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

IBM Security Trusteer Fraud Protection

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

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

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

1. SaaS IBM

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

1.1 Ofertas SaaS IBM de Rapport

- IBM Security Trusteer Rapport para Empresas
- Soporte Premium de IBM Security Trusteer Rapport para Empresas
- IBM Security Trusteer Rapport para Distribuidores
- Soporte Premium de IBM Security Trusteer Rapport para Distribuidores
- IBM Security Trusteer Rapport Fraud Feeds para Empresas
- Soporte Premium de IBM Security Trusteer Rapport Fraud Feeds para Empresas
- IBM Security Trusteer Rapport Fraud Feeds para Distribuidores
- Soporte Premium de IBM Security Trusteer Rapport Fraud Feeds para Distribuidores
- IBM Security Trusteer Rapport Phishing Protection para Empresas
- Soporte Premium de IBM Security Trusteer Rapport Phishing Protection para Empresas
- IBM Security Trusteer Rapport Phishing Protection para Distribuidores
- Soporte Premium de IBM Security Trusteer Rapport Phishing Protection para Distribuidores
- IBM Security Trusteer Rapport Mandatory Service para Empresas
- IBM Security Trusteer Rapport Mandatory Service para Distribuidores

1.2 Ofertas de SaaS IBM Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition
- Soporte Premium de IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition
- Soporte Premium de IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition
- Soporte Premium de IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition
- Soporte Premium de IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition
- IBM Security Trusteer Pinpoint Criminal Detection para Empresas

- Soporte Premium de IBM Security Trusteer Pinpoint Criminal Detection para Empresas
- IBM Security Trusteer Pinpoint Criminal Detection para Distribuidores
- Soporte Premium de IBM Security Trusteer Pinpoint Criminal Detection para Distribuidores
- IBM Security Trusteer Pinpoint Criminal Detection Mobile para Empresas
- Soporte Premium de IBM Security Trusteer Pinpoint Criminal Detection Mobile para Empresas
- IBM Security Trusteer Pinpoint Criminal Detection Mobile para Distribuidores
- Soporte Premium de IBM Security Trusteer Pinpoint Criminal Detection Mobile para Distribuidores
- IBM Security Trusteer Pinpoint Carbon Copy para Empresas
- Soporte Premium de IBM Security Trusteer Pinpoint Carbon Copy para Empresas
- IBM Security Trusteer Pinpoint Carbon Copy para Distribuidores
- Soporte Premium de IBM Security Trusteer Pinpoint Carbon Copy para Distribuidores
- IBM Security Trusteer Rapport Remediation para Distribuidores
- Soporte Premium de IBM Security Trusteer Rapport Remediation para Distribuidores

1.3 Ofertas SaaS IBM Móvil

- IBM Security Trusteer Mobile SDK para Empresas
- IBM Security Trusteer Mobile SDK para Distribuidores
- IBM Security Trusteer Mobile Browser para Empresas
- Soporte Premium de IBM Security Trusteer Mobile Browser para Empresas
- IBM Security Trusteer Mobile Browser para Distribuidores
- Soporte Premium de IBM Security Trusteer Mobile Browser para Distribuidores

2. Métricas de Cargo

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

a. **Participante Elegible**: es una unidad de medida con la que se puede adquirir SaaS IBM. Todo individuo o entidad que pueda ser elegido para participar en cualquier programa de entrega de servicios gestionado o seguido por SaaS IBM es un Participante Elegible. Deben adquirirse derechos de titularidad suficientes para cubrir a todos los Participantes Elegibles gestionados o seguidos por el SaaS IBM durante el período de medida especificado en el Documento Transaccional del Cliente.

   Cada programa de prestación de servicio gestionado por el SaaS IBM 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.

   Para estas ofertas, el programa de prestación de servicio incluye una única Aplicación para Empresas o para Distribuidores del Cliente con una página de inicio de sesión principal y páginas relacionadas para cada Aplicación para Empresas o para Distribuidores. Un Participante Elegible es un usuario final del Cliente con credenciales de inicio de sesión en la Aplicación para Empresas o para Distribuidores.

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

3. Cargos y Facturación

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

3.1 Cargo Mensual Parcial

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

4. Cumplimiento y Auditoría

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

Se puede realizar una auditoría para verificar el cumplimiento de la cantidad máxima de Participantes Elegibles o Dispositivos de Cliente.

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

El Documento Transaccional del Cliente establecerá si el SaaS IBM se renovará al finalizar el Período de Suscripción, designando una de estas opciones:

5.1 Renovación Automática

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

5.2 Facturación Continua

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

5.3 Renovación Necesaria

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

6. Soporte Técnico

Existe Soporte Técnico para SaaS IBM a disposición del Cliente y sus Participantes Elegibles, a fin de ayudarles a utilizar SaaS IBM.

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 SaaS IBM, hay una suscripción al Soporte Premium disponible, con un cargo adicional, a excepción de las ofertas de IBM Security Trusteer Mobile SDK e IBM Security Trusteer Rapport Mandatory Service.

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] de IBM: 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.
- 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] de IBM: http://www-01.ibm.com/software/support/handbook.html.

7. Condiciones Adicionales de la Oferta de SaaS IBM

7.1 Conformidad con Safe Harbor

IBM acata los Acuerdos de Safe Harbor entre EE.UU. y la UE desarrollados por el Departamento de Comercio de Estados Unidos en coordinación con la Comisión Europea. Los productos IBM Security Trusteer se incluyen en la certificación Safe Harbor entre EE.UU y la UE de IBM. Puede encontrar más información acerca de Safe Harbor y la lista de empresas bajo Acuerdos Safe en esta dirección: http://export.gov/safeharbor/.

7.2 Incremento de la Tarifa de Suscripción Anual del Cliente

IBM se reserva el derecho a ajustar la tarifa de suscripción del SaaS IBM un máximo de una vez cada doce (12) meses en un porcentaje que determinará IBM y que no superará el 3%. El ajuste de la tarifa de suscripción se hará efectivo en el aniversario de la fecha de inicio del período de cobertura. Este ajuste de tarifa no modificará los derechos de titularidad del Cliente con respecto al SaaS IBM ni la métrica de cargo mediante la cual se obtiene el SaaS IBM. Los Business Partners de IBM son independientes de IBM y determinan de forma unilateral sus precios y sus condiciones.

7.3 Soporte Premium

El Cliente tiene derecho de titularidad para el Soporte Premium solo para aquellas ofertas de SaaS IBM para las cuales haya suscrito la oferta asociada de Soporte Premium.

7.4 Uso Legítimo y Consentimiento

Autorización para la recopilación y el tratamiento de datos

El SaaS IBM se ha diseñado para ayudar al Cliente a mejorar su entorno de seguridad y los datos. SaaS IBM recopila la información de los Participantes Elegibles y los Dispositivos de Cliente que interactúan con las Aplicaciones para Empresas o para Distribuidores para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM. SaaS IBM recopila información que, de manera independiente o combinada, se puede considerar como 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 SaaS IBM. 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 entre Fronteras y el apartado Privacidad de los Datos de estas CDU, y el apartado Privacidad de los Datos y Seguridad de los Datos de las Condiciones Generales de las CDU.

Para ofertas de IBM Security Trusteer Pinpoint:

Entre los datos recopilados se pueden encontrar la dirección IP del usuario, el ID de usuario cifrado o de hash unidireccional, cookies de dominio si no se han filtrado, visitas a Aplicaciones protegidas y sitios de phishing, ubicaciones geográficas y credenciales especificadas en sitios de phishing.

Para las ofertas de IBM Security Trusteer Mobile SDK y para las ofertas de IBM Security Trusteer Mobile Browser:

Entre los datos recopilados se pueden encontrar la dirección IP del usuario, el ID de usuario cifrado o de hash unidireccional, la ubicación geográfica y visitas a Aplicaciones protegidas, información de la tarjeta SIM, nombre del dispositivo y vinculaciones del Cliente.

Para ofertas de IBM Security Trusteer Rapport:

Entre los datos recopilados se pueden encontrar la dirección IP del usuario, el ID de usuario cifrado o de hash unidireccional, eventos de seguridad, el nombre de usuario y la dirección de correo electrónico proporcionados a fin de ponerse en contacto con el soporte al Cliente de IBM, la Vinculación del Cliente, la contraseña cifrada especificada en sitios protegidos, visitas a Aplicaciones protegidas y sitios de phishing, número de tarjeta de pago cifrado, y archivos y datos recopilados de forma remota por el personal de IBM para inspeccionar el malware sospechoso, las actividades maliciosas o un funcionamiento incorrecto.

Consentimiento Informado de los Interesados:

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

Para las ofertas de IBM Security Trusteer Pinpoint y para las ofertas de IBM Security 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 SaaS IBM, así como para permitir la recopilación y el tratamiento de la información por parte de IBM mediante el SaaS IBM.

Para las ofertas de IBM Security Trusteer Rapport y para ofertas de IBM Security Trusteer Mobile Browser:

El Cliente autoriza a IBM a obtener los consentimientos perfectamente informados que sean necesarios para realizar un uso legítimo del SaaS IBM, así como recopilar y tratar la información, según lo descrito en el Acuerdo de Licencia de Usuario Final disponible enhttps://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 SaaS IBM, así como para permitir la recopilación y el tratamiento de la información por parte de IBM, como Encargado del tratamiento de Datos Personales del Cliente, mediante el SaaS IBM.

7.5 Transferencias entre Fronteras

El Cliente acepta que IBM podrá tratar el contenido, incluidos los Datos Personales, 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 países que la Comisión Europea considere que cuentan con niveles de seguridad adecuados: EE.UU.

7.6 Privacidad de los Datos

Si el Cliente pone Datos Personales a disposición de SaaS IBM 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/CE de la UE) de los Datos Personales. IBM solo tratará estos Datos Personales en la medida en la que sea necesario para que el SaaS IBM esté disponible, de acuerdo con las descripciones publicadas por IBM del SaaS IBM, y el Cliente acepta que cualquier tratamiento de este tipo se hará

siguiendo sus propias instrucciones. IBM proporcionará una notificación anticipada 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 SaaS IBM. El Cliente podrá resolver el Período de Suscripción actual de los SaaS IBM afectados enviando una notificación escrita a IBM dentro de los treinta (30) días posteriores a la notificación al Cliente, por parte de IBM, del cambio. El Cliente acepta que IBM puede tratar 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	410 Terry Ave. N Seattle, WA 98109 Estados Unidos
Connectria Corp.	Subencargado del tratamiento	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Estados Unidos
IBM Israel Ltd.	Subencargado del tratamiento	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Subencargado del tratamiento	1 New Orchard Rd. Armonk, NY 10504 Estados Unidos

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

El Cliente acepta que, para el servicio prestado 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	Munich, Alemania
IBM Israel Ltd.	Subencargado del tratamiento	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

El Cliente acepta que, para el servicio prestado 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	Según lo indicado en el Documento Transaccional
Amazon Web Services (Japón)	Subencargado del tratamiento	Tokio, Japón
IBM Israel Ltd.	Subencargado del tratamiento	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* Las ubicaciones identificadas en las tablas siguientes incluyen las direcciones de las oficinas corporativas del Encargado o Subencargado del tratamiento de datos. Los centros de datos se encuentran ubicados dentro del mismo país identificado.

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. Todos los conflictos o responsabilidades que surjan bajo estos acuerdos, incluso si aquellos son firmados por filiales, serán tratados por las partes como si el conflicto o la responsabilidad hubiese surgido entre las partes bajo las condiciones de este Acuerdo.

Apéndice A

1. Ofertas de SaaS IBM

IBM ofrece estos servicios como ofertas y servicios independientes, o como ofertas y servicios adicionales. Las ofertas específicas de SaaS IBM solicitadas se especifican en el Documento de Titularidad (POE) del Cliente.

1.1 Definiciones de Mayorista y Minorista

Los productos contra el fraude de IBM Security Trusteer tienen licencia de uso con determinados tipos de Aplicaciones. Una Aplicación se puede definir con uno de los tipos siguientes: para Empresas o para Distribuidores. Hay ofertas distintas disponibles para Aplicaciones para Empresas o Aplicaciones para Distribuidores.

- Una Aplicación para Distribuidores 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 para distribuidores.
- Una Aplicación para Empresas 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 para Distribuidores.

1.2 Ofertas de Suscripción básica a SaaS IBM

Ofertas para Empresas:

- IBM Security Trusteer Rapport para Empresas
- IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection para Empresas
- IBM Security Trusteer Pinpoint Criminal Detection Mobile para Empresas
- IBM Security Trusteer Mobile SDK para Empresas
- IBM Security Trusteer Mobile Browser para Empresas

Ofertas para Distribuidores:

- IBM Security Trusteer Rapport para Distribuidores
- IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection para Distribuidores
- IBM Security Trusteer Pinpoint Criminal Detection Mobile para Distribuidores
- IBM Security Trusteer Mobile SDK para Distribuidores
- IBM Security Trusteer Mobile Browser para Distribuidores

Para cada una de las ofertas de Aplicaciones para Empresas o para Distribuidores, existe un producto asociado de Soporte Premium disponible, con un cargo adicional, a excepción de las ofertas de IBM Security Trusteer Mobile SDK.

1.3 Ofertas adicionales de Suscripción a SaaS IBM para Ofertas de IBM Security Trusteer

Ofertas adicionales disponibles para IBM Security Trusteer Rapport para Empresas:

- IBM Security Trusteer Rapport Fraud Feeds para Empresas
- IBM Security Trusteer Rapport Phishing Protection para Empresas
- IBM Security Trusteer Rapport Mandatory Service para Empresas

Ofertas adicionales disponibles para IBM Security Trusteer Rapport para Distribuidores:

- IBM Security Trusteer Rapport Fraud Feeds para Distribuidores
- IBM Security Trusteer Rapport Phishing Protection para Distribuidores
- IBM Security Trusteer Rapport Mandatory Service para Distribuidores

Para cada uno de los complementos para Empresas o para Distribuidores de las ofertas de IBM Security Trusteer Rapport, excepto para los complementos de IBM Security Trusteer Rapport Mandatory Service, existe un producto asociado de Soporte Premium disponible, con un cargo adicional.

La Suscripción a IBM Security Trusteer Rapport para Empresas o IBM Security Trusteer Rapport para Distribuidores es un requisito previo para las ofertas adicionales asociadas de suscripción al SaaS IBM recogidas en este apartado.

1.4 Ofertas adicionales de Suscripción a SaaS IBM para Ofertas de IBM Security Trusteer Pinpoint Malware Detection

Ofertas adicionales disponibles para IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition, o IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy para Empresas

Ofertas adicionales disponibles para IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy para Distribuidores
- IBM Security Trusteer Rapport Remediation para Distribuidores

Existe una suscripción al Soporte Premium disponible, con un cargo adicional, para cada una de las ofertas adicionales de SaaS IBM recogidas en este apartado.

La Suscripción a ofertas de IBM Security Trusteer Pinpoint Malware Detection para Empresas u ofertas de IBM Security Trusteer Pinpoint Malware Detection para Distribuidores es un requisito previo para las ofertas adicionales asociadas de suscripción al SaaS IBM recogidas en este apartado.

1.5 Otras suscripciones adicionales a SaaS IBM

Las Suscripciones adicionales a SaaS IBM para 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.

1.6 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 para Empresas o para Distribuidores del Cliente para la cual se ha suscrito la cobertura de las ofertas SaaS IBM.

Software de Cliente del Titular de la Cuenta: se refiere al software de habilitación de Cliente de IBM Security Trusteer Rapport o al software de habilitación de Cliente de IBM Security Trusteer Mobile Browser, o a cualquier otro software que habilite al Cliente y que se proporcione con alguna de las suscripciones a SaaS IBM 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. Ofertas de IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport para Distribuidores y/o IBM Security Trusteer Rapport para Empresas ("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 Security Trusteer Rapport recopila datos relevantes sobre phishing y ataques con malware activos contra organizaciones de todo el mundo. IBM Security 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.

Esta oferta de SaaS IBM dispone de una métrica de cargo de Participante Elegible. La oferta para Empresas se vende en paquetes de 10 Participantes Elegibles. La oferta para Distribuidores se vende en paquetes de 100 Participantes Elegibles.

La oferta de SaaS IBM incluye lo siguiente:

a. Trusteer Management Application ("TMA"):

   TMA está disponible en el entorno alojado en cloud de IBM Security Trusteer, a través del cual el Cliente (y un número ilimitado de su personal autorizado) puede: (i) recibir informes de datos de incidencias y evaluaciones de riesgos, (ii) ver, configurar y establecer políticas relacionadas con informes de datos de incidencias, y (iii) ver la configuración del software de habilitación de Cliente, con licencia para el público 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 las ofertas de SaaS IBM.

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 como consecuencia de las interacciones en línea del Titular de la Cuenta con la Aplicación para Empresas o para Distribuidores para la que el Cliente haya suscrito la cobertura de ofertas de SaaS IBM. 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 para Empresas o para Distribuidores 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 para Empresas o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM. 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 Security 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 a la oferta de SaaS IBM Security 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 Ofertas Adicionales Opcionales SaaS IBM para IBM Security Trusteer Rapport para Empresas y/o IBM Security Trusteer Rapport para Distribuidores

La Suscripción a las ofertas de IBM Security Trusteer Rapport es un requisito previo para la suscripción a cualquiera de las siguientes ofertas adicionales de SaaS IBM. Si el SaaS IBM tiene la designación "para Empresas", la oferta adicional de SaaS IBM adquirida debe tener la misma designación. Si el SaaS IBM tiene la designación "para Distribuidores", la oferta adicional de SaaS IBM adquirida debe 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 para Empresas y/o para Distribuidores del Cliente y cuya configuración de Cliente incluye la recopilación de los ID de usuario.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds para Empresas y/o IBM Security Trusteer Rapport Fraud Feeds para Distribuidores

El Cliente (y un número ilimitado de su personal autorizado) puede utilizar TMA para recibir datos de incidencias relacionados con infecciones por malware y otras vulnerabilidades de punto final en el escritorio de un Titular de Cuenta determinado.

2.2.2 IBM Security Trusteer Rapport Phishing Protection para Empresas y/o IBM Security Trusteer Rapport Phishing Protection para Distribuidores

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 SaaS IBM 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.

2.2.3 IBM Security Trusteer Rapport Mandatory Service para Empresas y/o IBM Security Trusteer Rapport Mandatory Service para Distribuidores

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 para Empresas y/o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de las ofertas SaaS IBM.

El Soporte Premium de IBM Security Trusteer Rapport para Empresas es un requisito previo para IBM Security Rapport Mandatory Service para Empresas.

El Soporte Premium de IBM Security Trusteer Rapport para Distribuidores es un requisito previo para IBM Security Rapport Mandatory Service para Distribuidores.

El Cliente puede implementar la funcionalidad adicional de IBM Security Trusteer Rapport Mandatory Service solo si se ha solicitado y se ha configurado para su uso con la Aplicación para Empresas o para Distribuidores del Cliente para la cual el Cliente haya suscrito la cobertura de las ofertas de SaaS IBM.

3. Ofertas de IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint es un servicio basado en cloud 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 para Empresas y/o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas y los procesos de prevención del fraude de SaaS IBM.

La oferta de SaaS IBM incluye lo siguiente:

a. TMA:

   TMA está disponible 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) 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. Script web y/o API:

   Para el despliegue en sitios web con el fin de acceder a, o utilizar, el SaaS IBM.

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

En el caso de que se detecte malware en las ofertas de IBM Security Trusteer Pinpoint Malware Detection o que se detecte toma de control de cuentas en las ofertas de IBM Security Trusteer Pinpoint Criminal Detection, el Cliente debe seguir la Guía de Prácticas Recomendadas de Pinpoint. No utilice las ofertas de IBM Security Trusteer Pinpoint Malware Detection ni las ofertas de IBM Security Trusteer Pinpoint Criminal Detection 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 Security Trusteer Pinpoint (por ejemplo, notificaciones, mensajes, bloqueo de dispositivos o bloqueo del acceso a la Aplicación para Empresas o para Distribuidores inmediatamente después de una detección de malware o de toma de control de cuentas).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection para Empresas y/o IBM Security Trusteer Pinpoint Criminal Detection para Distribuidores

Detección sin Cliente de actividad sospechosa de toma de control de cuentas mediante navegadores conectados a una Aplicación para Empresas o para Distribuidores, mediante un ID de dispositivo, detección de phishing y detección de robo de credenciales mediante malware. Las ofertas de Cloud de IBM Security 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 para Empresas o para Distribuidores.

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 para Empresas y/o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de las ofertas de SaaS IBM. El Cliente también puede recibir los datos de incidencias a través de una modalidad de entrega de la API de fondo.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection Mobile para Empresas y/o IBM Security Trusteer Pinpoint Criminal Detection Mobile para Distribuidores

Las ofertas de IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD for Mobile) se han diseñado para proporcionar otra capa de protección y su objetivo es proteger contra la toma de control de cuentas y las actividades fraudulentas mediante la identificación del acceso delictivo a las cuentas y la prestación de una recomendación para el Cliente. Esta oferta de SaaS IBM recopila información procedente de la Aplicación para Empresas y para Distribuidores del Cliente, mediante la API de PPCD Mobile, y de los dispositivos móviles de los Participantes Elegibles. Las ofertas de IBM Security Trusteer PPCD Mobile se han diseñado para generar información compleja relacionada con los dispositivos móviles de los Participantes elegibles con otros orígenes de datos, como incidentes de infección por malware y phishing en tiempo real que se integran a través de otras ofertas de SaaS IBM de IBM Security Trusteer especificadas en estas Condiciones de Uso.

El Cliente puede acceder a las ofertas de IBM Security Trusteer PPCD Mobile, y utilizarlas, en el entorno alojado en cloud de IBM Security Trusteer, así como recibir datos de evaluación de riesgos de dispositivos móviles de Participantes Elegibles, generados a raíz de las interacciones en línea de estos dispositivos móviles con la Aplicación para Empresas o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de las ofertas SaaS IBM. En el contexto de estas ofertas, "dispositivos móviles" solo incluye teléfonos móviles y tabletas, no incluye sistemas PC ni MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition

Detección sin Cliente de navegadores infectados con malware financiero de tipo Man in the Browser (MitB) que se conectan a una Aplicación para Empresas y/o para Distribuidores. Las ofertas de IBM Security 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 para Empresas y/o para Distribuidores del Cliente.

b. Advanced Edition:

   La Advanced Edition para Empresas y/o para Distribuidores ofrece una capa adicional de detección y protección que se personaliza para ajustarse a la estructura y el flujo de las Aplicaciones para Empresas y/o para Distribuidores 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 para Empresas y/o para Distribuidores del Cliente.

   La Advanced Edition se ofrece al Cliente con una cantidad mínima de 100000 Participantes Elegibles para Distribuidores o 10000 Participantes Elegibles para Empresas, lo que equivale a 1000 paquetes de 100 Participantes Elegibles para Distribuidores o 1000 paquetes de 10 Participantes Elegibles para Empresas.

c. Standard Edition:

   La Standard Edition para Empresas o para Distribuidores es una solución de despliegue rápido que proporciona la funcionalidad principal de esta oferta de SaaS IBM, como se describe en este documento.

3.2 Ofertas Adicionales Opcionales SaaS IBM para IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition y/o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition

Para las ofertas de IBM Security Trusteer Rapport Remediation para Distribuidores, existe el requisito previo de IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition.

Para IBM Security Trusteer Pinpoint Carbon Copy para Distribuidores, existe el requisito previo de IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Standard Edition o IBM Security Trusteer Pinpoint Malware Detection para Distribuidores, Advanced Edition. Para IBM Security Trusteer Pinpoint Carbon Copy para Empresas, existe el requisito previo de IBM Security Trusteer Pinpoint Malware Detection para Empresas, Standard Edition o IBM Security Trusteer Pinpoint Malware Detection para Empresas, Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy para Empresas y/o IBM Security Trusteer Pinpoint Carbon Copy para Distribuidores

Ofertas de IBM Security 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 para Empresas o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM.

3.2.2 IBM Security Trusteer Rapport Remediation para Distribuidores

El objetivo de IBM Security Trusteer Rapport Remediation para Distribuidores 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 para Distribuidores del Cliente de manera ad-hoc, cuando los datos de incidencias de IBM Security Trusteer Pinpoint Malware Detection detecten infecciones por malware de tipo MitB. El Cliente debe tener una suscripción actualizada a IBM Security Trusteer Pinpoint Malware Detection activa en la Aplicación para Distribuidores del Cliente. El Cliente puede utilizar este producto de SaaS IBM únicamente en conexión con los Participantes Elegibles con acceso a la Aplicación para Distribuidores del Cliente, y solo con el fin de investigar y corregir un dispositivo (PC/MAC) infectado concreto de manera ad-hoc. IBM Security Trusteer Rapport Remediation para Distribuidores 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 para Distribuidores del Cliente, además de que su configuración de Cliente debe incluir

la recopilación de los ID de usuario. Para que no exista ninguna duda, esta oferta de SaaS IBM no incluye el derecho a utilizar Trusteer Splash ni a promocionar, de ninguna manera, el Software de Cliente del Titular de la Cuenta entre los Participantes Elegibles del Cliente.

4. Ofertas de IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser para Empresas y/o IBM Security Trusteer Mobile Browser para Distribuidores

IBM Security 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 para Empresas o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM, 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. Para esta oferta de SaaS IBM, incluya los dispositivos móviles, los teléfonos móviles o las tabletas y no incluya PC o Mac portátiles.

A través de TMA, el Cliente (y un número ilimitado de su personal autorizado) 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 para Empresas o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de las ofertas de SaaS IBM. 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 para Empresas o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de las ofertas de SaaS IBM.

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 para Empresas o para Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM. 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 Security 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.

4.2 IBM Security Trusteer Mobile SDK para Empresas y/o IBM Security Trusteer Mobile SDK para Distribuidores

Las ofertas de IBM Security Trusteer Mobile SDK se han diseñado para añadir otra capa de protección y su objetivo es proporcionar acceso web seguro a las Aplicaciones para Empresas o Distribuidores del Cliente para las cuales el Cliente haya suscrito la cobertura de ofertas de SaaS IBM, 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.

Las ofertas de IBM Security 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 Security Trusteer Mobile Library, así como el "Componente en Tiempo de Ejecución" o el "Elemento Redistribuible", un código de propiedad generado por IBM Security 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 ofertas de SaaS IBM ("Aplicación Móvil Integrada del Cliente").

IBM Security Trusteer Mobile SDK para Distribuidores está disponible en paquetes de 100 Participantes Elegibles o paquetes de 100 Dispositivos de Cliente, e IBM Security Trusteer Mobile SDK para Empresas 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 Security 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 deberán estar sujetas a las presentes Condiciones de Uso; 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 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 la oferta SaaS IBM.

IBM ha probado las aplicaciones de ejemplo creadas con las herramientas móviles proporcionadas en IBM Security 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.

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 Security Trusteer Mobile SDK por parte del Cliente se realiza conforme a las condiciones de estas CDU.

5. Despliegue de Ofertas de Protección contra el Fraude de SaaS IBM

La suscripción básica del Cliente incluye actividades requeridas de configuración y despliegue inicial, incluidos el inicio único inicial, la configuración, la Plantilla de Presentación, la prueba y la formación.

Pueden contratarse servicios adicionales, con un cargo adicional, bajo un acuerdo independiente.

Apéndice B

IBM proporciona el siguiente acuerdo de nivel de servicio ("SLA") de disponibilidad para SaaS IBM y es aplicable si se especifica en el Documento Transaccional del Cliente:

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

1. Definiciones

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

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

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

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

e. **Cliente**: significa entidad que suscribe SaaS IBM directamente a través de IBM, que no ha incumplido ninguna obligación material y que no tiene ninguna obligación material pendiente, incluidas las obligaciones de pago, del contrato con IBM por SaaS IBM.

f. **Tiempo de Inactividad**: es un período de tiempo durante el que el proceso de los sistemas de producción para el Servicio se ha detenido y ningún usuario puede utilizar todos los aspectos del Servicio para los que tiene permisos adecuados. El Tiempo de Inactividad no incluye el período de tiempo en que el Servicio deja de estar disponible como consecuencia de:

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

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

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

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

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

2. Créditos de Disponibilidad

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

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

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

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

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

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

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

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

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

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

3. Niveles de Servicio

Disponibilidad del SaaS IBM durante un Mes Contratado

Nivel de Servicio Alcanzado (durante un Mes Contratado)	Crédito de Disponibilidad (% de la Cuota de suscripción mensual para el Mes Contratado objeto de una Reclamación)
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

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

Ejemplo: 250 minutos de Tiempo de inactividad total durante un Mes Contratado

43.200 minutos en total en un Mes Contratado de 30 días -- 250 minutos de Tiempo de Inactividad = 42.950 minutos _____ 43.200 minutos en total	= 2% de Crédito de Disponibilidad para el 99,4% de Nivel de Servicio Alcanzado durante el Mes Contratado

3.1 Exclusiones

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

- Servicios versión beta o de prueba.
- Entornos que no son de producción, incluyendo, a título enunciativo y no limitativo, entornos de prueba, recuperación tras desastre, control de calidad o desarrollo.
- Las Reclamaciones realizadas por los usuarios, invitados, participantes e invitados permitidos del Cliente de IBM en relación con SaaS IBM.
- Si el Cliente ha incumplido alguna obligación esencial bajo las Condiciones de uso, incluido, a título enunciativo y no limitativo, el incumplimiento de alguna obligación de pago.