de 20 destinatarios;
7.3.3. Cuando el remitente del Correo Electrónico esté en la lista de remitentes bloqueados del Cliente, entre los que se incluyen aquellos definidos por el Usuario individual si el Cliente ha activado las configuraciones para el Usuario;
7.3.4. Los Correos Electrónicos que se envíen desde un aparato en peligro;
7.3.5. Los Correos Electrónicos que se envíen desde un aparato que figure la lista de bloqueo de un tercero;
7.3.6. Los Correos Electrónicos que se envíen a más de 20 destinatarios (en una única operación o en una serie de operaciones) y tengan al menos el 80% de los mismos en el contenido.

8. Índice de capturas de Spam del 99%

8.1. Este Nivel de Servicio de Capturas de Spam únicamente operará si el Cliente utiliza el Servicio Antispam para Correo Electrónico y aplica las Configuraciones Recomendadas por Symantec para Spam. Las disposiciones de la presente Cláusula 8 corresponden al número de Falsos Negativos de Spam medidos en un mes.
8.2. El Cliente puede tener derecho a un reembolso en virtud de la tabla siguiente:

Porcentaje de Capturas de Spam durante un mes natural	Porcentaje de reembolso de la Factura Mensual
>98% - <= 99%	25
> 97% - <= 98%	50
> 96% - <= 97%	75
< 96%	100

8.3. Este Nivel de Servicio de Captura de Spam no operará cuando el Correo Electrónico no se haya enviado a una dirección autorizada.
8.4 Un índice de Captura de Spam inferior al 95% se aplicará a los Correos Electrónicos que contengan configuraciones de caracteres asiáticos. En caso de que dicho índice de Captura de Spam sea inferior al 95% el Cliente estará autorizado a recibir un reembolso del 25% de la Factura Mensual. En caso de que el índice de Captura de Spam sea inferior al 90% el Cliente estará autorizado a recibir un reembolso del 100% de la Factura Mensual.

9. Solicitudes de Reembolso del Servicio Spam

9.1. Para poder ser susceptible de reembolso de conformidad con las Cláusulas 7 y 8, el Cliente deberá enviar los Correos Electrónicos sospechosos de ser Falsos Positivos de Spam o Falsos Negativos de Spam a **support.cloud@symantec.com** en un plazo de 5 días desde su recepción. Symantec investigará y confirmará si el Correo Electrónico es o no un Falso Positivo de Spam o Falso Negativo de Spam y registrará su conclusión. Al final del mes natural correspondiente, si el Cliente considera que el número de Falsos Positivos de Spam o Falsos Negativos de Spam confirmados le da derecho a reembolso de conformidad con la tabla anterior, el Cliente deberá enviar una Solicitud de Reembolso a Symantec en virtud de la Cláusula 2.1.

10. Protección frente a los Virus de Correo Electrónico – 100%

10.1. Este Nivel de Servicio de Protección de Virus en el Correo Electrónico operará únicamente si el Cliente utiliza el Servicio Antivirus para Correo Electrónico.
10.2. En caso de que los sistemas del Cliente resulten infectados por uno o más Virus en un mes natural durante el Periodo Mínimo y se notifique a Symantec mediante una llamada de ayuda validada y registrada que confirme que un Virus ha pasado al Cliente a través del Servicio Email AV, el Cliente podrá facturar a Symantec por los daños y perjuicios incurridos en un importe igual al 100% de la Factura Mensual existente en ese momento o por diez mil euros (10.000€), eligiendo la menor de las cantidades. La reparación establecida en la presente Cláusula 10.2 se efectuará como reparación única y exclusiva por contrato, extracontractualmente (entre la que se incluye la negligencia) o de cualquier otra forma respecto de toda infección por un Virus que haya pasado al Cliente o a un tercero a través el Servicio. Para evitar toda duda, la reparación establecida en esta Cláusula 10.2 no se aplicará en casos de autoinfección deliberada.
10.3. Los sistemas del Cliente se considerarán infectados si un Virus contenido en un Correo Electrónico recibido mediante el Servicio Email AV se ha activado en los sistemas del Cliente ya sea de manera automática o mediante intervención manual.
10.4. En caso de que Symantec detecte pero no detenga un Correo Electrónico infectado con un Virus, Symantec notificará esta situación al Cliente de inmediato facilitándole la información suficiente para que el Cliente pueda identificar y eliminar el Correo

Electrónico infectado con Virus. Si esta notificación tiene como resultado evitar la infección, no se aplicará la reparación establecida en la Cláusula 10.2 anterior. Si el Cliente no actúa de inmediato tras la recepción de dicha información se invalidará el Nivel del Servicio mencionado en la Cláusula 10.2 anterior.

10.5. El Servicio Email AV analizará lo más exhaustivamente posible el Correo Electrónico y sus adjuntos. Quizás no sea posible analizar adjuntos cuyo contenido esté directamente bajo el control del remitente (por ejemplo adjuntos protegidos por contraseñas y/o cifrados). Dichos Correos Electrónicos y/o adjuntos quedarán excluidos del Nivel del Servicio de la Cláusula 10.2 anterior.

10.6. Este Nivel de Servicio de Protección frente a Virus por Correo Electrónico no operará respecto de los virus que hayan sido liberados de forma intencionada por el Cliente.

11. Falsos Positivos de Virus por Correo Electrónico 0,0001%

11.1 El presente Nivel de Servicio de Falsos Positivos de Virus por Correo Electrónico operará únicamente cuando el Cliente utilice el Servicio Antivirus para Correo Electrónico.

11.2. Cuando el índice de capturas de Falsos Positivos supera el 0,0001% de todo el tráfico de correo electrónico del Cliente en cualquier mes natural, el Cliente tiene derecho a recibir un reembolso de conformidad con la tabla siguiente:

Porcentaje del índice de captura de Falsos Positivos durante el mes natural	Porcentaje del reembolso de la Factura Mensual
>0,0001 pero <= 0,001	25
> 0,001 pero <= 0,01	50
>0,01 pero <= 0,1	75
>0,1	100

12. Protección frente a los Virus Conocidos de la Web – 100%

12.1 Este Nivel de Servicio de Protección de Virus de la Web operará únicamente si el Cliente utiliza el Servicio Web v2 Protect.

12.2. En caso de que los sistemas del Cliente resulten infectados por uno o más Virus Conocidos en un mes natural y se notifique a Symantec mediante una llamada de ayuda validada y registrada que facilite los detalles de la URL desde la que se ha descargado el elemento y que confirme que un Virus Conocido ha pasado al Cliente a través del Servicio Web v2 Protect, el Cliente podrá facturar a Symantec por los daños y perjuicios incurridos en un importe igual al 100% de la Factura Mensual existente en ese momento o por diez mil euros (10.000€), eligiendo la menor de las cantidades. La reparación establecida en la presente Cláusula 12.2 se efectuará como reparación única y exclusiva por contrato, extracontractualmente (entre la que se incluye la negligencia) o de cualquier otra forma respecto de toda infección por un Virus Conocido que haya pasado al Cliente o a un tercero a través el Servicio Web v2 Protect. Para evitar toda duda, la reparación establecida en esta Cláusula 12.2 no se aplicará en casos de autoinfección deliberada o de descarga deliberada de un código malicioso por parte del Cliente.

12.3 Los sistemas del Cliente se considerarán infectados si un Virus Conocido contenido en una transacción Web recibida mediante el Servicio Web v2 Protect se activa en los sistemas del Cliente ya sea de manera automática o mediante intervención manual.

12.4 En caso de que Symantec detecte pero no detenga un Virus Conocido en una transacción Web recibida mediante el Servicio Web v2 Protect, Symantec notificará esta situación al Cliente de inmediato facilitándole la información suficiente para que el Cliente pueda identificar y eliminar el elemento pertinente. Si esta notificación tiene como resultado evitar la infección, no se aplicará la reparación establecida en la Cláusula 12.2 anterior. Si el Cliente no actúa de inmediato tras la recepción de dicha información se invalidará el Nivel del Servicio mencionado en la Cláusula 12.2 anterior.

12.5. El Servicio Web v2 Protect analizará lo máximo posible el elemento descargado de la Web. Puede que no sea posible analizar elementos que estén encapsulados o tunelados para fines de comunicación mediante los protocolos para Web (HTTP, y FTP sobre HTTP), transportado sobre HTTPS, comprimidos o modificados respecto de su forma original para su distribución, protección de licencia de producto, descarga o actualización o contenido que esté bajo el control directo del remitente (por ejemplo, elementos protegidos por contraseña y/o cifrados). Dichos elementos y/o archivos adjuntos no se incluirán en el Nivel de Servicio de la Cláusula 12.2.

13. Servicio Técnico 24 x 7 y Respuesta Fallida

13.1 Symantec, durante las veinticuatro (24) horas del día, los siete (7) días de la semana:

a) facilitará un servicio técnico al Cliente para los problemas que surjan con el Servicio; y

b) interactuará con el Cliente para resolver dichos problemas.

13.2 Cuando un Cliente informe de un problema, fallo o solicite información sobre el Servicio a través del teléfono o del correo electrónico a Symantec, su nivel de prioridad dependerá de y se responderá de la manera establecida en la siguiente tabla:

Nivel de Prioridad	Definición	Objetivo de las respuestas
Crítica	Pérdida del Servicio	95% de las llamadas respondidas en 2 horas
Alta	Pérdida parcial del Servicio o Servicio con problemas	85% de las llamadas respondidas en 4 horas
Baja	Posible problema en el Servicio o solicitud de información que no afecta al Servicio	75% de las llamadas respondidas en 8 horas

13.3 Los fallos que deriven de las acciones del Cliente o que requieran las medidas de los otros proveedores de servicio están fuera del control de Symantec y, como tales, están excluidos específicamente de los tiempos de respuesta de fallos de la Cláusula 13.2 anterior.

13.4 Siempre sujeto a la Cláusula 13.3, si el Cliente considera que está sufriendo un retraso en la respuesta de Symantec a una pregunta que exceda los parámetros definidos en la Cláusula 13.2 anterior, puede tener derecho a reembolso. Las Solicitudes de Reembolso deberán detallar la hora, fecha y número de registro del incidente. Si se aprueba, el Cliente recibirá un reembolso de conformidad con la siguiente tabla:

Prioridad	Retraso en la respuesta	Porcentaje del reembolso sobre la Factura Mensual
Crítica	Más de una vez en un mes natural	15
Alta	Más de dos veces en un mes natural	10
Baja	Más de tres veces en un mes natural	5

14. Servicio de Archivado (P)

Las disposiciones de esta Cláusula 14 se aplicarán únicamente al Servicio de Archivado (P).

14.1 Disponibilidad del Servicio de Archivado (P)

14.1.1El Servicio de Archivado (P) estará Disponible un 99,9% de cada mes natural, a excepción de las ventanas de Mantenimiento Previsto y mantenimiento de emergencia. En este caso, "Disponible" quiere decir que la infraestructura de hospedaje de Symantec está lista para recibir y archivar Correo Electrónico. Para los fines del cálculo de la no disponibilidad se aplicarán los siguientes criterios: a) la medición será efectuada por los sistemas de control de Symantec (dicha medida puede ser proporcionada al Cliente previa solicitud escrita), b) el control tendrá lugar en intervalos de 5 minutos con dos fallos requeridos para considerarlo como una interrupción, c) únicamente se medirá la infraestructura de Symantec, y dichas mediciones no incluirán las no disponibilidades resultantes de la interrupción del Dispositivo de Archivado, de la interrupción de la red del Cliente o de una interrupción de Internet.

14.1.2 Por cada uno (1) por ciento entero o fracción de no disponibilidad inferior al objetivo de 99,9% de disponibilidad con arreglo a la presente cláusula 14.1 en el mes natural en cuestión, el Cliente tendrá derecho a solicitar un reembolso equivalente al diez por ciento (10%) de la facturación mensual efectuada por Symantec respecto del Servicio de Archivado (P), sujeto a un máximo del 100% de la facturación mensual respecto del Servicio de Archivado (P) en cualquier mes natural. El Cliente podrá cancelar el Servicio de Archivado (P) bajo su propio criterio si en algún momento esta disponibilidad cae por debajo del noventa por ciento (90%) en un mes natural.

14.2 Nivel del Servicio del Dispositivo de Archivado

14.2.1 Si un Dispositivo de Archivado falla durante el periodo de garantía por razones cubiertas por la Garantía Limitada de Symantec (tal y como se define en la documentación recibida con el Dispositivo de Archivado), Symantec, sin que esto suponga ningún coste para el Cliente, trabajará con el Cliente para solucionar el problema del Dispositivo de Archivado (que puede requerir acceso

de una VPN (Virtual Private Network o red privada virtual) al Dispositivo de Archivado) en un plazo de cuatro (4) horas tras la recepción de la notificación del problema por parte del Cliente durante el horario laboral habitual, y en un plazo de ocho (8) horas tras la recepción de la notificación del problema por parte del Cliente fuera del horario laboral habitual. En un plazo de veinte (20) horas laborables habituales tras recibir notificación del problema, Symantec:

14.2.1.1 notificará al Cliente que el Dispositivo de Archivado está funcionando correctamente y que el problema no está originado por el Dispositivo de Archivado o el Programa; o

14.2.1.2 reparará el Dispositivo de Archivado mediante el uso de aparatos y/o programas; o

14.2.1.3 notificar al Cliente que es necesario sustituir el Dispositivo de Archivado, o

14.2.1.4 si Symantec es incapaz de reparar o sustituir el Dispositivo de Archivado, devolverá el importe mensual del Servicio de Archivado (P) del Periodo actual y cancelará el Servicio de Archivado (P).

14.2.2 En la eventualidad de que Symantec se vea obligado, con arreglo a lo dispuesto en la Cláusula anterior 14.2.1.3, a reemplazar el Dispositivo de Archivado del Cliente, lo cumplirá dentro de un plazo de cuarenta y ocho (48) horas laborables desde que Symantec notifique al Cliente que el nuevo Dispositivo de Archivado es necesario.

14.2.3 Si Symantec está obligado de conformidad con las Cláusulas 14.2.1.2 y 14.2.1.3 anteriores a reparar o sustituir el Dispositivo de Archivado o el Programa de Archivado y no cumple con dicha obligación en el plazo establecido en las Cláusulas 14.2.1 y 14.2.2 anteriores, Symantec devolverá al Cliente el cinco por ciento (5%) de la factura mensual por el Servicio de Archivado (P) de cada día que se retrase una vez transcurrido dicho plazo.

14.2.4 Los términos anteriores se consideran reparaciones únicas y exclusivas del Cliente respecto de todo defecto o incumplimiento de la garantía en relación con el Dispositivo de Archivado.

15. Servicio EC

15.1 Las estipulaciones a tenor de esta cláusula 15 serán de aplicación al servicio EC solamente.

15.1.1 EC estará Disponible un 99,9% de cada mes natural, a excepción de las ventanas de Mantenimiento Previsto y mantenimiento de emergencia. A estos efectos, "Disponible" quiere decir que la infraestructura de hospedaje de Symantec está lista para sincronizar el sistema clave y la información de Usuario. A los efectos de calcular el tiempo de no disponibilidad, serán de aplicación los siguientes criterios: a) la determinación de ese tiempo la llevarán a cabo los sistemas de seguimiento de Symantec (dicha medida puede ser proporcionada al Cliente previa solicitud escrita), b) solamente las infraestructuras hospedadas por Symantec serán determinadas y en dicha determinación no se tomará en cuenta la no disponibilidad a consecuencia de que la red del Cliente o de terceros esté fuera de servicio, o por motivos relativos al nombre del dominio ajenos a la voluntad de Symantec.

15.1.2 Por cada uno (1) por ciento entero o fracción de no disponibilidad inferior al objetivo de 99,9% de disponibilidad con arreglo a la presente cláusula 15.1 en el mes natural en cuestión, el Cliente tendrá derecho a un abono a su cuenta equivalente al diez por ciento (10%) de la Factura Mensual pagadera a Symantec en concepto del Servicio EC, sujeto a un abono máximo del 100% de la Factura Mensual pagadera por el Servicio EC en un mes natural dado. El Cliente tendrá derecho a rescindir su suscripción al Servicio EC a su libre albedrío en la eventualidad de que la disponibilidad del Servicio EC se sitúe por debajo del noventa por ciento (90%) en un mes natural dado.

16. Symantec Email Continuity Archive.cloud o Symantec Email Continuity Archive Lite.cloud

16.1 Las disposiciones de la presente cláusula 16 serán de aplicación al Servicio de Symantec Email Continuity Archive.cloud y al Servicio de Symantec Email Continuity Archive Lite.cloud únicamente.

16.1.1 Los Servicios de Symantec Email Continuity Archive.cloud y al Servicio de Symantec Email Continuity Archive Lite.cloud estarán disponibles un 99,95% de cada mes natural. La disponibilidad se calculará dividiendo el número total de horas que el Servicio de Symantec Email Continuity Archive.cloud y al Servicio de Symantec Email Continuity Archive Lite.cloud (según proceda) no estaba disponible (descontando el tiempo en el que la red del Cliente haya estado parada, periodos de mantenimiento, y no disponibilidad por problemas tipo DNS ajenos a la voluntad de Symantec) por el número previsto de horas de disponibilidad del Servicio de Symantec Email Continuity Archive.cloud y del Servicio de Symantec Email Continuity Archive Lite.cloud (según proceda) en el mes natural en cuestión.

16.1.2 Por cada uno (1) por ciento de disponibilidad inferior al objetivo del 99,95% conforme a la presente cláusula 16 en el mes natural en cuestión, el Cliente tendrá derecho a una nota de crédito equivalente a las cuotas pagadas a Symantec en relación con el Servicio de Symantec Email Continuity Archive.cloud y al Servicio de Symantec Email Continuity Archive Lite.cloud (según proceda) por un día del Servicio de Symantec Email Continuity Archive.cloud y al Servicio de Symantec Email Continuity Archive Lite.cloud.

17. Symantec EV.cloud

17.1 Symantec ofrecerá el 99,99% de disponibilidad del servidor para Symantec EV.cloud. Si la disponibilidad del servidor de un mes natural completo es de menos del 99,99%, Symantec emitirá un crédito al cliente según se detalla a continuación:

Disponibilidad del servidor	Porcentaje de crédito del cargo mensual
De 99,9% a 99,98%	5% del cargo mensual
De 98,0% a 99,8%	10% del cargo mensual
De 95,0% a 97,9%	15% del cargo mensual
De 90,0% a 94,9%	25% del cargo mensual
89,9% o menos	2,5% del cargo mensual por cada 1% de disponibilidad perdida, hasta un máximo de 100% del cargo mensual

17.2 Las Solicitudes de crédito deben incluir las fechas y las horas de indisponibilidad del servidor. Symantec comparará la información de no disponibilidad del servidor que el cliente proporcione con sus propios datos de supervisión de disponibilidad. Se emitirá un crédito si la no disponibilidad del servidor da origen a un crédito según la tabla de la Cláusula 17.1, antes mencionada. El crédito descrito en esta Cláusula será el único y exclusivo derecho del cliente en relación con la no disponibilidad del servidor. La no disponibilidad del servidor con fines de mantenimiento está excluida de los cálculos de disponibilidad del servidor.

18. Symantec Endpoint Protection.cloud

18.1 Las disposiciones de esta Cláusula 18 se aplicarán solamente al servicio Symantec Endpoint Protection.cloud.

18.1.1 Symantec Endpoint Protection.cloud estará 100% disponible cada mes natural, a excepción del mantenimiento planificado y mantenimiento de emergencia. En dicho caso, el término "disponible" significa que la infraestructura gestionada de Symantec está lista para sincronizar información de políticas. Con el fin de calcular los periodos en que el servicio no estará disponible, se aplicarán los siguientes criterios: a) los sistemas de control de Symantec llevarán a cabo las mediciones (si el cliente lo solicita por escrito, estas mediciones pueden proporcionársele), b) sólo se medirá la infraestructura gestionada de Symantec y dichas mediciones excluyen el periodo en que el servicio no estuvo disponible como consecuencia de interrupciones en la red del cliente, interrupciones de terceros o problemas con el DNS fuera del control directo de Symantec.

18.1.2 Por cada un (1) por ciento o parte del periodo en que el servicio no estuvo disponible más allá del objetivo de disponibilidad del 99,9% en virtud de esta Cláusula 18.1 en el mes natural en cuestión, el cliente tendrá derecho a recibir un equivalente en crédito al diez por ciento (10%) de los cargos mensuales debidos a Symantec en relación con el servicio Symantec Endpoint Protection.cloud Service, sujeto a un máximo del 100% de los cargos mensuales debidos en relación con el servicio Symantec Endpoint Protection.cloud Service en cualquier mes natural. El cliente puede finalizar este servicio de Symantec Endpoint Protection.cloud Service a su entera discreción si en cualquier momento esta disponibilidad disminuye a un noventa por ciento (90%) en cualquier mes natural.

18.1.3 El crédito descrito en la Cláusula 18.1.2 será el único y exclusivo derecho del cliente en relación con la no disponibilidad del servidor para el servicio Symantec Endpoint Protection.cloud. Los niveles de servicio en las Secciones 3.1, 3.4 y 11.1 del presente contrato de nivel de servicio no se aplicarán a los servicios Symantec Endpoint Protection.cloud.

19. Symantec Backup Exec.cloud

19.1. Las disposiciones de esta cláusula 19 se aplicarán solamente al servicio Symantec Backup Exec.cloud.

19.2. Symantec Backup Exec.cloud estará totalmente disponible cada mes natural, a excepción del período de mantenimiento planificado y mantenimiento de emergencia. En dicho caso, el término "disponible" significa que la infraestructura alojada de Symantec está lista para sincronizar información de políticas. Con el fin de calcular los períodos en que el servicio no estará disponible, se aplicarán los siguientes criterios: a) los sistemas de supervisión de Symantec llevarán a cabo las mediciones (si el cliente lo solicita por escrito, estas mediciones pueden proporcionársele); b) solo se medirá la infraestructura alojada de Symantec, y dicha medición excluirá el período en que el servicio no estuvo disponible como consecuencia de interrupciones en la red del cliente, interrupciones de terceros o problemas con el DNS fuera del control directo de Symantec.

19.3. Por cada uno por ciento (1%) o parte del período en que el servicio no estuvo disponible más allá del objetivo de disponibilidad en virtud de la cláusula 19.2 en el mes natural en cuestión, el cliente tendrá derecho a recibir un equivalente en crédito al diez por ciento (10%) de los cargos mensuales debidos a Symantec en relación con el servicio Symantec Backup Exec.cloud, sujeto a un máximo del cien por cien (100%) de los cargos mensuales debidos en relación con el servicio Symantec Backup Exec.cloud en cualquier mes calendario. El cliente puede finalizar el servicio Symantec Backup Exec.cloud a su entera opción si, en cualquier momento, esta disponibilidad cae por debajo de noventa por ciento (90%) en cualquier mes natural. El crédito descrito en la presente cláusula 19 será el único y exclusivo derecho del cliente en relación con la no disponibilidad del servidor para el servicio Symantec Backup Exec.cloud.