IBM Trusteer Fraud Protection

Esta Descripción del Servicio describe el Servicio de Cloud que IBM proporciona al Cliente. Por "Cliente" entendemos la parte contratante, así como sus destinatarios y usuarios autorizados del Servicio de Cloud. El Presupuesto y el Documento de Titularidad (POE) aplicables se proporcionan como Documentos Transaccionales independientes.

1. Servicio de Cloud

Los siguientes Servicios de Cloud están cubiertos por esta Descripción del Servicio:

Servicios de Cloud de Pinpoint Assure:

- IBM Trusteer Pinpoint Assure
- IBM Trusteer Pinpoint Assure Application
- IBM Trusteer Mobile Carrier Intelligence

Servicios de Cloud de Rapport:

- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications for Retail
- IBM Trusteer Rapport Additional Applications for Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Servicios de Cloud de Pinpoint:

- IBM Trusteer Pinpoint Malware Detection Standard Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business

- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard for Retail Premium Support
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Project Management and Consultancy Services
- IBM Trusteer Security Research Consultancy Services
- IBM Trusteer Training Services
- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application
- IBM Trusteer Pinpoint Detect Standard
- IBM Trusteer Pinpoint Detect Premium
- IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect
- IBM Trusteer Pinpoint Verify

Servicios de Cloud de Mobile:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail

1.1 Servicios de Cloud for Business y for Retail

Los Servicios de Cloud de IBM Trusteer se conceden para su uso con determinados tipos de Aplicaciones. Una Aplicación se puede definir con uno de los tipos siguientes: for Business o for Retail. Hay ofertas distintas disponibles para Aplicaciones for Business o Aplicaciones for Retail.

a. Una Aplicación for Retail se define como una aplicación de banca en línea, una aplicación móvil o una aplicación de comercio electrónico diseñada para los consumidores del servicio. La política del Cliente puede clasificar a determinadas pequeñas empresas como elegibles para el acceso for Retail.

b. Una Aplicación for Business se define como una aplicación de banca en línea, una aplicación móvil o una aplicación de comercio electrónico diseñada para ser utilizada por entidades corporativas, institucionales o equivalentes, o bien como cualquier aplicación que no sea for Retail.

1.1.1 Servicios de Cloud for Business

- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business
- IBM Trusteer Mobile SDK for Business

1.1.2 Servicios de Cloud for Retail

- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail
- IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail
- IBM Trusteer Mobile SDK for Retail

Para cada uno de los Servicios de Cloud for Business o for Retail, existe un producto asociado de soporte Premium (Premium Support) disponible, con un cargo adicional, a excepción de los Servicios de Cloud IBM Trusteer Mobile SDK.

1.1.3 Servicios de Cloud Adicionales para IBM Trusteer Rapport II

a. Servicios de Cloud Adicionales disponibles para IBM Trusteer Rapport II for Business:
   - IBM Trusteer Rapport Fraud Feeds for Business
   - IBM Trusteer Rapport Phishing Protection for Business
   - IBM Trusteer Rapport Mandatory Service for Business
   - IBM Trusteer Rapport Additional Applications for Business

b. Servicios de Cloud Adicionales disponibles para IBM Trusteer Rapport II for Retail:
   - IBM Trusteer Rapport Fraud Feeds for Retail
   - IBM Trusteer Rapport Phishing Protection for Retail
   - IBM Trusteer Rapport Mandatory Service for Retail
   - IBM Trusteer Rapport Additional Applications For Retail

Para cada uno de los complementos for Business o for Retail de los Servicios de Cloud IBM Trusteer Rapport, excepto para los complementos de IBM Trusteer Rapport Mandatory Service, existe un producto asociado de soporte Premium disponible (Premium Support), con un cargo adicional.

La Suscripción a IBM Trusteer Rapport II for Business o IBM Trusteer Rapport II for Retail es un requisito previo para los Servicios de Cloud recogidos en este apartado.

1.1.4 Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Malware Detection II

a. Servicios de Cloud Adicionales disponibles para IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:
   - IBM Trusteer Rapport Remediation for Business
   - IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

b. Servicios de Cloud Adicionales disponibles para IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail:

- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

El soporte Premium está disponible para ofertas específicas según lo indicado en el presente documento. La Suscripción a IBM Trusteer Pinpoint Malware Detection II for Business o IBM Security Trusteer Pinpoint Malware Detection for Retail es un requisito previo para los Servicios de Cloud adicionales asociados recogidos en este apartado.

1.1.5 Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Detect Standard y/o IBM Trusteer Pinpoint Detect Premium y/o IBM Trusteer Pinpoint Detect Standard for Retail y/o IBM Trusteer Pinpoint Detect Premium for Retail y/o IBM Trusteer Pinpoint Detect Standard for Business y/o IBM Trusteer Pinpoint Detect Premium for Business

a. Servicios de Cloud Adicionales disponibles para IBM Trusteer Detect Standard for Business y/o IBM Trusteer Pinpoint Detect Premium for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Digital Content Pack for Business
- IBM Trusteer New Account Fraud for Business

b. Servicios de Cloud Adicionales disponibles para IBM Trusteer Detect Standard for Retail y/o IBM Trusteer Pinpoint Detect Premium for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Digital Content Pack for Retail
- IBM Trusteer New Account Fraud for Retail

c. Servicios de Cloud Adicionales disponibles para IBM Trusteer Pinpoint Detect Standard y/o IBM Trusteer Pinpoint Premium:

- IBM Trusteer Pinpoint Detect Standard Application
- IBM Trusteer Pinpoint Detect Premium Application

d. Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Detect Premium

- IBM Trusteer Pinpoint Verify

La suscripción a IBM Trusteer Pinpoint Detect Standard, IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard for Retail, IBM Trusteer Pinpoint Detect Premium for Retail, IBM Trusteer Pinpoint Detect Standard for Business o IBM Trusteer Pinpoint Detect Premium for Business es un requisito previo para los Servicios de Cloud adicionales asociados recogidos en este apartado.

1.1.6 Otros Servicios de Cloud Adicionales

La suscripción a Servicios de Cloud adicionales con respecto a las suscripciones básicas anteriores que no aparezcan en este documento, como disponibles o en desarrollo, no se consideran actualizaciones y se deben conceder por separado.

1.2 Definiciones

Titular de la Cuenta: se refiere al usuario final del Cliente, que ha instalado el software de habilitación de Cliente, ha aceptado el acuerdo de licencia de usuario final ("EULA") y se ha autenticado al menos una vez en la Aplicación for Business o for Retail del Cliente para la cual se ha suscrito la cobertura de Servicios de Cloud.

Software de Cliente del Titular de la Cuenta: se refiere al software de habilitación de Cliente de IBM Trusteer Rapport o a cualquier otro software de habilitación de Cliente que se proporcione con alguna de las suscripciones a los Servicios de Cloud para su instalación en el dispositivo del usuario final.

Trusteer Splash: se refiere a la presentación que se ofrece al Cliente en función de las plantillas de presentación disponibles.

Página de Destino: se refiere a la página alojada por IBM que se proporciona al Cliente con la presentación del Cliente y el Software de Cliente del Titular de la Cuenta descargable.

1.3 Servicios de Cloud de IBM Trusteer Rapport

1.3.1 IBM Trusteer Rapport II for Retail y/o IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

El Servicio de Cloud Trusteer Rapport II es una reformulación de IBM Trusteer Rapport para ayudar a estandarizar los cargos relacionados con la protección de múltiples Aplicaciones; sustituye los cargos únicos al agregar Aplicaciones.

Trusteer Rapport II proporciona una capa de protección contra el phishing y los ataques de malware del tipo Man-in-the-Browser (MitB). Con una red de decenas de millones de puntos finales en todo el mundo, IBM Trusteer Rapport recopila datos relevantes sobre phishing y ataques con malware activos contra organizaciones de todo el mundo. IBM Trusteer Rapport aplica algoritmos de comportamiento concebidos para bloquear ataques de phishing e impedir la instalación y el funcionamiento de las oleadas de malware MitB.

El derecho de titularidad de este Servicio de Cloud está disponible bajo la métrica de cargo de Participante Elegible o la métrica de cargo de Dispositivo de Cliente. La oferta for Business se vende en paquetes de 10 Participantes Elegibles o 10 Dispositivos de Cliente. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles o 100 Dispositivos de Cliente.

Esta oferta de Servicio de Cloud incluye:

a. Trusteer Management Application ("TMA"):

   TMA está disponible en el entorno alojado en cloud de IBM Trusteer, a través del cual el Cliente (y un número ilimitado de su personal autorizado) puede: (i) ver y descargar informes de determinados datos de incidencias y evaluaciones de riesgos, (ii) ver la configuración del software de habilitación de Cliente, con licencia para los Participantes Elegibles del Cliente según un acuerdo de licencia de usuario final ("EULA"), gratuita y disponible para su descarga en los escritorios o dispositivos (PC/MAC) del Participante Elegible, también denominado suite de software Trusteer Rapport ("Software de Cliente del Titular de la Cuenta"). El Cliente solo puede comercializar el Software de Cliente del Titular de la Cuenta utilizando Trusteer Splash o Rapport API, y el Cliente no puede utilizar el Software de Cliente del Titular de la Cuenta para sus operaciones empresariales internas ni para uso de sus empleados (salvo para uso personal de estos).

b. Script web:

   Permite acceder a un sitio web con el fin de acceder o utilizar el Servicio de Cloud.

c. Datos de incidencias:

   El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir los datos de incidencias que haya generado el Software de Cliente del Titular de la Cuenta a raíz de las interacciones en línea del Titular de la Cuenta con la Aplicación for Business o for Retail para la que el Cliente haya suscrito la cobertura de Servicios de Cloud. Los datos de incidencias serán recibidos por el Software de Cliente del Titular de la Cuenta activo en los dispositivos de los Participantes Elegibles, que habrán aceptado el EULA, se habrán autenticado al menos una vez en la Aplicación for Business o for Retail del Cliente y cuya configuración de Cliente incluirá la recopilación de los ID de usuario.

d. Trusteer Splash:

   La plataforma de marketing de Trusteer Splash identifica y comercializa el Software de Cliente del Titular de la Cuenta para los Participantes Elegibles con acceso a las Aplicaciones for Business o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de Servicios de Cloud. El Cliente puede seleccionar entre las Plantillas de presentación disponibles. Se puede contratar una presentación personalizada bajo un acuerdo o especificación de trabajo independiente.

El Cliente puede aceptar proporcionar sus marcas registradas, logotipos o iconos para uso en relación con el TMA y sólo para la utilización con Trusteer Splash y para la visualización en el Software de Cliente del Titular de la Cuenta o en las páginas de inicio alojadas por IBM y en el sitio web de IBM Trusteer. Cualquier uso de las marcas registradas, logotipos o iconos que se proporcionen respetará las políticas relevantes de IBM sobre publicidad y uso de marcas registradas.

El Cliente debe suscribirse al Servicio de Cloud IBM Trusteer Rapport Mandatory Service si el Cliente quiere utilizar algún tipo de despliegue obligatorio del Software de Cliente del Titular de la Cuenta.

El despliegue obligatorio del Software de Cliente Titular de Cuenta incluye, a título enunciativo pero no limitativo, un despliegue obligatorio mediante cualquier mecanismo o medio que obligue a un Participante Elegible, directa o indirectamente, a descargar el Software de Cliente del Titular de la Cuenta, o cualquier método, herramienta, procedimiento, contrato o mecanismo no creado ni aprobado por IBM, creado para omitir los requisitos de licencia de este despliegue obligatorio del Software de Cliente del Titular de la Cuenta.

Trusteer Rapport II for Business y/o Trusteer Rapport II for Retail incluyen, cada una de las versiones, protección para una Aplicación. Para cada Aplicación adicional, el Cliente debe obtener un derecho de titularidad para IBM Trusteer Rapport Additional Applications.

1.3.2 Servicios de Cloud Adicionales Opcionales para IBM Trusteer Rapport II for Business y/o IBM Trusteer Rapport II for Retail

La suscripción a los Servicios de Cloud IBM Trusteer Rapport II un requisito previo para la suscripción a cualquiera de los siguientes Servicios de Cloud adicionales. Si el Servicio de Cloud tiene la designación "for Business", los Servicios de Cloud adicionales adquiridos deben tener la misma designación. Si el Servicio de Cloud tiene la designación "for Retail", los Servicios de Cloud adicionales adquiridos deben tener la misma designación. El Cliente recibirá datos de eventos de los Participantes Elegibles o de los Dispositivos de Cliente que ejecutan el Software de Cliente del Titular de la Cuenta y que han aceptado el EULA, se han autenticado al menos una vez en la Aplicación for Business y/o for Retail del Cliente y cuya configuración de Cliente incluye la recopilación de los ID de usuario.

1.3.3 IBM Trusteer Rapport Fraud Feeds for Business y/o IBM Trusteer Rapport Fraud Feeds for Retail

Al suscribirse a este Servicio de Cloud de complemento, el Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para ver, suscribir y configurar la entrega de comunicaciones de amenaza generados desde el Servicio de Cloud Trusteer Rapport. Las comunicaciones pueden enviarse por correo electrónico a direcciones de correo electrónico designadas o a través de SFTP como archivos de texto.

Esta oferta solo se aplica bajo la métrica de cargo de Participante Elegible.

1.3.4 IBM Trusteer Rapport Phishing Protection for Business y/o IBM Trusteer Rapport Phishing Protection for Retail

El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir notificaciones de datos de incidencias relacionadas con el envío de credenciales de inicio de sesión del Titular de Cuenta a un sitio sospechoso de realizar actividades de phishing o potencialmente fraudulento. Es posible que aplicaciones en línea legítimas (URL) se marquen como sitios de phishing por error y el Servicio de Cloud puede alertar a los Titulares de Cuenta de que un sitio legítimo es un sitio de phishing. En tal caso, el Cliente debe notificar a IBM dicho error e IBM lo corregirá. Este procedimiento es la única compensación a la que el Cliente tendrá derecho por dicho error.

El derecho de titularidad de este Servicio de Cloud está disponible bajo la métrica de cargo de Participante Elegible o la métrica de cargo de Dispositivo de Cliente. La oferta for Business se vende en paquetes de 10 Participantes Elegibles o 10 Dispositivos de Cliente. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles o 100 Dispositivos de Cliente.

Se puede obtener soporte Premium para estos servicios de cloud bajo la métrica de cargo de Participante Elegible o la métrica de cargo de Dispositivo de Cliente. La oferta for Business se vende en paquetes de 10 Participantes Elegibles o 10 Dispositivos de Cliente. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles o 100 Dispositivos de Cliente.

1.3.5 IBM Trusteer Rapport Mandatory Service for Business y/o IBM Trusteer Rapport Mandatory Service for Retail

El Cliente puede utilizar una instancia de la plataforma de marketing Trusteer Splash para ordenar la descarga del Software de Cliente del Titular de la Cuenta a los Participantes Elegibles con acceso a las Aplicaciones for Business y/o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de los Servicios de Cloud.

IBM Trusteer Rapport Premium Support for Business es un requisito previo para IBM Rapport Mandatory Service for Business.

IBM Trusteer Rapport Premium Support for Retail es un requisito previo para IBM Security Rapport Mandatory Service for Retail.

El Cliente puede implementar la funcionalidad adicional de IBM Trusteer Rapport Mandatory Service solo si se ha solicitado y se ha configurado para su uso con la Aplicación for Business o for Retail del Cliente para la cual el Cliente haya suscrito la cobertura de Servicios de Cloud.

El derecho de titularidad de este Servicio de Cloud está disponible bajo la métrica de cargo de Participante Elegible. La oferta de Business se vende en paquetes de 10. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles.

1.3.6 IBM Trusteer Rapport Large Redeployment y/o IBM Trusteer Rapport Small Redeployment

Los Clientes que vuelven a desplegar sus Aplicaciones de banca online durante el plazo del servicio y, en consecuencia, requieren cambios en su despliegue de IBM Trusteer Rapport II deben adquirir el Servicio de Cloud IBM Trusteer Rapport Redeployment.

El nuevo despliegue puede ser debido al cambio por parte del Cliente de la URL de alojamiento o dominio de la Aplicación, la aplicación de cambios en la configuración de presentación o el paso a una nueva plataforma de banca online.

Para el período de transición del nuevo despliegue de 6 meses, el Cliente tiene derecho de titularidad para Aplicaciones adicionales, una a una, ejecutándose sobre las Aplicaciones a las cuales ya está suscrito.

IBM Trusteer Rapport Large Redeployment se aplica a entornos con más de 20.000 usuarios, e IBM Trusteer Rapport Small Redeployment se aplica a entornos con un máximo de 20.000 usuarios.

1.3.7 IBM Trusteer Rapport Additional Applications for Business y/o IBM Trusteer Rapport Additional Applications for Retail

Para IBM Trusteer Rapport II for Business, el despliegue en cualquier Aplicación de tipo Business adicional más allá de la primera Aplicación requiere derecho de titularidad del Servicio de Cloud IBM Trusteer Rapport Additional Applications for Business. Para IBM Trusteer Rapport II for Retail, el despliegue en cualquier Aplicación de tipo Retail adicional más allá de la primera Aplicación requiere derecho de titularidad del Servicio de Cloud IBM Trusteer Rapport Additional Applications for Retail.

1.4 Servicios de Cloud de IBM Trusteer Pinpoint

IBM Trusteer Pinpoint es un servicio basado en la nube que se ha diseñado para proporcionar otra capa de protección y cuyo objetivo es detectar y mitigar los ataques de malware, phishing y toma de control de cuentas. Trusteer Pinpoint se puede integrar en las Aplicaciones for Business y/o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de Servicios de Cloud y los procesos de prevención del fraude.

Este Servicio de Cloud incluye:

a. TMA:

   TMA está disponible en el entorno alojado en cloud de IBM Trusteer, a través del cual el Cliente (y un número ilimitado del personal autorizado del Cliente) puede: (i) ver y descargar informes de datos de determinadas incidencias y evaluaciones de riesgos, y (ii) ver, suscribir y configurar la entrega de comentarios de amenazas de las ofertas Pinpoint.

b. Script web y/o API:

   Permite realizar el despliegue en un sitio web con el fin de acceder al Servicio de Cloud, o utilizarlo.

1.4.1 IBM Trusteer Pinpoint Malware Detection

En el caso de que se detecte malware en los Servicios de Cloud de IBM Trusteer Pinpoint Malware Detection II, el Cliente debe seguir la Guía de Prácticas Recomendadas de Pinpoint. No utilice los Servicios de Cloud IBM Trusteer Pinpoint Malware Detection II de ninguna manera que pueda afectar al uso habitual del Participante Elegible inmediatamente después de una detección de malware o de toma de control de cuentas, ya que esto podría permitir que otros vinculasen las acciones del Cliente con el uso de las ofertas de Servicios de Cloud IBM Trusteer Pinpoint (por ejemplo, notificaciones, mensajes, bloqueo de dispositivos o bloqueo del acceso a la Aplicación de tipo Business o Retail inmediatamente después de una detección de malware o de toma de control de cuentas).

1.4.2 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business y/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail y/o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business y/o IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

IBM Security Pinpoint Malware Detection II es una reformulación de IBM Trusteer Pinpoint Malware Detection para ayudar a estandarizar los cargos relacionados con la protección de múltiples Aplicaciones; sustituye los cargos únicos al agregar Aplicaciones.

Detección sin Cliente de navegadores infectados con malware financiero de tipo Man in the Browser (MitB) que se conectan a una Aplicación for Business y/o for Retail. Los Servicios de Cloud de IBM Trusteer Pinpoint Malware Detection proporcionan otra capa de protección y su objetivo es permitir que las organizaciones se centren en los procesos de prevención del fraude según el riesgo de infección por malware proporcionando al Cliente evaluaciones y alertas de presencia de malware financiero MitB.

a. Datos de incidencias:

   El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir los datos de incidencias que se hayan generado a raíz de las interacciones en línea de los Participantes Elegibles con las Aplicaciones for Business y/o for Retail del Cliente.

b. Advanced Edition:

   Las Advanced Edition for Business y/o for Retail ofrecen una capa adicional de detección y protección que se personaliza para ajustarse a la estructura y el flujo de las Aplicaciones for Business y/o for Retail del Cliente, y se puede adaptar al panorama de amenazas específico al que se enfrenta el Cliente. Se puede incorporar a distintas ubicaciones de las Aplicaciones for Business y/o for Retail del Cliente.

   La Advanced Edition se ofrece al Cliente con una cantidad mínima de 100.000 Participantes Elegibles for Retail o 10.000 Participantes Elegibles for Business, con 1.000 paquetes de 100 Participantes Elegibles for Retail o 1.000 paquetes de 10 Participantes Elegibles for Business.

c. Standard Edition:

   Las Standard Editions for Business y/o for Retail son soluciones de despliegue rápido que proporcionan la funcionalidad principal de este Servicio de Cloud, como se describe en este documento.

Este Servicio de Cloud incluye protección para una Aplicación. Para cada Aplicación adicional, el Cliente debe obtener un derecho de titularidad para IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.3 Servicios de Cloud Adicionales Opcionales para IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail y/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail y/o IBM Pinpoint Trusteer Pinpoint Malware Detection Standard Edition II for Business y/o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Para el Servicio de Cloud IBM Trusteer Rapport Remediation for Retail, existe el requisito previo de IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Para el Servicio de Cloud IBM Trusteer Rapport Remediation for Business, existe el requisito previo de IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.4.4 IBM Trusteer Rapport Remediation for Retail y/o IBM Trusteer Rapport Remediation for Business

El objetivo de IBM Trusteer Rapport Remediation for Retail e IBM Trusteer Rapport Remediation for Business es investigar, corregir, bloquear y eliminar las infecciones por malware de tipo man-in-the-browser (MitB) de los dispositivos (PC/MAC) infectados de los Participantes Elegibles del Cliente con acceso a la Aplicación del Cliente de manera ad-hoc, cuando los datos de incidencias de IBM Trusteer Pinpoint Malware Detection detecten infecciones por malware de tipo MitB. El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Malware Detection II activa en la Aplicación del Cliente. El Cliente puede utilizar esta oferta de Servicio de Cloud únicamente en conexión con los Participantes Elegibles con acceso a la Aplicación del Cliente, y solo con el fin de investigar y corregir un dispositivo concreto (PC/MAC) infectado de manera ad-hoc. IBM Trusteer Rapport Remediation debe estar ejecutándose en el dispositivo (PC/MAC) del Participante Elegible afectado, y este tiene que aceptar el

EULA y autenticarse al menos una vez en las Aplicaciones del Cliente, además su configuración de Cliente debe incluir la recopilación de los ID de usuario. A efectos aclaratorios, esta oferta de Servicio de Cloud no incluye el derecho a utilizar Trusteer Splash ni a promocionar, de ninguna manera, el Software Cliente del Titular de la Cuenta entre los Participantes Elegibles del Cliente.

1.4.5 IBM Trusteer Pinpoint Malware Detection Redeployment

Los Clientes que vuelven a desplegar sus Aplicaciones de banca online durante el plazo del servicio y, en consecuencia, requieren cambios en su despliegue de IBM Trusteer Pinpoint Malware Detection II deben adquirir IBM Trusteer Pinpoint Malware Detection Redeployment.

El nuevo despliegue puede ser debido al cambio por parte del Cliente de la URL de alojamiento o dominio de la Aplicación, la conversión de la Aplicación online a una nueva tecnología, el paso a una nueva plataforma de banca online o la adición de un nuevo flujo de inicio de sesión a una Aplicación existente.

Para el período de transición del nuevo despliegue de 6 meses, el Cliente tiene derecho de titularidad para Aplicaciones adicionales, una a una, ejecutándose sobre las Aplicaciones a las cuales ya está suscrito.

IBM Trusteer Pinpoint Malware Detection Additional Applications para IBM Trusteer Pinpoint Malware Detection II Standard Edition o IBM Trusteer Pinpoint Malware Detection II Advanced Edition, el despliegue en cualquier Aplicación adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.4.6 IBM Trusteer Pinpoint Malware Detection Additional Applications for Business y/o IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

- Para IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, el despliegue de cualquier Aplicación de tipo Retail adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Para IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business o IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, el despliegue de cualquier Aplicación de tipo Business adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.5 IBM Trusteer Fraud Protection Suite

IBM Trusteer Fraud Protection Suite ("Suite") es un conjunto de servicios basados en cloud diseñado para proporcionar una capa de protección contra el fraude; puede integrarse con otros productos de IBM para proporcionar una solución de gestión de ciclo de vida. La Suite incluye los siguientes servicios basados en cloud:

- IBM Trusteer Pinpoint Detect, que tiene como objetivo es detectar y mitigar los ataques de malware, phishing y toma de control de cuentas. Trusteer Pinpoint Detect se puede integrar en las Aplicaciones for Business y/o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de Servicio de Cloud y los procesos de prevención del fraude.
- IBM Trusteer Rapport for Mitigation, que tiene por objetivo desinfectar y proteger puntos finales infectados.

Los Servicios de Cloud incluirán lo siguiente:

a. TMA:

   TMA está disponible en el entorno alojado en cloud de IBM Trusteer, a través del cual el Cliente (y un número ilimitado de personal autorizado) puede: (i) recibir informes de datos de incidencias y evaluaciones de riesgos, y (ii) ver, configurar y establecer políticas de seguridad y políticas relacionadas con informes de datos de incidencias.

b. Datos de incidencias:

   El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir los datos de incidencias que se hayan generado a raíz de las interacciones en línea de los Participantes Elegibles con las Aplicaciones del Cliente para las cuales el Cliente haya suscrito la cobertura del Servicio de Cloud. El Cliente también puede recibir los datos de incidencias a través de una modalidad de entrega de la API de fondo.

c. Script web y/o API:

Permite realizar el despliegue en un sitio web con el fin de acceder al Servicio de Cloud, o utilizarlo.

Prácticas Recomendadas de Pinpoint

En el caso de que se detecte malware o suplantación de cuentas, el Cliente debe seguir la Guía de Prácticas Recomendadas de Pinpoint. No utilice los Servicios de Cloud IBM Trusteer Pinpoint Detect de ninguna manera que pueda afectar al uso habitual del Participante Elegible inmediatamente después de una detección de malware o de toma de control de cuentas, ya que esto podría permitir que otros vinculasen las acciones del Cliente con el uso de las ofertas de IBM Trusteer Pinpoint Detect (por ejemplo, notificaciones, mensajes, bloqueo de dispositivos o bloqueo del acceso a la Aplicación for Business o for Retail inmediatamente después de una detección de malware o de toma de control de cuentas).

1.5.1 IBM Trusteer Pinpoint Detect Standard for Retail y/o IBM Trusteer Pinpoint Detect Standard for Business

Este Servicio de Cloud combina los Servicios de Cloud IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection para ofrecer una solución única y unificada.

La solución ayuda a una detección sin cliente de actividades sospechosas de malware y/o suplantación de cuentas de los navegadores que se conectan a una Aplicación de tipo Retail o Business, utilizando ID de dispositivo, detección de phishing y detección de robo de credenciales a través de malware. Las ofertas IBM Trusteer Pinpoint proporcionan otra capa de protección y su objetivo es detectar los intentos de toma de control de cuentas y proporcionar directamente al Cliente indicadores de evaluación de riesgos de los navegadores o dispositivos móviles (mediante el navegador nativo o la aplicación móvil personalizada del Cliente) que acceden a una Aplicación de tipo Business o Retail.

En este Servicio de Cloud se incluye soporte estándar (según se define en el apartado Soporte Técnico siguiente). Para obtener soporte Premium, el Cliente debe adquirir Pinpoint Standard Premium Support.

Este Servicio de Cloud incluye protección para una Aplicación. Para cada Aplicación adicional, el Cliente debe obtener un derecho de titularidad para IBM Trusteer Pinpoint Detect Standard Additional Applications.

El servicio está disponible para adquirirse por paquetes de 100 Participantes Elegibles o por paquetes de 100 Conexiones. Si el Cliente elige comprar el servicio por Conexiones, puede aplicarse un cargo de Aplicación adicional a partir de la primera aplicación.

1.5.2 IBM Trusteer Pinpoint Detect Premium for Retail y/o IBM Trusteer Pinpoint Detect Premium for Business

Este Servicio de Cloud combina IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection para ofrecer una solución única, fácil de integrar y unificada.

La solución ayuda a una detección sin cliente de actividades sospechosas de malware y/o suplantación de cuentas de los navegadores que se conectan a una Aplicación de tipo Retail o Business, utilizando ID de dispositivo, detección de phishing y detección de robo de credenciales a través de malware. Las ofertas de Cloud de IBM Trusteer Pinpoint proporcionan otra capa de protección y su objetivo es detectar los intentos de toma de control de cuentas y proporcionar directamente al Cliente indicadores de evaluación de riesgos de los navegadores o dispositivos móviles (mediante el navegador nativo o la aplicación móvil personalizada del Cliente) que acceden a una Aplicación for Business o for Retail.

El servicio aporta servicios y funcionalidad adicionales, que incluyen: extensos servicios de configuración y despliegue, servicios de seguridad personalizada, servicios de investigación, etc. El servicio incluye un máximo de 200 horas de recursos compartidos para servicios de implementación por aplicación y 200 horas de recursos compartidos para análisis de seguridad por aplicación en la configuración. Los servicios continuados incluyen 20 horas de mantenimiento de implementación por año por aplicación y 100 horas de investigación de seguridad por aplicación por año. Cualquier esfuerzo adicional estará sujeto a una tarifa adicional.

Pinpoint Detect puede consumir transacciones desde los canales móviles y web. En caso de que se incluyan transacciones móviles, se aplica el cargo de Pinpoint por Conexiones. Este Servicio de Cloud incluye protección para una Aplicación. Para cada Aplicación adicional, el Cliente debe obtener un derecho de titularidad para IBM Trusteer Pinpoint Detect Premium Additional Applications.

El soporte Premium se incluye en este Servicio de Cloud.

El servicio IBM Trusteer Pinpoint Detect Premium for Retail y Business está disponible para adquirirse por paquetes de 100 Participantes Elegibles o IBM Trusteer Pinpoint Detect Premium por paquetes de 100 Conexiones. Si el Cliente elige comprar el servicio por Conexiones, puede aplicarse un cargo de Aplicación adicional a partir de la primera aplicación.

Pinpoint Detect Policy Manager:

Policy Manager se incluye en el servicio Pinpoint Detect Premium y se pone a disposición en el entorno alojado en cloud de IBM Security Trusteer, a través del cual el Cliente (y un número ilimitado de personal autorizado) puede: (i) diseñar, probar y desplegar en el entorno productivo lógica para detectar actividad fraudulenta, (ii) diseñar dashboards e informes y (iii) ver, configurar y establecer políticas de seguridad y políticas para detectar actividad sospechosa en la Aplicación del Cliente.

Los servicios de consultoría son necesarios para la activación de la función Policy Manager y para el soporte necesario de investigación a fondo adicional. Los detalles de los servicios de consultoría se describirán por separado en una especificación de trabajo.

Cuando se activa Policy Manager, IBM se reserva el derecho de acceder al entorno del Cliente con fines de soporte para ajustar las políticas del Cliente de cara a resolver los principales problemas que se deriven de los cambios de política.

El Cliente se compromete a proteger cualquier dato expuesto a través de Policy Manager frente a un uso incorrecto.

Cuando se activa la función Policy Manager, el Cliente debe seguir las directrices de IBM para la configuración de reglas, como se describe en la documentación. El Cliente reconoce que IBM no es responsable de ninguna situación que pueda derivarse del incumplimiento de estas recomendaciones por parte del Cliente.

Cualquier problema de degradación de la estabilidad y/o el servicio que pudiera surgir debido a la mala configuración de la función Policy Manager por parte del Cliente no se considerará como Tiempo de Inactividad para el cálculo del SLA.

1.5.3 Servicios opcionales para IBM Trusteer Pinpoint Detect Standard y/o IBM Trusteer Pinpoint Detect Premium

Para los Servicios de Cloud de este apartado, existe un requisito previo de derecho de titularidad de IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard.

1.5.4 IBM Trusteer Rapport for Mitigation for Business y/o IBM Trusteer Rapport for Mitigation for Retail

- El objetivo de IBM Trusteer Rapport for Mitigation for Retail es investigar, corregir, bloquear y eliminar las infecciones por malware de los dispositivos (PC/MAC) infectados de los Participantes Elegibles del Cliente con acceso a la Aplicación de tipo Retail del Cliente de manera ad-hoc, cuando los datos de incidencias de IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard detecten infecciones por malware. El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard activa en la Aplicación for Retail del Cliente. El Cliente puede utilizar este Servicio de Cloud únicamente en conexión con los Participantes Elegibles con acceso a la Aplicación for Retail del Cliente, y solo con el fin de investigar y corregir un dispositivo concreto (PC/MAC) infectado de manera ad-hoc. IBM Trusteer Rapport for Mitigation for Retail debe estar ejecutándose en el dispositivo (PC/MAC) del Participante Elegible afectado, y este tiene que aceptar el EULA y autenticarse al menos una vez en las Aplicaciones for Retail del Cliente, además de que su configuración de Cliente debe incluir la recopilación de los ID de usuario. A efectos aclaratorios, este Servicio de Cloud no incluye el derecho a utilizar Trusteer Splash ni a promocionar, de ninguna manera, el Software Cliente del Titular de la Cuenta entre los Participantes Elegibles del Cliente.
- El objetivo de IBM Trusteer Rapport for Mitigation for Business es investigar, corregir, bloquear y eliminar las infecciones por malware de los dispositivos (PC/MAC) infectados de los Participantes Elegibles del Cliente con acceso a la Aplicación de tipo Business del Cliente de manera ad-hoc, cuando los datos de incidencias de IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard detecten infecciones por malware. El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard activa en la Aplicación for Business del Cliente. El Cliente puede utilizar este Servicio de Cloud únicamente en conexión con los Participantes Elegibles con acceso a la Aplicación de tipo

Business del Cliente, y solo con el fin de investigar y corregir un dispositivo concreto (PC/MAC) infectado de manera ad-hoc. IBM Trusteer Rapport for Mitigation for Business debe estar ejecutándose en el dispositivo (PC/MAC) del Participante Elegible afectado, y este tiene que aceptar el EULA y autenticarse al menos una vez en las Aplicaciones de tipo Business del Cliente, además de que su configuración de Cliente debe incluir la recopilación de los ID de usuario. A efectos aclaratorios, este Servicio de Cloud no incluye el derecho a utilizar Trusteer Splash ni a promocionar, de ninguna manera, el Software Cliente del Titular de la Cuenta entre los Participantes Elegibles del Cliente.

1.5.5 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail y/o IBM Trusteer Pinpoint Detect Standard Additional Applications for Business y/o IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail y/o IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

El servicio incluye un máximo de 200 horas de recursos compartidos para servicios de implementación por aplicación y 200 horas de recursos compartidos para análisis de seguridad por aplicación en la configuración. Los servicios continuados incluyen 20 horas de mantenimiento de implementación por año por aplicación y 100 horas de investigación de seguridad por aplicación por año.

- Para IBM Trusteer Pinpoint Detect Standard for Retail, el despliegue de cualquier Aplicación de tipo Retail adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Para IBM Trusteer Pinpoint Detect Standard for Business, el despliegue de cualquier Aplicación de tipo Business adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.
- Para IBM Trusteer Pinpoint Premium for Retail, el despliegue de cualquier Aplicación de tipo Retail adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Para IBM Trusteer Pinpoint Premium for Business, el despliegue de cualquier Aplicación de tipo Business adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.5.6 IBM Trusteer Pinpoint Detect Standard Application y/o IBM Trusteer Pinpoint Detect Premium Application

Este servicio es aplicable para canales web y móviles.

El servicio incluye un máximo de 200 horas de recursos compartidos para servicios de implementación por aplicación y 200 horas de recursos compartidos para análisis de seguridad por aplicación en la configuración. Los servicios continuados incluyen 20 horas de mantenimiento de implementación por año por aplicación y 100 horas de investigación de seguridad por aplicación por año.

- El despliegue de IBM Trusteer Pinpoint Detect Standard requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Standard Application para cada Aplicación.
- El despliegue de IBM Trusteer Pinpoint Premium requiere derecho de titularidad de IBM Trusteer Pinpoint Detect Premium Application para cada Aplicación.

1.5.7 IBM Trusteer Pinpoint Detect Standard Redeployment y/o IBM Trusteer Pinpoint Detect Premium Redeployment

Los Clientes que vuelven a desplegar sus Aplicaciones de banca online durante el plazo del servicio y, en consecuencia, requieren cambios en su despliegue de IBM Trusteer Pinpoint Detect deben adquirir IBM Trusteer Pinpoint Detect Redeployment.

El nuevo despliegue puede ser debido al cambio por parte del Cliente de la URL de alojamiento o dominio de la Aplicación, la conversión de la Aplicación online a una nueva tecnología, el paso a una nueva plataforma de banca online o la adición de un nuevo flujo de inicio de sesión a una Aplicación existente.

Para el período de transición del nuevo despliegue de 6 meses, el Cliente tiene derecho de titularidad para Aplicaciones adicionales, una a una, ejecutándose sobre las Aplicaciones a las cuales ya está suscrito.

1.5.8 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support y/o IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Los Clientes que compran el Servicio de Cloud Pinpoint Detect Standard pueden comprar el servicio de soporte Premium. El alcance de los servicios de soporte Premium se indica en el apartado 4, a continuación.

1.5.9 IBM Trusteer Digital Content Pack for Retail y/o IBM Trusteer Digital Content Pack for Business

IBM Trusteer Digital Content Pack permite a los analistas de seguridad integrar nuevos modelos de fraude y a la vez es totalmente compatible con la creación y modificación de modelos ad-hoc para reaccionar ante las amenazas en evolución. Consiste en un extenso conjunto de reglas, perspectivas y políticas que se pueden adquirir como una parte adicional e integral de la solución. Digital Content Pack ayuda a reforzar aún más la integración entre las capacidades de prevención de fraude digital de Trusteer y los canales de pago sin efectivo de IBM Safer Payments. Mediante el aprovechamiento de sus reglas integradas y su lógica empresarial específica, Digital Content Pack permite a bancos y otras instituciones financieras mejorar aún más las capacidades existentes de detección y prevención del fraude.

IBM Trusteer Digital Content Pack for Retail está disponible en paquetes de 100 Participantes Elegibles. IBM Trusteer Digital Content Pack for Business está disponible en paquetes de 10 Participantes Elegibles.

Se requieren servicios de consultoría para la integración de Digital Content Pack con Pinpoint Detect e IBM Safer Payments, así como para los servicios de soporte que requieran una atención significativa. Los servicios de consultoría se adquieren por separado de conformidad con una especificación de trabajo independiente.

1.5.10 IBM Trusteer New Account Fraud for Retail y/o IBM Trusteer New Account Fraud for Business

Este servicio, disponible para los suscriptores de Pinpoint, está diseñado para detectar anomalías, indicar actividades sospechosas y generar alertas de forma anticipada en el proceso de creación de nuevas cuentas. Mediante informes de uso disponibles en TMA, el servicio monitoriza las cuentas nuevas para detectar actividades nuevas asociadas con el fraude, y la creación de perfiles posteriores a la cuenta y de cuentas jóvenes para proporcionar una señal de advertencia anticipada de que la nueva cuenta puede ser una cuenta mula o que se puede utilizar para llevar a cabo fraudes.

IBM Trusteer New Account Fraud for Retail e IBM Trusteer New Account Fraud for Business están disponibles en paquetes de 10 llamadas de API.

1.5.11 IBM Trusteer Pinpoint Verify

El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Detect Premium antes de suscribirse a este Servicio de Cloud.

Este Servicio de Cloud proporciona capacidades para que los usuarios pasen por un segundo factor de autenticación con el fin de verificar sus identidades al acceder a un servicio digital. Está disponible para Pinpoint Detect Premium, con el fin de proporcionar un segundo factor de autenticación para las aplicaciones protegidas. La decisión sobre cuándo desafiar a los usuarios para la autenticación de segundo factor se deriva de la aplicación protegida y puede basarse en las recomendaciones devueltas por la plataforma Pinpoint Detect Premium o por cualquier otra política definida por la aplicación protegida.

1.6 IBM Trusteer Pinpoint Assure

Este servicio marca las actividades sospechosas y genera alertas en el proceso de creación/registro de la nueva cuenta. El servicio monitoriza el proceso de registro de la cuenta para identificar la actividad asociada con el fraude para proporcionar una señal de advertencia anticipada de que la nueva cuenta puede ser una cuenta "mula" o utilizada para realizar un fraude a través de informes de uso disponibles en la TMA.

IBM Trusteer Pinpoint Assure está disponible en paquetes de 100 conexiones.

1.6.1 Servicios opcionales para IBM Trusteer Pinpoint Assure

1.6.2 IBM Trusteer Pinpoint Assure Application

Para IBM Trusteer Pinpoint Assure, el despliegue en cualquier Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Assure Application.

IBM Trusteer Pinpoint Assure está disponible para adquirirse por Aplicaciones.

1.6.3 IBM Trusteer Mobile Carrier Intelligence y/o IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Assure o IBM Trusteer Pinpoint Detect antes de suscribirse a este Servicio de Cloud.

Este Servicio de Cloud mejora IBM Trusteer Pinpoint Assure y/o IBM Trusteer Pinpoint Detect al proporcionar contexto e información adicional sobre los números móviles proporcionados a cualquiera de estos Servicios de Cloud, como ayuda para determinar el riesgo de fraude de una sesión determinada. El Cliente puede consultar el Servicio de Cloud para conocer las características de un número móvil determinado, como la información del operador asociado con el número.

Los datos proporcionados por este Servicio de Cloud con respecto a los números móviles ("Inteligencia Móvil") solo se pueden usar para fines internos del Cliente y solo se pueden conservar por un período de treinta (30) dias. El Cliente debe volver a consultar el Servicio de Cloud en relación con el mismo número de teléfono móvil después de dicho período, para obtener Inteligencia Móvil con respecto al número, no puede limitarse a reutilizar la Inteligencia Móvil recibida de una consulta previa. El Cliente no puede almacenar en la memoria caché, a excepción de lo permitido anteriormente, reutilizar o usar en conjunto o en parte con cualquier extracción de datos, o para archivar, cualquier información de tipo Inteligencia Móvil.

1.7 IBM Trusteer Remotely Delivered Services

IBM Trusteer Remotely Delivered Services está disponible como complemento opcional para los Servicios de Cloud Pinpoint Detect Premium y Pinpoint Assure.

1.7.1 IBM Trusteer Project Management and Consultancy Services

Este servicio ofrece un máximo de 200 horas de servicios profesionales durante los cuales IBM realizará algunos o todos los puntos siguientes:

a. Servicios iniciales de configuración: reuniones periódicas frecuentes, servicios de gestión de proyectos

b. Policy Manager: soporte continuado

La oferta está disponible para adquirirse por Compromisos.

1.7.2 IBM Trusteer Security Research Consultancy Services

Este servicio de consultoría incluye un máximo de 200 horas de recursos compartidos para el análisis de seguridad, de cara a prestar servicios adicionales además de la solución definida y el soporte Premium (cuando corresponda), e incluye:

a. Investigación extensa sobre fraude: reuniones semanales y formación.

b. Soporte de releases del Cliente de alta prioridad

c. Investigación y soporte continuados de reglas personalizadas

La oferta está disponible para adquirirse por Compromisos.

1.7.3 IBM Trusteer Training Services

Este servicio de consultoría está diseñado para proporcionar servicios adicionales además de la solución definida y el soporte Premium (cuando corresponda), e incluye servicios de formación en el portfolio de Trusteer para los empleados del Cliente.

La oferta está disponible para adquirirse por Compromisos.

1.8 Servicios de Cloud de IBM Trusteer Mobile

1.8.1 IBM Trusteer Mobile SDK for Business y/o IBM Trusteer Mobile SDK for Retail

Los Servicios de Cloud IBM Trusteer Mobile SDK se han diseñado para añadir otra capa de protección y su objetivo es proporcionar acceso web seguro a las Aplicaciones for Business o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de Servicios de Cloud, la evaluación de riesgos de los dispositivos móviles y la protección contra el pharming. La detección de Wi-Fi segura solo está disponible en plataformas Android.

Los Servicios de Cloud IBM Trusteer Mobile SDK incluyen un kit de desarrollador de software (SDK) para aplicaciones móviles de propiedad, un paquete de software que contiene documentación, bibliotecas de software de propiedad de programación y otros archivos y elementos relacionados, denominados IBM Trusteer Mobile Library, así como el "Componente en Tiempo de Ejecución" o el "Elemento Redistribuible", un código de propiedad generado por IBM Trusteer Mobile SDK que se puede incluir e integrar en las aplicaciones móviles autónomas protegidas para iOS o Android para las cuales el Cliente haya suscrito la cobertura de Servicios de Cloud ("Aplicación Móvil Integrada del Cliente").

IBM Trusteer Mobile SDK for Retail está disponible en paquetes de 100 Participantes Elegibles o paquetes de 100 Dispositivos de Cliente, e IBM Trusteer Mobile SDK for Business está disponible en paquetes de 10 Participantes Elegibles o paquetes de 10 Dispositivos de Cliente.

A través de TMA, el Cliente (y un número ilimitado de su personal autorizado) puede recibir informes de datos de eventos y evaluación de tendencias de riesgo. A través de la Aplicación Móvil Integrada del Cliente, el Cliente puede recibir análisis de riesgos e información sobre dispositivos móviles de los Participantes Elegibles que han descargado la Aplicación Móvil Integrada del Cliente, permitiendo al Cliente formular acciones de obligatoriedad de políticas preventivas antifraude dirigidas a controlar estos riesgos. En el contexto de esta oferta, "dispositivos móviles" solo incluye teléfonos móviles y tabletas, no incluye sistemas PC ni MAC.

El Cliente puede:

a. utilizar internamente IBM Trusteer Mobile SDK exclusivamente para desarrollar la Aplicación Móvil Integrada del Cliente;

b. incluir el Elemento Redistribuible (únicamente en formato de código objeto), de manera integral y no separable en la Aplicación Móvil Integrada del Cliente. Cualquier parte modificada o fusionada del Elemento Redistribuible conforme a esta licencia otorgada deberá estar sujeta a la presente Descripción del Servicio; y

c. comercializar y distribuir el Elemento Redistribuible para descargar en dispositivos móviles de Participantes Elegibles en el propietario del Dispositivo Cliente:

   - A excepción de lo expresamente permitido en el presente Contrato, el Cliente (1) no puede usar, copiar, modificar o distribuir el SDK; (2) no puede desensamblar, invertir la compilación o de otra manera convertir o alterar el diseño del SDK, con excepción de lo expresamente permitido por ley sin la posibilidad de renuncia contractual; (3) no puede sublicenciar, alquilar o arrendar el SDK; (4) no puede eliminar los archivos de aviso o de copyright en el Elemento Redistribuible; (5) no puede utilizar el mismo nombre de camino de acceso que los archivos/módulos de Elemento Redistribuible originales; y (6) no puede utilizar nombre o marcas registradas de IBM, sus licenciantes o distribuidores en relación con la comercialización de la Aplicación Móvil Integrada del Cliente sin el consentimiento previo por escrito de IBM, del distribuidor o del licenciante.
   - El Elemento Redistribuible debe permanecer integrado de una forma no separable dentro de la Aplicación Móvil Integrada del Cliente. El Elemento Redistribuible debe estar únicamente en forma de código objeto y debe estar conforme con todas las directrices, instrucciones y especificaciones del SDK y de su documentación. El acuerdo de licencia de usuario final del Cliente para la Aplicación Móvil Integrada del Cliente debe notificar al usuario final que el Elemento Redistribuible o sus modificaciones no deben i) utilizarse para ninguna finalidad distinta que habilitar la Aplicación Móvil Integrada del Cliente, ii) copiarse (excepto con finalidades de copia de seguridad), iii) distribuirse o transferirse adicionalmente o iv) someterse a ensamblado inverso, compilación inversa ni otro tipo de conversión, salvo en la medida permitida específicamente por la ley sin posibilidad de renuncia contractual. El acuerdo de licencia del Cliente debe tener como mínimo el mismo nivel de protección para IBM que las condiciones de este Acuerdo.
   - El SDK únicamente puede desplegarse como parte de las pruebas de unidad y desarrollo interno del Cliente en los dispositivos de prueba móviles especificados del Cliente. El Cliente no está autorizado a utilizar el SDK para procesar cargas de trabajo de producción o cargas de trabajo de simulación de producción, ni para probar la escalabilidad de cualquier código, aplicación o sistema. El Cliente no tiene autorización para utilizar ninguna parte del SDK con ninguna otra finalidad.

El Cliente es responsable exclusivo del desarrollo, las pruebas y el soporte de la Aplicación Móvil Integrada del Cliente. El Cliente es responsable de toda la asistencia técnica para la Aplicación Móvil

Integrada del Cliente y de cualquier modificación en los Elementos Redistribuibles realizada por el Cliente; según lo permitido en el presente documento.

El Cliente está autorizado para instalar y utilizar los Elementos Redistribuibles e IBM Security Mobile SDK solo para dar soporte al uso de Servicios de Cloud.

IBM no garantiza que cualquier aplicación o creación de resultados utilizando las herramientas móviles incluidas con IBM Security Mobile SDK funcionará, interoperará o será compatible con cualquier plataforma de sistema operativo móvil o dispositivo móvil específica.

Componentes de Origen y Materiales de Ejemplo - IBM Trusteer Mobile SDK puede incluir algunos componentes en formato de código fuente ("Componentes Originales") u otros materiales identificados como Materiales de Ejemplo. El Cliente puede copiar y modificar Componentes de Origen y Materiales de Ejemplo únicamente para el uso interno siempre que dicho uso sea dentro de los límites de los derechos de licencia de este Contrato, y siempre que el Licenciatario no modifique ni suprima ningún tipo de información ni aviso de copyright incluido en el Material de ejemplo. IBM proporciona los Componentes de Origen y los Materiales de Ejemplo sin la obligación de proporcionar soporte "TAL CUAL". Tenga en cuenta que los Componentes de Origen o los Materiales de Ejemplo se proporcionan únicamente como un ejemplo de cómo implementar el Integrable en el CIMA; los Componentes de Origen o los Materiales de Ejemplo pueden no ser compatibles con el entorno de desarrollo del Cliente, y el Cliente es el único responsable de las pruebas y la implementación del Integrable en su CIMA.

2. Contenido y Protección de Datos

La Ficha de Características de Protección y Tratamiento de Datos (Ficha de Datos) proporciona información específica del Servicio de Cloud sobre el tipo de Contenido habilitado para ser tratado, las actividades de tratamiento involucradas, las características de protección de datos y detalles específicos sobre la retención y la devolución de Contenido. Cualquier detalle o aclaración y condición, incluidas las responsabilidades del Cliente, sobre el uso del Servicio de Cloud y las características de protección de datos, en caso de que existan, se establecen en este apartado. Puede haber más de una Ficha de Datos aplicable al uso del Servicio de Cloud por parte del Cliente en función de las opciones que haya seleccionado el Cliente. Es posible que la Ficha de Datos esté disponible solo en inglés y que no esté disponible en el idioma local. Sin perjuicio de la práctica que sea habitual, las partes acuerdan que entienden el inglés y que es un idioma adecuado con respecto a la adquisición y el uso de los Servicios de Cloud. Las siguientes Fichas de Datos se aplican al Servicio de Cloud y a sus opciones disponibles. El Cliente reconoce que i) IBM puede, a su sola discreción, modificar ocasionalmente las Fichas de Datos y ii) tales modificaciones sustituirán a las versiones anteriores. El propósito de cualquier modificación de Fichas de Datos será i) mejorar o aclarar los compromisos existentes, ii) ajustarse a los estándares en vigor y a las leyes aplicables, o iii) proporcionar compromisos adicionales. Ninguna modificación de las Fichas de Datos degradará significativamente la protección de datos de un Servicio de Cloud.

Enlaces a Las Fichas de Datos aplicables:

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

IBM Trusteer Pinpoint Assure

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=CF0C527046E011E8ADCBA344DE8FB657

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

IBM Trusteer Pinpoint Verify

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

(La Ficha de Datos de IBM Cloud Identity Verify muestra IBM Trusteer Pinpoint Verify)

El Cliente es responsable de tomar las medidas necesarias para solicitar, habilitar o usar las funciones de protección de datos disponibles para un Servicio de Cloud y asume la responsabilidad derivada del uso de los Servicios de Cloud si no lleva a cabo tales acciones, incluido el cumplimiento de cualquier requisito de protección de datos u otros requisitos legales relacionados con el Contenido.

El Anexo de Tratamiento de Datos de IBM que se encuentra en http://ibm.com/dpa (DPA) y los Suplementos del DPA se aplican y se hace referencia a ellos como parte del Contrato, si el Reglamento General de Protección de Datos (GDPR) europeo (UE/2016/679) se aplica a los datos personales incluidos en el Contenido. Las Fichas de Datos aplicables para este Servicio de Cloud servirán como Suplemento del DPA. Si se aplica el DPA, es obligación de IBM proporcionar un aviso de cambios a los Subencargados y es el derecho del Cliente objetar a dichos cambios, como se indica en el DPA.

2.1 EULA y Base para el Tratamiento de Datos de Interesados

Para los Servicios de Cloud IBM Trusteer Rapport (incluyendo Rapport Remediation o Rapport for Mitigation cuando se despliega en conexión con los Servicios de Cloud Pinpoint):

A menos que se acuerde lo contrario, y conforme a la base de tratamiento que el Cliente ha establecido de forma independiente, el Cliente autoriza a IBM a proporcionar el Contrato de Licencia de Usuario Final disponible en https://www.trusteer.com/support/end-user-license-agreement para permitir a IBM recopilar y tratar la información necesaria para prestar los Servicios de Cloud.

2.2 Uso de Datos

IBM no utilizará ni revelará los resultados que surjan del uso del Servicio de Cloud por parte del Cliente que sean exclusivos del Contenido (Insights) del Cliente o que de otro modo identifiquen al Cliente. IBM, no obstante, puede utilizar Contenido y otras informaciones (excepto para Insights) derivadas del Contenido en el aprovisionamiento del Servicio de Cloud, tras eliminar los identificadores personales; de este modo, los datos personales ya no podrán atribuirse a una persona individual sin el uso de información adicional. IBM utilizará estos datos para fines de investigación, prueba y desarrollo de ofertas.

2.3 Almacenamiento y Tratamiento de Datos

2.3.1 Información Adicional de Ubicación de Tratamiento

Para los servicios Trusteer Pinpoint Verify, todas las ubicaciones de alojamiento y tratamiento se especifican en la Ficha de Datos relevante.

Para todos los otros servicios prestados a través del centro de datos de Alemania, IBM limitará el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los países siguientes: Alemania, Israel, Irlanda, Países Bajos y cualquier país adicional indicado en la Ficha de Datos aplicable a Subencargados del Tratamiento Terceros de IBM.

Para todos los otros servicios prestados a través del centro de datos de Japón, IBM limitará el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los países siguientes: Japón, Israel, Irlanda y cualquier país adicional indicado en la Ficha de Datos aplicable a Subencargados del Tratamiento Terceros de IBM.

Para todos los otros los servicios prestados a través del centro de datos de EE.UU., IBM limitará el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los países siguientes:

EE.UU., Israel, Irlanda, Singapur, Australia y cualquier país adicional indicado en la Ficha de Datos aplicable a Subencargados del Tratamiento Terceros de IBM.

También se pueden proporcionar servicios de mantenimiento de cuenta y soporte de IBM Trusteer según sea necesario, en función de la disponibilidad del personal de IBM pertinente, la ubicación del Cliente y el centro de datos donde se alojan los datos.

2.3.2 Datos del Titular de la Cuenta

Los datos del Titular de la Cuenta serán procesados en la región desde donde el Titular de la Cuenta originalmente haya instalado el Software Cliente de Titular de la Cuenta. Esto puede significar que el contenido puede ser procesado tanto en la región de origen como en la región acordada con el Cliente.

2.3.3 Soluciones Integradas

Para fines de aclaración, ya que Trusteer Fraud Protection es una solución integrada; si el Cliente termina uno de estos Servicios de Cloud, IBM puede retener los datos del Cliente con el propósito de proporcionar los Servicios de Cloud restantes al Cliente conforme a esta Descripción del Servicio.

3. Contrato de Nivel de Servicio (SLA)

IBM proporciona el siguiente contrato de Nivel de Servicio ("SLA") de disponibilidad para el Servicio de Cloud según lo especificado en un POE. El SLA no es una garantía. El SLA está disponible solamente para el Cliente y se aplica sólo para su uso en entornos productivos.

3.1 Créditos de Disponibilidad

El Cliente debe registrar un ticket de soporte de Severidad 1 en el help desk del servicio de asistencia técnica de IBM, en un período de veinticuatro (24) horas desde que el Cliente tuvo conocimiento en primera instancia de un evento que ha afectado la disponibilidad del Servicio de Cloud. El Cliente debe ayudar razonablemente a IBM en relación con cualquier diagnóstico y resolución de los posibles problemas.

Debe enviarse un ticket de soporte en caso de incumplimiento de un SLA, a más tardar tres (3) días laborables después del último día del mes contratado. La compensación por una reclamación válida de SLA será un crédito aplicable en una factura futura para el Servicio de Cloud, basado en el período durante el cual el tratamiento en el sistema productivo para el Servicio de Cloud no haya estado disponible ("Tiempo de Inactividad"). El Tiempo de Inactividad se mide desde el momento en que el Cliente notifica el evento hasta el momento en que el Servicio de Cloud se restaura y no incluye: tiempo relacionado con un corte de mantenimiento programado o anunciado; causas que queden fuera del control de IBM; problemas con contenido/tecnología, diseños o instrucciones del Cliente o un tercero; plataformas o configuraciones del sistema no compatibles, u otros errores del Cliente; o incidencias de seguridad o pruebas de seguridad del Cliente. IBM aplicará la compensación aplicable más alta en función de la disponibilidad acumulativa del Servicio de Cloud durante cada mes contratado, como se muestra en la tabla siguiente. La compensación total concedida en relación con cualquier mes contratado no puede superar el 10 por ciento de una doceava parte (1/12) del cargo anual por el Servicio de Cloud.

3.2 Niveles de Servicio

Disponibilidad del Servicio de Cloud durante un mes contratado

Disponibilidad durante un mes contratado	Compensación (% de la cuota de suscripción mensual* para el mes contratado que es objeto de una reclamación)
<99,9%	2%
< 99,0%	5%
< 95,0%	10%

* Si el Cliente ha adquirido el Servicio de Cloud a un Business Partner de IBM, la tarifa de suscripción mensual se calculará según el precio según catálogo actualizado del Servicio de Cloud en vigor para el mes contratado que es sujeto de la reclamación, con un descuento del 50%. IBM proporcionará una rebaja directamente el Cliente.

Los Niveles de Servicio y los créditos de Compensación asociados se miden por separado por Servicio de Cloud y por Aplicación del Cliente.

Cuando se calculan créditos de SLA para Servicios de Cloud basados en derechos de titularidad de Aplicación, la Disponibilidad se calculará a partir de las siguientes directrices:

- Cada Aplicación tendrá una parte compartida ponderada asignada en función del número contado de volumen de sesiones durante el mes contratado.
- El Tiempo de Inactividad de cada Servicio de Cloud por Aplicación se acumulará por separado para el mes contratado.

A continuación se muestra un ejemplo de cálculo para un mes de actividad y la ponderación asociada. Solo se presenta con fines ilustrativos:

Aplicaciones de tipo Retail	**Parte compartida del número total de sesiones en un mes contratado determinado**	**Tiempo de Inactividad total durante un mes contratado**	**Minutos Ponderados de Tiempo de Inactividad**
Aplicación de tipo Retail A	40%	300 minutos	40% x. 300 minutos = 120 minutos
Aplicación de tipo Retail B	20%	250 minutos	20% x 250 minutos = 50 minutos
Aplicación de tipo Retail C	40%	150 minutos	40% x 150 minutos = 60
			Total ponderado de Tiempo de Inactividad = 230 minutos

La Disponibilidad, expresada como porcentaje, se calcula de este modo: el número total de minutos en un mes contratado, menos el número total de minutos ponderados de Tiempo de Inactividad en un mes contratado, dividido por el número total de minutos en un mes contratado. Un cálculo de muestra basado en el ejemplo de ponderación anterior sería el siguiente:

$$\frac{\text{43.200 minutos en total en un mes contratado de 30 días - 230 minutos ponderados de Tiempo de Inactividad = 42.970 minutos}}{\text{43.200 minutos en total}} = \text{=2\% de crédito de Disponibilidad para un 99,4\% de disponibilidad durante el mes contratado}$$

4. Soporte Técnico

Existe Soporte Técnico para los Servicios de Cloud a disposición del Cliente y sus Participantes Elegibles, a fin de ayudarles a utilizar los Servicios de Cloud.

Se incluye Soporte Estándar en la suscripción de todas las ofertas. Trusteer Rapport Mandatory Service, un complemento de Trusteer Rapport, tiene un requisito previo de soporte Premium para la suscripción base a Trusteer Rapport.

Para cada oferta de Servicio de Cloud, hay una suscripción al soporte Premium disponible (Premium Support), con un cargo adicional, a excepción de **Servicios de Cloud IBM Trusteer Mobile SDK** y **Servicios de Cloud IBM Trusteer Rapport Mandatory Service**, **IBM Trusteer New Account Fraud**, **IBM Trusteer Pinpoint Assure**, **IBM Trusteer Digital Content Pack** y **IBM Trusteer Mobile Carrier Intelligence**. Póngase en contacto con el representante de Ventas de IBM o el Business Partner de IBM.

Soporte Estándar:

- Soporte de 8 AM a 5 PM, hora local.
- Los Clientes y sus Participantes Elegibles pueden enviar tickets de soporte por medios electrónicos, como se indica en el manual de SaaS de IBM, disponible en la dirección https://www.ibm.com/software/support/saas_support_guide.html.
- Los Clientes pueden acceder al Portal de Soporte del Cliente para ver notificaciones, documentos, informes de casos y Preguntas más frecuentes (FAQ) en: http://www-01.ibm.com/software/security/trusteer.

Soporte Premium (ofertas Premium Support):

- Soporte 24x7 para problemas de cualquier gravedad.

- Los Clientes pueden acceder al soporte directamente por teléfono y mediante solicitud de devolución de llamada.
- Los Clientes y sus Participantes Elegibles pueden enviar tickets de soporte por medios electrónicos, como se indica en el Manual de Soporte de Software como Servicio [SaaS].
- Los Clientes pueden acceder al Portal de Soporte del Cliente para ver notificaciones, documentos, informes de casos y Preguntas más frecuentes (FAQ) en: http://www.ibm.com/software/security/trusteer/support/.
- Para ver opciones e información de soporte, acceda al manual de SaaS de IBM, disponible en la dirección https://www.ibm.com/software/support/saas_support_guide.html.

5. Información de Derechos de Titularidad y Facturación

5.1 Métricas de Cargo

El Servicio de Cloud está disponible bajo la métrica de cargo especificada en el Documento Transaccional:

- Compromiso es una unidad de medición con la que se pueden obtener servicios. Un Contrato consiste en servicios de formación y/o profesionales relacionados con el Servicio de Cloud. Deben adquirirse derechos de titularidad suficientes para cubrir cada Contrato.
- Participante Elegible es una unidad de medición con la que se puede adquirir el Servicio de Cloud. Cada individuo o entidad elegible para participar en un programa de prestación de servicios gestionados o monitorizados por el Servicio de Cloud es un Participante Elegible. Deben adquirirse derechos de titularidad suficientes para cubrir a todos los Participantes Elegibles gestionados o seguidos por el Servicio de Cloud durante el período de medida especificado en el Documento Transaccional del Cliente.

  Cada programa de prestación de servicio gestionado por el Servicio de Cloud se analiza de forma independiente y luego se suma. Las personas o las entidades elegibles para varios programas de prestación de servicio requieren derechos de titularidad independientes.

  En el contexto de los derechos de titularidad de estos Servicios de Cloud, un Participante Elegible es un usuario final del Cliente con credenciales de inicio de sesión exclusivas sobre una Aplicación for Business o for Retail del Cliente.
- Dispositivo de Cliente es una unidad de medición con la que se puede adquirir el Servicio de Cloud. 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 prestados por, o acceda de cualquier otro modo al Servicio de Cloud durante el período de valoración especificado en el Documento Transaccional del Cliente.
- Aplicación es una unidad de medida con la que se puede adquirir el Servicio de Cloud. Una Aplicación es un programa de software con un nombre exclusivo. Deben adquirirse derechos de titularidad suficientes para cada Aplicación disponible para su acceso y uso durante el período de medida especificado en el POE o el Documento Transaccional del Cliente.

  Para los fines de este Servicio de Cloud, una Aplicación es una única Aplicación for Business o for Retail del Cliente.
- Llamada de API es una unidad de medida con la que se puede adquirir el Servicio de Cloud. Una Llamada de API es la invocación del Servicio de Cloud a través de una interfaz programable. Deben adquirirse derechos de titularidad suficientes para cubrir el número total de Llamadas de API, redondeado al diez, durante el periodo de medición especificado en el Documento de Titularidad (POE) o el Documento Transaccional del Cliente.
- Conexión es una unidad de medida con la que se puede adquirir el Servicio de Cloud. Una Conexión es un enlace o asociación de una base de datos, aplicación, servidor o cualquier otro tipo de dispositivo al Servicio de Cloud. Deben adquirirse derechos de titularidad suficientes para cubrir

el número total de Conexiones establecidas o realizadas a Servicio de Cloud durante el período de medida especificado en el POE o el Documento Transaccional del Cliente.

Para los fines de este Servicio de Cloud, una Conexión es una sesión o un flujo en la Aplicación del Cliente.

5.2 Cargo por Uso en Exceso

Si el uso actual del Servicio de Cloud durante el período de medición supera el derecho de titularidad especificado en el Documento de Titularidad (POE), se facturará un cargo por el uso en exceso bajo la tarifa especificada en el Documento Transaccional, el mes siguiente a la sucesión del uso en exceso.

5.3 Frecuencia de Facturación

En función de la frecuencia de facturación seleccionada, IBM facturará al Cliente los cargos adeudados al comienzo del período de frecuencia de facturación, excepto por los tipos de cargo de exceso y uso, que se facturarán a plazo vencido.

6. Opciones de Vigencia y Renovación

La vigencia del Servicio de Cloud empezará en la fecha en la que IBM notifique al Cliente que éste tiene acceso al Servicio de Cloud, según se describe en el POE. El POE especificará si el Servicio de Cloud se renueva automáticamente, sigue bajo una base de uso continuado o termina al finalizar la vigencia.

En relación con la renovación automática, a menos que el Cliente notifique su voluntad de no renovar como mínimo 90 días antes de la fecha de vencimiento, el Servicio de Cloud se renovará automáticamente por el plazo especificado en el POE. Las renovaciones están sujetas a un aumento de precio anual, según se especifique en un presupuesto. En el caso de que la renovación automática se realice después de la recepción de un aviso de retirada del Servicio de Cloud por parte de IBM, el plazo de renovación terminará en la fecha más próxima siguiente: el final del plazo de renovación actual o la fecha de retirada anunciada.

En relación con el uso continuado, el Servicio de Cloud seguirá estando disponible mensualmente, hasta que el Cliente notifique por escrito su voluntad de terminación con 90 días de antelación. El Servicio de Cloud seguirá estando disponible hasta el final del mes natural tras este período de 90 días.

7. Términos Adicionales

7.1 General

El Cliente acepta que IBM puede referirse públicamente al Cliente como suscriptor a los Servicios de Cloud en los comunicados de marketing o de tipo publicitario.

El Cliente no podrá utilizar los Servicios de Cloud, solos o en combinación con otros servicios o productos, como soporte a ninguna de las siguientes actividades de alto riesgo: diseño, construcción, control o mantenimiento de instalaciones nucleares, sistemas de tránsito masivo, sistemas de control de tráfico aéreo, sistemas de control de automoción, sistemas de armas, navegación de aviones o comunicaciones, ni ninguna otra actividad en la que un error del Servicio de Cloud pudiera dar lugar a una amenaza material de muerte o daños personales graves.

7.2 Software de Habilitación

El Servicio de Cloud requiere el uso de un software de habilitación que el Cliente descarga en los sistemas del Cliente para facilitar el uso del Servicio de Cloud. El Cliente puede utilizar el software de habilitación únicamente asociado con el uso del Servicio de Cloud. El software de habilitación se proporciona "TAL CUAL".

7.3 Despliegue de IBM Trusteer Fraud Protection

Para cada Aplicación a la cual se suscribe el Cliente, la suscripción básica del Cliente incluye actividades requeridas de configuración y despliegue inicial, en el cloud de IBM Trusteer, incluidos el inicio único inicial, la configuración, la Plantilla de Presentación, la prueba y la formación.

Las actividades de despliegue no incluyen las actividades de implementación que se requieren en las Aplicaciones o los sistemas del Cliente.

La fase de implementación de los distintos Servicios de Cloud está diseñada para implementarse en los plazos temporales que se detallan en las guías de despliegue pertinentes.

La finalización satisfactoria de estas fases de implementación dentro del plazo temporal estipulado depende del compromiso y la participación del equipo de gestión y del personal del Cliente. El Cliente debe proporcionar la información necesaria con la celeridad adecuada. El rendimiento de IBM depende de una información y unas decisiones tomadas a tiempo por parte del Cliente, y cualquier retraso puede suponer costes adicionales y/o retrasos en la finalización de estos servicios de implementación.

Para cada Aplicación a la cual se suscribe el Cliente, la suscripción básica del Cliente incluye actividades requeridas de configuración y despliegue inicial, en el cloud de IBM Trusteer, incluidos el inicio único inicial, la configuración, la Plantilla de Presentación, la prueba y la formación.

La suscripción del Cliente incluye soporte y pruebas para las páginas de la aplicación del Cliente, que se etiquetarán según lo recomendado por IBM en el despliegue inicial. IBM no es responsable de: (i) el despliegue parcial, (ii) la elección del Cliente de no desplegar los Servicios de Cloud según lo recomendado por IBM, o (iii) la elección del Cliente para llevar a cabo el despliegue, la configuración y las pruebas por su propia cuenta. (iv) Una protección o despliegue parciales puede comportar que el Cliente proporcione información inadecuada. Pueden contratarse servicios adicionales, incluyendo actividades de despliegue más allá del despliegue inicial, con un cargo adicional, bajo un contrato independiente.