

**Servicios de Seguridad Gestionados de IBM (Computación en la Nube) –
hosted e-mail and Web security - express managed e-mail security**

Índice

1.	Alcance de los Servicios	3
2.	Definiciones	3
3.	Servicios	4
3.1	Servicios Generales	4
3.1.1	Responsabilidades de IBM sobre los Servicios Generales	4
3.1.2	Sus Responsabilidades sobre los Servicios Generales	4
3.2	Contratos de Nivel de Servicios Generales	4
3.2.1	Disponibilidad de los SLAs Generales	5
3.2.2	Recursos Generales de SLA	5
3.3	Servicios de Codificación Limítrofe (Opcional)	6
3.3.1	Responsabilidades de IBM sobre los Servicios de Codificación Limítrofe	6
3.3.2	Sus responsabilidades sobre Codificación Limítrofe	7
3.3.3	Otros servicios de Codificación Limítrofe	7
3.3.4	Limitación de responsabilidades	7
3.4	Servicios de Codificación basados en Políticas	7
3.4.1	Responsabilidades de IBM por los servicios de Codificación basados en Políticas	8
3.4.2	Sus responsabilidades por los Servicios de Codificación Basados en Políticas	8
3.4.3	Servicios PBE adicionales	8
3.4.4	Limitaciones de los servicios	9
3.4.5	Limitación de responsabilidades	9
3.5	E-mail Antivirus	9
3.5.1	Responsabilidades de IBM por el E-mail Antivirus	9
3.5.2	Sus responsabilidades sobre el E-mail Antivirus	10
3.5.3	Contratos de nivel de servicio	10
3.6	E-mail Image Control	11
3.6.1	Responsabilidades de IBM respecto del E-mail Image Control	11
3.6.2	Sus responsabilidades respecto del E-mail Image Control	12
3.7	E-mail Antispam	12
3.7.1	Responsabilidades de IBM respecto del E-mail Antispam	12
3.7.2	Sus responsabilidades respecto del E-mail Antispam	13
3.7.3	Contratos de nivel de servicio	13
3.8	E-mail Content Control	14
3.8.1	Responsabilidades de IBM respecto del E-mail Content Control	15
3.8.2	Sus responsabilidades respecto del E-mail Content Control	15

Descripción de los Servicios

Servicios de Seguridad Gestionados de IBM (Computación en la Nube) – Hosted E-mail and Web security - express managed e-mail security

ADEMÁS DE LOS TÉRMINOS Y CONDICIONES CONTRACTUALES QUE SE ESPECIFICAN A CONTINUACIÓN, LA PRESENTE DESCRIPCIÓN DE SERVICIOS INCLUYE LAS “DISPOSICIONES GENERALES” DE LOS SERVICIOS DE SEGURIDAD GESTIONADOS DE IBM (“DISPOSICIONES GENERALES”) QUE SE ENCUENTRAN EN http://www-935.ibm.com/services/us/iss/html/contracts_worldwide_landing.html Y QUE SE INCORPORAN AQUÍ COMO REFERENCIA.

1. Alcance de los Servicios

Los Servicios de Seguridad Gestionados de IBM (Computación en la Nube) – hosted e-mail and Web security - express managed e-mail security (denominada “Seguridad de e-mail” o “Servicios”) pueden incluir:

- a. Servicios de antivirus de e-mail para ayudarlo a detectar virus y ciertos tipos de imágenes en el correo electrónico;
- b. Servicios de E-mail Image Control para ayudarlo a detectar imágenes pornográficas presentes en archivos de imagen adjuntos de los correos electrónicos entrantes y salientes;
- c. Servicios de E-mail Antispam para ayudar a salvaguardar el correo electrónico contra spam; y/o
- d. Servicios de E-mail Content Control para ayudar a detectar contenido en línea de acuerdo con la política de uso aceptable de su computadora (o su equivalente) en el correo electrónico.

Las funciones de los Servicios que aquí se describen dependen de la disponibilidad y de la mantenibilidad de los productos y funciones de los productos que se estén utilizando. Incluso en el caso de productos soportados, posiblemente no todas las funciones de los productos tengan soporte. IBM coloca a disposición, mediante previa solicitud, información sobre las funciones con soporte. Esto incluye hardware, software y firmware, ya sean o no suministrados por IBM.

2. Definiciones

E-mail en Masa – un grupo de más de 5.000 e-mails, con contenido sustancialmente similar, enviados o recibidos mediante una misma operación o mediante una serie de operaciones relacionadas.

Clúster de Torre Designado – un clúster de servidores de e-mail de carga equilibrada (un mínimo de dos), designados para suministrarle Seguridad de e-mail al Receptor de los Servicios.

Disponibilidad de los Servicios de e-mail – la capacidad de establecer una sesión de Protocolo de Transferencia de Correo Simple (“SMTP”) en el puerto 25 del Clúster de Torre Designado según se mida por los sistemas de rastreo de la disponibilidad de IBM.

Latencia – el tiempo promedio del recorrido completo para e-mails enviados cada cinco minutos hacia y desde cada Torre, según se mida por los sistemas de rastreo de la disponibilidad de IBM.

Open Relay – un servidor de e-mail, configurado para recibir e-mails de un tercero desconocido o no autorizado y reenviar los e-mails a uno o más receptores que no sean usuarios del sistema de e-mail al cual ese servidor de e-mail está conectado. El relevador de apertura también puede ser denominado “Spam Relay” o “Public Relay”.

Mantenimiento Planificado – períodos de mantenimiento que causan interrupción de los servicios debido a la no disponibilidad del Clúster de Torre Designado. Se le enviará una notificación al Receptor de los Servicios con una anticipación mínima de 5 días calendario de dicho mantenimiento. El Mantenimiento Planificado no deberá superar las ocho horas por mes calendario y no tendrá lugar durante el horario comercial local.

Cuarentena – aislamiento de e-mail con sospecha de portar contenido no deseado, por configuración del Receptor de los Servicios, antes de la toma de medidas por parte del Usuario o del borrado automático.

Receptor de los Servicios – cualquier entidad o individuo que reciba o utilice los Servicios, o los resultados o productos de los mismos.

Spam – e-mail comercial no solicitado.

Usuario – una persona o casilla de correo a nombre de la cual los Servicios están escaneando el e-mail.

Virus – código de programación que se implanta por sí solo en un archivo o memoria, infecta otros archivos y áreas de memoria y se ejecuta sin autorización.

3. Servicios

3.1 Servicios Generales

LOS SERVICIOS QUE AQUÍ SE DESCRIBEN SE SUMINISTRAN “EN EL ESTADO ACTUAL” Y SIN GARANTÍA NI INDEMNIZACIÓN DE NINGUNA ESPECIE POR PARTE DE IBM, EXPRESA O IMPLÍCITA, INCLUYENDO, SIN RESTRICCIONES, LAS GARANTÍAS DE COMERCIALIZACIÓN, ADECUACIÓN PARA UN PROPÓSITO EN PARTICULAR, Y NO CONTRAVENCIÓN DE LOS DERECHOS DE PROPIEDAD Y PROPIEDAD INTELECTUAL.

3.1.1 Responsabilidades de IBM sobre los Servicios Generales

IBM:

- a. le suministrará un acceso con contraseña a un portal electrónico exclusivo basado en Internet y a una herramienta de gestión que le permitirá visualizar datos y estadísticas cuando utilice los Servicios. Dicha herramienta también le ofrecerá una variedad de opciones de configuración y gestión;
- b. le suministrará los Servicios en un esquema de 24 horas al día, 7 días a la semana; y
- c. le brindará asistencia técnica para los Servicios en un esquema de 24 horas al día, 7 días a la semana.

3.1.2 Sus Responsabilidades sobre los Servicios Generales

Usted acepta:

- a. monitorear la cantidad de Usuarios, y notificarle a IBM si la cantidad real de Usuarios excede la cantidad ordenada o es inferior a la cantidad mínima requerida de diez Usuarios. IBM trabajará junto a usted para mejorar la Programación de manera de incluir Usuarios adicionales.
- b. asegurarse:
 - (1) de que todos los sistemas de correo electrónico soportados cuenten con una dirección de IP estática;
 - (2) de que los sistemas de correo electrónico soportados no envíen e-mail masivo, actúen como Open Relay ni envíen Spam; y
 - (3) ni usted ni ningún otro miembro de su Empresa usen los Servicios (o cualquier parte o cantidad de los mismos) para de alguna manera desarrollar o promover servicios comerciales similares a los Servicios referidos;
SI USTED NO CUMPLE CON ESTAS OBLIGACIONES Y OCURRE UNA INTERRUPCIÓN DE LOS SERVICIOS, IBM LE INFORMARÁ SOBRE DICHAS FALLAS Y SE RESERVA EL DERECHO DE RETENER EL SUMINISTRO O DE SUSPENDER TODOS O PARTE DE LOS SERVICIOS EN FORMA INMEDIATA Y HASTA QUE DICHO USO HAYA FINALIZADO.
- c. de suministrar todos los datos técnicos y demás informaciones que IBM pueda solicitar razonablemente, en ocasiones, para permitir la entrega de Servicios por parte de IBM;
- d. de mantener la seguridad de la contraseña que le fue suministrada para el acceso a la configuración exclusiva con base en Internet y a la herramienta de gestión e informe, y no darla a conocer a terceros;
- e. de proporcionarle a IBM el nombre, el teléfono y la dirección de e-mail de su administrador de correo electrónico, si usted optó por ello en su perfil; y
- f. de garantizar que el formulario de autorización de lanzamiento apropiado para redirigir los e-mails a una dirección de e-mail alternativa se envíe a IBM de manera oportuna.

3.2 Contratos de Nivel de Servicios Generales

Los Contratos de Nivel de Servicios (“SLAs”) de IBM establecen objetivos por tiempo de respuesta y contramedidas para eventos específicos que resultan de los Servicios. Los SLAs entran en vigor cuando

el proceso de despliegue ha finalizado, y cuando el soporte y la gestión han llegado exitosamente hasta usted. Las soluciones de SLA están disponibles siempre y cuando usted cumpla con sus obligaciones, según lo definido en esta Descripción de Servicios y en todos los documentos de contrato relacionados.

Los SLAs no se aplican:

- a. hasta 30 días posteriores a la activación del servicio Seguridad del correo electrónico;
- b. si las configuraciones de su sistema no cumplen con las directrices de configuración suministradas;
- c. durante períodos de Mantenimiento Planificado;
- d. durante períodos de no disponibilidad debido a fuerza mayor o actos u omisiones de su parte, de IBM, o de un tercero; o
- e. durante cualquier período de suspensión de la Seguridad del correo electrónico, de acuerdo con esta Descripción de Servicios y todos los documentos de contrato relacionados.

3.2.1 Disponibilidad de los SLAs Generales

Los incumplimientos en los SLAs que se describen a continuación comprenden las métricas medidas para la entrega de los Servicios. A menos que esté explícitamente detallado, no se deberán aplicar garantías de ningún tipo a los Servicios entregados en virtud de esta Descripción de Servicios. Los únicos recursos por falla en el cumplimiento de los plazos de los SLAs se especifican en la sección de esta Descripción de Servicios titulada "Recursos de los SLAs".

- a. Entrega de correo electrónico – Para que IBM pueda ejecutar los Servicios, su correo electrónico será enrutado a través de IBM. IBM transmitirá el 100% de todos los correos electrónicos enviados o recibidos con este propósito. Este SLA no se aplica para e-mails que contengan virus, ni para correos electrónicos detenidos por antispam de correos electrónicos.
- b. Disponibilidad de Servicios de e-mail – IBM mantendrá Disponibilidad de Servicios de correo electrónico para el 100% del mes calendario.

La Disponibilidad de los Servicios de correo electrónico sólo se aplica si el Clúster de Torre Designado tiene capacidad de:

- (1) recibir su e-mail entrante en nombre de su dominio las 24 horas, los 7 días de la semana; y
 - (2) aceptar los correos electrónicos salientes de su anfitrión SMTP correctamente configurado en nombre de su(s) dominio(s) las 24 horas, los 7 días de la semana.
- c. Latencia de correo electrónico – En todos los meses calendario, el tiempo promedio de recorrido completo de su Clúster de Torre Designado tendrá un máximo de un minuto. El tiempo del recorrido completo no incluirá atrasos causados por *mail loop* hacia/desde sus sistemas.

La latencia de e-mail no se aplica durante:

- (1) cualquier brote de virus en el que el radio del virus al correo electrónico sea mayor a 1:50; o
- (2) un ataque de Denegación de Servicio.

3.2.2 Recursos Generales de SLA

Los recursos de SLA están disponibles siempre y cuando usted cumpla con sus obligaciones, según se definen en esta Descripción de Servicios y en todos los documentos de contrato relacionados.

Como se describe en los siguientes cuadros, se emitirá un crédito como único recurso para el incumplimiento de cualquiera de los SLAs que se describen en la sección anterior, titulada "Disponibilidad de los SLAs", durante cualquier mes calendario determinado. No puede obtener más del 100% del cargo mensual por los Servicios en un mes calendario determinado.

Todas las solicitudes de crédito deben ser enviadas a IBM dentro de los cinco días siguientes a la finalización del mes, en los cuales tendrá lugar la elegibilidad. La elegibilidad de crédito está sujeta a verificación por parte de IBM.

- a. Recurso para la entrega de correo electrónico - En caso de que IBM no transmita un mensaje de e-mail, y si usted no ha incumplido con las condiciones de la presente Descripción de Servicios,

- b. Recurso de la Disponibilidad de Servicios de correo electrónico - Si la Disponibilidad de Servicios de e-mail está por debajo del 100% en cualquier mes calendario durante el período del contrato, se emitirá un crédito, según se muestra a continuación:

% Disponibilidad de Servicios de correo electrónico por Mes Calendario	Cargo Mensual del Crédito
Menos del 100% pero más del 99.0%	25%
Menos del 99.0% pero más del 98.0%	50%
Menos del 98%	100%
	Finalización de los Servicios, a criterio suyo. Si los Servicios se dan por finalizados, dicha finalización deberá constituir el único y exclusivo recurso en relación a la disponibilidad de los Servicios de menos del 98% en un mes calendario determinado.

- c. Recurso de Latencia de correo electrónico – Si la Latencia de correo electrónico es mayor al promedio de un minuto en cualquier mes calendario durante el período del contrato, se emitirá un crédito, según se muestra a continuación:

Tiempo Promedio de Recorrido Completo	Cargo Mensual del Crédito
Mayor a 1 minuto pero como máximo 1 minuto y 30 segundos	25%
Mayor a 1 minuto y 30 segundos pero como máximo 2 minutos	50%
Mayor a 2 minutos pero como máximo 2 minutos y 30 segundos	75%
Mayor a 2 minutos y 30 segundos	100%

3.3 Servicios de Codificación Limítrofe (Opcional)

Mediante solicitud de su parte, y para cada cargo adicional especificado en la Programación, IBM suministrará los Servicios de Codificación Limítrofe opcionales, como se describen a continuación.

Los Servicios de Codificación Limítrofe (“Codificación Limítrofe”) brindan canales de comunicación codificados designados para permitir la formación de una red de correos electrónicos privada y segura (“SPEN”) con organizaciones asociadas nominadas (“Asociados SPEN”). La Codificación Limítrofe se basa en el estándar del Grupo de Trabajo en Ingeniería de Internet (“IETF”) RFC 3207, Protocolo de Transferencia de Correo Simple (“SMTP”), Extensión de Servicios para SMTP Seguro sobre la Seguridad de la Capa de Transporte (“TLS”) (denominada “STARTTLS”).

3.3.1 Responsabilidades de IBM sobre los Servicios de Codificación Limítrofe

IBM:

- transmitirá correos electrónicos intercambiados por Codificación Limítrofe, entre sus dominios que utilicen Codificación Limítrofe (“dominios nominados”) y Asociados SPEN, sólo mediante conexiones TLS;
- usará SMTP no codificado para entregarle un correo electrónico enviado por usted a una organización no configurada como Asociado SPEN (“Asociado No SPEN”), a menos que se configure en forma diferente;
- hará todos los esfuerzos razonables a nivel comercial para negociar una conexión TLS oportuna con Asociados No SPEN solicitando una conexión TLS para enviarle un correo electrónico a usted. Si el Asociado No SPEN no solicita una conexión TLS, se utilizará SMTP no codificado para entregar el e-mail de Codificación Limítrofe al receptor;
- suministrará su certificado de servidor para autenticación cuando un servidor de correo electrónico externo origine una conexión TLS. Si está configurado de esa manera, la Codificación Limítrofe iniciará, intercambiará y verificará la solicitud de certificación de un cliente. Si no se puede validar un certificado suministrado, se abortará la conexión TLS;
- suministrará su certificado de cliente para autenticación cuando así sea solicitado por un servidor de correo receptor. Si no se puede establecer una conexión TLS, el correo electrónico será devuelto al servidor de correo de origen mediante una conexión TLS, con una razón apropiada por la falla;

- f. para cada certificado entregado por un servidor de correo remoto como parte de una conexión TLS, validará que una autoridad de certificación reconocida haya firmado el certificado, que el mismo no haya expirado, y que la información de dominio de correo electrónico corresponda con la esperada. Si un certificado no puede ser validado, la conexión en cuestión será abortada; y
- g. mantendrá una lista de autoridades de certificación reconocidas con objeto de validación de certificación.

3.3.2 Sus responsabilidades sobre Codificación Limítrofe

Usted acepta:

- a. suministrar a IBM una lista de Socios SPEN;
- b. ofrecer soporte a STARTTLS para hacer más seguros su servidor de correo y los servidores de correo de sus Socios SPEN;
- c. suministrar a IBM una lista de dominios específicos;
- d. garantizar que todos los certificados cumplen con el estándar X.509 v3
- e. en caso de que IBM necesite asignar recursos técnicos adicionales para la entrega de PBE debido a su incumplimiento de las tareas requeridas, pagar cualquier cargo relacionado; y
- f. ser el único responsable de su incumplimiento o el de cualquier tercero (inclusive cualquier Socio SPEN), de sus obligaciones respecto al registro y al mantenimiento de certificados válidos o de la puntualidad o la exactitud de dicha información.

3.3.3 Otros servicios de Codificación Limítrofe

Si usted utiliza la Codificación Limítrofe junto con la Codificación basada en Políticas (como se detalla a continuación), debe implementar el modelo de "Conexión segura" de la Codificación Limítrofe. En tal caso, se aplicarán las siguientes reglas respecto a la ejecución del intercambio de correo codificado:

- todos los intercambios de correo entre usted e IBM deben estar protegidos por la codificación TLS; y
- si la organización de un Socio SPEN le envía un correo electrónico, IBM aceptará la conexión y le enviará el correo electrónico a través de TLS.

Si usted utiliza la Codificación Limítrofe junto con la funcionalidad del sistema de firmas de Antispam de e-mails, se recomienda que incluya todos los dominios de sus Socios SPEN en la lista de remitentes aprobados por el Antispam de e-mails.

Si se suscribe a la "Conexión segura" de la Codificación Limítrofe:

- todo el correo dirigido a su dominio se enviará en formato cifrado; y
- todo el correo enviado desde su(s) dominio(s) especificado(s) será cifrado para que IBM pueda recibirlo. El formato del ruteo continuo (por ej. sin codificación o codificado) se determinará por las ejecuciones TLS que usted especifique y por la capacidad del servidor de destino de recibir correos electrónicos en TLS oportunos.

3.3.4 Limitación de responsabilidades

El único uso para el que la Codificación Limítrofe está destinada es el de permitirle hacer cumplir una política de uso (o su equivalente) de computadoras aceptable, ya existente y efectivamente implementada. El uso de la Codificación Limítrofe en algunos países puede estar sujeto a las leyes vigentes. Usted es responsable de verificar la legislación pertinente antes de implementar la Codificación Limítrofe. IBM no se responsabiliza por ningún inconveniente civil o criminal incurrido por usted como resultado de una operación de la Codificación Limítrofe.

3.4 Servicios de Codificación basados en Políticas

Los servicios Codificación basados en Políticas ("PBE") han sido creados para permitirle enviar y recibir e-mails codificados en base a su política de seguridad de correo electrónico. PBE está disponible únicamente si usted cuenta actualmente con una suscripción a los Servicios de Codificación Limítrofe y al Control del Contenido de Correos electrónicos.

3.4.1 Responsabilidades de IBM por los servicios de Codificación basados en Políticas

IBM:

- a. permitirá que el Control del contenido del correo electrónico defina las políticas de codificado de salida del correo electrónico;
- b. entregará el correo cifrado a través de la bandeja de entrada externa del destinatario;
- c. permitirá que el destinatario tenga acceso al correo cifrado a través de un portal web seguro;
- d. permitirá que el destinatario tenga acceso a un portal web seguro para responder a su correo electrónico en formato cifrado;
- e. le permitirá enviar correo electrónico cifrado directamente a la bandeja de entrada del destinatario sin que éste necesite descargar un programa;
- f. sin perjuicio de lo contrario en esta Descripción de servicios o un contrato relacionado, la provisión de PBE comenzará dentro de cuatro semanas calendario tras la fecha de inicio del período de contrato, que se define como el primer día hábil después de la notificación electrónica de IBM de su aceptación del pedido. Dicho suministro de PBE depende de que usted haya finalizado todas las diligencias técnicas obligatorias.

3.4.2 Sus responsabilidades por los Servicios de Codificación Basados en Políticas

Usted acepta:

- a. proporcionar todos los recursos, informaciones y autorizaciones necesarios para activar o corregir sus servicios de correo DNS para la conectividad con PBE;
- b. contratar un mínimo de 50 usuarios. Cada usuario PBE individual constituirá un usuario de E-mail Content Control;
- c. responsabilizarse por los costos iniciales de instalación y los costos periódicos de PBE branding y PBE branding enterprise. A petición suya, los cambios posteriores en la marca del portal web estarán disponibles con un cargo adicional de \$500 (dólares estadounidenses) por solicitud de cambio;
- d. ser el único responsable de la configuración de PBE en su ambiente y de la exactitud de dicha configuración;
- e. ser el único responsable de la aplicación de la configuración de PBE de acuerdo a sus necesidades. Usted configurará PBE a través de ClientNet mediante la selección de las opciones disponibles en virtud de los servicios de Control del contenido del correo electrónico;
- f. En caso de que IBM necesite asignar recursos técnicos adicionales para la prestación de PBE debido a su incumplimiento de las tareas requeridas, usted acepta pagar los cargos relacionados;
- g. y reconoce que el plazo para proveer pedidos y solicitudes de cambio de PBE será de cuatro semanas a partir de la fecha de aceptación de IBM de tal pedido o solicitud de cambio, siempre y cuando usted haya completado todas las diligencias técnicas obligatorias; y
- h. reconoce que la configuración de PBE está completamente bajo su control y que la exactitud de dicha configuración determinará la precisión de PBE.

3.4.3 Servicios PBE adicionales

- a. Suscribiéndose a "PBE Push Online" de PBE, el destinatario recibirá una notificación por correo electrónico con un anexo cifrado que contiene el correo original. El destinatario podrá ver el correo descifrado online (a través de una sesión SSL segura) en su navegador, haciendo clic en el anexo cifrado e ingresando su contraseña.
- b. Suscribiéndose a la "PBE Push Offline" de PBE, el destinatario recibirá una notificación por correo electrónico con un anexo cifrado que contiene el correo original. Siguiendo el registro inicial en línea, el destinatario podrá visualizar el correo descifrado fuera de línea usando una aplicación Java en su escritorio.
- c. Suscribiéndose a "PBE Pull" de PBE, el destinatario recibirá una notificación por correo electrónico. El destinatario podrá ver el correo descifrado en línea (a través de una sesión SSL segura) en su navegador, ingresando en el portal web seguro e ingresando su contraseña.

- d. Suscribiéndose a “PBE Compose” de PBE, el destinatario de un correo electrónico cifrado podrá enviar un nuevo correo electrónico a cualquiera de sus usuarios PBE.
- e. Suscribiéndose a “PBE Branding Enterprise” de PBE, usted también recibirá “PBE Branding” y “PBE Compose”.
- f. Suscribiéndose a “PBE Combo” de PBE, el Control del contenido del correo electrónico seleccionará el método de codificación (p.ej, “PBE Pull”, “PBE Push Online” o “PBE Push Offline”) según la regla de Control de contenido de correo electrónico que usted ha determinado.

3.4.4 Limitaciones de los servicios

- a. La cantidad de correos electrónicos seguros que usted puede enviar usando PBE en cualquier mes calendario no puede exceder 100 veces el uso registrado de PBE. Al enviar a varios destinatarios, cada dirección se contará como un correo electrónico seguro. En caso de que usted exceda la cantidad de correos electrónicos seguros permitidos en un determinado mes calendario, IBM aumentará el uso registrado y, a su entera discreción, modificará adecuadamente sus facturas posteriores.
- b. Los correos electrónicos enviados a través de PBE se limitan a un tamaño máximo de 15 MB por correo electrónico (comprimido).
- c. El Contrato de nivel de servicio de latencia de correos electrónicos no se aplica a PBE.

3.4.5 Limitación de responsabilidades

Usted reconoce y acuerda que la codificación de correos electrónicos a través del uso de PBE se realizará en los Estados Unidos y que IBM no puede aceptar responsabilidad alguna por cualquier incumplimiento de la legislación o reglamento aplicable en todo el mundo. IBM no se responsabiliza por cualquier daño o pérdida resultante directa o indirectamente de un incumplimiento por parte de PBE de sus obligaciones de codificación.

3.5 E-mail Antivirus

Si ha seleccionado este servicio, IBM le proporcionará un E-mail Antivirus que le ayudará a detectar los virus existentes en su correo electrónico y sus anexos entrantes y salientes. El E-mail Antivirus se limita al número de usuarios especificados en la Programación.

3.5.1 Responsabilidades de IBM por el E-mail Antivirus

Actividad 1 - Inicialización y notificación

IBM:

- a. proporcionará al remitente, al destinatario y, si así usted lo solicita en su perfil, al administrador de correo electrónico, alertas automáticos de los mensajes de correo electrónico o los anexos que contengan un virus;
- b. Si ha seleccionado desactivar las notificaciones, enviará el correo electrónico infectado con virus a un servidor seguro, diseñado para destruirlo automáticamente después de 30 días;
- c. a pedido suyo, y bajo circunstancias excepcionales, liberará un correo electrónico que pueda ser liberable a través de la herramienta de gestión, desde el servidor seguro a la dirección de correo electrónico del destinatario que se pretendía originalmente (o a las direcciones si se trata del nombre o el seudónimo de correo electrónico de un grupo), o redireccionará el correo electrónico infectado hacia una dirección de correo electrónico alternativa al recibir el formulario de autorización de liberación adecuado;
- d. conservar un correo electrónico entrante infectado con virus que haya sido determinado como particularmente infeccioso o dañino por IBM;
- e. notificarle acerca de correos electrónicos infectados con virus que hayan sido detectados aunque no interceptados por el E-mail Antivirus, y proporcionarle la información suficiente para permitirle eliminar dicho e-mail; y/o
- f. configurar la herramienta de gestión para generar informes semanales o mensuales, según lo seleccione usted en su perfil.

Actividad 2 - Soporte técnico y continuo

Durante el período de contrato, IBM:

- a. no transmitirá ni liberará intencionalmente, y dará instrucciones a sus subcontratistas involucrados en el E-mail Antivirus para que no transmitan ni liberen intencionalmente, ningún correo infectado por virus conocido o sospechoso a terceros, a menos que sea a IBM, a sus subcontratistas o a cualquier empleado de aplicación de la ley o a las entidades que participan en la detección y en la protección contra virus; y
- b. en caso de que el E-mail Antivirus sea suspendido o discontinuado por cualquier motivo, revertirá cualquier cambio importante de la configuración que se haya realizado en el momento de proporcionar el E-mail Antivirus, y será de su responsabilidad llevar a cabo todos los cambios necesarios en la configuración de sus servidores de correo electrónico, así como informar a su proveedor de servicios de Internet ("ISP") sobre la necesidad de redireccionar el correo electrónico entrante.

3.5.2 Sus responsabilidades sobre el E-mail Antivirus

Usted acepta:

- a. asumir la principal responsabilidad por todos los cambios en la configuración y en las operaciones y gestión de la cuarentena de correos electrónicos. En caso de necesitar asistencia, usted acepta:
 - (1) notificar de inmediato a IBM si necesita que las modificaciones sean desactivadas; o
 - (2) notificar inmediatamente a IBM si necesita la liberación del correo electrónico desde el servidor seguro (que la configuración propietaria basada en Internet y la herramienta de gestión y de informes muestran como liberable) al destinatario que se pretendía originalmente; y
- b. tomar todas las medidas necesarias para garantizar que usted y las personas que envíen correos electrónicos desde los dominios cubiertos por el Antivirus de correos electrónicos estén conscientes de las responsabilidades que tienen con respecto a la protección de datos y las leyes y/o normas de privacidad.

3.5.3 Contratos de nivel de servicio

Además de los contratos de nivel de servicio (SLA) generales descritos anteriormente, los siguientes SLA comprenden las métricas medidas para la entrega de antivirus de correos electrónicos. Los únicos recursos dispuestos para el incumplimiento de estos SLAs se especifican en la sección titulada "Soluciones de SLA", a continuación.

Los recursos de SLA están disponibles siempre que usted cumpla con sus obligaciones tal como se define en esta Descripción de servicios.

SLAs

- Detección de virus: el E-mail Antivirus detectará el 100% de los virus contenidos en los correos electrónicos analizados. Se considerará que sus sistemas están infectados si se ha activado un virus contenido en un mensaje de correo electrónico y recibido a través del Antivirus de correos electrónicos dentro de sus sistemas.

Si se detecta un mensaje de correo electrónico infectado por virus pero no se lo detiene, IBM puede notificarle inmediatamente y proporcionarle información suficiente para que usted pueda identificar y eliminar el correo electrónico infectado por el virus. Si se impide la infección, no se aplicará este SLA. Si usted no actúa con prontitud ante el aviso de un correo infectado por virus, no se aplicará este SLA.

- Tasa de captura de falsos positivos de virus: la tasa de captura de falsos positivos de virus no excederá el 0,0001% del total de su tráfico de correo electrónico en un mes calendario determinado.

Recursos de SLA

El único recurso ante el incumplimiento de cualquiera de los SLAs descritos en la sección titulada "SLAs" durante cualquier mes calendario será un crédito. Usted puede obtener no más de un crédito por cada SLA por día, que no supere un total de \$10.000 (dólares estadounidenses), o su equivalente en moneda local, para todos los SLAs, en un determinado mes calendario.

- Recurso de detección de virus: si IBM no cumple con el SLA de detección de virus, se otorgará un crédito por los cargos que se apliquen para un mes de tarifa de monitoreo Antivirus de correos electrónicos, o \$10.000 (dólares estadounidenses), según cuál monto sea menor.

Dicho crédito se aplicará sólo si usted ha notificado previamente a IBM, y en caso de que IBM haya confirmado y registrado que el virus atravesó el Antivirus de correos electrónicos. Este recurso es el único recurso exclusivo por cualquier infección de virus que haya sido transmitida a usted a través de los servicios de E-mail Antivirus. Este recurso no se aplicará a ninguna auto-infección deliberada.

IBM analizará todos los correos electrónicos y anexos posibles. Puede no ser posible analizar los anexos cuyo contenido se encuentre bajo el control directo del remitente (por ejemplo, anexos protegidos por contraseña o codificación). Dicho correo electrónico y sus anexos se excluyen de este SLA.

- Recurso de tasa de captura de falsos positivos de virus: si la tasa de captura de falsos positivos de virus excede el 0,0001% del total de su tráfico de correo electrónico en un determinado mes calendario, se le otorgará un crédito por los cargos que se aplican durante un mes de tasa de control de Antivirus de correos electrónicos, como se especifica a continuación.

Porcentaje de tasa de captura de falsos positivos de virus (durante el mes calendario)	Porcentaje de crédito de cargo mensual
Mayor que 0,0001% pero al menos 0,001%	25
Mayor que 0,003% pero al menos 0,03%	50
Mayor que 0,03% pero al menos 0,3%	75
Mayor que 0,3%	100

3.6 E-mail Image Control

Si usted lo ha seleccionado este servicio, IBM le brindará el servicio de E-mail Image Control para ayudarlo a detectar imágenes pornográficas contenidas en los archivos de imágenes en su correo electrónico y adjuntos entrantes o salientes. El E-mail Image Control se encuentra limitado a la cantidad de Usuarios que se especifican en el Programa.

IBM destaca que usted tiene completo control de la configuración del E-mail Image Control. El E-mail Image Control está diseñado para ser utilizado expresamente con el fin de permitirle poner en práctica una política existente del uso de la computadora (o su equivalente) que sea aceptable y que se pueda implementar de manera efectiva.

3.6.1 Responsabilidades de IBM respecto del E-mail Image Control

Activity 1 - Inicio y Notificación

IBM:

- Realizará un escaneo de su correo electrónico entrante y saliente de Internet respecto de imágenes potencialmente pornográficas contenidas en los archivos de imágenes adjuntos a un mensaje de correo electrónico.
- Pondrá opciones a su disposición con el fin de que usted determine las acciones a seguir frente a la detección de una imagen pornográfica sospechosa, a saber:
 - Sólo registrar;
 - Identificar dicho correo electrónico dentro de su encabezado (sólo para correo electrónico entrante);
 - Copiar dicho correo electrónico a una dirección predeterminada de correo electrónico;
 - Redireccionar dicho correo electrónico a una dirección predeterminada de correo electrónico; y
 - Eliminar dicho correo electrónico; y
- Proporcionará alertas automáticas al remitente y, si se tratara de un correo electrónico entrante, proporcionará alertas al receptor acerca de un correo electrónico entrante o adjunto que pudiera contener una imagen pornográfica sospechosa.

Activity 2 - Soporte técnico y continuo

Durante el período del contrato, IBM:

- a. No almacenará ningún elemento sospechoso de contener una imagen pornográfica, bajo ninguna circunstancia; y
- b. En caso de suspender o dar por finalizado el servicio de Control de imágenes por correo electrónico por cualquier motivo, IBM revocará todos los cambios relevantes de configuración realizados al momento de establecer el servicio de Control de imágenes por correo electrónico y será su responsabilidad realizar todos los cambios necesarios de configuración a sus servidores de correo electrónico, e informar a su PSI respecto de la necesidad de redirigir el correo electrónico entrante.

3.6.2 Sus responsabilidades respecto del E-mail Image Control

Usted acepta:

- a. Establecer las opciones de configuración para el E-mail Image Control para sus dominios, de conformidad con sus necesidades. Existen opciones disponibles para especificar el nivel de sensibilidad de detección de pornografía. La sensibilidad puede establecerse como alta, media o baja. Se detectarán más imágenes pornográficas a un nivel alto de sensibilidad y se detectarán menos imágenes pornográficas a un nivel bajo de sensibilidad. Sin embargo, la determinación de lo que constituye imágenes pornográficas es subjetiva. Por lo tanto, el nivel de detección pornográfica no puede ser medido con precisión; y
- b. Tomar todas las medidas necesarias para asegurar que usted, y todas aquellas personas que envíen correos electrónicos desde los dominios cubiertos por el E-mail Image Control, tomen conocimiento de todas las responsabilidades que usted tiene con respecto a las leyes y/o normas de protección y privacidad de datos.

3.7 E-mail Antispam

Si usted lo ha seleccionado este servicio, IBM le brindará el servicio de E-mail Antispam con el fin de ayudarlo a protegerse del correo electrónico no deseado mediante un escaneo de su correo electrónico y adjuntos entrantes de Internet para detectar el correo no deseado y manejarlo de conformidad con las pautas predeterminadas. El E-mail Antispam se encuentra limitado a la cantidad de Usuarios que se especifican en el Programa.

3.7.1 Responsabilidades de IBM respecto del E-mail Antispam

Activity 1 - Inicio y Notificación

IBM:

- a. Le brindará la capacidad de configurar una lista negra. Si selecciona este método de detección y recibe un correo electrónico entrante proveniente de un dominio enumerado en la lista negra, se seguirá una acción tal como se encuentre definido en las opciones de configuración establecidas por usted en su perfil;
- b. Le brindará la capacidad de configurar una lista blanca. Si selecciona este método de detección y recibe un correo electrónico entrante proveniente de un dominio enumerado en la lista blanca, dicho correo electrónico eludirá automáticamente cualquier otro método de detección de correo no deseado.
- c. Al activar el E-mail Antispam, iniciará la acción de correo no deseado como “eliminación del correo no deseado”. Usted puede solicitar una opción diferente con anterioridad a la activación del E-mail Antispam, o puede modificar esta opción ingresando a la herramienta de administración de Internet. Se encuentran disponibles las siguientes opciones para determinar la acción a seguir al momento de detectarse un correo no deseado:
 - (1) Rotular el correo no deseado dentro de su encabezado (el correo no deseado continúa siendo enviado al destinatario designado);
 - (2) Redireccionar el correo no deseado a una dirección predeterminada de correo electrónico;
 - (3) Poner en cuarentena el correo no deseado; o
 - (4) Eliminar el correo no deseado;
- d. Si selecciona la opción de “Poner en cuarentena el correo no deseado”, se le brindará un servicio de Cuarentena del correo no deseado para cada uno de los dominios que usted especifique. La opción por defecto de notificar al Usuario que el correo no deseado ha sido almacenado se

- (1) Notificaciones a recibir diariamente;
- (2) Notificaciones a recibir en diferentes intervalos; o
- (3) No se reciben notificaciones.

Activity 2 - Soporte técnico y continuo

Durante el período del contrato, IBM:

- a. Almacenará el correo no deseado sospechoso durante un período máximo de 14 días luego de lo cual será eliminado automáticamente;
- b. Brindará el servicio de Cuarentena del correo no deseado a un Usuario luego de que usted haya configurado cada dominio de conformidad con sus necesidades;
- c. Configuraré el servicio de Cuarentena del correo no deseado de la cuenta del Usuario de modo que el Usuario tenga acceso a la misma;
- d. Rotulará y enviará el correo no deseado sospechoso al destinatario, si por alguna razón el servicio de Cuarentena del correo no deseado no permite aceptar correo electrónico; y
- e. En caso de suspender o dar por finalizado el servicio de E-mail Antispam por cualquier motivo, IBM revocará todos los cambios relevantes de configuración realizados al momento de establecer el servicio de E-mail Antispam y será su responsabilidad realizar todos los cambios necesarios de configuración a sus servidores de correo electrónico, e informar a su PSI respecto de la necesidad de redirigir el correo electrónico entrante.

3.7.2 Sus responsabilidades respecto del E-mail Antispam

Usted acepta:

- a. Hacerse responsable por los cambios realizados en la opción por defecto del correo no deseado (“eliminación del correo no deseado”) a través de la herramienta de manejo de Internet, si es que desea otra opción;
- b. Establecer las opciones de configuración del E-mail Antispam para sus dominios, de conformidad con sus necesidades.
- c. Asumir la responsabilidad principal respecto de todos los cambios de configuración, y operaciones y administración de Cuarentena del correo electrónico. Si usted solicita asistencia, acuerda:
 - (1) Notificar a IBM de manera inmediata en caso de necesitar desactivar las notificaciones; o
 - (2) Notificar a IBM de manera inmediata en caso de solicitar la divulgación de un correo electrónico por parte del servidor seguro (mostrado como autorizado a ser divulgado por la configuración propietaria basada en Internet, la herramienta de administración y reporte), al destinatario a quien dicho correo electrónico iba dirigido originalmente.
- d. Tomar todas las medidas necesarias para asegurar que usted, y todas aquellas personas que envíen correos electrónicos desde los dominios cubiertos por el E-mail Antispam, tomen conocimiento de todas las responsabilidades que usted tiene con respecto de las leyes y/o normas de protección y privacidad de datos.

3.7.3 Contratos de nivel de servicio

Además de los SLAs generales que se describen más arriba, los siguientes SLAs abarcan las métricas de medición para el envío del E-mail Antispam. Los únicos recursos de reparación por el incumplimiento de estos SLAs se especifican en la sección titulada “Recursos de reparación de un SLA”, a continuación. Los recursos de un SLA se encuentran disponibles siempre y cuando usted cumpla con sus obligaciones tal como se define en esta Descripción de servicios.

SLAs

- Índice de captura del correo no deseado – el E-mail Antispam detectará el 99% del correo no deseado contenido en el correo electrónico escaneado.

Se aplicará un Índice más bajo de captura del correo no deseado al correo electrónico que contenga caracteres asiáticos. En caso de que dicho Índice de captura del correo no deseado se encuentre por debajo del 99%, usted tiene derecho a una acreditación del 25% de su cargo

mensual. En caso de que dicho Índice de captura del correo no deseado se encuentre por debajo del 96%, usted tiene derecho a una acreditación del 100% de su cargo mensual.

El SLA del Índice de captura del correo no deseado no es aplicable si:

- (1) Usted no hubiera implementado los ajustes recomendados para el E-mail Antispam; o
 - (2) El mensaje de correo electrónico no hubiera sido enviado a una dirección legítima.
- Índice de captura de correo no deseado positivo falso – el Índice de captura de correo no deseado positivo falso no excederá el 0,0003% de su tráfico de correo electrónico total en un determinado mes calendario.

Los siguientes correos electrónicos se encuentran excluidos de la garantía del Índice de captura de correo no deseado positivo falso:

- (1) Correo electrónico que no constituye un correo electrónico legítimo del negocio;
- (2) Correo electrónico que contiene más de 20 destinatarios;
- (3) Correo electrónico de remitentes que se encuentran en su lista de remitentes bloqueados, incluyendo a aquellos definidos como Usuarios individuales, si usted ha activado los ajustes de nivel del Usuario;
- (4) Correo electrónico enviado desde una máquina comprometida;
- (5) Correo electrónico enviado desde una máquina que se encuentra enumerada en el listado de remitentes bloqueados de un tercero;
- (6) Correo electrónico enviado a más de 20 destinatarios y que posee al menos 80% del mismo contenido.

El crédito será otorgado sólo para el correo electrónico positivo falso que envíe a support@message-labs.com dentro de los cinco días posteriores a la recepción del mensaje de correo electrónico.

Recursos de SLA

Se otorgará un crédito a modo de único recurso por el incumplimiento de cualquiera de los SLAs que se describen en la sección titulada "SLAs", durante cualquier mes calendario determinado. Usted no puede obtener más de un crédito por cada SLA por día y no debe exceder un total de US\$ 10.000, o el equivalente en su moneda local, en un determinado mes calendario.

- Recurso de reparación del índice de captura de correo no deseado – En caso de que IBM no cumpla con el SLA del índice de captura del correo no deseado, se otorgará un crédito por todo o parte del cargo mensual correspondiente al servicio de E-mail Antispam, tal como se indica en la tabla a continuación, o US\$ 10.000, según el monto menor.

Índice de captura de correo no deseado durante el mes calendario	Cargo mensual a ser acreditado
Mayor a 98% y menor al 99%	25%
Mayor a 97% y menor a 98%	50%
Mayor a 96% y menor a 97%	75%
Menor a 96%	100%

- Recurso del índice de captura de correo no deseado positivo falso – En caso de que IBM no cumpla con el SLA del índice de captura del correo no deseado positivo falso, se otorgará un crédito por todo o parte del cargo mensual correspondiente al servicio de E-mail Antispam, tal como se indica en la tabla a continuación.

Índice de captura de correo no deseado positivo falso (durante un mes calendario)	Crédito del cargo mensual
Mayor a 0,0003% y 0,003% como máximo	25%
Mayor a 0,003% y 0,03% como máximo	50%
Mayor a 0,03% y 0,3% como máximo	75%
Mayor a 0,3%	100%

3.8 E-mail Content Control

Si usted lo ha seleccionado en el Programa, IBM le brindará el servicio de E-mail Content Control para su correo electrónico que se encuentre de acuerdo con la política aceptable del uso de la computadora (o su equivalente). El E-mail Content Control se encuentra limitado a la cantidad de Usuarios que se especifican en el Programa.

E-mail Content Control le permitirá construir una serie de normas (de aquí en adelante denominadas “normas”) mediante las cuales se filtra el correo electrónico entrante y saliente de Internet. IBM destaca que usted tiene completo control de la configuración del E-mail Content Control. La exactitud de las normas y la configuración determinarán la precisión del servicio de E-mail Content Control. El E-mail Content Control está diseñado para ser utilizado expresamente con el fin de permitirle poner en práctica una política existente del uso de la computadora (o su equivalente) que sea aceptable y que se pueda implementar de manera efectiva.

Si el servicio de E-mail Content Control se utiliza en conjunto con la acción de Cuarentena de los servicios de E-mail Antispam, esto podría ocasionar que un correo electrónico no deseado se ponga en Cuarentena antes de ser filtrado por el E-mail Content Control.

3.8.1 Responsabilidades de IBM respecto del E-mail Content Control

Activity 1 - Inicio y Notificación

IBM:

- a. Le proporcionará la capacidad de ayudarlo a configurar su propia estrategia de filtro de correo electrónico basada en sus reglas, de conformidad con su política aceptable del uso de la computadora (o su equivalente);
- b. Le proporcionará listados de palabras sugeridas (denominado “Listados de palabras”) que usted puede utilizar para crear las reglas;
- c. Escaneará tanto correo electrónico y sus adjuntos como sea posible, en base a las reglas y a su configuración. Puede que no resulte posible escanear adjuntos con contenido bajo el control directo del remitente; y
- d. Pondrá a su disponibilidad opciones para determinar las acciones a seguir al momento de detectar un correo electrónico sospechoso de reunir los criterios de las reglas, lo cual deberá estar de acuerdo con su política aceptable del uso de la computadora. Las opciones incluyen lo siguiente:
 - (1) Rotular el correo electrónico dentro de los encabezados del correo electrónico;
 - (2) Redireccionar el correo electrónico a una dirección de correo electrónico predeterminada;
 - (3) Copiar el correo electrónico a una dirección de correo electrónico predeterminada;
 - (4) Comprimir los adjuntos del correo electrónico;
 - (5) Registrarse sólo a la herramienta propietaria de administración y reporte basada en Internet; y
 - (6) Eliminar el correo electrónico.

Activity 2 - Soporte técnico y continuo

En caso de suspender o dar por finalizado el servicio de Control E-mail Content Control por cualquier motivo durante el período del contrato, IBM revocará todos los cambios relevantes de configuración realizados al momento de establecer el servicio de E-mail Content Control y será su responsabilidad realizar todos los cambios necesarios de configuración a sus servidores de correo electrónico, e informar a su PSI respecto de la necesidad de redirigir el correo electrónico entrante.

3.8.2 Sus responsabilidades respecto del E-mail Content Control

Usted acepta:

- a. Revelar los Listados de palabras solo a aquellas personas en su empresa que se encuentren involucradas en los asuntos que se detallan a continuación y que tienen una necesidad específica de tomar conocimiento. Usted toma conocimiento de que los Listados de palabras podrían ser considerados ofensivos y acepta indemnizar a IBM y a sus subcontratistas por todo daño (incluyendo gastos razonables y los honorarios de un abogado) que pudiera ser ocasionado a un tercero (incluyendo a todos sus empleados) con respecto a todo reclamo o acción que surja del hecho de que IBM o sus subcontratistas le proporcionen los Listados de palabras;
- b. Permitir que IBM recopile y publique listados de palabras por defecto utilizando las reglas o palabras obtenidas de sus listados de palabras;
- c. Asistir a un curso de capacitación acerca de la configuración del E-mail Content Control;
- d. Asumir la responsabilidad principal por la divulgación de correo electrónico, mostrado como autorizado a ser divulgado desde el servidor seguro al destinatario a quien iba dirigido

- e. Establecer las opciones de configuración del E-mail Content Control para cada uno de sus dominios, de conformidad con sus necesidades; y
- f. Tomar todas las medidas necesarias para asegurar que usted, y todas aquellas personas que envíen correos electrónicos desde los dominios cubiertos por el E-mail Content Control, tomen conocimiento de, y cumplen con, todas las responsabilidades u obligaciones que usted tiene con respecto a las leyes y/o normas de protección y privacidad de datos.