IBM Trusteer Fraud Protection

Esta Descripción de Servicios 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 de Servicios:

Servicios de Cloud de Rapport:

- IBM Trusteer Rapport for Business
- Soporte Premium de IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Retail
- Soporte Premium de IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- Soporte Premium de IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Retail
- Soporte Premium de IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Phishing Protection for Business
- Soporte Premium de IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Retail
- Soporte Premium de IBM Trusteer Rapport Phishing Protection for Retail
- 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 for Business Standard Edition
- Soporte Premium de IBM Trusteer Pinpoint Malware Detection for Business, Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail, Standard Edition
- Soporte Premium de IBM Trusteer Pinpoint Malware Detection for Retail, Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- Soporte Premium de IBM Trusteer Pinpoint Malware Detection for Business, Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail, Advanced Edition
- Soporte Premium de IBM Trusteer Pinpoint Malware Detection for Retail, Advanced Edition
- IBM Trusteer Pinpoint Criminal Detection for Business
- Soporte Premium de IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Retail
- Soporte Premium de IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Carbon Copy for Business

- Soporte Premium de IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Pinpoint Carbon Copy for Retail
- Soporte Premium de IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Rapport Remediation for Retail
- Soporte Premium de IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business, Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail, Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business, Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail, Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications 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 Criminal Detection Redeployment
- 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 Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- 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 con integración de gestión de acceso for Retail
- IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso for Business
- IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Retail
- IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Servicios de Cloud de Mobile:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- Soporte Premium de IBM Trusteer Mobile Browser for Business

- IBM Trusteer Mobile Browser for Retail
- Soporte Premium de IBM Trusteer Mobile Browser 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 for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso for Business
- IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Business

1.1.2 Servicios de Cloud for Retail

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail, Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail, Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso for Retail
- IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

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

1.1.3 Servicios de Cloud Adicionales para IBM Trusteer Rapport

a. Servicios de Cloud Adicionales disponibles para IBM Trusteer Rapport 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 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, con un cargo adicional.

La Suscripción a IBM Trusteer Rapport for Business o IBM Trusteer Rapport 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 y/o IBM Trusteer Pinpoint Malware Detection II

a. Servicios de Cloud Adicionales disponibles para IBM Trusteer Pinpoint Malware Detection for Business, Advanced Edition o IBM Trusteer Pinpoint Malware Detection for Business, Standard Edition o para IBM Trusteer Pinpoint Malware Detection II for Business, Advanced Edition o IBM Trusteer Pinpoint Malware Detection II for Business, Standard Edition:

- IBM Trusteer Pinpoint Carbon Copy 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 for Retail, Advanced Edition o IBM Trusteer Pinpoint Malware Detection for Retail, Standard Edition o para IBM Trusteer Pinpoint Malware Detection II for Business, Advanced Edition o IBM Trusteer Pinpoint Malware Detection II for Business, Standard Edition:

- IBM Trusteer Pinpoint Carbon Copy 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 for Business o IBM Trusteer Pinpoint Malware Detection for Retail o IBM Trusteer Pinpoint Malware Detection II for Business o IBM Trusteer Pinpoint Malware Detection II for Retail es un requisito previo para los Servicios de Cloud de IBM adicionales asociados recogidos en este apartado.

1.1.5 Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Criminal Detection y/o IBM Trusteer Pinpoint Criminal Detection II

a. Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Criminal Detection for Business y/o IBM Trusteer Pinpoint Criminal Detection II:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

b. Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Criminal Detection for Retail y/o IBM Trusteer Pinpoint Criminal Detection II for Retail:

- IBM Trusteer Pinpoint Criminal 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 Criminal Detection for Business o IBM Trusteer Pinpoint Criminal Detection for Retail o IBM Trusteer Pinpoint Criminal Detection II for Business o IBM Trusteer Pinpoint Criminal Detection II for Retail es un requisito previo para los Servicios de Cloud de IBM adicionales asociados recogidos en este apartado.

1.1.6 Servicios de Cloud Adicionales para IBM Trusteer Pinpoint Detect Standard y/o IBM Trusteer Pinpoint Detect Premium y/o IBM Security Pinpoint Detect Standard con integración de gestión de acceso y/o IBM Security Detect Premium con integración de gestión de acceso

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

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

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

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

La suscripción a IBM Trusteer Detect Standard o IBM Trusteer Pinpoint Detect Premium o IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso o IBM Security Detect Premium con integración de gestión de acceso es un requisito previo para los Servicios de Cloud adicionales asociados recogidos en este apartado.

1.1.7 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 al software de habilitación de Cliente de IBM Trusteer Mobile Browser, 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.

2. Servicios de Cloud de IBM Trusteer Rapport

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

Trusteer Rapport proporciona una capa de protección contra el phishing y los ataques de malware de 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.

Este Servicio de Cloud dispone de una métrica de Participante Elegible. La oferta for Business se vende en paquetes de 10 Participantes Elegibles. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles.

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, acuerdo 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.

2.2 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. La oferta for Business se vende en paquetes de 10 Participantes Elegibles. La oferta for Retail se vende en paquetes de 100 Participantes Elegibles.

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, acuerdo 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.

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

La Suscripción a los Servicios de Cloud IBM Trusteer Rapport o IBM Trusteer Rapport II es un requisito previo para la suscripción a cualquiera de los Servicios de Cloud siguientes 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 incidencias de los Participantes Elegibles 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.

2.3.1 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.

2.3.2 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.

2.3.3 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.

El Soporte Premium de IBM Trusteer Rapport for Business es un requisito previo para IBM Rapport Mandatory Service for Business.

El Soporte Premium de IBM Trusteer Rapport 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.

2.3.4 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 o 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.

2.3.5 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 de cualquier Aplicación Empresarial 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 de cualquier Aplicación de Distribuidor adicional más allá de la primera Aplicación requiere derecho de titularidad del Servicio de Cloud IBM Trusteer Rapport Additional Applications for Retail.

3. 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.

3.1 IBM Trusteer Pinpoint Malware Detection e IBM Trusteer Pinpoint Criminal Detection

En el caso de que se detecte malware en los Servicios de Cloud IBM Trusteer Pinpoint Malware Detection o los Servicios de Cloud IBM Trusteer Pinpoint Malware Detection II, que se detecte toma de control de cuentas en los Servicios de Cloud IBM Trusteer Pinpoint Criminal Detection o los Servicios de Cloud IBM Trusteer Pinpoint Criminal Detection II, el Cliente debe seguir la Guía de Prácticas Recomendadas de Pinpoint. No utilice los Servicios de Cloud IBM Trusteer Pinpoint Malware Detection, los Servicios de Cloud IBM Trusteer Pinpoint Malware Detection II, los Servicios de Cloud IBM Trusteer Pinpoint Criminal Detection o los Servicios de Cloud IBM Trusteer Pinpoint Criminal 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 los Servicios de Cloud IBM Trusteer Pinpoint (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).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business y/o IBM Trusteer Pinpoint Criminal Detection for Retail

Detección sin Cliente de actividad sospechosa de toma de control de cuentas mediante navegadores conectados a una Aplicación for Business o for Retail, mediante un ID de dispositivo, detección de phishing y detección de robo de credenciales mediante malware. Los Servicios de Cloud de IBM Trusteer Pinpoint Criminal Detection 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.

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 para las cuales el Cliente haya suscrito la cobertura de los Servicios de Cloud. El Cliente también puede recibir los datos de incidencias a través de una modalidad de entrega de la API de fondo.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business y/o IBM Trusteer Pinpoint Criminal Detection for Retail II

IBM Security Pinpoint Criminal Detection II es una reformulación de IBM Trusteer Pinpoint Criminal 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 actividad sospechosa de toma de control de cuentas mediante navegadores conectados a una Aplicación for Business o for Retail, mediante un ID de dispositivo, detección de phishing y detección de robo de credenciales mediante malware. Los Servicios de Cloud IBM Trusteer Pinpoint Criminal Detection II 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.

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 para las cuales el Cliente haya suscrito la cobertura de los Servicios de Cloud. El Cliente también puede recibir los datos de incidencias a través de una modalidad de entrega de la API de fondo.

   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 Criminal Detection Additional Applications.

3.4 IBM Trusteer Pinpoint Malware Detection for Business, Advanced Edition y/o IBM Trusteer Pinpoint Malware Detection for Retail, Advanced Edition y/o IBM Trusteer Pinpoint Malware Detection for Business, Standard Edition y/o IBM Trusteer Pinpoint Malware Detection for Retail, Standard Edition

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:

   La Advanced Edition for Business y/o for Retail ofrece 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 100000 Participantes Elegibles for Retail o 10000 Participantes Elegibles for Business, lo que equivale a 1000 paquetes de 100 Participantes Elegibles for Retail o 1000 paquetes de 10 Participantes Elegibles for Business.

c. Standard Edition:

   La Standard Edition for Business o for Retail es una solución de despliegue rápido que proporciona la funcionalidad principal de este Servicio de Cloud, como se describe en este documento.

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

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:

   La Advanced Edition for Business y/o for Retail ofrece 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 100000 Participantes Elegibles for Retail o 10000 Participantes Elegibles for Business, lo que equivale a 1000 paquetes de 100 Participantes Elegibles for Retail o 1000 paquetes de 10 Participantes Elegibles for Business.

c. Standard Edition:

   La Standard Edition for Business o for Retail es una solución de despliegue rápido que proporciona 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.

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

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

- Para IBM Trusteer Pinpoint Carbon Copy for Business, existe como requisito previo IBM Trusteer Pinpoint Malware Detection for Business, Standard Edition o IBM Trusteer Pinpoint Malware Detection for Business, Advanced Edition o IBM Trusteer Pinpoint Malware Detection II for Business, Standard Edition o IBM Trusteer Pinpoint Malware Detection II for Business, Advanced Edition.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business and/or IBM Trusteer Pinpoint Carbon Copy for Retail

Ofertas de IBM Trusteer Pinpoint Carbon Copy diseñadas para proporcionar otra capa de protección y un servicio de monitorización que puede ayudar a detectar si las credenciales de un Participante Elegible se han visto comprometidas por ataques de Phishing sobre las Aplicaciones for Business o for Retail del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de Servicio de Cloud.

3.6.2 IBM Trusteer Rapport Remediation for Retail and/or 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 o 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 de que su configuración de Cliente debe incluir la recopilación de los ID de usuario. A efectos de claridad, 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.

3.6.3 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 y/o 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.

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

3.7 Servicios de Cloud Adicionales Opcionales para IBM Trusteer Pinpoint Criminal Detection for Business y/o IBM Trusteer Pinpoint Criminal Detection for Retail y/o IBM Trusteer Pinpoint Criminal Detection II for Business y/o IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal 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 del Servicio de Cloud IBM Trusteer Pinpoint Criminal Detection deben adquirir IBM Trusteer Pinpoint Criminal 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.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business y/o IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Para IBM Trusteer Pinpoint Criminal Detection II for Business, el despliegue de cualquier Aplicación Empresarial adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. Para IBM Trusteer Pinpoint Criminal Detection II for Retail, el despliegue de cualquier Aplicación de Distribuidor adicional más allá de la primera Aplicación requiere derecho de titularidad de IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. 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 for Business y/o for Retail 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).

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

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 programa cliente de actividades sospechosas de malware y/o suplantación de cuentas de los navegadores que se conectan a una Aplicación for Business o for Retail, 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.

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 Detect Premium.

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.

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

Este Servicio de Cloud combina IBM Trusteer Pinpoint Criminal Detection e IBM Trusteer Pinpoint Malware Detection para ofrecer una solución única, unificada y fácil de integrar, con servicios y funcionalidad adicionales, que incluyen: servicios de configuración y despliegue ampliados, servicios de seguridad personalizada, servicios de investigación, etc.

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.

4.3 IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso for Business y/o IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso for Retail

El Servicio de Cloud IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso incluye la funcionalidad de IBM Security Pinpoint Detect Standard según se detalla en el apartado 4.1 anterior.

IBM Trusteer Pinpoint Detect Standard con integración de gestión de acceso se utiliza al adquirirse con sistemas de gestión de acceso, como IBM Security Access Management ("ISAM"). Cuando se adquiere con ISAM, ambas ofertas deben estar habilitadas. Esta oferta incluye la opción de integración con el sistema de gestión de acceso. No incluye derecho de titularidad para el sistema de gestión de acceso.

Esta oferta 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.

En este Servicio de Cloud se incluye soporte estándar (según se define en el apartado Soporte Técnico). IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Business y/o IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso for Retail

El Servicio de Cloud IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso incluye la funcionalidad de IBM Security Pinpoint Detect Premium según se detalla en el apartado 4.2 anterior, y la opción de integración con el sistema de gestión de acceso.

IBM Trusteer Pinpoint Detect Premium con integración de gestión de acceso se utiliza al adquirirse con sistemas de gestión de acceso, como IBM Security Access Management ("ISAM"). Cuando se adquiere con ISAM, ambas ofertas deben estar habilitadas. Este Servicio de Cloud incluye la opción de integración

con el sistema de gestión de acceso. No incluye derecho de titularidad para el sistema de gestión de acceso.

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 esta oferta.

4.4 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 for Retail o IBM Trusteer Pinpoint Detect Standard for Retail.

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

El objetivo de IBM Trusteer Rapport for Mitigation 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 for 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 de claridad, 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.

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

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

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

4.5.2 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.

5. Servicios de Cloud de IBM Trusteer Mobile

5.1 IBM Trusteer Mobile Browser for Business y/o IBM Trusteer Mobile Browser for Retail

IBM Trusteer Mobile Browser se ha diseñado para añadir otra capa de protección y su objetivo es proporcionar acceso seguro en línea de los dispositivos móviles de Participantes Elegibles con acceso a las Aplicaciones for Business o Distribuidores 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 phishing. La detección de Wi-Fi segura solo está disponible en plataformas Android. Este Servicio de Cloud incluye los dispositivos móviles, los teléfonos móviles o las tabletas y no incluyen PC o Mac portátiles.

A través de TMA, el Cliente puede recibir datos de incidencias, análisis e información estadística relacionada con Dispositivos cuyos Participantes Elegibles: (i) hayan descargado el Software de Cliente del Titular de la Cuenta, una aplicación con licencia para el público sujeta a un acuerdo de licencia de usuario final ("EULA") gratuita y disponible para su descarga en los dispositivos móviles de los Participantes Elegibles, y (ii) hayan aceptado el EULA y se hayan autenticado, al menos una vez, en las Aplicaciones for Business o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de los Servicios de Cloud. El Cliente solo puede comercializar el Software de Cliente del Titular de la Cuenta utilizando Trusteer Splash y no puede utilizar el Software de Cliente del Titular de la Cuenta para sus operaciones internas de empresa.

a. Datos de incidencias:

   El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir los datos de incidencias generados a raíz de las interacciones en línea de los dispositivos móviles con las Aplicaciones for Business o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de Servicios de Cloud.

b. 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 ("Plantillas de Presentación"). 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 o 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.

5.2 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 Distribuidores 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 de Servicios; 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 Acuerdo, 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 ha probado las aplicaciones de ejemplo creadas con las herramientas móviles proporcionadas en IBM Trusteer Mobile SDK ("Herramientas Móviles") para determinar si se ejecutarán correctamente con determinadas versiones de plataformas de sistemas operativos para móviles de Apple (iOS), Google (Android) y otros proveedores (colectivamente "Plataformas de SO para Dispositivos Móviles"), aunque las Plataformas de SO para Dispositivos Móviles las suministran terceros, no quedan bajo el control de IBM y están sujetas a posibles cambios sin aviso previo a IBM. Por todo ello, e independientemente que

se exprese lo contrario, IBM no garantiza que ninguna aplicación u otro tipo de producto que se haya creado utilizando las Herramientas de Movilidad se ejecutará adecuadamente, interoperará correctamente o será compatible en relación con cualquier Plataforma de SO para Dispositivos Móviles o en relación con cualquier dispositivo móvil.

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 Acuerdo, 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 Originales y Materiales de Ejemplo sin tener obligación alguna de prestar soporte y lo proporciona "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDA CUALQUIER GARANTÍA DE TITULARIDAD, NO INFRACCIÓN O NO INTERFERENCIA, Y TODAS LAS GARANTÍAS Y CONDICIONES IMPLÍCITAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UN OBJETIVO CONCRETO. 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.

El Cliente acuerda crear, conservar y proporcionar a IBM y a sus auditores registros precisos por escrito, salidas de las herramientas del sistema y otra información sobre el sistema suficiente para verificar que el uso de IBM Trusteer Mobile SDK por parte del Cliente se realiza conforme a esta Descripción de Servicios.

6. Soporte Premium

El Cliente tiene derecho al Soporte Premium solo para aquellos Servicios de Cloud para los cuales haya suscrito la oferta asociada de Soporte Premium.

7. 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/costos 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 acuerdo independiente.

8. Privacidad y seguridad de datos

Este Servicio de Cloud cumple los principios de privacidad y seguridad de los datos de IBM para SaaS IBM que están disponibles en http://www.ibm.com/cloud/data-security y los términos adicionales que se proporcionan en este apartado. Cualquier cambio en los principios de privacidad y seguridad de los datos de IBM no significará una disminución de la seguridad del Servicio de Cloud.

Este Servicio de Cloud puede utilizarse para procesar contenido que contenga datos personales si el Cliente, como responsable del tratamiento de datos, determina que las medidas de seguridad técnicas y organizativas son apropiadas para los riesgos presentados por el procesamiento y la naturaleza de los datos a proteger. El Cliente reconoce que este Servicio de Cloud no ofrece dispositivos para la protección de datos personales sensibles o datos sujetos a requisitos regulatorios adicionales.

Este Servicio de Cloud está incluido en la certificación Privacy Shield de IBM y se aplica cuando el Cliente opta por alojar el Servicio de Cloud en un centro de datos ubicado en los Estados Unidos, y está sujeto a la Política de Privacy Shield de IBM, disponible en http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Características y Responsabilidades de Seguridad

El Servicio de Cloud implementa las características de seguridad siguientes:

El Servicio de Cloud encripta el contenido durante la transmisión de datos a/desde la red de IBM y cuando está en espera de la transmisión de datos desde el punto final.

8.2 Uso Legítimo y Consentimiento

Uso Legítimo

El uso de este Servicio de Cloud puede implicar distintas leyes o normativas. El Servicio de Cloud únicamente puede utilizarse con objetivos conformes a la ley y de forma lícita. El Cliente acepta utilizar el Servicio de Cloud de acuerdo con las políticas, normativas y leyes aplicables y es plenamente responsable de su cumplimiento.

Autorización para la recopilación y el tratamiento de datos

El Servicio de Cloud recopila la información de los Dispositivos del Cliente y los Participantes Elegibles que interactúan con las Aplicaciones for Business o for Retail para las cuales el Cliente haya suscrito la cobertura del Servicio de Cloud. El Servicio de Cloud recopila información que, de manera independiente o combinada, se puede considerar Datos Personales en algunas jurisdicciones. Datos Personales es cualquier información que puede utilizarse para identificar a una persona individual, como un nombre, una dirección de correo electrónico, una dirección postal o un número de teléfono que se proporcione a IBM para almacenar, procesar o transferir en representación del Cliente.

Las prácticas de recopilación y tratamiento de datos se pueden actualizar para mejorar la funcionalidad del Servicio de Cloud. El documento con la descripción completa de las prácticas de recopilación y tratamiento de datos se actualiza cuando es necesario y está a disposición de los Clientes que lo soliciten. El Cliente autoriza a IBM a recopilar esta información y tratarla de acuerdo con los requisitos del apartado Transferencias Internacionales y el apartado Privacidad de los Datos de esta Descripción de Servicios.

Para las ofertas de IBM Trusteer que incluyen Trusteer Management Application (TMA):

Los datos siguientes se recopilan y almacenan en Trusteer Management Application (TMA) para administradores de TMA de la empresa patrocinadora: dirección de correo electrónico (como inicio de sesión), contraseña hash, nombre, apellidos, cargo y departamento.

Para Servicios de Cloud de IBM Trusteer Pinpoint:

Los datos recopilados pueden incluir lo siguiente:

- identificadores de usuario o de punto final como un ID de Usuario de hash unidireccional o cifrado, un ID de Usuario Persistente (PUID), una Clave de Agente de Rapport y el ID de Sesión del Cliente o;
- datos relacionados con la aplicación protegida, como atributos/elementos específicos de la aplicación de banca online de los respectivos clientes según se representan en el navegador del usuario final, visitas al sitio web e historial de navegación;
- información del entorno de software instalado, configuración y atributos de navegador y dispositivo, y la longitud del historial del navegador;

- indicación de fecha y hora e información del hardware;
- cabeceras del navegador y datos del protocolo de comunicación, como la dirección IP del usuario, cookies, cabecera de referencia y otras cabeceras HTTP;
- datos de movimiento del ratón del usuario final, como las coordenadas del puntero del ratón, los clics y el movimiento de la rueda de desplazamiento (y sus equivalentes) y la indicación de tiempo y hora mientras se interactúa con la aplicación de banca electrónica del Cliente;
- sitios de phishing e información enviada a sitios de phishing; y
- a discreción exclusiva del Cliente, datos transaccionales (importes transaccionales, divisas transaccionales y códigos de destinación, identificadores de tarjetas bancarias de transacciones de hash unidireccional, identificadores de cuentas de tarjetas de transacciones de hash unidireccional, valores binarios si la transacción es un nuevo tenedor, fecha y hora de la transacción) y calificación de riesgo de los datos opcional.
- A discreción exclusiva del Cliente, teclear ritmos en el teclado y secuencias de teclas utilizadas por el usuario final para introducir un nombre de usuario, una contraseña y otro texto (pero no las letras, números o caracteres especiales en sí, y sin capacidad de discernir el nombre de usuario o la contraseña);

El Cliente entiende y acepta que IBM no recopila, almacena, gestiona ni realiza el mantenimiento de los libros y/o registros oficiales del Cliente.

Cuando el Cliente se suscribe a la oferta IBM Trusteer Rapport for Remediation o a algunos de los casos de soporte de Pinpoint, IBM puede recomendar que el Software Cliente de Titular de la Cuenta de Rapport se instale en la máquina de un Participante Elegible con el fin de investigar y estudiar la infección de malware sospechoso. Los datos recogidos para las ofertas Rapport se exponen a continuación.

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

Los datos recopilados pueden incluir lo siguiente:

- direcciones URL y de protocolo Internet (IP) de los sitios web que un Titular de la Cuenta visita y que IBM considera que son potencialmente fraudulentas, de phishing o de explotación, junto con información sobre la naturaleza de las amenazas identificadas;
- direcciones URL y direcciones IP de los sitios web que un Titular de la Cuenta visita y que están controladas por el Cliente y protegidas por el Servicio de Cloud, tales como sitios de banca online; direcciones IP del Titular de la Cuenta;
- información sobre identificación de hardware, sistemas operativos, software de aplicaciones, hardware periférico, configuración de seguridad, configuración del sistema y conexiones de red del punto final, así como ID, nombre, patrones de uso y otra información de identificación personal del punto final;
- información relacionada con la instalación y el funcionamiento del programa, el ID del programa, la versión del programa, las incidencias de seguridad generadas a partir del punto final e información sobre los errores del programa;
- estadísticas de uso e información estadística acerca de las amenazas detectadas por el programa; archivos de registro que contienen los bloqueos del navegador, fecha y hora de la infección e información sobre la naturaleza de las amenazas identificadas o el mal funcionamiento;
- Afiliación del Cliente, también referida como Empresa Patrocinadora. Se establece una afiliación cuando un usuario final descarga Rapport del sitio web del Cliente, selecciona un Cliente en particular al descargar Rapport desde el sitio de soporte de Trusteer o inicia sesión en la aplicación bancaria del Cliente. Un usuario final puede tener más de una afiliación de Cliente;
- una copia del ID de Usuario cifrado que el Titular de la Cuenta utiliza para interactuar con el Cliente (opcional);
- una copia cifrada de un número de tarjeta de crédito que el Titular de la Cuenta introduce en un sitio después de que el programa informa al Titular de la Cuenta que el programa considera el sitio como de riesgo;

- archivos y otra información del punto final que los expertos de seguridad de IBM sospechen que pueden estar relacionados con malware u otra actividad maliciosa, o que puedan estar asociados con un mal funcionamiento general del programa; y
- Información de contacto personal, incluyendo el nombre y el correo electrónico, cuando el usuario final se ponga en contacto con Soporte Técnico.

Para las ofertas de IBM Trusteer Mobile SDK y para los Servicios de Cloud IBM Trusteer Mobile Browser:

Los datos recopilados pueden incluir lo siguiente:

- identificadores de usuario, como un ID de Usuario de hash unidireccional o cifrado;
- información del dispositivo, como la dirección IP, el ID de dispositivo de hash, indicación de fecha y hora, valores MD5 de paquetes instalados y otra información de hardware y software del dispositivo;
- versión Mobile SDK o Mobile Browser y fecha de instalación;
- visitas a aplicaciones protegidas;
- afiliación del Cliente; y
- datos de riesgo del dispositivo (por ejemplo, presencia de malware, ocultadores de root, estado de encriptación Wi-Fi, si un dispositivo está destrabado/"jailbroken");
- rastreo de la pila de bloqueo (en caso de una terminación inesperada de la aplicación);
- datos internos del teléfono (por ejemplo, modelo, fabricante);
- interacciones de la pantalla táctil de los usuarios finales, incluyendo coordenadas x/y, área táctil y tipo de acción (hacia abajo, hacia arriba y hacia arriba);
- datos del sensor de movimiento, uso de energía/recursos, ajustes de conectividad, sensores ambientales como la temperatura, la luz y la presión atmosférica, así como ajustes generales del dispositivo (volumen, timbre, brillo de la pantalla, etc.).

8.3 Consentimiento Informado de los Interesados

Para los Servicios de Cloud IBM Trusteer Pinpoint y para Servicios de Cloud IBM Trusteer Mobile SDK:

El Cliente declara que ha obtenido, u obtendrá, los consentimientos perfectamente informados, permisos o licencias que sean necesarios para realizar un uso legítimo del Servicio de Cloud, así como para permitir la recopilación y el tratamiento de la información, incluidos los Datos Personales, por parte de IBM mediante el Servicio de Cloud.

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) y los Servicios de Cloud IBM Trusteer Mobile Browser:

El Cliente autoriza a IBM a obtener los consentimientos perfectamente informados que sean necesarios para realizar un uso legítimo del Servicio de Cloud, así como recopilar y tratar la información, según lo descrito en el Acuerdo de Licencia de Usuario Final disponible en https://www.trusteer.com/support/end-user-license-agreement. En caso de que el Cliente determine que él (y no IBM) será quien gestione las comunicaciones de consentimiento con los usuarios finales, el Cliente declara que ha obtenido, u obtendrá, los consentimientos perfectamente informados, permisos o licencias que sean necesarios para realizar un uso legítimo del Servicio de Cloud, 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 Servicio de Cloud.

8.4 Uso de Datos de Seguridad

Como parte del Servicio de Cloud que incluye actividades de información, IBM preparará y mantendrá información sin identificación y/o agregada recopilada del Servicio de Cloud ("Datos de Seguridad"). Los Datos de Seguridad no identificarán al Cliente, a sus Participantes Elegibles o a una persona individual, salvo en lo dispuesto en el apartado (d), a continuación. El Cliente acepta que IBM puede utilizar y/o copiar de forma permanente los Datos de Seguridad solo para los fines siguientes:

a. la publicación y/o difusión de los Datos de Seguridad (por ejemplo, en recopilaciones y/o análisis relacionados con la seguridad cibernética),

b. el desarrollo o la mejora de productos o servicios,

c. la realización de investigación internamente o con terceros, y

d. el uso legal compartido de información de infractores terceros confirmados.

8.5 Transferencias Internacionales

El Cliente acepta que IBM podrá tratar el contenido, incluidos los Datos Personales identificados en el apartado Uso Legítimo y Consentimiento anterior, de acuerdo con las leyes y requisitos relevantes fuera de las fronteras de un país, para Encargados o Subencargados del tratamiento de datos en los siguientes países de fuera del Espacio Económico Europeo y no incluidos entre los países que la Comisión Europea considere que cuentan con niveles de seguridad adecuados: EE.UU.

8.6 Privacidad de los Datos

Si el Cliente pone Datos Personales a disposición del Servicio de Cloud en los Estados Miembros de la UE, Islandia, Liechtenstein, Noruega o Suiza, o si el Cliente dispone de Participantes Elegibles o Dispositivos de Cliente en dichos países, el Cliente es el Responsable exclusivo del tratamiento de los Datos Personales y designa a IBM como Encargado del tratamiento (tal y como estos términos se definen en la Directiva 95/46/EC de la UE) de los Datos Personales. IBM solo tratará estos Datos Personales en la medida en la que sea necesario para que la oferta de Servicio de Cloud esté disponible, de acuerdo con las descripciones publicadas por IBM de los Servicios de Cloud, y el Cliente acepta que cualquier tratamiento de este tipo se hará siguiendo sus propias instrucciones. IBM proporcionará una notificación anticipada a través del Portal del Cliente dentro de un margen razonable si IBM realiza un cambio material en la ubicación de procesamiento o en la forma de asegurar los Datos Personales como parte del Servicio de Cloud. El Cliente podrá resolver el período de suscripción actual del Servicio de Cloud afectado enviando una notificación escrita a IBM dentro de los treinta (30) días posteriores a la notificación al Cliente, por parte de IBM, del cambio.

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.

a. El Cliente acepta que, para los servicios prestados a través del centro de datos de Alemania, según se determine durante el proceso de aprovisionamiento, IBM puede tratar el contenido que incluya Datos Personales fuera de las fronteras del país para los siguientes Encargados o Subencargados del tratamiento de datos:

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
Entidad contratante de IBM	Encargado del tratamiento	Según lo indicado en el Documento Transaccional
Amazon Web Services (Alemania)	Subencargado del tratamiento	Alemania
IBM Ireland Ltd.	Encargado del tratamiento	Irlanda
IBM Israel Ltd.	Encargado del tratamiento	Israel

Para los servicios prestados a través del centro de datos de Alemania, algunos servicios de soporte al Cliente pueden ser proporcionados por empleados de Trusteer situados en cualquier país de la Unión Europea.

b. El Cliente acepta que, para los servicios prestados a través del centro de datos de Japón, según se determine durante el proceso de aprovisionamiento, IBM puede tratar el contenido que incluya Datos Personales fuera de las fronteras del país para los siguientes Encargados o Subencargados del tratamiento de datos:

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
Entidad contratante de IBM	Encargado del tratamiento	Japón, según lo indicado en el Documento Transaccional

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
Amazon Web Services (Japón)	Subencargado del tratamiento	Japón
IBM Ireland Ltd.	Encargado del tratamiento	Irlanda
IBM Israel Ltd.	Encargado del tratamiento	Israel

c. El Cliente acepta que, para los servicios prestados a través del centro de datos de EE.UU., IBM puede tratar el contenido que incluya Datos Personales fuera de las fronteras del país para los siguientes Encargados o Subencargados del tratamiento de datos:

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
Entidad contratante de IBM	Encargado del tratamiento	Según lo indicado en el Documento Transaccional
Amazon Web Services LLC	Subencargado del tratamiento	Estados Unidos
IBM Ireland Ltd.	Encargado del tratamiento	Irlanda
IBM Israel Ltd.	Encargado del tratamiento	Israel
IBM Corp	Encargado del tratamiento	Estados Unidos

d. Para los servicios prestados a través de los Centros de Datos enumerados en el apartado 8.5.c anterior, relativo a los centros de datos de EE.UU., IBM también puede realizar procesos a través de uno o más de los siguientes subencargados del tratamiento de datos aplicables, según se determine durante el proceso de aprovisionamiento:

Nombre del Encargado/Subencargado del tratamiento	Rol (Encargado o Subencargado del tratamiento de datos)	Ubicación
Amazon Web Services (Australia)	Subencargado del tratamiento	Australia
Amazon Web Services (Singapur)	Subencargado del tratamiento	Singapur
Amazon Web Services (Irlanda)	Subencargado del tratamiento	Irlanda

e. El Cliente acepta que IBM puede, con un aviso a través del Portal del Cliente, migrar el procesamiento de Amazon Web Services a los centros de datos de IBM. Además, IBM puede, con un aviso a través del Portal del Cliente, cambiar las listas de subencargados del tratamiento de datos anteriores.

f. 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.

g. Los datos de soporte al Cliente se almacenan en un servidor cloud de Salesforce.com que se encuentra en Irlanda.

h. 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 de Servicios.

9. Acuerdo de Nivel de Servicio (SLA)

IBM proporciona el siguiente acuerdo 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.

9.1 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 plazo temporal durante el cual el procesamiento 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 pueden superar el 10 por ciento de una doceava parte (1/12) del cargo anual por el Servicio de Cloud.

9.2 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)
< 99,5%	2%
< 98,0%	5%
< 96,0%	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 Servicio 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 Distribuidores	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 Distribuidor A	40%	300 minutos	40% x. 300 minutos = 120 minutos
Aplicación de Distribuidor B	20%	250 minutos	20% x 250 minutos = 50 minutos
Aplicación de Distribuidor 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:

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

10. 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, con un cargo adicional, a excepción de los Servicios de Cloud IBM Trusteer Mobile SDK y los Servicios de Cloud IBM Trusteer Rapport Mandatory Service. Póngase en contacto con su 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 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-01.ibm.com/software/security/trusteer/support/.
- Para ver opciones e información de soporte, acceda al Manual de Soporte de Software como Servicio [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Soporte Premium:

- 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-01.ibm.com/software/security/trusteer/support/.
- Para ver opciones e información de soporte, acceda al Manual de Soporte de Software como Servicio [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

11. Información de Derechos de Titularidad y Facturación

11.1 Métricas de Cargo

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

a. **Participante Elegible**: es una unidad de medida 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.

b. **Dispositivo de Cliente**: es una unidad de medida 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 medida especificado en el Documento Transaccional del Cliente.

c. **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 el Servicio de Cloud, una aplicación es una única Aplicación for Business o for Retail del Cliente.

d. **Contrato**: es una unidad de medida con la que se pueden obtener los servicios. Un Compromiso consiste en servicios de formación y/o profesionales relacionados con los Servicios de Cloud. Deben adquirirse derechos de titularidad suficientes para cubrir cada Contrato.

11.2 Cargo Mensual Parcial

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

12. Cumplimiento y Auditoría

El acceso a los Servicios de Cloud IBM Trusteer Fraud Protection está sujeto a una cantidad máxima de Aplicaciones, Participantes Elegibles y/o Dispositivos de Cliente, según lo especificado en el Documento Transaccional. El Cliente es responsable de garantizar que el número de Aplicaciones, Participantes Elegibles y/o Dispositivos de Cliente no supere la cantidad máxima especificada en el Documento Transaccional.

IBM puede realizar una auditoría para verificar el cumplimiento de la cantidad máxima de Aplicaciones, Participantes Elegibles y/o Dispositivos de Cliente.

13. 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.

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.

14. Software de Habilitación

Este Servicio de Cloud incluye el software de habilitación, que debe utilizarse únicamente junto con el uso del Servicio de Cloud por parte del Cliente, y únicamente durante el plazo del Servicio de Cloud.

15. Incremento de la Tarifa de Suscripción Anual a IBM Trusteer

IBM se reserva el derecho a ajustar la tarifa de suscripción de los Servicios de Cloud. El ajuste de la tarifa de suscripción se reflejará en los precios especificados en y para el plazo de la Oferta aplicable. Pueden aplicarse ajustes adicionales en la tarifa de suscripción, que serán aplicables un máximo de una vez cada doce (12) meses en un porcentaje que determinará IBM y que no superará el 3%, cuando el plazo de los Servicios de Cloud se amplíe mediante la renovación automática o el uso continuado. Estos ajustes de tarifa no modificarán los derechos de titularidad del Cliente con respecto a los Servicios de Cloud ni a la métrica de cargo mediante la cual se obtiene el Servicio de Cloud. Los Business Partners de IBM son independientes de IBM y determinan sus precios y condiciones unilateralmente.