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
- IBM Application Security on Cloud Consulting Services

2. Métricas de Cargo

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

a. **Trabajo**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un Trabajo es un objeto dentro de SaaS IBM que no puede dividirse más y representa un proceso informático que incluye todos sus subprocesos. Deben adquirirse derechos de titularidad suficientes para cubrir el número total de Trabajos procesados o gestionados por SaaS IBM durante el período de medida especificado en un Documento de Titularidad (POE) o Documento Transaccional del Cliente.

b. **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 Usuarios Autorizados con acceso al SaaS IBM durante el período de medida especificado en el POE o el Documento Transaccional del Cliente.

   Para las finalidades de este SaaS IBM:

   - Para pruebas dinámicas: un sitio web direccionable a través de una dirección URL pública o privada. Cada Instancia de Aplicación concede a un sitio derechos de titularidad de hasta 1.000 páginas en un único dominio.
   - Para pruebas estáticas: una unidad de código ejecutable en un solo lenguaje de programación. Cada Instancia de Aplicación concede derechos de titularidad para escanear unidades de código hasta un máximo de 1.000.000 líneas.
   - Para pruebas móviles: una unidad de código binario que se puede ejecutar en un dispositivo móvil. Cada plataforma móvil diferente (por ejemplo, iOS y Android) constituye diferentes Instancias de Aplicación.

c. **Instancia**: es una unidad de medida con la que se puede adquirir SaaS IBM. Una Instancia es el acceso a una configuración específica de SaaS IBM. Deben adquirirse derechos de titularidad suficientes para cada Instancia de SaaS IBM disponible para su acceso y uso durante el período de medida especificado en el Documento de Titularidad (POE) del Cliente o en el Documento Transaccional.

   Para cada derecho de titularidad de Instancia no hay límite en el número de Trabajos realizados o Instancias de Aplicación (aplicaciones conectadas), a condición, sin embargo, que no haya más de treinta (30) Trabajos ejecutándose de forma simultánea en un momento determinado.

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

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.

3.2 Cargo por Uso en Exceso

Si el uso actual del SaaS IBM durante el período de medida supera el derecho de titularidad especificado en el Documento de Titularidad (POE), se facturará al Cliente por el uso en exceso según se establece en el Documento Transaccional.

3.3 Cargos de Configuración

Se facturará al Cliente por la configuración, como se especifica en el Documento de Transacción.

4. Opciones de Vigencia y Renovación

La vigencia del SaaS IBM empezará en la fecha en la que IBM notifique al Cliente que éste tiene acceso al SaaS IBM, según se describe en el POE. El POE especificará si el SaaS IBM se renueva automáticamente, sigue bajo una base de uso continuado o termina al finalizar la vigencia.

En relación con la renovación automática, a menos que el Cliente notifique su voluntad de no renovar como mínimo 30 días antes de la fecha de vencimiento, el SaaS IBM se renovará automáticamente por el plazo especificado en el POE.

En relación con el uso continuado, el SaaS IBM seguirá estando disponible mensualmente, hasta que el Cliente notifique por escrito su voluntad de terminación con 30 días de antelación. El SaaS IBM seguirá estando disponible hasta el final del mes natural tras este período de 30 días.

5. 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 productivo 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

Severidad	Definición de Severidad	Objetivos de Tiempo de Respuesta	Cobertura de Tiempo de Respuesta
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 no cumplir las fechas límite.	En el plazo de dos horas laborables	L-V horas laborables
3	**Impacto de negocio menor:** Indica que el servicio o la función se pueden utilizar y no significa un impacto de negocio crítico en las operaciones.	En el plazo de cuatro horas laborables	L-V horas laborables
4	**Impacto de negocio mínimo:** Una consulta o una solicitud no técnica	En el plazo de 1 día laborable	L-V horas laborables

5.1 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.

6. Condiciones Adicionales de la Oferta de SaaS IBM

Es posible que los escaneos de seguridad no identifiquen todos los riesgos de seguridad de una aplicación, y no están diseñados ni previstos para ser utilizados en entornos peligrosos que requieran un funcionamiento totalmente libre de errores, incluyendo, a título enumerativo y no limitativo, el funcionamiento de sistemas de navegación, los sistemas de control del tráfico aéreo, los sistemas armamentísticos, los sistemas de soporte vital, las instalaciones nucleares, o cualquier otra aplicación en la que un fallo de identificación de los riesgos de seguridad pueda provocar la muerte, lesiones o daños graves a las personas o a la propiedad. Los escaneos de seguridad no están garantizados para funcionar ininterrumpidamente ni sin errores.

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 escanear. Determinadas leyes prohíben cualquier intento no autorizado de penetrar o acceder a sistemas informáticos. El Cliente autoriza a IBM a llevar a cabo los Servicios descritos en el presente documento y acepta que los Servicios disponen del acceso autorizado a los sistemas informáticos del Cliente. IBM puede divulgar esta concesión de autorización a un tercero, si se considera necesario para prestar los Servicios.

Las pruebas 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;

g. el SaaS IBM puede interceptar el tráfico de la red monitorizada con el fin de buscar sucesos.

cualquier derecho o penalización del Acuerdo de Nivel de Servicio o recurso proporcionado por IBM y relativo a los sitios web o las aplicaciones que son sujeto de las pruebas quedará sin vigencia durante las actividades de prueba.

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 exploración 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 SaaS IBM 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 SaaS IBM 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.

A los efectos de claridad, el contenido del Cliente que se describe en el apartado de protección de datos personales de las Condiciones de Uso de IBM - Condiciones Generales también se tiene en consideración para incluir datos que puedan ser accesibles para IBM durante las Pruebas de Intrusión en Aplicaciones.

6.1 Sistemas Propiedad de un Tercero

Para los sistemas (que para los fines de este documento incluyen, a título enunciativo pero no limitativo, las aplicaciones y direcciones IP) propiedad de un tercero que serán sometidos a las pruebas descritas en este documento, el Cliente acepta:

a. que antes de que IBM inicie las pruebas en un sistema de terceros, el Cliente obtendrá una carta firmada por el propietario de cada uno de los sistemas en la que se autorice a IBM a suministrar los Servicios en dichos sistemas y se indique la aceptación por parte del propietario de las condiciones establecidas en el apartado "Permiso para la Realización de Pruebas" y proporcionará a IBM una copia de dicha autorización;

b. será responsable de comunicar al propietario del sistema acerca de cualquier riesgo, exposición y vulnerabilidad identificados en estos sistemas debido a las pruebas remotas realizadas por IBM; y

c. organizar y facilitar el intercambio de información entre el propietario del sistema e IBM, según IBM lo considere necesario.

El Cliente acuerda:

- informar a IBM de forma inmediata cuando exista un cambio en la propiedad de cualquier sistema sometido a las pruebas descritas en este documento;
- no divulgar los Entregables, o el hecho de que IBM ha realizado los Servicios, fuera de la Empresa del Cliente sin el consentimiento previo por escrito de IBM; e
- indemnizar completamente a IBM por cualquier pérdida o responsabilidad en la que IBM incurra por reclamaciones de terceros que surjan del incumplimiento por parte del Cliente de los requisitos de este apartado, titulado "Sistemas Propiedad de un Tercero", y por cualquier citación o reclamación de terceros contra IBM o los subcontratistas o agentes de IBM por: (a) la realización de pruebas de riesgos de seguridad, exposiciones o vulnerabilidades de los sistemas sujetos a las pruebas descritas en este documento, (b) el suministro de los resultados de las pruebas al Cliente, o (c) el uso o la divulgación por parte del Cliente de dichos resultados.

6.2 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.

Como parte del SaaS IBM, que incluye actividades de información, IBM preparará y mantendrá información sin identificación y/o agregada recopilada del SaaS IBM (denominado "Datos de Seguridad"). Los Datos de Seguridad no identificarán al Cliente o a una persona individual, salvo en lo dispuesto en el apartado (d), a continuación. El Cliente, según se establece en el presente documento, acepta también que IBM puede utilizar y/o copiar los Datos de Seguridad solo para los fines siguientes:

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

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

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

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

6.3 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los impuestos se basan 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.

6.4 Información Personal y Servicios y Contenido Regulado

Este SaaS IBM no ha sido diseñado para cumplir ningún requisito de seguridad específico para el contenido regulado, como información personal o información personal sensible. El Cliente es responsable de determinar si este SaaS IBM cubre las necesidades del Cliente en relación con el tipo de contenido que el Cliente utiliza conjuntamente con el SaaS IBM.

IBM no opera como proveedor de servicios regulado por la Federal Communications Commission ("FCC") o los organismos reguladores estatales ("Reguladores Estatales"), y no tiene intención de proporcionar servicios que estén regulados por la FCC o los Reguladores Estatales. Si la FCC o cualquier Regulador Estatal impone requisitos u obligaciones normativos en relación con los servicios proporcionados por IBM en virtud del presente acuerdo, IBM puede: (a) modificar, reemplazar o sustituir los productos con cargo al Cliente, y/o (b) cambiar la forma en la que presta esos servicios al Cliente para evitar la aplicación de dichos requisitos u obligaciones a IBM (por ejemplo, actuando como agente del Cliente para la adquisición de tales servicios a un tercer proveedor común).

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 fines públicos y redes privadas con el propósito de 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

1.1 IBM Application Analyzer

IBM Application Analyzer puede solicitarse por Instancia de Aplicación, por Trabajo (escaneo) o como una Instancia completa y permite los siguientes tipos de escaneo:

- Dynamic Analyzer: Pruebas de sitios web de preproducción o de producción a través de técnicas DAST
- Mobile Analyzer: Pruebas de binarios iOS o Android a través de técnicas IAST
- Static Analyzer: Pruebas de flujos de datos de código de bytes o código fuente a través de técnicas SAST

1.2 Servicio de Configuración

IBM Application Security on Cloud Consulting Services es un servicio de configuración convertido en producto para Application Analyzer. El servicio utiliza consultores de IBM para proporcionar orientación y asistencia con las pruebas y la gestión del riesgo de las aplicaciones. IBM Application Security on Cloud Consulting Services se adquiere como bloques de Compromisos que pueden gastarse en las cantidades que se indican a continuación para solicitar y hacer uso de los servicios específicos siguientes:

a. **Fast Start** [Utiliza una (1) unidad de Compromiso]

El servicio Fast Start ofrece experiencia y orientación para el uso de la seguridad de las características de pruebas y gestión de riesgos de Application Security on Cloud. Una vez que el Cliente haya confirmado que ha iniciado la sesión correctamente en el portal de Application Security on Cloud, IBM organizará una conferencia web de un máximo de dos (2) horas y dos (2) participantes activos para prestar formación sobre funciones y configuraciones básicas de AppSec en SaaS IBM, incluyendo tipos de escaneo, ejecución de escaneo, revisión de informes e instalación de los conectores y las herramientas asociados. El servicio Fast Start se completa después de la finalización de (a) el seminario de formación web del Cliente, (b) la instalación de los conectores y las herramientas aplicables, y (c) la asistencia al Cliente para configurar y ejecutar el primer escaneo del Cliente.

b. **Assessment Review** [Utiliza dos (2) unidades de Compromiso]

El servicio Assessment Review proporciona asistencia para revisar el resultado de una prueba, incluyendo la comprensión y priorizando la resolución de vulnerabilidades en la aplicación. IBM facilitará una conferencia web de un máximo de una (1) hora y dos (2) participantes activos para proporcionar una visión general de las vulnerabilidades encontradas y el riesgo general de

seguridad de la aplicación, así como un debate detallado de las vulnerabilidades de seguridad de la aplicación detectadas, incluyendo (1) cómo se ha probado la vulnerabilidad, (2) cómo se han detectado las vulnerabilidades, (3) ¿cuál es el riesgo de cada vulnerabilidad, y (4) proporcionar recomendaciones generales de fixes para ayudar a resolver la vulnerabilidad. La revisión se basará exclusivamente en el resultado de la prueba y no será una revisión del código fuente. El Cliente revisará el resultado de la prueba e identificará para IBM el resultado de la prueba para su revisión antes de la conferencia web. El servicio Assessment Review se completa tras la finalización de la conferencia web.

c. **Scan for Me** [Utiliza cuatro (4) unidades de Compromiso]

El servicio Scan for Me proporciona un experto en seguridad de aplicaciones de IBM, que configurará y ejecutará una exploración, validará los resultados y llevará a cabo una reunión informativa para revisar los resultados. El Cliente permitirá a un consultor de IBM acceder al entorno ASoC del Cliente para configurar y ejecutar un escaneo, validar los resultados, proporcionar recomendaciones sobre la priorización de la resolución y organizar una reunión informativa sobre los resultados. IBM facilitará una conferencia web de un máximo de una (1) hora y dos (2) participantes activos para proporcionar una visión general de las vulnerabilidades encontradas y el riesgo general de seguridad de la aplicación, así como un debate detallado de las vulnerabilidades de seguridad de la aplicación detectadas, incluyendo (1) cómo se ha probado la vulnerabilidad, (2) cómo se han detectado las vulnerabilidades, (3) ¿cuál es el riesgo de cada vulnerabilidad, y (4) proporcionar recomendaciones generales de fixes para ayudar a resolver la vulnerabilidad. Si se solicita, y como máximo 30 días después del escaneo inicial, IBM proporcionará un nuevo escaneo utilizando la configuración de escaneo del original para verificar únicamente los fixes de seguridad, no para probar nuevas funcionalidades, validará los resultados y entregará el informe al Cliente. El servicio Scan for Me se completa tras la finalización de la conferencia web para revisar los resultados del escaneo inicial o, si es aplicable, la finalización del nuevo escaneo conforme a lo solicitado por el Cliente, y la posterior entrega del informe del nuevo escaneo al Cliente.

d. **Advisor on Demand** [Utiliza siete (7) unidades de Compromiso]

El servicio Advisor on Demand proporciona hasta veinte (20) horas de tiempo de un consultor de IBM, que se pueden utilizar para las actividades relacionadas con el SaaS IBM. El consultor de IBM colaborará en relación con los temas de seguridad en aplicaciones específicos, incluyendo, a título enunciativo pero no limitativo, la gestión de programas, la priorización de pruebas de seguridad, las estrategias de resolución, análisis de código fuente y reparación de código fuente. IBM trabajará con el Cliente para idear y crear una planificación del proyecto con los requisitos específicos del Cliente, incluidos los objetivos del proyecto, las tecnologías pertinentes, los plazos temporales deseados, los materiales entregables previstos y el número estimado de compromisos de servicio de Advisor on Demand. El Cliente debe proporcionar acceso a las aplicaciones, los sistemas y la documentación necesarios para llevar a cabo los servicios. El servicio Asesor on Demand se completa cuando se ha realizado un máximo de 20 horas de asesoramiento experto en seguridad y/o cuando la planificación del proyecto y/o los materiales entregables documentados definidos en la planificación del proyecto hayan sido entregados al Cliente.

e. **Pruebas de Intrusión en Aplicaciones**

Tres opciones:

(1) **Prueba de Intrusión en Aplicaciones de Conformidad/Nivel Inicial**: incluye un máximo de cuarenta (40) horas de tiempo de Consultor; se centra en los defectos de lógica de un solo paso y las versiones más simples de los defectos de inyección. Utiliza quince (15) unidades de Compromiso.

(2) **Prueba de Intrusión en Aplicaciones Estándar**: incluye un máximo de sesenta (60) horas de tiempo de Consultor; amplía el enfoque para incluir defectos de lógica en los flujos de trabajo de múltiples pasos, versiones complejas de defectos de inyección y análisis de tipos de datos complejos. Utiliza veintiún (21) unidades de Compromiso.

(3) **Prueba de Intrusión de Aplicaciones Avanzada**: un máximo de ochenta (80) horas de tiempo de Consultor; amplía el enfoque para incluir la ingeniería inversa de los ejecutables compilados, la disección de protocolos de red personalizados, análisis en profundidad de las bibliotecas y los marcos disponibles públicamente. Utiliza veintisiete (27) unidades de Compromiso.

El servicio de pruebas de intrusión en aplicaciones proporciona un recurso de IBM para realizar las pruebas y la explotación de una aplicación, la entrega de un informe de prueba, y una reunión informativa para explicar los resultados detectados y los riesgos asociados.

IBM organizará una llamada de inicio del proyecto de un máximo de una (1) hora de duración y dos (2) participantes activos para revisar el entorno y la organización del Cliente, incluyendo la plataforma de aplicaciones, la arquitectura, el marco, infraestructura de soporte, los problemas o preocupaciones de seguridad conocidos asociados con la aplicación, el calendario de pruebas preliminar y el plan de contacto de emergencia.

IBM llevará a cabo la prueba de intrusión en aplicaciones incluyendo, a título enunciativo pero no limitativo: la identificación de vulnerabilidades comunes, como inyección de SQL y script entre sitios, la evaluación de las fortalezas y debilidades de los controles de seguridad existentes, como la validación de entrada, la autenticación y la autorización, la verificación de la correcta aplicación de la lógica de negocio, la validación del uso adecuado de los protocolos de seguridad, la identificación de defectos de manipulación de la sesión y la verificación de los controles de seguridad adecuados en el inicio de sesión, la recuperación de contraseñas, la política de contraseñas y otras funciones de gestión de usuarios. Los resultados se documentarán en el Informe de Pruebas de Intrusión en Aplicaciones. IBM organizará una conferencia web para la reunión informativa de un máximo de una (1) hora. El servicio de Pruebas de Intrusión en Aplicaciones se completa cuando se ha utilizado el tiempo de consultoría asignado, se ha llevado a cabo la conferencia web y el Informe de Pruebas de Penetración de Aplicaciones final ha sido entregado al Cliente.

1.2.1 Responsabilidades de los Servicios de Configuración

IBM se encargará de:

- proporcionar los Servicios de Configuración utilizando unidades de Compromiso adquiridas por el Cliente y según lo establecido en el POE; y
- haber completado un Servicio de Configuración cuando se hayan completado los criterios de finalización que se describen en el apartado 1.2.

El Cliente acuerda:

- ser responsable de todos los cargos asociados con los solicitudes de Compromiso realizadas por el Cliente durante la vigencia del contrato;
- aceptar que las unidades de Compromiso adquiridas deben ser utilizadas dentro del plazo inicial del contrato y caducan si no se han utilizado en la fecha final del período contratado; y
- comenzar una solicitud formal de todos los Servicios de Configuración al menos 30 días antes de la fecha de finalización de la suscripción.

En la ejecución de cualquier Servicio de Configuración, IBM puede solicitar información y cooperación razonable al Cliente. La negativa a proporcionar la información o la cooperación requeridas de manera oportuna por parte del Cliente puede, según lo determine IBM, comportar cargos por unidad de Compromiso según se requiera por los servicios o el retraso en la ejecución del servicio aplicable.

Para que IBM pueda realizar la prueba con precisión, el Cliente está de acuerdo en seguir las instrucciones de IBM en relación con la preparación y el mantenimiento del entorno durante el período de prueba.