IBM Cognos Controller on Cloud

Lo siguiente es la Descripción de Servicio de su Pedido:

1. Servicio de Cloud

La oferta del Servicio de Cloud 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 confirma la fecha de inicio y final de los Servicios de Cloud. La facturación empezará tras la provisión del Servicio de Cloud.

1.1 IBM Cognos Controller User on Cloud

IBM Cognos Controller es un software de consolidación financiera que da soporte al proceso de cierre, consolidación y notificación. La oferta permite a los usuarios suministrar resultados financieros, crear informes financieros y de gestión, y proporciona una visión empresarial de métricas y ratios de tipo financiero.

IBM Cognos Controller User on Cloud puede consolidar y administrar el sistema, así como realizar notificaciones relacionadas con el mismo.

1.2 IBM Cognos Controller Jump Start on Cloud

El servicio remoto IBM Cognos Controller Jump Start on Cloud incluye hasta 80 horas de coaching y asistencia, incluyendo la identificación facilitada de un caso de uso inicial de IBM Cognos Controller on Cloud (CCoC), coaching sobre planificación de proyectos e iniciación de la implementación IBM CCoC, coaching sobre prácticas probadas para crear informes de IBM CCoC y coaching sobre mantenimiento y administración de IBM CCoC. El Servicio se adquiere por Compromiso y caduca a los 90 días de su adquisición, independientemente de si se han utilizado todas las horas.

1.3 IBM Cognos Controller Additional Non-Production Instance

Esta oferta añade instancias de No Producción adicionales de IBM Cognos Controller. Solo podrá ser utilizado como parte de las actividades no productivas del Cliente, incluyendo, a título enunciativo y no limitativo, las pruebas, el ajuste de rendimiento, el diagnóstico de errores, benchmarking, desarrollo, actividades de control de calidad o desarrollo de extensiones o ampliaciones de uso interno de la oferta mediante interfaces de programación de aplicaciones publicadas.

2. Descripción de las Medidas de Seguridad

2.1 Políticas de Seguridad

IBM dispone de un equipo de seguridad de la información y también mantiene políticas de privacidad y seguridad, que se comunican 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. 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 alojamiento. Se prohíbe el uso de Wi-Fi dentro de los centros de datos de IBM que dan soporte a este Servicio de Cloud.

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 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 monitorización/ejecución. 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 Servicio de Cloud. El Cliente comprende que el SLA no constituye ninguna garantía.

3.1 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 el Servicio de Cloud.

c. "Reclamación" es una reclamación enviada por el Cliente a IBM respecto a que un SLA no ha sido satisfecho durante un Mes Contratado.

d. "Cliente" es una entidad que se suscribe para el Servicio directamente a través de IBM, que no ha incumplido ninguna obligación esencial y que no haya incumplido ninguna obligación material, incluidas las obligaciones de pago, de este contrato con IBM por el Servicio.

e. "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.

f. "Tiempo de inactividad" es un período de tiempo durante el que el proceso de los sistemas de producción para el Servicio de Cloud se ha detenido y los usuarios del Cliente no pueden utilizar todos los aspectos del Servicio de Cloud para los que tiene permisos. El Tiempo de inactividad no incluye el período de tiempo en que el Servicio de Cloud deja de estar disponible como consecuencia de:

(1) Una parada de mantenimiento planificada o anunciada;

(2) Eventos 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 Servicio de Cloud; 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.

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

h. "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 Evento 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 Evento que ha afectado al uso del Servicio de Cloud. El Cliente debe proporcionar toda la información necesaria acerca del Evento y asistir razonablemente a IBM en el diagnóstico y la resolución del Evento.

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 Evento 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 Servicio de Cloud.

3.3 Niveles de Servicio

Disponibilidad del Servicio de Cloud durante un Mes Contratado

Disponibilidad durante un Mes Contratado	**Crédito de Disponibilidad (% de la Cuota de suscripción mensual para el Mes Contratado objeto de una Reclamación)**
99% – 99,75%	2%
95% – 98,99%	5%
Menos del 95,0%	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: 476 minutos de Tiempo de Inactividad total durante un Mes Contratado

43.200 minutos en total en un Mes Contratado de 30 días - 476 minutos de Tiempo de Inactividad = 42.724 minutos _____ 43.200 minutos en total en un Mes Contratado de 30 días	= 5% de Crédito de Disponibilidad para 98,9% de disponibilidad durante el Mes Contratado

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 Servicio de Cloud del Cliente, ni a ningún servicio beta o de prueba que proporcione IBM. El SLA únicamente se aplica a los Servicios de Cloud 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 Servicios de Cloud se ponen a disposición bajo una de las siguientes métricas de cargo, según se especifica en el Documento de Pedido:

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

b. Usuario Autorizado es una unidad de medida con la que se puede adquirir el Servicio de Cloud. Un Usuario Autorizado es una persona individual que recibe acceso al Servicio de Cloud. El Cliente deberá obtener un derecho de titularidad dedicado independiente para cada Usuario Autorizado que acceda a la oferta de Servicio de Cloud 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 durante el período de medida especificado en el Documento de Pedido. Un derecho de titularidad para un Usuario Autorizado es exclusivo para dicho Usuario Autorizado y no se puede compartir ni se puede volver a asignar salvo en caso de transferencia permanente del derecho de titularidad del Usuario Autorizado a otra persona. Para los fines del Servicio de Cloud, el Cliente puede proporcionar acceso a los usuarios externos de la Empresa del Cliente. Dichos usuarios se considerarán Usuarios Autorizados y tendrán la titularidad correspondiente.

c. 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 Servicio de Cloud. Deben adquirirse derechos de titularidad suficientes para cubrir cada Compromiso.

4.2 Cargos y Facturación

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

4.3 Cargos de Configuración

Los cargos de configuración se especificarán en un Documento de Pedido.

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 Servicio de Cloud está disponible.

4.5 Cargos On Demand

Las opciones On-Demand incluidas en el Documento de Pedido no se facturarán hasta que el Cliente solicite la activación de la pieza On-Demand. Cuando se active, el Cliente recibirá una factura de acuerdo con la tarifa establecida en el Documento de Pedido.

5. Opciones de Vigencia y Renovación

5.1 Vigencia

La vigencia del Servicio de Cloud empezará en la fecha en la que IBM notifique al Cliente que éste tiene acceso al Servicio de Cloud, 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 Servicio de Cloud 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 Servicios de Cloud

El Documento de Pedido del Cliente establecerá si el Servicio de Cloud se renovará al finalizar el plazo, designando el plazo 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 el plazo de expiración del Servicio de Cloud 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 Servicio de Cloud una vez finalizada la vigencia y se le facturará por el uso del Servicio de Cloud de forma continuada. Para dejar de utilizar el Servicio de Cloud 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 Servicio de Cloud 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 Servicio de Cloud se resolverá al final de la vigencia y el acceso del Cliente al Servicio de Cloud se eliminará. Para seguir utilizando el Servicio de Cloud 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

El Soporte Técnico para Servicio de Cloud está disponible durante el Período de Suscripción.

El horario habitual de atención de soporte por teléfono y correo electrónico es el siguiente:

Correo electrónico o ticket de soporte: en cualquier momento, los tickets se procesan conforme a los niveles de severidad asignados. Los niveles de severidad 2 a 4 se gestionarán durante las horas laborables.

Teléfono: de lunes a viernes, 9.00 – 17.00 horas locales (excepto los festivos señalados por IBM).

Soporte fuera del horario laboral:

El Soporte fuera del horario laboral (fuera del horario normal de funcionamiento establecido anteriormente) sólo está disponible para los problemas de Severidad 1 en días laborables, fines de semana y durante las vacaciones.

Línea de Atención Telefónica de Soporte: 1-877-465-5444 en Estados Unidos.

Correo electrónico: vsupport@ca.ibm.com

Para iniciar un ticket por correo electrónico, los clientes deben utilizar la dirección provisional de contacto de Varicent/IBM.

Portal web de soporte: http://support.varicent.com

Consulte el enlace adjunto de la guía de soporte técnico:http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html.

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

7. Conformidad con Safe Harbor

IBM no ha determinado la conformidad de este Servicio de Cloud con los Acuerdos de Safe Harbor de EE.UU. / Suiza.

8. Información Adicional

8.1 Ubicaciones con Ventajas Derivadas

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

8.2 Ausencia de Información Personal relativa a la Salud

El Servicio de Cloud 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.

8.3 Cookies

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

8.4 Recuperación de Desastres y Copia de Seguridad del Contenido

Este Servicio de Cloud también incluye los siguientes servicios de recuperación de desastres y copia de seguridad del contenido:

En el caso de una condición de catástrofe, siendo la definición de catástrofe la de una "Fuerza Mayor" que 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 Servicio de Cloud que esté fuera del control razonable de IBM, IBM intentará restaurar el acceso del Cliente al Servicio de Cloud, como se indica a continuación:

a. Opción estándar: IBM proporcionará el hardware, software y la infraestructura de red en la red del centro de datos de Cloud para permitir que el Cliente reanude el acceso al Servicio de Cloud en un plazo de 14 días.

b. Opción Premium: IBM proporcionará el hardware, software y la infraestructura de red en la red del centro de datos de Cloud para permitir que el Cliente reanude el acceso al Servicio de Cloud en un plazo de 5 días.

El entorno se restaurará utilizando la copia de seguridad del Contenido más reciente, como se describe a continuación, con una pérdida del Contenido del conjunto de datos del Contenido restaurado que no supere las 24 horas.

Las Copias de seguridad se realizan diariamente y se copiarán en una ubicación fuera de las instalaciones en caso de que se produzca un suceso de Fuerza Mayor en la ubicación principal. IBM conserva las copias de seguridad de forma continuada: cada 7 días se realiza una copia de seguridad completa de la BD y cada día posterior dentro de la semana se realiza una copia de seguridad diferencial. IBM retendrá los últimos 7 días de las copias de seguridad diferenciales diarias y las 4 copias de seguridad completas anteriores (lo cual cubrirá un intervalo de 28 días de actividad). A medida que se van creando copias de seguridad completas, las versiones más antiguas se van eliminando. Las copias de seguridad se cifran cuando se encuentran en un sistema de copia de seguridad basado en disco y durante la transmisión a la ubicación fuera de las instalaciones.