

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

IBM Application Security on Cloud

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 las 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:

- IBM Application Security Analyzer

2. Métricas de Cargo

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

- Instancia de Aplicación:** es una unidad de medida con la que se puede adquirir SaaS IBM. Se requiere un derecho de titularidad de Instancia de Aplicación por cada instancia de una Aplicación que esté conectada a SaaS IBM. Si una Aplicación tiene varios componentes, cada uno de los cuales con un objetivo y/o un usuario destinatario distinto, y cada uno de ellos puede ser conectado a o gestionado por SaaS IBM, cada componente se considera una Aplicación independiente. Además, los entornos de pruebas, desarrollo, puesta en escena, transferencia y producción para una Aplicación son considerados como instancias independientes de la Aplicación y cada uno debe tener un derecho de titularidad. Varias instancias de Aplicación en un único entorno son consideradas como instancias independientes de la Aplicación y cada una debe tener un derecho de titularidad. Deben adquirirse Derechos de Titularidad suficientes para cubrir el número de Instancias de Aplicación conectadas a SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o Documento Transaccional del Cliente.
- Acceso:** es una unidad de medida con la que se puede adquirir SaaS IBM. Un Acceso son los derechos para utilizar SaaS IBM. El Cliente debe obtener un único derecho de titularidad de Acceso para poder utilizar SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o 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 Pago por Uso

Las opciones de Pago por Uso se facturarán el mes siguiente al uso del servicio, según la tarifa establecida en el Documento Transaccional.

3.2 Cargo Mensual Parcial

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

4. Soporte Técnico

Durante el Período de Suscripción y después de que IBM notifique al Cliente que el acceso a SaaS IBM está disponible, se proporciona soporte técnico a través de foros online y como soporte estándar durante el período temporal durante el cual el Cliente incurra en cargos de tipo Pago por Uso. Desde dentro del SaaS IBM, los Clientes pueden enviar un ticket de soporte o abrir una sesión de chat para obtener

ayuda. IBM pondrá a disposición el manual IBM Software as a Service Support Handbook, que proporciona información de contacto de soporte técnico, así como otro tipo de información y procesos.

Severidad	Definición de Severidad	Objetivos de Tiempo de Respuesta	Cobertura de Tiempo de respuesta
1	Impacto de negocio crítico / caída del servicio: La función de impacto de negocio no está operativa o la interfaz crítica ha fallado. Esto se aplica normalmente a un entorno de producción e indica una incapacidad de acceso a los servicios, que causa un impacto crítico en las operaciones. Esta condición requiere una solución inmediata.	En el plazo de una hora	24x7
2	Impacto de negocio significativo: El uso de una característica de negocio del servicio o una función del servicio está muy restringido o el Cliente corre el riesgo de pasarse las fechas límite.	En el plazo de dos horas laborales	L-V horas laborales
3	Impacto de negocio menor: Indica que el servicio o la función no se pueden utilizar y no significa un impacto de negocio crítico en las operaciones.	En el plazo de cuatro horas laborales	L-V horas laborales
4	Impacto de negocio mínimo: Una consulta o una solicitud no técnica	En el plazo de 1 día laborable	L-V horas laborales

4.1 Acceso a los Datos del Cliente

IBM podrá acceder a los datos del Cliente con el objetivo de diagnosticar problemas con el servicio y facilitar las exploraciones de la aplicación del Cliente por parte del servicio. IBM accederá a los datos únicamente con el objetivo de solucionar defectos o proporcionar soporte para los servicios o productos de IBM.

5. Condiciones Adicionales de la Oferta de SaaS IBM

Es posible que las Exploraciones de Seguridad no identifiquen todos los riesgos de seguridad en una aplicación.

SaaS IBM puede utilizarse para ayudar al Cliente a cumplir con las obligaciones que pueden derivarse de la legislación, las regulaciones, los estándares o las prácticas. Las orientaciones, los usos sugeridos o las instrucciones que se proporcionen con el Servicio no constituyen asesoramiento legal, financiero ni profesional; se recomienda al Cliente que obtenga su propio asesoramiento legal o de otro tipo de expertos. El Cliente es responsable exclusivo de garantizar que tanto él como sus actividades, aplicaciones y sistemas cumplen con todas las leyes, regulaciones, estándares y prácticas aplicables. El uso de este Servicio no garantiza el cumplimiento de la legislación, las regulaciones, los estándares o las prácticas.

El SaaS IBM realiza pruebas invasivas y no invasivas en el sitio web y las aplicaciones móviles o web que el Cliente selecciona para explorar, pruebas que implican ciertos riesgos, incluyendo, sin limitación, lo siguiente:

- a. los sistemas informáticos del Cliente se pueden colgar o pueden fallar mientras se ejecutan las aplicaciones sometidas a prueba, dando como resultado la no disponibilidad temporal del sistema o pérdida de datos;
- b. el rendimiento de los sistemas del Cliente, al igual que el rendimiento de los routers y firewall asociados, puede verse degradado temporalmente durante las pruebas;
- c. pueden generarse cantidades excesivas de mensajes de registro, con el consiguiente consumo excesivo de espacio en disco del archivo de registro;
- d. algunos datos pueden modificarse o suprimirse como resultado del sondeo de vulnerabilidades;

- e. los sistemas de detección de intrusiones pueden activar las alarmas;
- f. la función de correo electrónico de la aplicación que se está probando puede recopilar mensajes de correo electrónico;
- y
- g. el Servicio de Cloud puede interceptar el tráfico de la red monitorizada con el fin de buscar sucesos.

En caso de que el Cliente introduzca credenciales de inicio de sesión autenticado para la aplicación bajo prueba en el Servicio, el Cliente sólo debe introducir tales credenciales para las cuentas de prueba, no para los usuarios en entornos de producción. El uso de credenciales de usuario de entornos de producción puede dar lugar a la transmisión de datos personales a través del Servicio.

El SaaS IBM puede configurarse para explorar aplicaciones web en fase de producción. Cuando el Cliente establece el tipo de escaneo como de "producción", el servicio está diseñado para realizar las exploraciones bajo un método que reduce los riesgos mencionados anteriormente; sin embargo, en determinadas situaciones el Servicio de Cloud puede comportar una degradación del rendimiento o inestabilidad dentro de la infraestructura y los sitios de producción probados. IBM no ofrece ninguna garantía o manifestación con respecto a la conveniencia de utilizar el Servicio de Cloud para explorar los sitios de producción.

ES RESPONSABILIDAD DEL CLIENTE LA DETERMINACIÓN DE LA ADECUACIÓN O LA SEGURIDAD DEL SERVICIO EN RELACIÓN CON EL SITIO WEB, LA APLICACIÓN WEB, LA APLICACIÓN MÓVIL O EL ENTORNO TÉCNICO DEL CLIENTE.

El SaaS IBM está diseñado para identificar una variedad de posibles problemas de seguridad y conformidad en aplicaciones móviles y web, y en servicios web. No prueba todas las vulnerabilidades o riesgos de conformidad, ni actúa como barrera frente a los ataques de seguridad. Las amenazas, legislaciones y normas de seguridad cambian continuamente, y el Servicio puede que no siempre refleje estos cambios. La seguridad y la conformidad de las aplicaciones web, los sistemas y los empleados del Cliente, así como todas las medidas correctivas, son responsabilidad exclusiva del Cliente. La utilización o no utilización de la información proporcionada por el Servicio depende única y exclusivamente del Cliente.

Determinadas leyes prohíben cualquier intento no autorizado de penetrar o acceder a sistemas informáticos. **EL CLIENTE ES RESPONSABLE DE GARANTIZAR QUE EL CLIENTE NO UTILIZARÁ EL SERVICIO PARA EXPLORAR NINGÚN SITIO WEB Y/O APLICACIONES QUE NO SEAN SITIOS WEB Y/O APLICACIONES DE SU PROPIEDAD O DE LOS CUALES NO LE HAYA SIDO OTORGADA AUTORIZACIÓN PARA EXPLORAR.**

5.2 Cookies

El Cliente reconoce y acepta que IBM puede, como parte de la operativa normal y el soporte de SaaS IBM, recopilar información personal del Cliente (empleados y contratistas) en relación con el uso de SaaS IBM, a través de seguimiento y de otras tecnologías. IBM lo hace para recopilar estadísticas de uso e información acerca de la eficacia de SaaS IBM, con la finalidad de mejorar la experiencia de usuario y/o personalizar las interacciones con el Cliente. El Cliente confirma que va a obtener o ha obtenido el consentimiento para permitir a IBM procesar los Datos Personales recopilados con la finalidad mencionada dentro de IBM, de otras empresas de IBM y sus subcontratistas, allí donde IBM y los subcontratistas de IBM ejecuten actividades profesionales, de acuerdo con la legislación aplicable. IBM cursará adecuadamente cualquier petición de los empleados y subcontratistas del Cliente para acceder, actualizar, corregir o eliminar su información personal de contacto recopilada.

5.3 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los tributos se realizan en las ubicaciones que el Cliente identifica como receptoras de los servicios SaaS IBM. IBM aplicará los tributos en base a las direcciones de facturación enumeradas a la hora de solicitar SaaS IBM como ubicación del beneficiario principal, a menos que el Cliente proporcione información adicional a IBM. El Cliente es responsable de mantener esta información actualizada y de comunicar cualquier cambio a IBM.

Apéndice A

1. Descripción General de IBM Application Security on Cloud

IBM Application Security on Cloud proporciona un único lugar para ayudar al Cliente a identificar las vulnerabilidades de seguridad (como inyección SQL, XSS y fugas de datos) para diversas aplicaciones. El servicio incluye varios tipos de técnicas de escaneo de seguridad de las aplicaciones, cada una de las cuales identifica los problemas de seguridad en la aplicación específica.

IBM Application Security on Cloud proporciona las prestaciones siguientes:

- Escaneo de aplicaciones móviles para buscar vulnerabilidades de seguridad. Se lleva a cabo a través de tecnologías de análisis de seguridad dinámico (blackbox) e interactivo (glassbox).
- Escaneo de sitios web de producción o preproducción para buscar vulnerabilidades de seguridad. Se lleva a cabo a través de tecnologías de análisis de seguridad dinámico (blackbox).
- Escaneo de flujos de datos dentro de las aplicaciones web y de escritorio para buscar vulnerabilidades de seguridad. Se lleva a cabo a través de tecnologías de análisis de seguridad estático (whitebox).
- Los informes detallados de vulnerabilidades de seguridad que incluyen tanto los resúmenes detallados de las conclusiones y las medidas de terminación que pueden seguir los desarrolladores.
- Integración con diversas plataformas DevOps como Maven e IBM UrbanCode.