

Descripción del Cloud Service de IBM

IBM Digital Data Exchange

Lo siguiente es la Descripción de Servicio de su Pedido:

1. Cloud Service

Esta oferta de Cloud Service, incluyendo la oferta básica y las características opcionales disponibles, se describe a continuación y según se seleccione en un Documento de Pedido. El Documento de Pedido consistirá en el Presupuesto que se presenta y el Documento de Titularidad (POE) que el Cliente recibirá de IBM confirmando la fecha de inicio y final para la vigencia de los Cloud Services, así como el inicio de la facturación.

1.1 IBM Digital Data Exchange

IBM Digital Data Exchange es una solución que aporta a los Clientes una única interfaz para la configuración y el despliegue de etiquetas de páginas móviles y sitios web.

IBM Digital Data Exchange permite a los Clientes gestionar etiquetas de IBM y de Business Partners de IBM para desplegarlas en un sitio móvil o web del Cliente. La interfaz de usuario de IBM Digital Data Exchange proporciona control directo sobre el proceso de etiquetado, dando a los usuarios la capacidad de definir etiquetas de página y grupos de páginas en base a un conjunto de reglas para determinar la ejecución de etiquetas. Una vez adquirido IBM Digital Data Exchange, el Cliente puede gestionar el despliegue actual y anterior de las etiquetas de IBM, de Business Partners de IBM y código de propiedad o Javascript personalizado para diversos entornos.

2. Descripción de la Seguridad

2.1 Políticas de Seguridad

IBM mantiene las políticas de privacidad y seguridad que se publican y se comunican a los empleados de IBM. IBM requiere una formación en privacidad y seguridad a las personas individuales de todo el mundo que ofrecen soporte en los centros de datos de IBM y mantenemos un equipo de seguridad que se centra en la seguridad de la información. Las políticas de seguridad y los estándares de IBM se revisan y se evalúan anualmente. Las incidencias de seguridad de IBM se gestionan de acuerdo con un procedimiento completo de respuestas ante incidencias.

2.2 Control de Acceso

IBM mantiene una separación lógica de los datos del Cliente. Los datos del Cliente residen en su propio esquema específico de Cliente y han sido diseñados para ser accesibles a través del Cloud Service o de la exportación de datos especificada por el Cliente. El acceso al Cloud Service y a los datos del Cliente los controla y gestiona el administrador designado por el Cliente. IBM utiliza una tecnología de túnel VPN cifrado y autenticación multifactorial a la hora de acceder a los sistemas cliente. El acceso está restringido a las personas que requieren acceso para poder mantener y administrar el Cloud Service y la oferta de hardware y software asociada en instalaciones de centro de datos de terceros. IBM utiliza tráfico de red Wi-Fi (conocido como 802.11) cifrado utilizando WPA2 con la opción de algoritmo de cifrado AES y proporciona SSID sin difusión y autenticación mutua entre el servidor y los dispositivos finales a la hora de acceder a los sistemas que contienen datos del Cliente.

2.3 Integridad y Disponibilidad del Servicio

Las modificaciones de los recursos del sistema operativo (OSR) y el software de aplicaciones se rigen por el proceso de gestión de cambios de IBM. Se utiliza hardware, software, registros de acceso, acceso de solo lectura y controles de cifrado dentro de la infraestructura de red y en las estaciones de trabajo de las personas que trabajan en centros de datos de IBM o con datos del Cliente en centros de datos de IBM para ayudar a reducir la posibilidad de propagación y ejecución de virus informáticos y otras formas de código nocivo conocidas. IBM utiliza el cifrado a través de la red mediante conexiones SSL estándar (https) y la infraestructura utiliza soluciones de tecnología para la seguridad integral, incluyendo firewall, prevención de intrusiones y tecnologías antimalware. El escaneo de vulnerabilidades de TCP/IP lo realizan habitualmente los administradores autorizados para detectar y resolver posibles vulnerabilidades de seguridad del sistema. Los datos de almacén de IBM se copian en un almacenamiento secundario en el centro de datos de IBM, y el archivado terciario (cinta) se cifra y se duplica para el almacenamiento en las instalaciones de recuperación de desastres externa de un tercero.

2.4 Registros de Actividad

IBM mantiene los registros de su actividad para sistemas, aplicaciones, repositorios de datos, dispositivos de middleware y de infraestructura de red que están configurados para registrar la actividad. IBM mantiene registros de i) intentos de acceso mediante inicio de sesión satisfactorios y no satisfactorios, ii) intentos satisfactorios y no satisfactorios de obtener acceso a la infraestructura desde una ubicación externa, iii) actualización de los intentos de acceso a OSR y iv) actividades realizadas utilizando una autoridad administrativa de seguridad o sistema.

2.5 Seguridad Física

IBM restringe el acceso únicamente al personal autorizado del centro de datos de IBM en IBM y en los centros de datos proporcionados por terceros de IBM. El entorno del Cloud Service de IBM incluye la autenticación multifactorial para el acceso físico, implicando un único código y una exploración biométrica, así como personal de seguridad ininterrumpido (24x7), seguridad atendida y vigilancia de vídeo. IBM prohíbe la visualización, copia, alteración o eliminación no autorizadas de cualquier soporte que contenga datos del Cliente. Los soportes extraíbles en los cuales se almacenen los datos del Cliente (incluyendo lápices de memoria, CD y DVD) se cifran utilizando por lo menos AES de 256 bits (o equivalente). Los sistemas portátiles y de sobremesa proporcionados por IBM requieren la implementación del cifrado de todo el disco (PGP) allí donde los privilegios de acceso a datos confidenciales o del Cliente sean necesarios. IBM destruye los soportes extraíbles y cualquier dispositivo del Cliente (como discos, unidades USB, DVD, cintas de copia de seguridad, impresoras y portátiles) que contenga datos del Cliente, o hace que los datos del Cliente en estos soportes físicos sean ininteligibles y no puedan reconstruirse mediante ningún medio técnico antes de que el soporte vuelva a utilizarse. IBM trocea el papel residual y lo desecha de un modo seguro y confidencial para hacer que el papel residual sea ilegible.

2.6 Cumplimiento

IBM certifica sus prácticas de privacidad anualmente de acuerdo con los principios Safe Harbor del Departamento de Comercio de los EE.UU.: aviso, selección, transferencia de salida, acceso y precisión, seguridad y supervisión/ejecución. El tipo SSAE 16 de auditoría estándar del sector (antiguamente SAS 70), o equivalente, se lleva a cabo anualmente en nuestros centros de datos de producción. IBM revisa las actividades relacionadas con seguridad y la privacidad para que cumplan con los requisitos de negocio de IBM. IBM realiza evaluaciones y auditorías regularmente para confirmar el cumplimiento con las políticas de seguridad de la información. Las políticas de seguridad establecidas proporcionan, para las auditorías de seguridad, la aplicación periódica de parches de seguridad y gestión y control de contraseñas. La formación y los conocimientos en seguridad del personal de IBM se completan anualmente con empleados de IBM y de proveedores. Se recuerda al personal los objetivos de su trabajo y sus responsabilidades para cumplir con la conducta ética comercial, confidencialidad y obligaciones de seguridad de IBM, anualmente.

3. Objetivos de Nivel de Servicio

El deseo de IBM es que el Cliente pueda disfrutar de SaaS IBM con un índice de disponibilidad del 99%. El SLO no es un compromiso contractual sino un conjunto de objetivos que el equipo de Soporte al Cliente de IBM se esfuerza por cumplir o superar mediante sus procesos, tecnología y personal.

4. Información de Derechos de Titularidad y Facturación

4.1 Métricas de Cargo

El Cloud Service se pone a disposición bajo las siguientes métricas de cargo, según se especifica en el Documento de Pedido:

- a. Millón de Llamadas a Servidor (MSC) es una unidad de medida con la que se puede adquirir el Cloud Service. Una Llamada a Servidor son datos que se transfieren al Cloud Service y se procesan en él como resultado de un evento etiquetado, iniciado por un visitante seguido para un ID de Entidad. Una Llamada a Servidor procesada para diferentes ID de Entidad se contará como una única Llamada a Servidor para cada ID de Entidad único. Un ID de Entidad separa y/o controla los derechos de acceso a datos en el Cloud Service, que pueden incluir datos procesados de uno o varios sitios web del Cliente. Cada derecho de titularidad de MSC representa un Millón de Llamadas a Servidor. Deben adquirirse derechos de titularidad suficientes de Millón de Llamadas a Servidor para cubrir el número de Llamadas de Servidor durante el período de medida especificado en el Documento de Pedido.

4.2 Cargos y Facturación

El importe que se debe abonar por el Cloud Service se especifica en el Documento de Pedido.

5. Opciones de Vigencia y Renovación

5.1 Vigencia

La vigencia del Cloud Service empezará en la fecha en la que IBM notifique al Cliente que éste tiene acceso al Cloud Service según se describe en el Documento de Pedido. La parte del Documento de Titularidad (POE) del Documento de Pedido confirmará la fecha exacta de inicio y finalización de la vigencia. El Cliente podrá incrementar su nivel de uso del Cloud Service durante la vigencia poniéndose en contacto con IBM o con un Business Partner de IBM. Confirmaremos el nivel de uso incrementado en un Documento de Pedido.

5.2 Opciones de Renovación de la Vigencia de los Cloud Services

El Documento de Pedido del Cliente establecerá si el Cloud Service se renovará al finalizar la vigencia, designando la vigencia como uno de los siguientes:

5.2.1 Renovación Automática

Si el Documento de Pedido del Cliente establece que la renovación del Cliente es automática, el Cliente podrá resolver la vigencia de expiración del Cloud Service mediante solicitud por escrito, con una antelación mínima de noventa (90) días antes de la fecha de expiración de la vigencia establecida en el Documento de Pedido. Si IBM o el Business Partner de IBM no recibe dicho aviso de resolución antes de la fecha de expiración, la vigencia que venza se renovará automáticamente por el plazo de un año o por la misma duración que la vigencia original establecida en el Documento de Titularidad (POE).

5.2.2 Facturación Continua

Si el Documento de Pedido indica que la facturación del Cliente es continua, el Cliente seguirá teniendo acceso a Cloud Service y se le facturará por el uso del Cloud Service en una base continuada. Para dejar de utilizar Cloud Service y detener el proceso de facturación continua, el Cliente deberá proporcionar a IBM o a su propio Business Partner de IBM un aviso de solicitud de cancelación del Cloud Service 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.

5.2.3 Renovación Necesaria

Si el Documento de Pedido indica que el tipo de renovación del Cliente es "resolver", el Cloud Service se resolverá al final de la vigencia y el acceso del Cliente al Cloud Service se eliminará. Para seguir utilizando el Cloud Service 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 una nueva vigencia de la suscripción.

6. Soporte Técnico

Se proporciona Soporte Técnico para la oferta SaaS IBM y el Software de Habilitación, según corresponda, durante el Período de Suscripción. Dicho soporte técnico está incluido en SaaS IBM y no está disponible como oferta independiente.

En el URL siguiente se puede encontrar información de soporte técnico: http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

7. Software de Habilitación

- a. Esta oferta de Cloud Service puede incluir software de habilitación. El Cliente puede utilizar el software de habilitación junto con el uso del Cloud Service, durante la vigencia del Cloud Service. En la medida en que el software de habilitación contiene código de muestra, el Cliente tiene el derecho adicional de realizar trabajos derivados del código de muestra y utilizarlos en conformidad con esta concesión. El software de habilitación se proporciona bajo el SLA, si existe, como componente del Cloud Service, pero por otro lado se proporciona "TAL CUAL", sin garantía.

8. Información Adicional

8.1 Detalles de los Derechos de Titularidad

En la cuota de suscripción a IBM Digital Data Exchange se incluye lo siguiente:

- a. Se proporcionará al Cliente una única instancia de IBM Digital Data Exchange.
- b. Habilitación estándar de hasta cinco (5) horas de servicios de implementación de la inscripción inicial del Cliente a IBM Digital Data Exchange. Los servicios caducan a los 90 días a partir de la fecha en que el Cliente recibe la notificación de IBM de que su acceso al Cloud Service está disponible independientemente de si se han utilizado todas las horas.

8.2 Aviso y Política de Privacidad

El Cliente acepta (i) proporcionar un enlace claro y visible a las condiciones de uso y política de privacidad del sitio web del Cliente, que incluya un enlace con la recopilación de datos y las prácticas de uso por parte de IBM y del Cliente (<http://www.ibm.com/software/marketing-solutions/privacy/index.html>); (ii) proporcionar avisos relacionados con la colocación por parte de IBM en nombre del Cliente de cookies y beacons de gifs/web claros en los ordenadores de los visitantes, junto con una explicación de la finalidad y el uso de esta tecnología; y (iii) en la medida que lo exija la ley, obtener el consentimiento de los visitantes del sitio web antes de que el Cliente, o IBM en nombre del Cliente, coloque cookies y beacons gifs/web en los dispositivos de los visitantes del sitio web.

El Cliente reconoce y acepta que IBM puede, como parte de la operativa normal y el soporte de los Cloud Services, recopilar información personal del Cliente (empleados y contratistas) en relación con el uso de los Cloud Services, a través de seguimiento y de otras tecnologías. IBM lo hace para recopilar estadísticas de uso e información acerca de la eficacia de los Cloud Services de 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 la información personal recopilada 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 ley aplicable. IBM cursará adecuadamente cualquier petición de los empleados y subcontratistas del Cliente para acceder, actualizar, corregir o eliminar su información personal de contacto.

8.3 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los tributos se realizan en las ubicaciones que el Cliente identifica como receptoras de los Cloud Services. IBM aplicará los tributos en base a las direcciones de facturación enumeradas a la hora de solicitar un Cloud Service 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.