IBM Trusteer Pinpoint Verify

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 Verify incluye Step-Authenticate, una autenticación incremental que puede iniciarse en determinados casos de alto riesgo para ayudar a garantizar que las interacciones digitales habilitadas mediante seguridad estén protegidas por Pinpoint. Esto reduce el riesgo cuando Trusteer predice un riesgo de actividad fraudulenta prevista o cuando la actividad de usuario requiere un mayor nivel de garantía de identidad.

1.1 Ofertas

1.1.1 IBM Trusteer Pinpoint Verify

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

Este Servicio de Cloud proporciona capacidades para que los usuarios pasen por un segundo factor de autenticación con el fin de verificar sus identidades al acceder a un servicio digital. Está disponible para Pinpoint Detect y Pinpoint Assure, para proporcionar una autenticación de segundo factor para las aplicaciones protegidas. La decisión de cuándo solicitar a los usuarios la autenticación de segundo factor proviene de la aplicación protegida y puede basarse en las recomendaciones devueltas por las plataformas Pinpoint Detect o Pinpoint Assure, o por cualquier otra política definida por la aplicación protegida. Este Servicio de Cloud está basado en la tecnología IBM Cloud Identity Verify.

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.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=D7AB2D30CB2C11E99CFB3A1B59E5A549

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/.

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 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 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.

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 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.

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.