# IBM Trusteer Pinpoint Detect

Esta Descripción del Servicio describe el Servicio de Cloud. Los documentos de pedidos aplicables proporcionan precios y detalles adicionales sobre el pedido del Cliente.

## 1. Servicio de Cloud

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. Trusteer Management Application (TMA) y Trustboard:

   TMA es la aplicación de gestión tradicional de Trusteer que permite a los Clientes evaluar y clasificar alertas. Trustboard es una nueva aplicación de gestión que se utiliza principalmente para la investigación. Los Clientes pueden elegir utilizar TMA o Trustboard en cualquier momento. TMA y Trustboard están disponibles 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. IBM Trusteer Pinpoint Detect e IBM Trusteer Pinpoint Verify se utilizan como parte del inicio de sesión de TMA y Trustboard.

b. Script web y/o API:

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

Una "Sesión" es una interacción entre la Aplicación (Web o Móvil) del Cliente y el Servicio de Cloud que genera una o varias evaluaciones de riesgo en tiempo real. Una Sesión se mide desde el momento del principio de la interacción hasta el final de la interacción. El final de una interacción se registra cuando se produce uno de los siguientes sucesos:

- La interacción se restablece de forma normal cerrando la sesión de la aplicación.
- Se cierra el navegador, la aplicación o el separador.
- Se suprimen las cookies.
- Se excede el tiempo de espera.

Una Sesión puede incluir un número cualquiera de actividades como, por ejemplo: inicio de sesión, navegación, pago, configuración de pago, etc., según se define en la Aplicación del Cliente. Se aclara que para los fines de este Servicio de Cloud, una Conexión (como se define a continuación) es equivale a una Sesión.

### 1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles.

#### 1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail y/o IBM Trusteer Pinpoint Detect Standard for Business

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

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

puede utilizarse para los accesos del personal remoto, con el fin de evaluar el riesgo de dispositivos gestionados y no gestionados.

En este Servicio de Cloud se incluye soporte Premium (según se define en el apartado Soporte Técnico siguiente).

El servicio está disponible para adquirirse por paquetes de 100 Participantes Elegibles o por paquetes de 100 Conexiones.

### 1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail y/o IBM Trusteer Pinpoint Detect Premium for Business

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

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

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

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

El soporte Premium se incluye en este Servicio de Cloud.

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

**Pinpoint Detect Policy Manager:**

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

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

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

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

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

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

### 1.1.3 IBM Trusteer Pinpoint Detect for Connections

Este Servicio de Cloud proporciona protección, detección de intentos de toma de control de la cuenta, y puntuaciones de evaluación de riesgo/confianza de navegadores y/o dispositivos móviles (mediante el navegador nativo de la aplicación móvil del Cliente) que acceden a una aplicación for Business o for Retail. La solución utiliza varios indicadores de riesgo que analizan el dispositivo, la conexión y el comportamiento del usuario final, y los comparan con el historial del usuario para identificar usos sospechosos.

El Servicio de Cloud puede consumir conexiones de canales móviles y web. IBM Trusteer Pinpoint Detect incluye derechos de titularidad de IBM Trusteer Mobile SDK, si es aplicable.

El Servicio de Cloud está disponible en paquetes de 100 Conexiones al año.

## 1.2 Servicios Opcionales

Para los Servicios de Cloud de esta sección, hay un requisito previo de derecho de titularidad de IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard o IBM Trusteer Pinpoint for Connections.

### 1.2.1 IBM Trusteer Pinpoint Detect Standard Application

La Aplicación de Cliente hace referencia a una Aplicación Web o Móvil. Una Aplicación Web agrupa todas las funciones ofrecidas a los Participantes Elegibles del Cliente a través de varias páginas web, desde una pantalla de inicio de sesión o identificación, y supervisadas como una Aplicación individual en la consola de Trusteer (Trusteer Management Application). Una Aplicación Móvil agrupa todas las funciones ofrecidas a los Participantes Elegibles del Cliente a través de un programa de software que puede descargarse de una tienda de aplicaciones (store), desde una pantalla de inicio de sesión o identificación, y supervisadas como una Aplicación individual en la consola de Trusteer (Trusteer Management Application).

La integración de IBM Trusteer Pinpoint requiere el derecho de titularidad de IBM Trusteer Pinpoint Application para cada Aplicación.

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

### 1.2.2 IBM Trusteer Pinpoint Detect Premium Application

La Aplicación de Cliente hace referencia a una Aplicación Web o Móvil. Una Aplicación Web agrupa todas las funciones ofrecidas a los Participantes Elegibles del Cliente a través de varias páginas web, desde una pantalla de inicio de sesión o identificación, y supervisadas como una Aplicación individual en la consola de Trusteer (Trusteer Management Application). Una Aplicación Móvil agrupa todas las funciones ofrecidas a los Participantes Elegibles del Cliente a través de un programa de software que puede descargarse de una tienda de aplicaciones (store), desde una pantalla de inicio de sesión o identificación, y supervisadas como una Aplicación individual en la consola de Trusteer (Trusteer Management Application).

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

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

### 1.2.3 IBM Trusteer New Account Fraud for Retail y/o IBM Trusteer New Account Fraud for Business

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

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

### 1.2.4 IBM Trusteer Digital Content Pack for Retail y/o IBM Trusteer Digital Content Pack for Business

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

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

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

### 1.2.5 IBM Trusteer Pinpoint Malware Detection

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

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

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

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

a. Datos de incidencias:

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

b. Advanced Edition:

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

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

c. Standard Edition:

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

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

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

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

**1.2.8 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:

Los Clientes pueden elegir utilizar TMA o Trustboard en cualquier momento. El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA o Trustboard 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.

**1.2.9 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 de 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:

Los Clientes pueden elegir utilizar TMA o Trustboard en cualquier momento. El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA o Trustboard 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.

### 1.2.10 IBM Trusteer Rapport Remediation for Retail y/o IBM Trusteer Rapport Remediation for Business

El objetivo de IBM Trusteer Rapport Remediation for Retail e IBM Trusteer Rapport Remediation for Business es investigar, corregir, bloquear y eliminar las infecciones por malware de tipo man-in-the-browser (MitB) de los dispositivos (PC/MAC) infectados de los Participantes Elegibles del Cliente con acceso a la Aplicación del Cliente de manera ad-hoc, cuando los datos de incidencias de IBM Trusteer Pinpoint Malware Detection detecten infecciones por malware de tipo MitB. El Cliente debe tener una suscripción actualizada a IBM Trusteer Pinpoint Malware Detection II activa en la Aplicación del Cliente. El Cliente puede utilizar esta oferta de Servicio de Cloud únicamente asociada con los Participantes Elegibles con acceso a la Aplicación del Cliente, y exclusivamente como una herramienta con el fin de investigar y corregir un determinado dispositivo infectado (PC/MAC) de manera ad-hoc. IBM Trusteer Rapport Remediation debe estar ejecutándose en el dispositivo (PC/MAC) del Participante Elegible afectado, y este tiene que aceptar el EULA y autenticarse al menos una vez en las Aplicaciones del Cliente, además su configuración de Cliente debe incluir la recopilación de los ID de usuario. A efectos aclaratorios, esta oferta de Servicio de Cloud no incluye el derecho a utilizar Trusteer Splash ni a promocionar, de ninguna manera, el Software Cliente del Titular de la Cuenta entre los Participantes Elegibles del Cliente. Para los fines de esta Descripción del Servicio, el Titular de la Cuenta hace referencia 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 de tipo Business o Retail del Cliente para la cual se ha suscrito la cobertura de Servicio de Cloud. El Software de Cliente del Titular de la Cuenta es el software de habilitación de Cliente de IBM Trusteer Rapport o cualquier otro software de habilitación de Cliente que se proporciona con los Servicios de Cloud para su instalación en el dispositivo del usuario final.

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

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

### 1.2.12 IBM Trusteer Rapport for Mitigation for Business y/o IBM Trusteer Rapport for Mitigation for Retail

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

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

### 1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail y/o IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

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

### 1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail y/o IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

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

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

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

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

### 1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

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

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

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

## 1.3 Servicios de Aceleración

### 1.3.1 IBM Trusteer Pinpoint Detect Standard Redeployment y/o IBM Trusteer Pinpoint Detect Premium Redeployment

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

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

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

### 1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

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

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

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

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

### 1.3.3 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.

# 2. Fichas de Características de Protección y Tratamiento de Datos

El Anexo de Tratamiento de Datos (DPA) de IBM, en http://ibm.com/dpa, y las Fichas de Características de Protección y Tratamiento de Datos (referidas como fichas de datos o Suplementos del DPA) en los enlaces siguientes proporcionan información adicional de protección de datos para los Servicios de Cloud y sus opciones sobre los tipos de Contenido que pueden tratarse, las actividades de tratamiento involucradas, las características de protección de datos y detalles específicos sobre la retención y la devolución de Contenido. El DPA se aplica a los datos personales contenidos en el Contenido, siempre y cuando: i) se cumpla el Reglamento General de Protección de Datos de la Unión Europea (EU/2016/679) (GDPR); o ii) se aplique otra legislación sobre protección de datos identificada en http://ibm.com/dpa/dpl.

Se puntualiza que las Fichas de Datos generalmente listan todas las ubicaciones donde IBM (incluidos los subencargados de terceros) aloja y trata Datos Personales, independientemente del centro de datos desde el que se desplieguen los servicios. Para ver una lista de las ubicaciones de alojamiento y

tratamiento específicas del centro de datos desde el que se despliegan los servicios, consulte la Sección 5.2 a continuación (Información Adicional de Ubicación de Tratamiento).

**IBM Trusteer Pinpoint Criminal Detect**

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

**IBM Trusteer Pinpoint Detect**

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

**IBM Trusteer Pinpoint Malware Detection**

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

**IBM Trusteer Mobile SDK**

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

# 3. Nivel de Servicio y Soporte Técnico

## 3.1 Acuerdo de Nivel de Servicio (SLA)

IBM proporciona al Cliente el siguiente contrato de nivel de servicio (SLA) de disponibilidad. IBM aplicará la compensación aplicable más alta en función de la disponibilidad acumulativa del Servicio de Cloud, como se muestra en la tabla siguiente. El porcentaje de disponibilidad se calcula como el número total de minutos en un mes contratado, menos el número total de minutos de Inactividad del Servicio en un mes contratado, dividido por el número total de minutos en un mes contratado. La definición de Inactividad del Servicio, el proceso de reclamación y la información acerca de cómo ponerse en contacto con IBM con respecto a los problemas de disponibilidad del servicio se encuentran en el manual de soporte del Servicio de Cloud de IBM, en la dirección https://www.ibm.com/software/support/saas_support_overview.html.

| Disponibilidad | Crédito (% de la tarifa de suscripción mensual*) |
|---|---|
| Menos del 99,9% | 2% |
| Menos del 99% | 5% |
| Menos del 95% | 10% |

* La tarifa de suscripción es el precio contratado para el mes que está sujeto a la reclamación.

## 3.2 Soporte Técnico

El Soporte Técnico para el Servicio de Cloud, incluyendo detalles de contacto de soporte, niveles de gravedad, horas de disponibilidad de soporte, tiempos de respuesta y otros procesos e información de soporte, se encuentra seleccionando el Servicio de Cloud en la guía de soporte de IBM disponible en la dirección https://www.ibm.com/support/home/pages/support-guide/.

**Soporte Premium (ofertas Premium Support):**

Hay una suscripción al Soporte Premium disponible para el Servicio de Cloud con un cargo adicional, que incluye:

- Soporte 24x7 para problemas de cualquier gravedad.
- Los Clientes pueden acceder al soporte directamente por teléfono y mediante solicitud de devolución de llamada.
- Los Clientes y sus Participantes Elegibles pueden enviar tickets de soporte por medios electrónicos, como se indica en el Manual de Soporte de Software como Servicio [SaaS].
- Los Clientes pueden acceder al Portal de Soporte del Cliente para ver notificaciones, documentos, informes de casos y Preguntas más frecuentes (FAQ) en: http://www.ibm.com/software/security/trusteer/support/.

# 4. Cargos

## 4.1 Métricas de Cargo

Las métricas de cargo por el Servicio de Cloud se especifican en el Documento Transaccional.

Se aplican a este Servicio de Cloud las métricas de cargo siguientes:

- Un Compromiso es un servicio profesional o de formación relacionado con los Servicios de Cloud.
- Un Participante Elegible es un individuo o una entidad elegible para participar en un programa de prestación de servicios gestionados o monitorizados por los Servicios de Cloud.
- Una Aplicación es un programa de software con un nombre exclusivo desarrollado o puesto a disposición para ser accedido o utilizado por los Servicios de Cloud.
- Una Llamada de API es la invocación de los Servicios de Cloud a través de una interfaz programable.
- Una Conexión es un enlace o asociación de una base de datos, aplicación, servidor o cualquier otro tipo de dispositivo disponible en los Servicios de Cloud.

## 4.2 Cargos de Servicios Remotos

Un servicio remoto vencerá transcurridos 90 días a partir de la fecha de compra, independientemente de si se ha utilizado el servicio remoto.

# 5. Términos Adicionales

Para los Contratos de Servicio de Cloud (o contratos de cloud base equivalentes) firmados antes del 1 de enero de 2019, se aplican las condiciones disponibles en https://www.ibm.com/acs.

## 5.1 EULA y Base para el Tratamiento de Datos de Interesados

Para los Servicios de Cloud de IBM Trusteer Rapport (incluidos Rapport Remediation o Rapport for Mitigation cuando se despliega en relación con los Servicios de Cloud de Pinpoint): a menos que se acuerde lo contrario, y conforme a la base de tratamiento que el Cliente ha establecido de forma independiente, el Cliente autoriza a IBM a proporcionar el Acuerdo de Licencia de Usuario Final disponible en https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA para permitir a IBM recopilar y tratar la información necesaria para prestar los Servicios de Cloud.

Para los Servicios de Cloud de IBM Trusteer Rapport, el Cliente autoriza a IBM, como encargado del tratamiento de datos de la Empresa Patrocinadora, a utilizar el Programa para recopilar malware y artefactos de malware, por ejemplo, archivos relacionados con actividades maliciosas o archivos relacionados con un mal funcionamiento inusual del Programa. IBM no utiliza el Programa para buscar archivos con información personal del usuario final; no obstante, los archivos recopilados pueden contener datos personales que hayan sido obtenidos por el malware sin el permiso del usuario final. IBM: 1) eliminará sin demora cualquier archivo que no sea relevante para dicho análisis, y 2) conservará los archivos pertinentes solo durante el análisis y en ningún caso durante más de tres meses.

## 5.2 Información Adicional de Ubicación de Tratamiento

Todo el alojamiento y tratamiento de Datos Personales, incluido el realizado por los subencargados de terceros identificados en la Ficha de Datos, se realizará en las ubicaciones que se especifican a continuación:

Para todos los servicios proporcionados a través del centro de datos de Alemania, IBM limitará el alojamiento y el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los siguientes países: Alemania, Israel, Irlanda y Países Bajos.

Para todos los servicios proporcionados a través del centro de datos de Japón, IBM limitará el alojamiento y el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los siguientes países: Japón, Israel e Irlanda.

Para todos los servicios proporcionados a través del centro de datos de EE.UU., IBM limitará el alojamiento y el tratamiento de Datos Personales al país de la entidad contratante de IBM y a los siguientes países: EE.UU., Israel, Irlanda, Singapur y Australia.

Además de las ubicaciones citadas anteriormente, con respecto a todos los servicios proporcionados a través de los centros de datos de Alemania, Japón y EE.UU., (1) los datos se soporte pueden alojarse o tratarse en Alemania y Francia en Salesforce.Com como subencargado de terceros de IBM y (2) para los clientes que optan a enviar datos a proveedores de Mobile Carrier Intelligence, los Datos Personales pueden alojarse y tratarse en los países de los subencargados de terceros aplicables, tal como se especifica en la Hoja de Datos. Con independencia de lo establecido en contra en la Ficha de Datos, los subencargados de terceros especificados en la cláusula (2) de la frase inmediatamente anterior puede que no cumplan los estándares ISO 27001 o SOC2.

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

### 5.3 Datos del Titular de la Cuenta

A modo de aclaración, si hay más de un cliente de IBM afiliado con el Software de Cliente del Titular de la Cuenta de un determinado Titular de la Cuenta (dichos clientes de IBM se denominan "Clientes Afiliados") e IBM proporciona los servicios bajo esta Descripción del Servicio a través de centros de datos en distintas regiones, los datos del Titular de la Cuenta pueden tratarse en todas o cualquiera de las ubicaciones asociadas con cada uno de los centros de datos especificados en la Sección 5.2 anterior.

### 5.4 Soluciones Integradas

A modo de aclaración, las distintas ofertas bajo la marca Trusteer pueden constituir una solución integrada. Por lo tanto, si el Cliente termina cualquiera de estos Servicios de Cloud, IBM puede conservar los datos del Cliente con el propósito de proporcionar al Cliente el resto de los Servicios de Cloud bajo esta Descripción del Servicio, así como otros servicios de Trusteer de conformidad con las descripciones de servicio aplicables a esos otros servicios de Trusteer.

### 5.5 Software de Habilitación

El Servicio de Cloud contiene el Software de Habilitación siguiente:

- IBM Rapport Agents

### 5.6 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).

### 5.7 Datos recopilados como parte del despliegue

El despliegue del Servicio de Cloud puede implicar que el Cliente proporcione ciertos datos a IBM. Dichos datos no deben incluir información que pueda identificar o atribuir a personas individuales específicas. En las Directrices de Despliegue del Trusteer que se proporcionarán al Cliente se incluyen más directrices sobre los datos proporcionados a IBM como parte del despliegue.

## 6. Sustitución de Condiciones

### 6.1 Uso de Datos

Lo siguiente prevalece sobre cualquier disposición contradictoria el apartado Contenido y Protección de Datos de las condiciones básicas del Servicio de Cloud entre las partes: IBM no utilizará ni revelará los resultados que surjan del uso del Servicio de Cloud por parte del Cliente que sean exclusivos del Contenido (Insights) del Cliente o que de otro modo identifiquen al Cliente. IBM, no obstante, puede utilizar Contenido y otras informaciones derivadas del Contenido (excepto Insights) como parte del Servicio de Cloud, con la finalidad de mejorar el Servicio de Cloud. IBM también puede compartir identificadores de amenazas y otra información de seguridad incluida en el Contenido para la protección y la detección de amenazas.