Condiciones de Uso de IBM – Condiciones Específicas de la Oferta SaaS

IBM MobileFirst Protect (SaaS)

Las Condiciones de Uso ("CDU") constan de estas Condiciones de Uso de IBM - Condiciones Específicas de la Oferta SaaS ("Condiciones Específicas de la Oferta SaaS") y un documento con el título Condiciones de Uso de IBM - Condiciones Generales ("Condiciones Generales") disponible en el URL siguiente: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

En caso de conflicto, los Términos de Oferta específicos de SaaS prevalecen sobre las Condiciones Generales. Al hacer un pedido, acceder o utilizar SaaS IBM, el Cliente acepta las Condiciones de Uso.

Las Condiciones de Uso se rigen por el Acuerdo Internacional Passport Advantage de IBM, el Acuerdo Internacional Passport Advantage Express de IBM o el Acuerdo Internacional de IBM para Ofertas Seleccionadas de SaaS IBM, según proceda ("Acuerdo") y conjuntamente con las Condiciones de Uso conforman el acuerdo completo.

1. SaaS IBM

Las siguientes ofertas de SaaS IBM están cubiertas por estas Condiciones Específicas de la Oferta de SaaS:

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Management Suite (SaaS)
- IBM MobileFirst Protect – Management Suite (SaaS) Step up para Clientes actuales

- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Secure Mail (SaaS)
- IBM MobileFirst Protect – Secure Mail (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) Step up para Clientes actuales
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

2. IBM MaaS360 Professional Bundle Prime (SaaS) Charge Metrics

SaaS IBM se vende bajo una de las siguientes métricas de cargo según se especifica en el Documento Transaccional:

a. **Usuario Autorizado**: es una unidad de medida con la que se puede adquirir SaaS IBM. El Cliente debe obtener derechos de titularidad independientes y dedicados para cada Usuario Autorizado al que se permita acceso a SaaS IBM de cualquier modo, ya sea directo o indirecto (por ejemplo, a través de un programa multiplexor, un dispositivo o un servidor de aplicaciones) mediante cualquier método. Deben adquirirse derechos de titularidad suficientes para cubrir el número de Usuarios Autorizados con acceso a SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o Documento Transaccional del Cliente.

b. **Gigabyte**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un Gigabyte se define como 2 a la 30.º potencia bytes de datos (1.073.741.824 bytes). Deben adquirirse derechos de titularidad suficientes para cubrir el número total de Gigabytes procesados por SaaS IBM durante el período de medida especificado en un Documento de Titularidad (POE) o Documento Transaccional.

c. **Dispositivo de Cliente Gestionado**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un Dispositivo de Cliente es un único dispositivo informático de usuario, un sensor de finalidad especial o un dispositivo de telemetría que solicita la ejecución de, o que recibe para su ejecución, un conjunto de mandatos, procedimientos o aplicaciones de, o que proporciona datos a, otro sistema informático al que se hace referencia normalmente como servidor o que es gestionado de cualquier otra manera por el servidor. Distintos Dispositivos de Cliente pueden compartir el acceso a un servidor común. Un Dispositivo de Cliente puede tener cierta capacidad de procesado o se puede programar para que el usuario pueda trabajar con el mismo. El Cliente debe obtener derechos de titularidad de Dispositivo de Cliente Gestionado para cada Dispositivo Cliente gestionado por el SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o Documento Transaccional del Cliente.

d. **Dispositivo de Cliente**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un Dispositivo de Cliente es un único dispositivo informático de usuario, un sensor de finalidad especial o un dispositivo de telemetría que solicita la ejecución de, o que recibe para su ejecución, un conjunto de mandatos, procedimientos o aplicaciones de, o que proporciona datos a, otro sistema informático al que se hace referencia normalmente como servidor o que es gestionado de cualquier otra manera por el servidor. Distintos Dispositivos de Cliente pueden compartir el acceso a un servidor común. Un Dispositivo de Cliente puede tener cierta capacidad de procesado o se puede programar para que el usuario pueda trabajar con el mismo. El Cliente debe obtener derechos de titularidad para cada Dispositivo de Cliente que ejecute, proporcione datos a, utilice los servicios que proporciona, o al que acceda de otro modo SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) del Cliente o en el Documento Transaccional.

3. Cargos y Facturación

El importe que se debe abonar para SaaS IBM se especifica en un Documento Transaccional.

3.1 Cargo Mensual Parcial

Puede evaluarse un cargo mensual parcial, según lo especificado en el Documento Transaccional, sobre una base prorrateada.

3.2 Cargo por Uso en Exceso

Si el uso actual del SaaS IBM por parte del Cliente durante el período de medida supera los derechos de titularidad especificados en el Documento de Titularidad (POE), se facturará al Cliente por el uso en exceso, según se establece en el Documento Transaccional.

4. Opciones de Renovación del Plazo de Suscripción de SaaS IBM

El Documento de Titularidad (POE) del Cliente establecerá si SaaS IBM se renovará al finalizar el Plazo de Suscripción, designando el plazo como uno de los siguientes:

4.1 Renovación Automática

Si el Documento de Titularidad (POE) del Cliente establece que la renovación del Cliente es automática, el Cliente podrá terminar el Plazo de Suscripción de SaaS IBM que vence mediante solicitud por escrito al representante de ventas o Business Partner de IBM del Cliente, con una antelación mínima de noventa (90) días antes de la fecha de vencimiento establecida en el POE. Si IBM o su Business Partner de IBM no recibe dicho aviso de terminación antes de la fecha de vencimiento, el Plazo de Suscripción que vence se renovará automáticamente por el plazo de un año o por la misma duración que el Plazo de Suscripción original establecido en el POE.

LA CANTIDAD DEL DERECHO DE TITULARIDAD DE RENOVACIÓN SERÁ IGUAL AL IMPORTE MAYOR ENTRE LA CANTIDAD DEL PEDIDO ORIGINAL O EL USO INFORMADO MENSUAL PARA EL MES ANTERIOR A LA GENERACIÓN DE LA FACTURA DE RENOVACIÓN A MENOS QUE IBM RECIBA UNA NOTIFICACIÓN QUE ESPECIFIQUE UNA CANTIDAD DE DERECHO DE TITULARIDAD DISTINTA.

LA CANTIDAD DEL DERECHO DE TITULARIDAD DE RENOVACIÓN PARA LA OFERTA STEP UP SERÁ IGUAL A LA CANTIDAD DEL PEDIDO ORIGINAL.

4.2 Facturación Continua

Si el POE indica que la renovación del Cliente es continua, el Cliente seguirá teniendo acceso a SaaS IBM y se le facturará por el uso de SaaS IBM en base a una facturación continua. Para dejar de utilizar SaaS IBM y detener el proceso de facturación continua, el Cliente deberá proporcionar a IBM o a su Business Partner de IBM un aviso de solicitud por escrito de cancelación de SaaS IBM del Cliente, con una antelación mínima de noventa (90) días. Una vez que el Cliente haya cancelado el acceso, se facturarán al Cliente los cargos de acceso correspondientes al mes en el que se llevó a cabo la cancelación.

4.3 Renovación Necesaria

Si el POE indica que el tipo de renovación del Cliente es "terminar", SaaS IBM se terminará al final del Plazo de Suscripción y el acceso del Cliente a SaaS IBM se eliminará. Para seguir utilizando SaaS IBM más allá de la fecha de finalización, el Cliente deberá realizar un pedido al representante de ventas de IBM del Cliente o al Business Partner de IBM para adquirir un nuevo Plazo de Suscripción.

5. Soporte Técnico

El Soporte Técnico para SaaS IBM es un soporte de segundo nivel estructurado para un equipo de Operaciones de un Cliente, no un soporte para Usuarios Finales, y está disponible durante el período de suscripción.

El soporte se proporciona a través de diversos canales; 24 x 7. La información relativa al soporte para la solución SaaS IBM está disponible en el portal del producto.

Destinos de Capacidad de Respuesta Prevista:

Severidad	Definición de Severidad	Inicial Objetivos de Tiempo de Respuesta	Cobertura de Tiempo de Respuesta
1	**Impacto de negocio crítico / caída del servicio:** La función de impacto de negocio no está operativa o la interfaz crítica ha fallado. Esto se aplica normalmente a un entorno de producción e indica una incapacidad de acceso a los servicios, que causa un impacto crítico en las operaciones. Esta condición requiere una solución inmediata.	30 minutos	24x7
2	**Impacto de negocio elevado:** El uso de una característica de negocio del servicio o una función del servicio está muy restringido o el Cliente corre el riesgo de pasarse las fechas límite.	1 hora laborable	24 x 7
3	**Impacto de negocio medio:** Indica que el servicio o la función no se pueden utilizar y no significa un impacto de negocio crítico en las operaciones.	2 horas laborales	24 x 7
4	**Impacto de negocio bajo:** Una consulta o una solicitud no técnica	3 horas laborales	24 x 7

6. Condiciones Adicionales de la Oferta de SaaS IBM

6.1 Limitación de Step-up

Para la oferta SaaS IBM designada como "Step up para Clientes actuales" ("Step up SaaS") el Cliente debe haber adquirido previamente o simultáneamente derechos de titularidad de licencia adecuados para el programa de IBM asociado, según se identifica en el nombre de la oferta Step up SaaS. Por ejemplo, un Cliente que adquiera "IBM MobileFirst Protect – Devices (SaaS) - Step up para Clientes actuales" debe tener derechos de titularidad con licencia para el programa de IBM asociado de IBM MobileFirst Protect. Los derechos de titularidad del Cliente para Step up SaaS no pueden superar los derechos de titularidad del Cliente en el programa de IBM asociado.

Al adquirir Step up SaaS, el Cliente no puede utilizar los mismos derechos de titularidad de licencia de programa de IBM asociado en los entornos instalados en sus locales que los derechos de titularidad de Step up SaaS. Por ejemplo, si el Cliente tiene 250 derechos de titularidad de Dispositivo de Cliente Gestionado para el programa de IBM asociado y elige adquirir 100 derechos de titularidad de Dispositivo de Cliente Gestionado para Step up SaaS, el Cliente puede gestionar 100 Dispositivos de Cliente Gestionado para Step up SaaS desde el entorno SaaS IBM y 150 Dispositivos de Cliente Gestionado desde el software instalado en sus instalaciones.

El Cliente manifiesta que el Cliente ha adquirido (1) los derechos de titularidad de licencia y (2) la Suscripción y Soporte necesarios para los programas de IBM asociados. Durante el Período de Suscripción de Step up SaaS, el Cliente deberá mantener la Suscripción y el Soporte para los derechos de titularidad del programa de IBM asociado utilizados junto con los derechos de titularidad de Step up SaaS. En el caso de que se resuelva la licencia del Cliente para utilizar el programa de IBM asociado o la

Suscripción y el Soporte para los programas de IBM asociados, el derecho de uso de Step up SaaS por parte del Cliente también se resolverá.

6.2 Cookies

El Cliente acepta que IBM puede utilizar cookies y tecnologías de seguimiento para recoger datos de Carácter Personal con el fin de recopilar información y estadísticas de uso diseñadas para ayudar a mejorar la experiencia del usuario y/o personalizar las interacciones con los usuarios de acuerdo con lo establecido en http://www-01.ibm.com/software/info/product-privacy/index.html.

6.3 Transferencias entre Fronteras

Si el Cliente pone Información Personal a disposición para ofertas de SaaS IBM en los Estados Miembros de la UE, Islandia, Liechtenstein, Noruega o Suiza, Turquía y cualquier otro país europeo que haya promulgado alguna legislación local de protección o privacidad de datos, el Cliente acepta que IBM puede procesar el Contenido, incluyendo cualquier Información Personal, conforme a las leyes y requisitos pertinentes a través de una frontera del país a los procesadores y subprocesadores en los siguientes países de fuera del Espacio Económico Europeo y los países considerados por la Comisión Europea como poseedores de niveles adecuados de seguridad:

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
IBM Corporation	Subencargado del tratamiento	1 New Orchard Rd. Armonk, NY 10504, EE.UU.
IBM India Private Limited	Subencargado del tratamiento	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 India

El Cliente acepta que IBM puede, bajo aviso previo, modificar esta lista de países cuando razonablemente lo determine necesario para el aprovisionamiento de los SaaS IBM.

6.4 Privacidad de Datos en la UE

Si el Cliente pone datos personales a disposición para ofertas SaaS IBM en los Estados Miembros de la UE, Islandia, Liechtenstein, Noruega, Suiza, Turquía y cualquier otro país europeo que haya promulgado alguna legislación local de protección o privacidad de datos, o si el Cliente ha autorizado a usuarios o dispositivos en estos países, el Cliente como controlador único nombra a IBM como procesador para procesar (tal como se definen estos términos en la Directiva 95/46/CE) Información Personal. IBM solo tratará esta Información Personal en la medida en la que sea necesario para que el SaaS IBM esté disponible, de acuerdo con las descripciones publicadas por IBM del SaaS IBM, y el Cliente acepta que cualquier tratamiento de este tipo está en conformidad con sus propias instrucciones.

6.5 Conformidad con Safe Harbor

Las ofertas SaaS IBM se incluyen en la certificación de Safe Harbor entre EE.UU. y la UE ("US-EU Safe Harbor") de Fiberlink Communications Corporation (subsidiaria de IBM). IBM y Fiberlink acatan el Acuerdo de Safe Harbor entre EE.UU. y la UE establecido por el Departamento de Comercio de Estados Unidos en relación con la obtención, el uso y la retención de información obtenida de la Unión Europea. Para obtener más información sobre Safe Harbor o para acceder a la declaración de la certificación de Fiberlink, vaya a http://www.export.gov/safeharbor/.

Cuando el Acuerdo Safe Harbor entre EE.UU. y la UE de IBM no se aplique a una transferencia de Información Personal del EEE, las partes o sus filiales pueden firmar acuerdos estándar no modificados de Clausulas Modelo de la Unión Europea (EU Model Clause) en sus roles correspondientes, con las cláusulas opcionales eliminadas, conforme a la Decisión de la CE 2010/87/EU. Todas las disputas o responsabilidades que surjan de estos acuerdos, incluso si son firmadas por afiliadas, serán tratadas por las partes como si hubiesen surgido entre ellas bajo los términos y condiciones de este Contrato.

6.6 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los impuestos se basan en las ubicaciones que el Cliente identifica como receptoras de los servicios SaaS IBM. IBM aplicará los tributos en base a las direcciones de facturación enumeradas a la hora de solicitar SaaS IBM como ubicación del beneficiario principal, a menos que el Cliente proporcione información adicional a IBM. El Cliente es responsable de mantener esta información actualizada y de comunicar cualquier cambio a IBM.

6.7 Datos Normativos

Sin perjuicio de cualquier disposición en contrario, y únicamente para la investigación, el análisis y la creación de informes normativos, IBM podrá conservar y utilizar los datos que reflejen las experiencias individuales de los usuarios autorizados del Cliente con SaaS IBM, en formato agregado y anónimo (es decir, de modo que el Cliente o los usuarios autorizados del Cliente no puedan identificarse como la fuente de los datos y de modo que se elimine cualquier información que pueda identificar al Cliente o a los usuarios autorizados del Cliente).

6.8 Uso Legítimo y Consentimiento

6.8.1 Autorización para la recopilación y el tratamiento de datos

El SaaS IBM está diseñado para suministrar, gestionar, asegurar, monitorizar y controlar dispositivos móviles. El SaaS IBM recopila información de los usuarios y dispositivos autorizados por el Cliente para interactuar con el SaaS IBM para el cual se ha suscrito el Cliente. SaaS IBM recopila información que, de manera independiente o combinada, se puede considerar Información Personal en algunas jurisdicciones. Los datos recopilados pueden incluir el nombre de usuario autorizado, el número de teléfono, la dirección de correo electrónico registrada y la ubicación del dispositivo, ID de usuario e historial de navegación segura, información sobre el hardware, el software y la configuración del dispositivo de usuario final, y la información generada por el dispositivo. El Cliente autoriza a IBM para recopilar, procesar y utilizar esta información de conformidad con los términos de las presentes Condiciones de Uso.

6.8.2 Consentimiento Informado de los Interesados

El uso del SaaS IBM puede implicar distintas leyes o normativas. El SaaS IBM únicamente puede utilizarse con objetivos conformes a derecho y de forma legítima. El Cliente acepta utilizar el SaaS IBM de acuerdo con las políticas, normativas y leyes aplicables y es plenamente responsable de su cumplimiento.

El Cliente declara que ha obtenido, u obtendrá, los consentimientos perfectamente informados, permisos o licencias que sean necesarios para realizar un uso legítimo del SaaS IBM, así como para permitir la recopilación y el tratamiento de la información, por parte de IBM, como Encargado del tratamiento de Datos Personales del Cliente, mediante el SaaS IBM. El Cliente por la presente autoriza a IBM a obtener los consentimientos perfectamente informados que sean necesarios para realizar un uso legítimo del SaaS IBM, así como recopilar y tratar la información, según lo descrito en el acuerdo de licencia de usuario final disponible en http://www.ibm.com/software/sla/sladb.nsf/.

6.9 Retención de Datos

IBM eliminará cualquier información recopilada, que puede incluir Información Personal, tras la terminación de estas Condiciones de Uso, a excepción de lo que sea necesario conservar de acuerdo a los propósitos establecidos anteriormente o conforme a alguna legislación, norma o regulación aplicable. En tal caso, IBM conservará la información recopilada durante el tiempo requerido para dicho propósito, legislación, norma o regulación aplicable.

Apéndice A

MobileFirst Protect es una plataforma cloud fácil de usar con toda la funcionalidad esencial para la gestión integral de los dispositivos móviles de hoy en día, incluyendo dispositivos iPhone, iPad, Android, dispositivos Kindle Fire, así como smartphones Windows Phone y BlackBerry. A continuación encontrará una breve descripción de las ofertas SaaS IBM:

1. IBM MobileFirst Protect – Devices (SaaS)

Las características básicas de gestión de dispositivos de movilidad (MDM) incluyen la inscripción de dispositivos, la configuración, la gestión de políticas de seguridad y las acciones del dispositivo, como enviar mensajes, localizar, bloquear y borrar. Las características avanzadas de MDM incluyen reglas de conformidad automatizadas, configuración de privacidad BYOD, y paneles de información e informes de Mobility Intelligence.

2. IBM MobileFirst Protect – Applications (SaaS)

MobileFirst Protect Applications ofrece la posibilidad de añadir aplicaciones y distribuirlas a los dispositivos compatibles que gestiona MobileFirst Protect. Esto incluye el MobileFirst Protect App Catalog, una aplicación en el dispositivo para permitir a los usuarios ver, instalar y ser alertados acerca de las aplicaciones gestionadas y actualizadas.

3. IBM MobileFirst Protect – Application Security (SaaS)

MobileFirst Protect Application Security ofrece una protección adicional de los datos personales para las aplicaciones empresariales que utilizan el WorkPlace SDK durante el desarrollo, o para que las aplicaciones de iOS carguen la aplicación (.ipa), el perfil de aprovisionamiento y firmen el certificado para ser integrado automáticamente. Mobile Application Security integra la aplicación con Secure Productivity Suite. Esto permite un inicio de sesión único, el acceso a la intranet a través de Mobile Enterprise Gateway y la aplicación obligada de la configuración de seguridad.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

MobileFirst Protect Enterprise Gateway for Apps ofrece a los usuarios fuera de la red de la empresa un acceso seguro y transparente a los recursos internos de la aplicación sin necesidad de una conexión VPN, de dispositivo completo.

5. IBM MobileFirst Protect – Content (SaaS)

MobileFirst Protect Content permite al administrador agregar y distribuir documentos a los dispositivos compatibles gestionados por IBM MobileFirst Protect - Devices. Incluye IBM MobileFirst Protect Doc Catalogue, un contenedor protegido por contraseña en el dispositivo que proporciona una forma segura y sencilla para los usuarios de acceder, ver y compartir documentos. Incluye acceso directo a contenido distribuido y repositorios, como SharePoint, Box y Google Drive. El acceso a recursos compartidos de archivos de Windows y SharePoint privados está disponible con MobileFirst Protect Mobile Enterprise Gateway. Los documentos gestionados a través de MobileFirst Protect pueden ser controlados en versión, auditados y asegurados a través de las opciones de la política de prevención de pérdida de datos (DLP), como requerir autenticación, limitar la funcionalidad de copiar y pegar, y bloquear la apertura o el uso compartido en otras aplicaciones.

6. IBM MobileFirst Protect – Document Sync (SaaS)

MobileFirst Protect Document Sync proporciona a los usuarios la capacidad de sincronizar fácilmente y de forma segura el contenido del usuario a través de dispositivos móviles gestionados. Los administradores pueden garantizar que las políticas, tales como la restricción de cortar-copiar-pegar y el bloqueo del contenido frente a la apertura o el uso compartido en otras aplicaciones, están vigentes para el contenido del usuario a través de los dispositivos. El contenido se almacena de forma segura, en el entorno cloud y en el dispositivo, y se accede al mismo sólo a través de MobileFirst Protect Doc Catalogue.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor es una suite de productos potente que permite a los usuarios trabajar con documentos empresariales sobre la marcha. MobileFirst Protect Secure Editor permite:

- Crear y editar archivos .DOC, .PPT y .XLS.
- Modo de presentación para las diapositivas
- Trabajo fácil con archivos adjuntos de correo electrónico y otros archivos de MobileFirst Protect para iOS.

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

Con MobileFirst Protect Enterprise Gateway for Documents, las organizaciones pueden utilizar MobileFirst Protect Content para ofrecer, además, a los dispositivos fuera de la red de la empresa un acceso directo y seguro a los sitios internos de Connections, los sitios de SharePoint, recursos compartidos de archivo de Windows y otros almacenes de archivos sin necesidad de una conexión VPN de dispositivo completo. El uso de MobileFirst Protect Gateway for Documents requiere también la adquisición de MobileFirst Protect Content. Es compatible con iOS 5.0 y Android 4.0 o versiones superiores.

9. IBM MobileFirst Protect – Email Management (SaaS)

MobileFirst Protect Email Management incluye características clave en soporte de Microsoft Exchange ActiveSync y Lotus Traveler.

- Exchange ActiveSync: proporciona soporte para dispositivos móviles que se conectan a Microsoft Exchange a través del protocolo ActiveSync. Las características incluyen funciones de gestión de dispositivos móviles básicas, tales como la posibilidad de configurar los dispositivos, crear; obligar a cumplir las políticas de ActiveSync (código de acceso, bloquear o permitir el acceso a correo electrónico); y tomar medidas del dispositivo, tales como bloquear y limpiar, y un informe detallado sobre los atributos del dispositivo.
- Lotus Traveler: proporciona soporte para dispositivos móviles que se conectan a IBM Lotus Notes® a través del protocolo de Lotus Traveler. Las características incluyen la capacidad de configurar dispositivos, bloquear o permitir dispositivos, obligar a cumplir las políticas de código de acceso, limpiar dispositivos y desarrollar informes detallados sobre los atributos del dispositivo.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser es un navegador web con todas las funciones para permitir el acceso seguro a los sitios de intranet corporativa y garantizar la conformidad de las políticas de contenido mediante la definición de políticas de seguridad y filtrado de sitios web para asegurar que los usuarios únicamente acceden al contenido web aprobado que se basa en una serie de categorías de contenido, tales como las redes sociales o sitios de malware o de contenido para adultos. Incluye la capacidad de inhabilitar los navegadores web nativos y de terceros, a través de la política de aplicación o de listas negras cuando se combina con dispositivos MobileFirst Protect. Permite excepciones de lista blanca a sitios web, restringir cookies; características de copiar, pegar e imprimir; y habilitar el modo Quiosco.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser permite a los dispositivos soportados acceder a sitios web internos aprobados sin requerir una conexión VPN de nivel de dispositivo completo.

12. IBM MobileFirst Protect for Blackberry (SaaS)

Proporciona soporte para dispositivos móviles conectados a BlackBerry Enterprise Server (BES) mediante el uso de las API de BlackBerry. Las características incluyen acciones remotas como enviar un mensaje, restablecer códigos de acceso, asignar la política de BES y borrar, así como informes detallados sobre los atributos del dispositivo. Se requiere la instalación de MobileFirst Protect Cloud Extender. Únicamente disponible para dispositivos visualizados o gestionados con MobileFirst Protect a través de BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses permite al administrador crear políticas de uso de datos y asignarlos a dispositivos compatibles que son administrados por MobileFirst Protect, y asignar estas políticas a nivel de dispositivo, grupo o global y configurar los umbrales de alerta y los mensajes para el uso de datos en la red y en itinerancia.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Suite/Paquete de productos que incluye MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content y MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Suite/Paquete de productos que incluye MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content y MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail ofrece una aplicación de productividad de oficina separada y segura para que los usuarios puedan acceder y gestionar correo electrónico, calendario, contactos y con la capacidad de controlar los correos electrónicos y los archivos adjuntos para prevenir la fuga de datos mediante la restricción de la capacidad de reenviar o mover el contenido a otras aplicaciones, para obligar a realizar la autenticación, restringir cortar-copiar-pegar y bloquear los archivos adjuntos de correo electrónico únicamente para visualizarlos.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

MobileFirst Protect Gateway Suite permite a las aplicaciones soportadas en iOS y Android volver a comunicarse de forma segura y directa con los recursos de la red interna de la empresa.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Suite/Paquete de productos que incluye MobileFirst Protect Content, MobileFirst Protect Document Editor y MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

MobileFirst Protect Threat Management proporciona una mayor seguridad móvil con detección de malware móvil y detección avanzada de jailbreaking/rooting. Con MobileFirst Protect Threat Management, el Cliente podrá configurar y gestionar las políticas de conformidad en relación con el malware detectado y otras vulnerabilidades de seguridad.

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) ofrece a los usuarios la posibilidad de cargar paquetes y documentos de aplicación al sistema de distribución de contenido de MobileFirst.

Los Clientes con MobileFirst Protect Content Service también tendrán que comprar por lo menos un derecho de titularidad para MobileFirst Content Service Storage (SaaS) y MobileFirst Content Service Bandwidth (SaaS).

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) ofrece a los usuarios la posibilidad de comprar una cantidad total de almacenamiento de datos disponible para utilizar con MobileFirst Protect Content Service (SaaS).

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) ofrece a los usuarios la posibilidad de comprar una cantidad total de ancho de banda disponible para utilizar con MobileFirst Protect Content Service (SaaS).

23. IBM MobileFirst Protect – Professional (SaaS)

Proporciona a las pequeñas y medianas empresas una forma rápida y sencilla de configurar de forma remota smartphones y tabletas, obligar a cumplir las políticas de seguridad, impulsar aplicaciones y documentos y proteger los datos de los dispositivos corporativos y personales. El Cliente puede tener acceso a las prestaciones de gestión de la movilidad adecuadas para su negocio de forma rápida, fácil y asequible.

24. IBM MobileFirst Protect – Laptop (SaaS)

Proporciona al Cliente prestaciones para inscribirse, configurar, administrar, proteger e informar en dispositivos basados en OS X y Windows PC, junto a smartphones y tabletas. Las organizaciones pueden mantener perfiles y políticas de seguridad coherentes tanto en dispositivos corporativos como de propiedad de los empleados dentro de la misma consola de gestión de MobileFirst Protect.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) para PC basados en Windows proporciona informes de gestión de inventarios e inscripción por red inalámbrica con información sobre hardware, sistema operativo y software. El módulo de informes de seguridad de punto final proporciona informes interactivos y análisis de datos para aplicaciones proporcionadas por el Cliente, como antivirus, copia de seguridad/restauración, cifrado de datos y firewall personal, así como los parches del sistema operativo que faltan. El módulo de protección de datos personales proporciona análisis e informes interactivos para los servicios de seguridad, incluido el cifrado de datos, la prevención de fugas de datos y la copia de seguridad/restauración, así como otras aplicaciones integradas. Es compatible con Windows XP SP3, Windows Vista, Windows 7, Windows 8+ y Windows 8+ Pro (incluyendo 32 bits y 64 bits, cuando sea aplicable).

Las acciones de dispositivo son:

- Enviar mensaje al dispositivo
- Bloquear el dispositivo
- Localizar el dispositivo (Requiere MobileFirst Protect Laptop Location)
- Detener/Iniciar/Reiniciar servicios
- Conclusión/Reinicio
- Borrar el disco duro
- Configurar valores de parche
- Distribuir software

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) para Mac OS X proporciona informes de gestión de inventarios e inscripción por red inalámbrica con información sobre hardware, sistema operativo y software. El módulo de informes de seguridad de punto final proporciona informes interactivos y análisis de datos para aplicaciones proporcionadas por el Cliente, como antivirus, copia de seguridad/restauración, cifrado de datos y firewall personal, así como los parches del sistema operativo que faltan. El módulo de protección de datos personales proporciona análisis e informes interactivos para los servicios de seguridad de datos, incluido el cifrado de datos. El módulo de gestión de la configuración proporciona gestión remota de varias configuraciones de dispositivo y usuario, incluyendo: contraseña, correo electrónico, VPN y Wi-Fi. Compatible con Mac OS X versión 10.7.3 o superior.

Las acciones de dispositivo son:

- Bloquear el dispositivo
- Borrar el disco duro
- Cambiar la política de dispositivos

25. IBM MobileFirst Protect – Laptop Location (SaaS)

MobileFirst Protect Laptop Location (SaaS) aporta la capacidad de localizar portátiles o tabletas compatibles. MobileFirst Protect informa acerca de la ubicación de las coordenadas de direcciones IP o Wi-Fi y convierte estos datos en direcciones fácilmente reconocibles. Cuando un dispositivo está online, puede recuperarse su ubicación actual. MobileFirst Protect almacena las ubicaciones notificadas a lo largo del tiempo, por lo que el historial de ubicaciones está disponible para su revisión. Requiere IBM MobileFirst Protect Laptop (SaaS) para Windows. Es compatible con Windows XP SP3, Windows Vista, Windows 7, Windows 8+ y Windows 8+ Pro (incluyendo 32 bits y 64 bits, cuando sea aplicable).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Proporciona las prestaciones de la oferta MobileFirst Protect – Laptop (SaaS) y añade las prestaciones siguientes:

- Permite cargar paquetes a la plataforma MobileFirst Protect Content Service (SaaS) y planificar la distribución de la carga útil en los dispositivos, administrados mediante el servicio MobileFirst Protect Laptop (SaaS) para Microsoft Windows. El Cliente controla todos los aspectos de la distribución, incluyendo las instrucciones de instalación y el enfoque a nivel de dispositivo, grupo o global. El Cliente es responsable del empaquetado y la creación del archivo de instalación. IBM no proporciona soporte para la creación de paquetes de instalación.

27. IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)

Proporciona a las organizaciones la posibilidad de mantener perfiles y políticas de seguridad coherentes tanto en dispositivos corporativos como de propiedad de los empleados dentro de la misma consola de gestión.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

Incluye IBM MobileFirst Protect – Devices (SaaS), IBM MobileFirst Protect – Applications (SaaS), IBM MobileFirst Protect – Content (SaaS) e IBM MobileFirst Protect – Expenses (SaaS).

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Incluye IBM MobileFirst Protect – Secure Mail (SaaS), IBM MobileFirst Protect – Applications (SaaS), IBM MobileFirst Protect – Application Security (SaaS), IBM MobileFirst Protect – Content (SaaS) e IBM MobileFirst Protect – Browser (SaaS).

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Incluye IBM MobileFirst Protect – Content (SaaS), IBM MobileFirst Protect – Document Editor (SaaS), IBM MobileFirst Protect – Document Sync (SaaS) e IBM MobileFirst Protect – Content (SaaS).

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Proporciona a las pequeñas y medianas empresas una forma de configurar de forma remota smartphones y tabletas, obligar a cumplir las políticas de seguridad, impulsar aplicaciones y documentos y proteger los datos de los dispositivos corporativos y personales.

Apéndice B

IBM proporciona el siguiente Acuerdo de Nivel de Servicio de Disponibilidad ("SLA") para SaaS IBM y es aplicable si se especifica en el Documento de Titularidad (POE) o en un Documento Transaccional.

Se aplicará la versión de este SLA, que es la vigente al comienzo o a la renovación del período de suscripción del Cliente. El Cliente comprende que el SLA no constituye ninguna garantía.

1. Definiciones

a. **Contacto Autorizado**: hace referencia a la persona que el Cliente ha indicado a IBM como persona autorizada para enviar Reclamaciones bajo este SLA.

b. **Crédito de Disponibilidad**: es la compensación que IBM proporcionará para una Reclamación validada. El Crédito de Disponibilidad se aplicará en forma de crédito o de descuento para una factura futura de cargos de suscripción para SaaS IBM.

c. **Reclamación**: es una reclamación enviada por el Contacto autorizado del Cliente a IBM de acuerdo con este SLA referente a un Nivel de servicio no satisfecho durante un Mes Contratado.

d. **Mes Contratado**: indica cada mes completo durante el plazo del SaaS IBM medido desde las 12:00 a.m. (GMT) del primer día del mes a las 11:59 p.m. (GMT) del último día del mes.

e. **Cliente** o **Usted**: es una entidad que se suscribe para el SaaS IBM directamente a través de IBM, que no ha incumplido ninguna obligación esencial y que no tiene ninguna obligación material pendiente, incluidas las obligaciones de pago, de este contrato con IBM por el SaaS IBM.

f. **Tiempo de Inactividad**: hace referencia al Tiempo de Inactividad de la Aplicación y/o al Tiempo de Inactividad del Proceso Entrante aplicable al Nivel de servicio correspondiente que se muestra en esta tabla. El Tiempo de Inactividad no incluye el período de tiempo en que SaaS IBM deja de estar disponible como consecuencia de:

- Tiempo de Inactividad del Sistema Planificado;
- Fuerza Mayor;
- Problemas con aplicaciones, equipos o datos del Cliente o de terceros;
- Actos u omisiones del Cliente o de terceros (incluida cualquier persona que acceda a SaaS IBM mediante las contraseñas o el equipo del Cliente);
- La no observancia de las configuraciones necesarias del sistema y de las plataformas soportadas para acceder a SaaS IBM; o
- La conformidad de IBM con cualquier diseño, especificación o instrucción proporcionada por el Cliente o por un tercero en nombre del Cliente.

g. **Evento**: es una circunstancia o un conjunto de circunstancias que no permiten satisfacer un Nivel de Servicio.

h. **Fuerza Mayor**: hace referencia a catástrofe natural, terrorismo, acción laboral, incendio, inundación, terremoto, motín, guerra, actos gubernamentales, órdenes o restricciones, virus, ataques de denegación de servicio y otras conductas dolosas, errores de programas de utilidad y de conectividad de la red, o cualquier otra causa de no disponibilidad del SaaS IBM que esté fuera del control razonable de IBM.

i. **Tiempo de Inactividad del Sistema Planificado**: indica una parada planificada de SaaS IBM con la finalidad de llevar a cabo el mantenimiento.

j. **Nivel de Servicio**: es el estándar definido más adelante según el cual IBM mide el nivel de servicio que proporciona en este SLA.

2. Créditos de Disponibilidad

a. A fin de poder tener derecho a enviar una Reclamación, el Cliente debe haber registrado un ticket de soporte para cada Evento en el servicio de asistencia técnica al Cliente de IBM para el Servicio SaaS IBM aplicable, de conformidad con el procedimiento de IBM para notificar problemas de soporte de Severidad 1. El Cliente debe proporcionar toda la información detallada necesaria acerca del Evento y asistir razonablemente a IBM en el diagnóstico y la resolución del Evento en la

medida de lo necesario para los tickets de soporte de Gravedad 1. El ticket debe registrarse en un período de veinticuatro (24) horas desde que el Cliente reconoce que el Evento ha afectado a su uso de SaaS IBM.

b. El Contacto Autorizado del Cliente debe enviar la Reclamación para un Crédito de Disponibilidad a más tardar tres (3) días laborables después del último día del Mes Contratado que es objeto de la Reclamación.

c. El Contacto Autorizado debe proporcionar a IBM todos los detalles razonables en relación con la Reclamación, incluyendo, a título enunciativo y no limitativo, descripciones detalladas de todos los Sucesos relevantes y del Nivel de Servicio que se reclama como no satisfecho.

d. IBM medirá internamente el Tiempo de Inactividad total combinado durante cada Mes Contratado, aplicable al Nivel de Servicio correspondiente que se muestra en esta tabla. Los Créditos de disponibilidad se basarán en la duración del Tiempo de Inactividad medido desde el primer momento en que le impactó el Tiempo de Inactividad. Si el Cliente comunica un Suceso de Tiempo de inactividad de aplicación y un Suceso de Tiempo de Inactividad de Recogida de Datos Entrantes que ocurren simultáneamente, IBM tratará los períodos de solapamiento del Tiempo de Inactividad como un único período de Tiempo de Inactividad y no como dos períodos de Tiempo de Inactividad separados. Para cada Reclamación válida, IBM aplicará el Crédito de Disponibilidad aplicable más alto en función del Nivel de Servicio alcanzado durante cada Mes Contratado, como se muestra en estas tablas. IBM no será responsable de múltiples Créditos de Disponibilidad para los mismos Eventos en el mismo Mes Contratado.

e. En el caso del Servicio empaquetado (SaaS IBM individuales empaquetados y vendidos conjuntamente por un precio combinado único), el Crédito de Disponibilidad se calculará en base al precio mensual único combinado para el Servicio Empaquetado, y no a la cuota de suscripción mensual para cada SaaS IBM individual. El Cliente solo puede enviar Reclamaciones relacionadas con un SaaS IBM individual de un paquete en un Mes Contratado, e IBM no será responsable de los Créditos de Disponibilidad en relación con más de un SaaS IBM de un paquete en un Mes Contratado.

f. Si el Cliente ha adquirido el SaaS IBM de un distribuidor de IBM válido en una transacción de reventa en la que IBM mantiene la responsabilidad principal del cumplimiento del SaaS IBM y los compromisos del SLA, el Crédito de Disponibilidad se basará en el Precio Sugerido por Relación (RSVP) publicado para el SaaS IBM vigente en ese momento y en vigor para el Mes Contratado objeto de la Reclamación, con un descuento del 50%.

g. Los Créditos de disponibilidad totales concedidos en relación con cualquier Mes Contratado no deberán superar, bajo ninguna circunstancia, el diez por ciento (10%) de una doceava parte (1/12) del cargo anual pagado por el Cliente a IBM para el SaaS IBM.

h. IBM utilizará su criterio razonable para validar las Reclamaciones en función de la información disponible en los registros de IBM, que prevalecerán en caso de conflicto con los datos de los registros del Cliente.

i. LOS CRÉDITOS DE DISPONIBILIDAD PROPORCIONADOS AL CLIENTE DE CONFORMIDAD CON ESTE SLA SON LA ÚNICA Y EXCLUSIVA COMPENSACIÓN QUE RECIBIRÁ EL CLIENTE EN RELACIÓN CON CUALQUIER RECLAMACIÓN.

3. Niveles de Servicio

Disponibilidad del SaaS IBM durante un Mes Contratado

Nivel de Servicio Alcanzado (durante un Mes Contratado)	**Crédito de Disponibilidad (% de la Cuota de suscripción mensual para el Mes Contratado objeto de una Reclamación)**
Menos del 99,8 %	2%
Menos del 98,8 %	5%
Menos del 95,0 %	10%

El "Nivel de Servicio Alcanzado", expresado como porcentaje, se calcula de este modo: (a) número total de minutos en un Mes Contratado, menos (b) número total de minutos de Tiempo de Inactividad en un Mes Contratado, dividido por (c) el número total de minutos en un Mes Contratado.

Ejemplo: 50 minutos de Tiempo de Inactividad total durante un Mes Contratado

43.200 minutos en total en un Mes Contratado de 30 días - 50 minutos de Tiempo de Inactividad = 43.150 minutos _____ 43.200 minutos en total	=2% de Crédito de Disponibilidad para el 99,8% de Nivel de Servicio Alcanzado durante el Mes Contratado

4. Exclusiones

Este SLA sólo está disponible para los Clientes de IBM. Este SLA no se aplica en los siguientes casos:

- Servicios versión beta o de prueba.
- Entornos que no son de producción, incluyendo, a título enunciativo y no limitativo, entornos de prueba, recuperación tras desastre, control de calidad o desarrollo.
- Las Reclamaciones realizadas por los usuarios, invitados, participantes e invitados permitidos del Cliente de IBM en relación con SaaS IBM.
- Software de Habilitación.