

## Descripción del Cloud Service de IBM

### IBM OpenPages GRC on Cloud

Lo siguiente es la Descripción de Servicio de su Pedido:

#### 1. Cloud Service

La oferta de Cloud Service se describe a continuación y se especifica en un Documento de Pedido para las ofertas bajo derechos de titularidad seleccionadas. El Documento de Pedido consistirá en el Presupuesto que se presenta y el Documento de Titularidad (POE) que el Cliente recibirá confirmando la fecha de inicio y final para la vigencia de los Cloud Services, así como el inicio de la facturación.

#### 1.1 IBM OpenPages GRC on Cloud

IBM OpenPages GRC on Cloud (un componente obligatorio) ofrece una configuración estándar de Operational Risk Management que proporciona la capacidad de identificar, gestionar, monitorizar e informar acerca de iniciativas de riesgo y conformidad a nivel de toda la empresa. Puede utilizarse para combinar todos los datos de riesgo, incluyendo autoevaluaciones de riesgo y control (RCSA), eventos de pérdida, análisis de escenarios, pérdidas externas e indicadores de riesgo clave (KRI) en un único módulo integrado.

Estas son las prestaciones de Operational Risk Management:

- Características principales:
  - (1) Permite la identificación, la medición y la mitigación de riesgos.
  - (2) Permite la prueba y la documentación de controles internos.
- Eventos de pérdida, que permiten las actividades siguientes:
  - (1) Seguimiento, evaluación y gestión de eventos internos y externos que pueden suponer riesgos operativos.
  - (2) Gestión de eventos y recuperaciones de múltiple impacto que se asocian a pérdidas operativas.
- Eventos de pérdida externos que proporcionan la capacidad de importar datos de pérdidas desde bases de datos de IBM Algo FIRST, Operational Risk data eXchange Association (ORX) y Operational Risk Consortium (ORIC) (se requieren suscripciones por separado) en IBM OpenPages Operational Risk Management para el análisis de escenarios, benchmarking y la generación de informes. El Cliente puede también exportar los datos de pérdidas en herramientas analíticas o aplicaciones de asignación de capital.
- Indicadores de riesgo clave (KRI), que pueden utilizarse para realizar un seguimiento de las métricas y mostrar la posible presencia o estado de una tendencia o condición de riesgo.
- Análisis de escenarios, que es una técnica de evaluación que puede utilizarse para identificar y medir tipos de riesgo específicos, especialmente eventos de severidad elevada y baja frecuencia.
- Elaboración de informes, monitorización y analítica.
- Implementación de IBM SoftLayer en cloud.

#### 1.2 IBM OpenPages GRC Non-Production Instance on Cloud

IBM OpenPages GRC Non-Production Instance on Cloud proporciona una instancia de no producción del Cloud Service para actividades de desarrollo interno y prueba.

#### 1.3 IBM OpenPages GRC Data Storage on Cloud

IBM OpenPages GRC Data Storage on Cloud (un componente obligatorio) proporciona almacenamiento de datos GRC a la instancia de Servicio Cloud del Cliente. El almacenamiento se venderá en asignaciones de 150 gigabytes.

## **1.4 IBM OpenPages GRC Administrator User on Cloud**

Los usuarios de IBM OpenPages GRC Administrator User on Cloud (uno obligatorio, como mínimo) tienen permitido el acceso a todas las funciones administrativas y las prestaciones de Operational Risk Management del Cloud Service.

## **1.5 IBM OpenPages Operational Risk Management User on Cloud**

Los usuarios de IBM OpenPages Operational Risk Management User on Cloud únicamente tienen permiso para interactuar con las prestaciones de Operational Risk Management descritas anteriormente.

## **1.6 IBM OpenPages GRC Operational Risk Management Jump Start on Cloud**

IBM OpenPages GRC Operational Risk Management Jump Start on Cloud (un componente obligatorio) proporciona servicios para la implementación inicial del Cloud Service e incluye asistencia y coaching inicial para planificación de proyectos, mantenimiento, administración y revisión de prácticas demostradas.

# **2. Descripción de la Seguridad**

## **2.1 Políticas de Seguridad**

IBM mantiene las políticas de privacidad y seguridad que comunica a los empleados de IBM. IBM requiere una formación en privacidad y seguridad al personal que ofrece soporte en los centros de datos de IBM. Disponemos de un equipo de 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**

El acceso a los datos del Cliente, si se requiere, sólo está permitido a representantes de soporte de IBM autorizados de acuerdo con los principios de segregación de tareas. El personal de IBM utiliza una autenticación de dos factores a un host de gestión intermedio "gateway". Todas las conexiones son canales cifrados al acceder a los datos del Cliente. Se registran todos los accesos a los datos del Cliente y la transferencia de datos hacia o desde el entorno de hosting. Se prohíbe el uso de Wi-Fi dentro de los centros de datos de IBM que dan soporte a este Cloud Service.

## **2.3 Integridad y Disponibilidad del Servicio**

Las modificaciones del sistema operativo y el software de aplicaciones se rigen por el proceso de gestión de cambios de IBM. Los cambios de las reglas de firewall también se rigen por el proceso de gestión de cambios y los revisa el personal de seguridad de IBM antes de la implementación. IBM monitoriza el centro de datos 24x7. El escaneo de vulnerabilidades internas y externas lo realizan normalmente los administradores autorizados y los proveedores de terceros para ayudar a detectar y resolver posibles vulnerabilidades de seguridad del sistema. Se utilizan sistemas de detección de Malware (antivirus, detección de intrusiones, escaneo de vulnerabilidades y prevención de intrusiones) en todos los centros de datos de IBM. Los servicios de los centros de datos de IBM dan soporte a una gran cantidad de protocolos de entrega de información para la transmisión de datos en redes públicas. Algunos ejemplos son HTTPS/SFTP/FTPS/S/MIME y VPN de sitio a sitio. Los datos de copia de seguridad pensados para el almacenamiento fuera del sitio se cifran antes del transporte.

## **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. Para minimizar la posibilidad de manipulación indebida y permitir un análisis central, alertas e informes, el registro de actividad se realiza en tiempo real en repositorios de registros centrales. Los datos se firman para prevenir la manipulación indebida. Los registros se analizan en tiempo real y a través de unos informes de análisis periódicos para poder detectar comportamientos anómalos. Se avisa al personal de operaciones de las anomalías y éstos se ponen en contacto con un especialista en seguridad disponible 24x7, si es necesario.

## **2.5 Seguridad Física**

IBM mantiene los estándares de seguridad física diseñados para restringir el acceso físico no autorizado a los centros de datos de IBM. Existen puntos de acceso limitado en los centros de datos, que están controlados por una autenticación de dos factores y están monitorizados por las cámaras de vigilancia. El acceso está permitido sólo al personal autorizado que dispone de acceso aprobado. El personal de

operaciones verifica la aprobación y emite un identificador de acceso que otorga el acceso necesario. Los empleados con dichos identificadores no deben utilizar otros identificadores de acceso y sólo pueden disponer del identificador de acceso al centro de datos durante su período de actividad. La utilización de identificadores está registrada. Los visitantes que no sean de IBM se registrarán al entrar en las instalaciones y serán escoltados mientras estén en las instalaciones. Las áreas de entrega y de descarga y otros puntos donde puedan entrar personas no autorizadas están controladas y aisladas.

## **2.6 Cumplimiento**

IBM realiza auditorías bajo la norma SSAE 16 del sector (o alguna norma equivalente) anualmente en los 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. Los empleados de IBM y de los proveedores completan la formación de conocimiento y seguridad del personal, anualmente. 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. Acuerdo de Nivel de Servicio (SLA)**

IBM proporciona el siguiente acuerdo de nivel de servicio ("SLA") de disponibilidad para el Cloud Service. El Cliente comprende que el SLA no constituye ninguna garantía.

### **3.1 Definiciones**

- a. "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 el Cloud Service.
- b. "Reclamación" es una reclamación enviada por el Cliente a IBM de acuerdo con este SLA referente a un Nivel de Servicio no satisfecho durante un Mes Contratado.
- c. "Mes Contratado" indica cada mes completo durante el plazo, medido desde las 12:00 a.m. (horario de la costa este de los Estados Unidos) del primer día del mes a las 11:59 p.m. (horario de la costa este de los Estados Unidos) del último día del mes.
- d. "Tiempo de inactividad" es un periodo de tiempo durante el que el proceso de los sistemas de producción para el Cloud Service se ha detenido y los usuarios del Cliente no pueden utilizar todos los aspectos del Cloud Service para los que tiene permisos. El Tiempo de inactividad no incluye el periodo de tiempo en que el Cloud Service deja de estar disponible como consecuencia de:
  - (1) Una parada de mantenimiento planificada o anunciada;
  - (2) Sucesos o causas que queden fuera del control de IBM (por ejemplo, desastres naturales, interrupciones de Internet, mantenimiento de emergencia, etc.);
  - (3) Problemas con aplicaciones, equipos o datos del Cliente o de terceros;
  - (4) La no observancia del Cliente de las configuraciones necesarias del sistema y de las plataformas soportadas para acceder al Cloud Service; o
  - (5) La conformidad de IBM con cualquier diseño, especificación o instrucción proporcionada por el Cliente a IBM o por un tercero a IBM en representación del Cliente.
- e. "Suceso" es una circunstancia o un conjunto de circunstancias que no permiten satisfacer un Nivel de Servicio.
- f. "Nivel de Servicio" es el estándar definido más adelante según el cual IBM mide el nivel de servicio que proporciona en este SLA.

### **3.2 Créditos de disponibilidad**

- a. Para enviar una Reclamación, el Cliente debe registrar un ticket de soporte de Severidad 1 (según se define a continuación, en el apartado Soporte Técnico) para cada Suceso en el servicio de asistencia técnica de IBM, en un período de veinticuatro (24) horas desde que el Cliente tuvo conocimiento en primera instancia del Suceso que ha afectado al uso del Cloud Service. El Cliente debe proporcionar toda la información necesaria acerca del Suceso y asistir razonablemente a IBM en el diagnóstico y la resolución del Suceso.
- b. El Cliente debe enviar la Reclamación 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. Los Créditos de disponibilidad se basarán en la duración del Tiempo de inactividad medido desde el primer momento en que le impactó el Tiempo de inactividad. 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 la tabla siguiente. IBM no será responsable de múltiples Créditos de disponibilidad para el mismo Suceso en el mismo Mes Contratado.
- d. Los Créditos de disponibilidad totales concedidos en relación con cualquier Mes contratado no deberán superar, bajo ninguna circunstancia, el 10 por ciento (10 %) de una doceava parte (1/12) del cargo anual pagado por el Cliente a IBM para el Cloud Service.

### 3.3 Niveles de Servicio

Disponibilidad del Cloud Service durante un Mes Contratado

| Disponibilidad durante un Mes Contratado | Crédito de Disponibilidad<br>(% de la Cuota de suscripción mensual para el Mes Contratado que está sujeto a una Reclamación) |
|--|--|
| < 98 %                                   | 2 %  |
| < 97 %                                   | 5 %  |
| < 93 %                                   | 10 %   |

La Disponibilidad, expresada como porcentaje, se calcula de este modo: (a) el número total de minutos en un Mes Contratado, menos (b) el 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: 900 minutos de Tiempo de inactividad total durante un Mes Contratado

|   |  |
|---|--|
| 43.200 minutos en total en un Mes Contratado de 30 días<br>- 900 minutos de Tiempo de Inactividad<br>= 42.300 minutos | = 2 % de Crédito de<br>Disponibilidad para el 97,9 % de<br>Nivel de Servicio Alcanzado |
| <hr style="width: 50%; margin: 0 auto;"/> 43.200 minutos en total   |  |

### 3.4 Información Adicional acerca de este SLA

Este SLA se pone a disposición únicamente de los Clientes de IBM y no se aplica a las reclamaciones realizadas por los usuarios, los participantes y los invitados permitidos del Cloud Service del Cliente, ni a ningún servicio beta o de prueba que proporcione IBM. El SLA únicamente se aplica a los Cloud Services que están en uso de producción. No se aplica a entornos que no son de producción, incluyendo, a título enunciativo y no limitativo, entornos de prueba, recuperación tras desastre, control de calidad o desarrollo.

## 4. Información de Derechos de Titularidad y Facturación

### 4.1 Métricas de Cargo

Los Cloud Services se ponen a disposición bajo las siguientes métricas de cargo, según se especifica en el Documento de Pedido:

- a. Usuario Autorizado es una unidad de medida con la que se puede adquirir el Cloud Service. El Cliente debe obtener derechos de titularidad independientes y dedicados para cada Usuario Autorizado al que se permita acceso al Cloud Service de cualquier modo, ya sea directo o indirecto (por ejemplo, a través de un programa multiplexor, un dispositivo o un servidor de aplicaciones) mediante cualquier método. Deben adquirirse derechos de titularidad suficientes para cubrir el número de Usuarios Autorizados con acceso al Cloud Service durante el período de medida especificado en el Documento de Pedido del Cliente.
- b. Compromiso es una unidad de medida con la que se pueden obtener servicios. Un Compromiso consiste en servicios de formación y/o profesionales relacionados con el Cloud Service. Deben adquirirse derechos de titularidad suficientes para cubrir cada Compromiso.
- c. Gigabyte es una unidad de medida con la que se puede adquirir el Cloud Service. Un Gigabyte se define del 2.º al 30.º byte de potencia de datos (1,073,741,824 bytes). Deben adquirirse derechos de titularidad suficientes para cubrir el número total de Gigabytes procesados por el Cloud Service durante el período de medida especificado en el Documento de Pedido del Cliente.

- d. Instancia es una unidad de medida con la que se puede adquirir el Cloud Service. Una Instancia es el acceso a una configuración específica del Cloud Service. Deben adquirirse derechos de titularidad suficientes para cada Instancia del Cloud Service disponible para su acceso y uso durante el período de medida especificado en el Documento de Pedido.

## **4.2 Cargos y Facturación**

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

## **4.3 Cargos de Configuración**

Los servicios de configuración estándar y sus cargos aplicables se proporcionan a través de la oferta IBM OpenPages Operational Risk Management Jump Start on Cloud.

Si el Cliente requiere configuración adicional de los servicios, debe contratar los servicios OpenPages GRC on Cloud de IBM a través de una Especificación de Trabajo complementaria.

## **4.4 Cargo Mensual Parcial**

El cargo mensual parcial es una tarifa diaria prorrateada. El cargo mensual parcial se calcula según los días que faltan del mes parcial a partir de la fecha en que IBM notifica al Cliente que su acceso a la oferta de Cloud Service está disponible.

## **4.5 Cargo por Uso en Exceso**

Si el uso actual del Cloud Service por parte del Cliente durante el período de medida excede el derecho de titularidad especificado en el apartado POE del Documento de Pedido, se facturará al Cliente por el uso en exceso, según se establece 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 el plazo poniéndose en contacto con IBM o con su propio Business Partner de IBM. Confirmaremos el nivel de uso incrementado en un Documento de Pedido.

## **5.2 Opciones de Renovación del Plazo de los Cloud Services**

El Documento de Pedido del Cliente establece si el Cloud Service se renueva al finalizar el plazo. Para ello, se asigna al plazo una de las siguientes designaciones:

### **5.2.1 Renovación Automática**

Si el Documento de Pedido del Cliente establece que la renovación del Cliente es automática, el Cliente podrá resolver el plazo de expiración del Cloud Service mediante solicitud por escrito, con una antelación mínima de noventa (90) días antes de la fecha de expiración del plazo 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, el plazo que venza se renovará automáticamente por el plazo de un año o por la misma duración que el plazo original establecido 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 al Cloud Service una vez finalizada la vigencia y se le facturará por el uso del Cloud Service de forma continuada. Para dejar de utilizar el 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 del plazo 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 un nuevo plazo de suscripción.

## 6. Soporte Técnico

Se ofrece soporte técnico para el Cloud Service durante la vigencia del Cloud Service de conformidad con lo establecido en [http://www-01.ibm.com/software/support/acceleratedvalue/SaaS\\_Handbook\\_V18.pdf](http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf) u otro URL proporcionado posteriormente por IBM. El soporte técnico está incluido en el Cloud Service y no está disponible como oferta independiente.

## 7. Conformidad con Safe Harbor

IBM no ha determinado la conformidad de este Cloud Service con las infraestructuras de puerto seguro (Safe Harbor Framework) de EE.UU. / Suiza.

## 8. Información Adicional

### 8.1 Recopilación de Datos

El Cliente reconoce y acepta que IBM puede, como parte de la operativa normal y el soporte del Cloud Service, recopilar información personal del Cliente (empleados y contratistas) en relación con el uso del Cloud Service, a través de seguimiento y de otras tecnologías. IBM lo hace para recopilar estadísticas de uso e información acerca de la eficacia del Cloud Service 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 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 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.

### 8.2 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.

### 8.3 Limitación de No Producción

Si el Cloud Service se designa como de "No Producción", sólo podrá utilizarse para actividades internas de no producción incluyendo, a título enunciativo y no limitativo, pruebas, ajuste del rendimiento, diagnóstico de errores, benchmarking interno, desarrollo, actividades de control de calidad o desarrollo de extensiones o ampliaciones de uso interno en el Cloud Service mediante interfaces de programación de aplicaciones publicadas. El Cliente no tiene autorización para utilizar ninguna parte del Cloud Service con ninguna otra finalidad sin adquirir las autorizaciones de producción pertinentes.

### 8.4 Sin Garantía de Cumplimiento

El Cloud Service 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 Cloud Service 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 únicamente es el responsable de garantizar que tanto él como sus actividades cumplen con todas las leyes, regulaciones, estándares y prácticas aplicables. El uso del Cloud Service no garantiza el cumplimiento de la legislación, las regulaciones, los estándares o las prácticas.

El Cliente también reconoce que el Cloud Service es una herramienta para ayudar al Cliente y no es un sustituto del conocimiento, juicio y experiencia de la dirección del Cliente y de sus empleados en el asesoramiento a terceros y en la toma de decisiones sobre inversión y otros negocios y gestión de riesgos. El Cliente es responsable de los resultados obtenidos a partir del uso del Cloud Service.

### 8.5 Enlaces con Sitios web de Terceros u Otros Servicios

Si el Cliente o un Usuario del Cloud Service transmite Contenido a un sitio web de un tercero u otro servicio enlazado con Cloud Service o accesible por éste, el Cliente y el Usuario del Cloud Service permitirán a IBM habilitar la transmisión de Contenido; sin embargo, dicha interacción se llevará a cabo únicamente entre el Usuario de IBM y el sitio web o servicio del tercero. IBM no ofrece ninguna garantía ni manifestación sobre los datos, servicios o sitios de terceros, y no se responsabilizará de ellos.

## **8.6 Restricciones acerca del Uso en Beneficio de un Tercero**

El Cliente no debe utilizar el Cloud Service ni ninguno de sus componentes, incluyendo, sin limitación, los informes y los datos de salida producidos por el Cloud Service para proporcionar prestación de servicios, servicios de alojamiento o cualquier tipo de servicios de tecnología de la información comercial a terceros, a menos que se acuerde por escrito con IBM.

## **8.7 Ausencia de Información Personal relativa a la Salud**

El Cloud Service no está diseñado para cumplir con la Ley de Transferencia y Responsabilidad de Seguros Médicos ("HIPAA") de Estados Unidos, y no puede utilizarse para la transmisión o almacenamiento de ninguna Información Personal relativa a la Salud.