Symantec™ Email Security.cloud

Descripción de servicios

Marzo de 2019

Esta Descripción del servicio describe Symantec Email Security.cloud ("Servicio"). Todos los términos en mayúscula de la presente descripción tendrán el significado asignado en el Acuerdo (definido a continuación) o en la sección Definiciones.

Esta Descripción del servicio, con cualquier anexo incluido como referencia, es parte del acuerdo que el Cliente firmó digital o manualmente con Symantec que regula la utilización del Servicio o, en caso de no existir dicho acuerdo firmado, de los Términos y condiciones de los servicios online de Symantec (en adelante, el "Acuerdo").

Índice

Symantec™ Email Security.cloud

Descripción de servicios

Marzo de 2019

1: Funcionalidad y capacidades empresariales y técnicas

Descripción general del servicio

Symantec™ Email Security.cloud es un servicio alojado que filtra mensajes de correo electrónico y ayuda a proteger a las organizaciones contra el Software malicioso (incluido phishing y ataques dirigidos), el spam y el correo electrónico masivo no deseado. Este Servicio ofrece opciones de protección de datos y cifrado, que le ayudan a controlar la información confidencial enviada por correo electrónico. Admite varios tipos de buzones de correo de diferentes proveedores.

Funciones del servicio

- Los Administradores del cliente pueden acceder a la consola de gestión del Servicio mediante un inicio de sesión seguro protegido por contraseña. La consola de gestión ofrece al Cliente la posibilidad de configurar y gestionar el Servicio, acceder a informes y ver datos y estadísticas cuando están disponibles como parte del Servicio.
- El Servicio se gestiona veinticuatro (24) horas al día, los siete (7) días de la semana y se supervisa para determinar la disponibilidad de hardware, la capacidad de servicio y la utilización de los recursos de red. El servicio se supervisa de forma regular para comprobar el cumplimiento de los niveles de servicio y se implementan los ajustes que sean necesarios.
- La elaboración de informes sobre el Servicio está disponible por medio de la consola de gestión. La elaboración de informes incluye estadísticas y/o registros de actividad. Por medio de la consola de gestión, el Cliente puede elegir generar informes, que se pueden configurar para enviarlos por Correo electrónico de forma programada o descargarlos de la consola de gestión.
- El Servicio está diseñado para permitir al Cliente implementar una política de uso del equipo válida y aplicable o su equivalente.
- Las listas de palabras sugeridas y las políticas o las reglas de plantillas proporcionadas por Symantec contienen palabras que pueden considerarse ofensivas.
- Si un Servicio se suspende o se da por finalizado por cualquier motivo, Symantec revertirá todos los cambios de configuración realizados tras el aprovisionamiento del Servicio, y será responsabilidad del Cliente realizar todos los cambios de configuración necesarios cuando se restablezca el Servicio.

Opciones y funciones del Servicio

El Servicio se ofrece en dos (2) opciones: Email Protect o Email Safeguard. El Servicio se debe comprar para cada Usuario de la opción o complemento seleccionados (sujeto a cualquier restricción descrita en la descripción de este Servicio).

Funciones por opción de servicio

	Email Protect	Email Safeguard
Email Antimalware: Protección contra Software malicioso, incluida la protección contra ataques dirigidos y phishing	✓	✓
Email Antispam: Protección contra spam, suplantación de identidad (con seguimiento de vínculos en tiempo real) y correo masivo	✓	✓
Email Data Protection: Controles de políticas de filtrado de contenido personalizables		✓

Email Image Control: Detección de imágenes ofensivas		✓
Filtrado saliente	✓	✓
Cifrado TLS aplicado		✓
Cifrado de TLS oportunista	✓	✓
Registro de direcciones: Control de destinatarios no válidos	✓	✓
Herramienta de sincronización de LDAP de grupos y usuarios	✓	✓
Seguimiento de mensajes	✓	✓
Panel de información sobre informes	✓	✓
Elaboración de informes resumidos (PDF) y detallados (CSV)	✓	✓
Notificaciones y portal de cuarentena de spam del usuario final	✓	✓
Gestión de renuncias de responsabilidad	✓	✓
Policy Based Encryption Essentials		✓
Controles de falsificación de correo electrónico		✓

Puede encontrar información adicional sobre funciones del Servicio individuales en la ayuda en pantalla en http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ES_ES.

Complementos de servicios

	Email Protect	Email Safeguard
Advanced Threat Protection: Correo electrónico	Disponible	Disponible
Policy Based Encryption Advanced	_	Disponible
Email Fraud Protection	Disponible	Disponible
Email Threat Isolation	Disponible	Disponible

Puede encontrar información adicional sobre complementos del Servicio individuales en la ayuda en pantalla en http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ES_ES. La Descripción del servicio para Email Fraud Protection puede encontrarse en: https://www.symantec.com/about/legal/repository.

Advanced Threat Protection: Email detecta las amenazas enviadas por correo electrónico con el espacio aislado de Symantec Cynic™, identifica los ataques dirigidos mediante correo electrónico a la organización o al usuario de destino, e identifica las URL que se vuelven maliciosas después del envío de los correos electrónicos con Symantec Click-time™ URL Protection. Con nuestro espacio aislado de Cynic™ para clientes de O365, puede retirar los correos electrónicos que hayan sido determinados como maliciosos después de la entrega. Además, puede ayudar a los clientes a reparar los ataques de correo electrónico al incluir en lista negra los correos electrónicos basados en indicadores de peligro. Ofrece funciones de elaboración de informes detallados sobre el software malicioso, que incluyen información sobre la dirección URL, la categoría del software malicioso, el método de detección y los hashes de archivos. Se incluyó una API de fuente de datos para permitir la elaboración de informes de software malicioso mediante una dirección URL autenticada sin importar archivos ni enviar datos por correo electrónico. Advanced Threat Protection: Email también proporciona acceso al servicio Phishing Readiness, un simulador de ataques de phishing usado para determinar la vulnerabilidad del personal ante dichos ataques. El uso del servicio Phishing Readiness está controlado por los términos y las condiciones ubicados en https://www.symantec.com/about/legal/repository.

Policy Based Encryption Advanced ofrece: (i) un portal de entrega web pull; (ii) compatibilidad con entrega PGP y S/MIME; (iii) capacidad para intentar el cifrado TLS antes de recurrir a tecnologías de cifrado menos transparentes; y (iv) entrega de archivo PDF cifrado push (el único método de cifrado proporcionado como parte de la función Policy Based Encryption Essentials del plan Email Safeguard). Policy Based Encryption Advanced cuenta con una licencia por usuario de envío, que puede ser un subconjunto de la cantidad total de usuarios para la opción Email Safeguard. Si un cliente requiere el uso de la opción Policy Based Encryption Advanced para la entrega segura de declaraciones, Symantec le podrá permitir adquirir licencias de usuario adicionales en función de la cantidad de declaraciones que se deban entregar, según una fórmula definida por Symantec.

Symantec™ Email Fraud Protection es un servicio en la nube que automatiza la aplicación de DMARC (autenticación de mensajes, informes y conformidad basada en dominios). Symantec Email Fraud Protection hace que cada paso de la aplicación de DMARC sea más simple y más transparente en comparación con el método manual. Su aplicación reduce el riesgo de ataques de suplantación de identidad en el correo entrante, ya que todos los correos electrónicos que se originan en fuentes no autenticadas se ponen en cuarentena o se rechazan. Una vez que se aplica DMARC, los destinatarios de correo electrónico o los agentes de transferencia de correo saben que pueden confiar en el dominio del cliente, lo que a su vez aumenta las tasas de entrega de correo electrónico.

Symantec™ Email Threat Isolation fortalece la protección contra spear phishing, robo de credenciales y ataques de correo electrónico avanzados mediante el aislamiento de vínculos maliciosos y la representación segura de páginas web peligrosas. Email Threat Isolation le permite a Symantec ofrecer la protección más segura contra amenazas de correo electrónico sofisticadas que hacen uso de vínculos maliciosos, como los ataques de spear phishing avanzados o el robo de credenciales.

Email Threat Isolation crea un entorno de ejecución seguro entre los usuarios y sus vínculos de correo electrónico o archivos adjuntos, ejecutando sesiones web de forma remota y enviando solamente información de representación segura a los navegadores de los usuarios. . Como consecuencia, Symantec ayuda a evitar que las amenazas que contienen vínculos y archivos adjuntos maliciosos lleguen a los usuarios. Email Threat Isolation también detiene los ataques de phishing que buscan robar credenciales al representar los sitios web de phishing en modo de solo lectura, lo que impide que los usuarios escriban credenciales corporativas y otra información confidencial.

Acuerdo de nivel de servicio

- Symantec proporciona el acuerdo de nivel de servicio aplicable (“SLA”) para el Servicio tal como se especifica en el Anexo-A.

Plataformas admitidas y requisitos técnicos

- Las plataformas compatibles y los requisitos técnicos para el Servicio se proporcionan en http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ES_ES.

Componentes de software del servicio alojado

- El Servicio incluye los Componentes de servicio de software disponibles en la consola de gestión, al que se puede acceder con el pago del precio aplicable.

2: Responsabilidades del cliente

Symantec solo puede brindar el Servicio si el Cliente proporciona la información requerida o realiza las acciones requeridas; de lo contrario, el rendimiento del Servicio de Symantec puede retrasarse, deteriorarse o verse impedido, y/o la elegibilidad de los beneficios del Acuerdo de nivel de servicio puede anularse según se indica a continuación.

- Autorización de la configuración: El Cliente debe proporcionar la información necesaria para que Symantec comience a prestar el Servicio.
- Personal adecuado del Cliente: El Cliente debe proporcionar personal adecuado para que asista a Symantec en la prestación del Servicio, conforme a una solicitud razonable de Symantec.
- El cliente es responsable de la información, la contraseña u otras credenciales de inicio de sesión de su cuenta.
- El Cliente acepta usar medios razonables para proteger las credenciales y notificará a Symantec inmediatamente sobre cualquier uso no autorizado conocido de la cuenta del Cliente.
- Credenciales de renovación: Si corresponde, el Cliente debe aplicar las credenciales de renovación proporcionadas con el Instrumento de suscripción o Confirmación del pedido aplicables como parte de la gestión de cuentas para continuar recibiendo el Servicio o mantener la información de la cuenta y los datos del Cliente disponibles durante el Período de servicio.
- Comparación entre configuraciones del cliente y configuraciones predeterminadas: El Cliente debe configurar las funciones del Servicio con la consola de gestión, si corresponde, o bien se aplicará la configuración predeterminada. En algunos casos, no existe configuración predeterminada y no se prestará ningún Servicio hasta que el Cliente elija una configuración. La configuración y el uso de los Servicios son responsabilidad absoluta del Cliente y, por lo tanto, Symantec no es responsable por el uso de los Servicios por parte del Cliente ni tampoco será responsable civil o penalmente por ninguna consecuencia que pueda sufrir el Cliente como resultado de la puesta en funcionamiento del Servicio.

Política de uso aceptable

- El Cliente es responsable de cumplir con la Política de uso aceptable de los servicios online de Symantec.

3: Información sobre los derechos y la suscripción

Medidores de cargos

El Servicio se encuentra disponible en virtud del siguiente Medidor, según lo especificado en la Confirmación del pedido:

- "**Usuario**" hace referencia a un individuo y/o dispositivo autorizado para usar el Servicio, de forma total o parcial, y/u obtener beneficios de dicho Servicio.

Cambios en la Suscripción

Si el Cliente recibió la Suscripción o el Derecho de Cliente directamente de Symantec, la comunicación relacionada con los cambios de la Suscripción o el Derecho de Cliente deberá establecerse con la siguiente dirección (o la dirección de reemplazo, según lo publicado por Symantec): CLD_cancellations_MLABS@symantec.com, a menos que se indique lo contrario en el acuerdo del Cliente con Symantec. Todo aviso enviado según este procedimiento será considerado entregado en el momento en que se reciba. Si el Cliente ha recibido la Suscripción o los Derechos de cliente mediante un revendedor de Symantec, debe contactar con el revendedor del Cliente.

4: Atención y asistencia técnica

Nota: Esta sección solo se aplica si el Cliente tiene derecho a recibir Asistencia y Soporte al Cliente directamente de Symantec ("Soporte"). En caso de que un Cliente tenga derecho a recibir Asistencia y Soporte de un revendedor de Symantec, consulte el acuerdo del Cliente con dicho revendedor para obtener detalles acerca de dicho Soporte, teniendo en cuenta que el Soporte descrito aquí no sería aplicable al Cliente.

Atención al cliente

Symantec proporcionará la siguiente atención como parte del Servicio durante el horario laboral correspondiente la región:

- Recibir y procesar pedidos para la implementación del Servicio;
- Recepción y procesamiento de solicitudes de modificaciones permitidas en las funciones del Servicio; y

- Responder a preguntas sobre facturación.

Soporte técnico

El Soporte de nivel de entrada se incluye como parte del Servicio tal como se especifica a continuación.

- El Soporte está disponible veinticuatro (24) horas al día, los siete (7) días de la semana, para ayudar al Cliente a configurar las funciones del Servicio y para resolver los problemas del Servicio de los que tenga noticia. El soporte de los Servicios se realizará de acuerdo con los términos y las condiciones publicados y las políticas de soporte técnico publicadas en https://support.symantec.com/en_US/article.TECH236428.html.
- Una vez que se asigna un nivel de gravedad al envío del Cliente al Soporte, Symantec hará todos los esfuerzos razonables para responder según los objetivos de respuesta definidos en la tabla que se encuentra a continuación. Los errores que surjan de actos realizados por el Cliente o que exijan acciones de otros proveedores de servicios están fuera del control de Symantec y, por ese motivo, están excluidos de este compromiso de Asistencia.

Gravedad del problema	**Objetivos de respuesta del Soporte (24x7)***
Gravedad 1: Se ha producido un problema en el que no hay ninguna solución inmediata disponible en una de las siguientes situaciones: (i) El servidor de producción del Cliente u otro sistema crítico se ha caído o ha perdido mucho tiempo de servicio; o (ii) una parte sustancial de los datos críticos del Cliente presenta un riesgo significativo de pérdida o daño.	En un período de 30 minutos
Gravedad 2: Se ha producido un problema por la avería de una funcionalidad principal. El Cliente puede continuar sus operaciones de manera limitada, aunque la productividad a largo plazo puede verse afectada negativamente.	En un período de 2 horas
Gravedad 3: Se ha producido un problema que tiene un efecto adverso limitado en las operaciones comerciales del Cliente.	El siguiente día laborable, a la misma hora**
Gravedad 4: Se ha producido un problema en el que las operaciones comerciales del Cliente no se han visto afectadas negativamente.	Durante el siguiente día laborable; Symantec recomienda que el Cliente envíe su sugerencia de aplicar nuevas funciones o mejoras en los foros de Symantec

Los Objetivos de respuesta de Soporte anteriores son alcanzables durante las operaciones de servicio normales y no se aplican durante el Mantenimiento del Servicio y/o la infraestructura de soporte como se describe en la sección Mantenimiento a continuación.

** Los Objetivos de tiempos de respuesta corresponden al tiempo para responder a la solicitud y no al tiempo de resolución (el tiempo que lleva cerrar la solicitud).*

*** Un "día laborable" se refiere al horario comercial regional estándar y los días de la semana en la zona horaria local del Cliente; se excluyen los fines de semana y los días festivos locales. En la mayoría de los casos, el "horario comercial" es de 9:00 a.m. a 5:00 p.m. en la zona horaria local del Cliente.*

Mantenimiento del Servicio y/o soporte de la infraestructura del Servicio

Symantec deberá realizar un mantenimiento periódicamente. Symantec realizará esfuerzos comercialmente razonables para realizar el mantenimiento de rutina en momentos en que la actividad colectiva del Cliente sea baja para minimizar las interrupciones. El Cliente no recibirá una notificación previa de estas actividades de mantenimiento de rutina. Para todos los demás tipos de mantenimiento, y como se indica a continuación, Symantec se esforzará por informar a las partes afectadas por adelantado mediante la publicación de una alerta en la página de Symantec Status (https://status.symantec.com/). Para obtener información sobre el estado del Servicio, mantenimiento planificado y problemas conocidos, visite la página de Symantec Status y suscríbase a la página de Symantec Email Security.cloud para recibir las últimas actualizaciones. **Las principales funciones del Servicio, como Análisis de seguridad y Entrega de correo electrónico, permanecen ininterrumpidas durante todas las actividades de mantenimiento.**

- ***Mantenimiento programado:*** Mantenimiento programado significa períodos de mantenimiento previstos durante los cuales el Servicio se puede interrumpir o impedir debido a la falta de disponibilidad de la Infraestructura de servicio. Symantec se esforzará para realizar el Mantenimiento programado en momentos en que la actividad colectiva del Cliente sea reducida, en la zona horaria en que se encuentra situada la Infraestructura afectada y solamente en una parte, no en la totalidad de la red. Durante el Mantenimiento programado, el Servicio podrá ser desviado a secciones de la Infraestructura a las que no se les realiza mantenimiento, lo que podría provocar que el Servicio no se vea interrumpido. Para el Mantenimiento programado, Symantec hará todo lo comercialmente razonable para publicar una notificación al cliente con siete (7) días naturales de antelación en la página de Symantec Status. Los clientes también pueden recibir notificaciones a través de SMS, correo electrónico o Twitter mediante la suscripción a la página de Symantec Status.
- ***Mantenimiento no programado:*** Mantenimiento no programado significa períodos de mantenimiento previstos que no permiten la notificación estándar de siete (7) días y durante los cuales el Servicio puede verse interrumpido o impedido debido a la falta de disponibilidad de la Infraestructura del Servicio. Symantec realizará esfuerzos comercialmente razonables para dar al Cliente una notificación de, como mínimo, un (1) día natural de anticipación, a través de la página de Symantec Status. Durante el Mantenimiento no programado, el Servicio podrá ser desviado a secciones de la Infraestructura a las que no se les realiza mantenimiento, lo que podría provocar que el Servicio no se vea interrumpido. En ocasiones, Symantec realizará Mantenimientos de emergencia. Mantenimiento de emergencia se define como un mantenimiento que *debe implementarse lo más rápido posible para resolver o prevenir un incidente importante*. Symantec se esforzará por informar a las partes afectadas por adelantado mediante la publicación de una alerta en la página de Symantec Status no menos de una (1) hora antes del inicio del mantenimiento.
- ***Mantenimiento de la consola de gestión:*** Para el Mantenimiento de la consola de gestión, Symantec hará todo lo comercialmente razonable para publicar una notificación al cliente con catorce (14) días naturales de antelación en la página de Symantec Status. Symantec se esforzará para llevar a cabo el mantenimiento en la consola de gestión en momentos en que la actividad colectiva del Cliente sea reducida para minimizar la interrupción de la disponibilidad de la consola de gestión. En ocasiones, Symantec puede realizar actualizaciones menores a la Consola de gestión. Para estas actividades de mantenimiento de rutina, los Clientes no recibirán una notificación previa.

5: Términos adicionales

- Es posible acceder al Servicio y usarlo globalmente, con sujeción a limitaciones de cumplimiento de exportación y limitaciones técnicas aplicables conforme a los estándares de Symantec vigentes en ese momento.
- Symantec se reserva el derecho de modificar y actualizar las funciones y la funcionalidad del Servicio, con el objetivo de proporcionar un Servicio igual o mejorado (siempre que Symantec no reduzca materialmente la funcionalidad principal del Servicio). El Cliente reconoce y acepta que Symantec se reserva el derecho de actualizar esta Descripción del servicio en cualquier momento durante el Plazo de la suscripción para reflejar con precisión el Servicio que se proporciona, y la Descripción del servicio actualizada entrará en vigor en el momento de la publicación.
- El uso de cualquier Componente de servicio en forma de software se regirá por el acuerdo de licencia que acompaña al software. Si ningún acuerdo de licencia de usuario final (EULA) acompaña al Componente del servicio, se regirá por los términos y las condiciones que se encuentran en http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. Cualquier derecho u obligación adicional en relación con el uso de dicho Componente del servicio será como se establece en esta Descripción del servicio.
- A menos que se especifique lo contrario en la Descripción del servicio, con el Servicio (incluido cualquier Componente de software del Servicio alojado proporcionado con él) se podrán emplear materiales de código abierto y de otros fabricantes sujetos a licencias independientes.
- Symantec puede actualizar el Servicio en cualquier momento para mantener la efectividad del Servicio.
- Toda plantilla suministrada por Symantec solo servirá de guía para permitir que el Cliente cree sus propias políticas personalizadas y otras plantillas.
- Los siguientes límites se aplican al Servicio:
    - Mensajes entrantes y salientes, por Usuario, por mes natural = diez mil (10 000). El límite no incluye Spam ni Software malicioso dirigido al Cliente.
    - Symantec se reserva el derecho a facturar al Cliente los Usuarios adicionales, según se haya notificado, por los meses restantes en el Acuerdo de servicio donde el uso supera el límite de mensajes.
    - Programación de reintento de correo entrante y saliente = siete (7) días naturales.
    - Tamaño máximo del correo electrónico predeterminado = cincuenta megabytes (50 MB). Los Clientes pueden especificar cualquier tamaño máximo de correo electrónico hasta mil megabytes (1000 MB). Se bloquearán y se eliminarán todos los Correos

electrónicos recibidos por el Servicio que superen el límite especificado, y se enviará una alerta de notificación por Correo electrónico al remitente, al destinatario deseado y al Administrador.
  - Seguimiento de mensajes = los datos quedan disponibles para realizar búsquedas de resolución de problemas durante 30 días; se aplican límites adicionales al número de resultados que puede devolver una sola búsqueda.
  - Cuarentena de Software malicioso = los correos electrónicos se eliminan automáticamente después de treinta (30) días.
  - Cuarentena de spam = los correos electrónicos se eliminan automáticamente después de catorce (14) días, a menos que se configure de otra forma.
  - Disponibilidad de datos de informes del panel de información = cuarenta (40) días para obtener información detallada; doce (12) meses para obtener información resumida.
  - Disponibilidad de datos de elaboración de informes de resumen (PDF) = doce (12) meses.
  - Disponibilidad de datos de elaboración de informes detallados (CSV) = cuarenta (40) días.

- Las siguientes limitaciones se aplican al Cifrado basado en políticas:
  - Correos electrónicos salientes de Cifrado basado en políticas (Z) por usuario, por mes = trescientos (300).
  - Correo electrónico saliente de Policy Based Encryption Essentials/Advanced por Usuario, por mes = cuatrocientos ochenta (480).
  - Cuando el envío se dirige a varios destinatarios, cada dirección única se cuenta como un Correo electrónico seguro. En caso de que el Cliente supere la cantidad de Correos electrónicos seguros permitidos durante cualquier mes natural, Symantec se reserva el derecho a facturar al Cliente el uso real.
  - Los Correos electrónicos enrutados mediante el servicio Policy Based Encryption se limitan a un tamaño máximo de cincuenta megabytes (50 MB).
  - Si usa cifrado pull con el servicio Policy Based Encryption (Z), los correos electrónicos se almacenan de forma predeterminada durante 90 días en el portal de entrega segura antes de caducar.
  - Si usa cifrado pull con el servicio Policy Based Encryption Advanced, los correos electrónicos se almacenan de forma predeterminada durante 30 días en el portal de entrega segura antes de caducar.
  - Estos Niveles de servicio de latencia y disponibilidad no se aplicarán a este Servicio.

- A fin de garantizar que todos los mensajes estén protegidos en todo momento durante su transmisión, Symantec recomienda al Cliente configurar dominios que se utilicen para Policy Based Encryption, como la aplicación del cifrado de TLS en todos los mensajes entrantes y salientes de la infraestructura del servicio.
- Los Clientes deben enrutar el Correo electrónico entrante por medio de Symantec usando la información de enrutamiento proporcionada por Symantec y no deben enrutar el Correo electrónico a una Dirección IP o Torre específica.
- El Servicio solo está disponible para un Cliente que tiene su propio nombre de dominio de Correo electrónico y que tiene la capacidad de configurar los registros de MX y/o DNS para ese nombre de dominio.
- El Cliente debe aceptar el Correo electrónico entrante de todos los rangos IP solicitados para garantizar la continuidad del servicio en caso de que una parte de la Infraestructura no esté disponible.
- El Cliente debe especificar los nombres de host o las direcciones IP del servidor de correo para la entrega de Correos electrónicos entrantes a la organización.
- El Cliente debe garantizar que todos los dominios (incluidos los subdominios) que requieren el Servicio están suministrados. El Cliente acepta que es posible que las funciones del Servicio no funcionen correctamente y que la entrega de Correo electrónico puede no estar disponible para los dominios no suministrados. El Cliente acepta proporcionar y mantener una lista de direcciones válidas de Correo electrónico para recibir el Servicio (la "Lista de validación"). Es responsabilidad del Cliente verificar dicha Lista de validación antes de que el Servicio esté disponible y durante el Plazo. El Servicio rechazará los Correos electrónicos enviados a las direcciones de Correo electrónico que no se encuentran en la Lista de validación, o que están escritas incorrectamente. El Cliente acepta que los SLA no se aplicarán a los Correos electrónicos enviados a direcciones no válidas. Para evitar dudas, los Clientes que usen el sistema de Cuarentena de spam deben mantener una Lista de validación y tener habilitada la capacidad de registro de direcciones. Si el Cliente no puede proporcionar dicha Lista de validación y solicita que la capacidad de registro de direcciones esté deshabilitada, Symantec revisará cada solicitud caso por caso y se reservará el derecho de rechazar solicitudes, a entera discreción de Symantec.

- El Cliente puede liberar Mensajes de correo electrónico que, según su categoría, contengan Software malicioso, o Spam, o solicitar que Symantec libere tales mensajes dentro del dominio del Cliente. EL CLIENTE ACEPTA QUE SYMANTEC NO PUEDE ASUMIR NINGUNA RESPONSABILIDAD ANTE EL ENVÍO DE TALES MENSAJES DE CORREO ELECTRÓNICO A SOLICITUD DEL CLIENTE.
- Symantec no se hace responsable de los daños o las pérdidas generados directa o indirectamente por la incapacidad del Servicio de identificar Spam o por identificar incorrectamente un correo electrónico como Software malicioso o Spam. Symantec se reserva el derecho a analizar todos los Correos electrónicos salientes.
- Se aplicará un mensaje de exención de responsabilidad predeterminado a los Correos electrónicos que analiza el Servicio desde el momento del suministro del Servicio, cuyo contenido podrá ser editado por el Cliente mediante la consola de gestión. Symantec se reserva el derecho de actualizar el mensaje de exención de responsabilidad predeterminado en cualquier momento.
- El Cliente cumplirá con todas las leyes correspondientes en relación con el uso del Servicio. En determinados países, es posible que se requiera el consentimiento del personal individual. La configuración y el uso de los Servicios es absoluta responsabilidad del Cliente y, por lo tanto, Symantec no es responsable por el uso de los Servicios por parte del Cliente ni tampoco será responsable civil o penalmente por ninguna consecuencia que pueda sufrir el Cliente como resultado de la puesta en funcionamiento del Servicio.
- En caso de que la prestación continuada del Servicio al Cliente pusiera en peligro la seguridad del Servicio, incluidos, entre otros, intentos de hacking, ataques de denegación de servicio, bombas de correo u otras actividades maliciosas dirigidas a los dominios del Cliente o provenientes de ellos, el Cliente acepta que Symantec podrá suspender temporalmente el Servicio al Cliente. En tal caso, Symantec informará de inmediato al Cliente y trabajará con él para resolver dichos problemas. Symantec restablecerá el Servicio una vez eliminada la amenaza para la seguridad.
- En caso de que el Servicio se suspenda por algún motivo, no se aplicará a los Correos electrónicos del Cliente y los Correos electrónicos no se enrutarán por medio de la Infraestructura de Symantec. El Cliente es responsable de redireccionar el Correo electrónico durante la suspensión y de confirmar que todas las configuraciones sean precisas si se restablece el Servicio.
- En caso de que el Servicio finalice por algún motivo, la cuenta del Cliente se eliminará y el Cliente no tendrá acceso al Servicio.
- El Cliente no debe permitir que sus sistemas: (i) actúen como Retransmisión abierta o Proxy abierto; o (ii) envíen spam. Symantec se reserva el derecho a revisar el cumplimiento de esta sección por parte del Cliente en cualquier momento. Para evitar dudas, cualquier vulneración de esta cláusula constituirá un incumplimiento sustancial del Acuerdo, y Symantec se reserva el derecho a suspender de inmediato el servicio, de forma total o parcial, y hasta que se subsane la vulneración o a rescindir el Acuerdo en relación con el Servicio afectado.
- Si en algún momento (i) los sistemas de Correo electrónico del Cliente se incluyen en una lista negra, (ii) el Cliente provoca que los sistemas de Symantec se incluyan en alguna lista negra debido al envío de Spam o (iii) el Cliente no cumple alguna de las obligaciones establecidas en esta Descripción del servicio, Symantec informará al Cliente y se reserva el derecho, a su exclusiva discreción, a suspender de inmediato el Servicio, interrumpirlo o finalizarlo, de forma total o parcial.
- Al Cliente se le permite usar el Servicio solamente para sus fines comerciales propios. El Cliente acepta no revender el Servicio ni la documentación asociada a ningún tercero, ni tampoco sublicenciarlos, arrendarlos ni ponerlos a su disposición. El Cliente acepta no usar el Servicio para desarrollar un producto o un servicio competitivo, no copiar las funciones ni la interfaz de usuario, no ejecutar evaluaciones del Servicio y no realizar comparaciones u otros análisis comparativos para publicarlos fuera de la organización del Cliente sin la previa autorización escrita de Symantec.

6: Definiciones

"**Registro de direcciones**" es una función obligatoria del Servicio que rechaza los correos electrónicos entrantes enviados a las direcciones de correo electrónico que no están incluidas en la lista de direcciones de correo electrónico válidas del Cliente ("Lista de validación").

"**Administrador**" hace referencia a un Usuario cliente con autorización para gestionar el Servicio en nombre del Cliente. Los Administradores pueden gestionar un Servicio de forma total o parcial, según lo designe el Cliente.

"**Configuración de prácticas recomendadas de antispam"** hace referencia a las pautas de configuración recomendadas de Symantec para el Servicio que se ofrecen al Cliente durante el proceso de suministro o que se publican en el recurso de ayuda en pantalla.

"**Administrador de conexión**" hace referencia a los métodos de detección incluidos en la etapa de protocolo de enlace SMTP.

"**Solicitud de crédito**" hace referencia a la notificación que el Cliente debe enviar a Symantec por Correo electrónico a support.cloud@symantec.com con la línea de asunto "Solicitud de crédito" (a menos que Symantec notifique lo contrario).

"**Clúster de torre designada**" hace referencia a dos (2) o más Torres designadas para proporcionarle Email Security Services al Cliente.

"**Configuración de nivel de dominio**" hace referencia a la configuración de dominio personalizable para un dominio particular dentro de la consola de gestión para Email Security Services.

"**Correo electrónico**" hace referencia a cualquier mensaje SMTP entrante o saliente que pasa por un Servicio.

"**Email Security Services"** son las opciones Email Safeguard y Email Protect y cualquier servicio complementario disponible.

"**Falso positivo de Software malicioso en el Correo electrónico"** hace referencia un correo electrónico legítimo identificado incorrectamente como que contiene Software malicioso.

"**Acuerdo de licencia para el usuario final (EULA)"** hace referencia a los términos y condiciones que se incluyen con el Software (según se define a continuación).

"**Configuración global**" hace referencia a las acciones dentro de la consola de gestión que se aplican a todos los dominios y niveles de grupo para el Servicio.

"**Configuración de nivel de grupo"** hace referencia a la configuración de grupo personalizable para un grupo particular dentro de la consola de gestión para funciones aplicables del Servicio.

"**Infraestructura"** hace referencia a cualquier tecnología de Symantec o de un emisor de licencias, y a la propiedad intelectual que se usa para prestar los Servicios.

"**Software malicioso conocido**" hace referencia a Software malicioso para el cual, en el momento de la recepción del contenido por parte de Symantec, una firma ya haya estado a disposición durante un mínimo de una (1) hora para ser utilizada por las tecnologías antivirus implementadas por Symantec.

"**Software malicioso**" o "**programa malicioso**" hace referencia a cualquier software utilizado para interrumpir operaciones informáticas o móviles o, sin la debida autorización, utilizados para recopilar información confidencial y/o para obtener acceso a sistemas informáticos privados.

"**Falso positivo de Software malicioso**" hace referencia a un correo electrónico legítimo identificado incorrectamente como que contiene Software malicioso.

"**Miembro"** hace referencia al Cliente y a los terceros con quienes el Cliente crea una red cifrada mediante el Servicio complementario anterior de Límite de cifrado de correo electrónico.

"**Cargo mensual**" hace referencia al cargo mensual por los Servicios pertinentes según se definen en el Acuerdo.

"**Ayuda en pantalla**" hace referencia a la información adicional que está disponible en http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ES_ES.

"**Proxy abierto**" hace referencia a un servidor proxy configurado para permitir que terceros desconocidos o no autorizados accedan a servidores DNS, páginas web u otros datos, los almacenen o los reenvíen a los fines del Servicio.

"**Retransmisión abierta**" hace referencia a un servidor de Correo Electrónico configurado para recibir Correo electrónico proveniente de un tercero desconocido o no autorizado y reenviarlo a uno o más destinatarios que no son usuarios del sistema de Correo electrónico al cual ese servidor de Correo electrónico está conectado. También se puede referir a la Retransmisión abierta como "retransmisión de spam" o "retransmisión pública".

El significado de "**Confirmación del pedido**" se indica en los términos y condiciones de los Servicios online de Symantec, si corresponde. Si no existen términos y condiciones aplicables al Servicio, la "Confirmación del pedido" hará referencia al Instrumento de suscripción, según se define en este acuerdo.

"**Servicio**" hace referencia a la opción Protect o Safeguard de Symantec Email Security.cloud, adquirida por el Cliente.

"**Componente del servicio**" hace referencia a ciertos productos de software activadores, periféricos de hardware y documentación asociada que Symantec puede proporcionar por separado como parte accesoria de un Servicio.

"**Crédito de servicio**" hace referencia a la cantidad de dinero que se abonará en la factura siguiente del Cliente después del envío de una Solicitud de crédito y de la validación por Symantec de que ese crédito le corresponde al Cliente.

"**Software del servicio**" hace referencia al Software (según se define a continuación), como el Servicio lo requiera, que debe instalarse en cada equipo del Cliente para recibir el Servicio. El Software del Servicio incluye el Software y la documentación asociada que Symantec puede proporcionar por separado como parte del Servicio.

"**Software**" hace referencia a cada programa de software de Symantec o de un emisor de licencias, en formato de código objeto, otorgado al Cliente con licencia por Symantec y que se rige por los términos del EULA que lo acompaña, el cual incluye, entre otros, nuevas versiones o actualizaciones conforme a lo que aquí se establece.

"**Spam**" hace referencia a Correo electrónico comercial no solicitado.

"**Falso negativo de spam**" hace referencia a un Correo electrónico spam no identificado como Spam por el servicio.

"**Falso positivo de spam**" hace referencia a un Correo electrónico incorrectamente identificado como Spam por el Servicio.

"**Configuración recomendada de spam**" hace referencia a las pautas recomendadas de configuración de Symantec para el servicio que se ofrecen al Cliente durante el proceso de prestación o que se publican en el recurso de ayuda en pantalla.

"**Instrumento de suscripción**" hace referencia a uno o más de los siguientes documentos aplicables que definen con más detalle los derechos y las obligaciones del Cliente relacionados con el Servicio: un certificado de Symantec o un documento similar emitido por Symantec, o un acuerdo por escrito entre el Cliente y Symantec, que acompaña, precede o sigue el Servicio.

"**Términos de Symantec Hosted Services**" hace referencia a los términos del servicio alojado de Symantec a los que se accede desde https://www.symantec.com/about/legal/service-agreements.jsp.

"**Términos y condiciones del Servicio online de Symantec**" hace referencia a los términos y condiciones del Servicio online de Symantec a los que se accede desde https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Tracker**" hace referencia a una herramienta de Symantec que se utiliza para medir la disponibilidad y la latencia del Servicio.

"**Torre"** hace referencia a un clúster de servidores de Correo electrónico de carga equilibrada.

"**Usuario"** hace referencia a una persona individual que envía o recibe correo electrónico y está protegida por una parte del Servicio.

Anexo A

Acuerdo de nivel de servicio

General

- El Cliente puede tener derecho a un Crédito de servicio si Symantec no cumple con el nivel de servicio definido. Si el Cliente considera que tiene derecho a un Crédito de servicio, debe enviar una Solicitud de crédito antes de los diez (10) días laborables posteriores a la finalización del mes natural en el que se produjo el supuesto incumplimiento del nivel de servicio. El Cliente acepta que los registros solo se mantendrán durante una cantidad limitada de días naturales y, por lo tanto, las Solicitudes de crédito que se envíen después del período mencionado no se considerarán válidas.
- Las Solicitudes de crédito se realizan contactando con la Asistencia técnica de Symantec. Visite la página de destino de la asistencia de productos para obtener instrucciones detalladas: https://support.symantec.com/en_US/email-security-cloud.html.
- Todas las Solicitudes de crédito estarán sujetas a la verificación por parte de Symantec de acuerdo con las disposiciones aplicables del presente Acuerdo de nivel de servicio. Symantec puede solicitar información adicional del Cliente para validar la Solicitud de crédito.
- Este Acuerdo de nivel de servicio no regirá en los siguientes casos: (i) durante períodos de Mantenimiento programado o Mantenimiento de emergencia, períodos de falta de disponibilidad por fuerza mayor o actos u omisiones del Cliente o de un tercero; (ii) durante cualquier período en el que Symantec suspenda el servicio de acuerdo con los términos del Acuerdo; (iii) en casos de vulneración del Acuerdo por parte del Cliente (incluidos, sin carácter limitativo, los casos en que el Cliente tiene facturas vencidas); (iv) si el Cliente no configuró el Servicio según el Acuerdo; o (v) durante períodos de prueba de servicio.
- Los recursos establecidos en este Acuerdo de nivel de servicio serán los únicos y exclusivos recursos de los que dispondrá el Cliente por disposición contractual, extracontractual (incluida, sin limitación, la negligencia) o de otro tipo con respecto a este Acuerdo de nivel de servicio.
- La responsabilidad acumulativa máxima de Symantec en virtud de este Acuerdo de nivel de servicio en cualquier mes calendario será un crédito equivalente a un valor igual al que sea inferior de los dos siguientes: el 100% del Cargo mensual o diez mil dólares/cinco mil libras esterlinas/diez mil euros (10,000 $/5,000 £/10,000 €), dependiendo de la moneda en la que se facture al Cliente.
- Si el Servicio afectado se compra como parte de un paquete de Servicios, el Crédito de servicio se calculará en función del Servicio afectado y no en todo el paquete de Servicios.

Excepciones al Acuerdo de nivel de servicio para Email Security Services

Este Acuerdo de nivel de servicio no regirá en los siguientes casos: (i) en relación con los Correos electrónicos que no hayan pasado por el Servicio (incluyendo, sin carácter limitativo, el caso en que el Cliente no haya tomado las medidas necesarias para garantizar que solo aceptará Correo electrónico entrante de la Infraestructura de Symantec); (ii) en relación con los Correos electrónicos entrantes y salientes que se enviaron inicialmente a Symantec y que contenían más de 500 destinatarios por cada sesión de SMTP; (iii) para Clientes suministrados en cualquier Torre designada como Torre de clúster masiva; o (iv) en relación con Correos electrónicos entrantes y salientes para dominios de clientes no suministrados por el Servicio.

Disponibilidad del servicio

El nivel de servicio de disponibilidad del Servicio hace referencia a la capacidad de establecer una sesión SMTP en el puerto 25 desde el MTA del Cliente a la infraestructura de Symantec, en cumplimiento con RFC5321. El nivel de servicio de disponibilidad del Servicio no se aplica al portal de gestión ni al sistema de Cuarentena de spam. Este nivel de servicio no se aplicará si el Cliente configuró el Servicio incorrectamente o debido a circunstancias imprevistas o causas ajenas al control razonable de Symantec, incluidos, entre otros, desastres naturales, guerras, ataques terroristas, disturbios, acciones gubernamentales o una falla de red o dispositivo externa a los centros de datos de Symantec, incluso en el sitio del Cliente o entre el sitio del Cliente y el centro de datos de Symantec.

Si la Disponibilidad del servicio es inferior al cien por ciento (100%) en cualquier mes calendario, el Cliente puede presentar una Solicitud de Crédito y puede recibir un crédito de servicio equivalente a un valor igual al que sea inferior de los dos siguientes: el 100% del cargo mensual o diez mil dólares/cinco mil libras esterlinas/diez mil euros (10,000 $/5,000 £/10,000 €) dependiendo de la moneda en que se facture al cliente:

Porcentaje de disponibilidad por mes natural	Porcentaje de crédito del cargo mensual

inferior al 100% y superior o igual al 99%	25%
inferior al 99% y superior o igual al 98%	50%
inferior al 98%	100%

Si la disponibilidad del Servicio disminuye por debajo del noventa y ocho por ciento (98%) en cualquier mes natural, según la confirmación de Symantec, el Cliente tendrá derecho a rescindir el Servicio pertinente y recibir un reembolso proporcional de los cargos pagados por adelantado correspondientes al plazo remanente después de que dicha rescisión se haya hecho efectiva.

Entrega de correo electrónico

El nivel de servicio de entrega de correo electrónico se define por la capacidad de Symantec de entregar todo el Correo electrónico enviado a o desde el Cliente en las siguientes condiciones:

a) El Correo electrónico debe haber sido recibido por Symantec; y

b) El Correo electrónico no debe contener ningún Software malicioso, Spam ni otro contenido que haya ocasionado la interceptación por parte del Servicio.

De acuerdo con las condiciones mencionadas anteriormente, si Symantec no entrega un Correo electrónico que el Cliente envíe o recibe, y el Cliente no ha incumplido los términos del Acuerdo, el Cliente podrá dar por finalizado el Servicio mediante una notificación por escrito entregada con treinta (30) días naturales de anticipación.

Latencia de correo electrónico

El Nivel de servicio de latencia de correo electrónico se aplica si el tiempo medio de recorrido (según la medición de Symantec Tracker, para Correos electrónicos enviados cada cinco [5] minutos hacia y desde cada torre del clúster de torre designado del Cliente) supera los retrasos establecidos en la siguiente tabla, en un mes natural. Si el Cliente considera que el nivel de servicio de latencia no se ha cumplido, puede enviar una Solicitud de crédito y podrá recibir un Crédito de servicio conforme a la siguiente tabla:

Tiempo medio de recorrido (segundos)	Porcentaje de crédito del cargo mensual
superior al 60 e inferior o igual al 90	25%
superior al 90 e inferior o igual al 120	50%
superior al 120 e inferior o igual al 180	75%
superior al 180	100%

El nivel de servicio de latencia no se aplica si:

a) El Cliente no ha proporcionado una Lista de validación a Symantec y el Cliente sufre un ataque de denegación de servicio.

b) Existen períodos de retraso causados por un bucle de correo enviado o recibido por los sistemas del Cliente; o

c) El servidor principal de Correo electrónico del Cliente no puede aceptar correo electrónico en el intento de entrega inicial.

Falsos positivos de spam

El nivel de servicio de falsos positivos de spam define el índice máximo de captura de falsos positivos de spam. El nivel de servicio de falsos positivos de spam solo se aplica si el Cliente implementa la configuración de prácticas recomendadas de antispam como se detalla en el recurso de ayuda en pantalla. Si el índice medio de captura de Falsos positivos de spam supera el 0,0003% del tráfico de Correo electrónico entrante del Cliente en un mes natural, el Cliente podrá enviar una Solicitud de crédito y recibir un Crédito de servicio según se indica en la tabla siguiente:

Índice medio de captura de Falsos positivos de spam (%)	Porcentaje de crédito del cargo mensual
superior al 0,0003 e inferior o igual al 0,003	25%
superior al 0,003 e inferior o igual al 0,03	50%
superior al 0,03 e inferior o igual al 0,3	75%
superior al 0,3	100%

Los siguientes correos electrónicos no constituirán Correos electrónicos de Falsos positivos de spam con relación a los fines de este nivel de servicio:
a) Correos electrónicos que no son correos electrónicos comerciales legítimos.
b) Correos electrónicos que incluyen más de 20 destinatarios.
c) Correos electrónicos en los que el remitente del Correo electrónico se encuentre en la lista de remitentes bloqueados, incluyendo sin limitación, los definidos por el usuario individual si el Cliente ha habilitado la configuración a nivel de usuario.
d) Correos electrónicos que se envíen desde un equipo afectado.
e) Correos electrónicos que se envíen desde un equipo que se encuentra en la lista de bloqueados de un tercero.
f) Correos electrónicos interceptados por análisis de Spam saliente.

Para reunir los requisitos de Crédito de servicio, el Cliente debe informar de los Correos electrónicos que supuestamente son falsos positivos a la Asistencia técnica de Symantec en un plazo de cinco (5) días naturales a partir de la recepción del Correo electrónico. Symantec investigará y confirmará si el Correo electrónico es un Falso positivo de spam y registrará el resultado.

Índice de captura de spam

El nivel de servicio de índice de captura de spam define el índice mínimo de captura de spam. El nivel de servicio solo se aplica si el Cliente implementa la Configuración de prácticas recomendadas de antispam como se detalla en el recurso de ayuda en pantalla. El nivel de servicio corresponde a la cantidad de Falsos negativos de spam calculada en un mes natural. El Cliente puede enviar una Solicitud de crédito y recibir un Crédito de servicio conforme a la siguiente tabla:

Índice de captura de spam (%)	Porcentaje de crédito del cargo mensual
superior al 98 e inferior o igual al 99	25%
superior al 97 e inferior o igual al 98	50%
superior al 96 e inferior o igual al 97	75%
inferior al 96	100%

Este Nivel de servicio de índice de captura de spam no se aplicará si el Correo electrónico no se envió a una dirección de Correo electrónico válida. Se aplicará un Índice de captura de spam inferior al noventa y cinco por ciento (95%) a los correos electrónicos que contengan más del cincuenta por ciento (50%) de conjuntos de caracteres de doble byte. Si dicho Índice de captura de spam disminuye por debajo del noventa y cinco por ciento (95%), el Cliente tendrá derecho a un Crédito de servicio del veinticinco por ciento (25%) del cargo mensual. Si el Índice de captura de spam disminuye por debajo del noventa por ciento (90%), el Cliente tendrá derecho a un Crédito de servicio equivalente al cien por ciento (100%) del cargo mensual.

Para reunir los requisitos de Crédito de servicio, el Cliente debe informar de los Correos electrónicos que supuestamente son falsos negativos a la Asistencia técnica de Symantec en un plazo de cinco (5) días naturales a partir de la recepción del Correo electrónico. Symantec investigará y confirmará si el Correo electrónico es un Falso negativo de spam y registrará el resultado.

Protección contra Software malicioso

Si los sistemas del Cliente están infectados por Software malicioso conocido o desconocido que se propaga a través de Correos electrónicos que pasan a través del servicio de análisis en la nube, el Cliente puede tener derecho a un Crédito de servicio por el monto que se define a continuación. El Cliente debe notificar a Symantec dentro de los cinco (5) días posteriores a conocer dicho Software malicioso y Symantec debe registrar, investigar y validar dicha notificación. El Cliente debe enviar una Solicitud de crédito y, si esta es validada, recibirá un Crédito de servicio equivalente a un valor igual al que sea inferior de los dos siguientes: el cien por ciento 100% del Cargo mensual o diez mil dólares/cinco mil libras esterlinas/diez mil euros (10 000 $/5000 £/10 000 €) (según la moneda de la factura del Cliente). El recurso especificado en esta sección será el único y exclusivo recurso del que dispondrá el Cliente por disposición contractual, agravio (incluida, sin carácter taxativo, la negligencia) o de otra manera, en relación con cualquier infección por Software malicioso transmitida al Cliente o a un tercero mediante el Servicio. Para evitar dudas, el recurso especificado en esta sección no se aplicará en casos de autoinfección deliberada.

Los sistemas del Cliente se consideran infectados si se recibió Software malicioso adjunto a un correo electrónico a través del Servicio y el Software malicioso se activó dentro del sistema del Cliente ya sea automáticamente o con intervención manual. En caso de que Symantec detecte, pero no detenga, un correo electrónico con un archivo adjunto que incluye un Software malicioso, y publique una actualización en la página de Symantec Status o notifique a los Clientes, proporcionando suficiente información para permitir que el Cliente identifique y elimine el Correo electrónico infectado, no se aplicará la solución establecida arriba.

El servicio analizará tantos Correos electrónicos y sus archivos adjuntos como sea posible. Es posible que no se puedan analizar archivos adjuntos con contenido que está bajo el control directo del remitente (por ejemplo, archivos adjuntos protegidos por contraseña y/o cifrados y/o con una contraseña enviada por separado desde el Correo electrónico). Estos Correos electrónicos o archivos adjuntos están excluidos del nivel de servicio, y el recurso que se menciona anteriormente no se aplicará.

Este Nivel de servicio de protección contra Software malicioso no regirá en relación con el Software malicioso que el Cliente haya enviado deliberadamente o por medio de Symantec a petición del Cliente.

Este Nivel de servicio de protección contra Software malicioso solo se aplicará al Software malicioso según se define en esta Descripción del servicio, y no se aplicará a lo siguiente: spyware, publicidad no deseada, vínculos URL a sitios web que alojan contenido malicioso o troyanos desconocidos.

Falsos positivos de Software malicioso

El nivel de servicio de falsos positivos de Software malicioso define el índice máximo de captura de falsos positivos de Software malicioso. Si el índice de captura de Falsos positivos de Software malicioso de correo electrónico supera el 0,0001 % del tráfico de Correo electrónico del Cliente en un mes natural, el Cliente podrá enviar una Solicitud de crédito y recibir un Crédito de servicio según se indica en la tabla siguiente:

Índice medio de captura de Falsos positivos de Software malicioso (%)	Porcentaje de crédito del cargo mensual
superior al 0,0001 e inferior o igual al 0,001	25%
superior al 0,001 e inferior o igual al 0,01	50%
superior al 0,01 e inferior o igual al 0,1	75%
superior al 0,1	100%

Asistencia técnica y respuesta ante errores 24 horas al día, todos los días del año

La asistencia técnica está disponible veinticuatro (24) horas al día, todos los días del año para:
a) proporcionar asistencia técnica al Cliente por problemas relacionados con el Servicio; y
b) comunicarse con el Cliente para resolver dichos problemas.