

IBM Cognos Controller on Cloud

A seguir está a Descrição do Serviço para o seu Pedido:

1. Serviço em Nuvem

A oferta de Serviço em Nuvem é descrita abaixo e é especificada em um Documento de Transação para as ofertas autorizadas selecionadas. O Documento de Transação consistirá da Cotação e da Prova de Titularidade (PoE), o que confirma a data de início e o termo dos Serviços em Nuvem. A fatura começará após o fornecimento do Serviço em Nuvem.

1.1 IBM Cognos Controller User on Cloud

O IBM Cognos Controller é o software de consolidação financeira que suporta o processo de fechamento, consolidação e relatório. A oferta permite que os usuários entreguem resultados financeiros, criem relatórios financeiros e de gerenciamento e fornece uma visualização corporativa das principais proporções e métricas financeiras.

O IBM Cognos Controller User on Cloud pode consolidar, relatar e administrar o sistema

1.2 IBM Cognos Controller Jump Start on Cloud

O serviço remoto IBM Cognos Controller Jump Start on Cloud inclui até 80 horas de treinamento e assistência, incluindo a identificação facilitada de um caso de uso inicial do IBM Cognos Controller Cloud (CCOC), coaching no planejamento do projeto e iniciação da implementação do IBM CCOC, coaching em práticas comprovadas para a criação de relatórios do IBM CCOC e coaching em manutenção e administração do IBM CCOC são comprados por Engajamento e expiram 90 dias a partir da compra, independente de todas as horas terem ou não sido usadas.

1.3 IBM Cognos Controller Additional Non-Production Instance

Esta oferta inclui instâncias de Não Produção adicionais do IBM Cognos Controller. Ela só pode ser usada como parte das atividades do cliente que não sejam de produção, incluindo, mas não a elas limitada, testes, ajuste de desempenho, diagnóstico de falhas, comparativos, preparação, atividade de controle de qualidade e/ou desenvolvimento de inclusões ou extensões usadas internamente para a oferta usando interfaces de programação do aplicativo publicado.

2. Descrição de Segurança

2.1 Políticas de Segurança

A IBM tem uma equipe de segurança de informações e também mantém políticas de privacidade e segurança que são comunicadas aos funcionários da IBM. A IBM requer treinamento de privacidade e segurança para o pessoal que suporta datacenters IBM. As políticas e as normas de segurança da IBM são revisadas e reavaliadas anualmente. Os incidentes de segurança da IBM são gerenciados de acordo com um procedimento abrangente de resposta a incidente.

2.2 Controle de Acesso

O acesso aos dados de clientes, se necessário, é permitido apenas pelos representantes de suporte IBM, de acordo com os princípios de segregação de funções. A equipe IBM usa autenticação de dois fatores para um host de gerenciamento de "gateway". Todas as conexões são canais criptografados ao acessar dados de cliente. Todo o acesso a dados de cliente e toda a transferência de dados para dentro e para fora do ambiente de hosting são registrados. O uso do WIFI é proibido nos datacenters IBM que suportam este Serviço em Nuvem.

2.3 Integridade e Disponibilidade de Serviço

Modificações nos sistemas operacionais e no software de aplicativo são controladas pelo processo de gerenciamento de mudanças da IBM. Mudanças nas regras do firewall também são controladas pelo processo de gerenciamento de mudanças e são revisadas pela equipe de segurança IBM antes da implementação. A IBM monitora o datacenter 24x7. A varredura de vulnerabilidade interna e externa é conduzida regularmente por administradores autorizados e fornecedores terceiros para ajudar a detectar e resolver exposições potenciais de segurança do sistema. Sistemas de detecção de malware (antivírus, detecção de intrusão, varredura de vulnerabilidade e prevenção de intrusão) são usados em todos os datacenters IBM. Os serviços de datacenter da IBM suportam uma variedade de protocolos de entrega

de informações para a transmissão de dados sobre redes públicas. Exemplos incluem HTTPS/SFTP/FTPS/S/MIME e VPN de site a site. Os dados de backup destinados a armazenamento externo são criptografados antes do transporte.

2.4 Criação de Log de Atividade

A IBM mantém logs de sua atividade para sistemas, aplicativos, repositórios de dados, middleware e dispositivos de infraestrutura de rede aptos e configurados para atividade de criação de log. Para minimizar a possibilidade de violação e para permitir análise central, alerta e relatório, a criação de log de atividade é executada em tempo real para os repositórios de criação de log. Os dados são subscritos para evitar violação. Os logs são analisados em tempo real e através de relatórios de análise periódica para detectar comportamento anormal. A equipe de operações é alertada sobre as anomalias e entra em contato com um especialista em segurança on-call 24x7, quando necessário.

2.5 Segurança Física

A IBM mantém normas de segurança física projetadas para restringir o acesso físico não autorizado a datacenters IBM. Existem apenas pontos de acesso limitados nos datacenters, que são controlados por autenticação de dois fatores e monitorados por câmeras de segurança. O acesso somente é permitido para a equipe autorizada que possui acesso aprovado. A equipe de operações verifica a aprovação e emite um badge de acesso que concede o acesso necessário. Os funcionários que recebem esse badge devem entregar outros badges de acesso e somente podem possuir o badge de acesso do datacenter durante o período de sua atividade. O uso de badges é registrado. Os visitantes que não sejam da IBM são registrados ao entrar nas instalações e são acompanhados durante a permanência nas instalações. Áreas de entrega, docas de carregamento e outros pontos em que pessoas desautorizadas possam entrar nas instalações são controlados e isolados.

2.6 Conformidade

A IBM certifica suas práticas de privacidade anualmente como consistente com o U.S. Department of Commerce's Safe Harbor Principles (Princípios de Porto Seguro do Departamento de Comércio dos EUA): Aviso, Escolha, Transferência Progressiva, Acesso e Exatidão, Segurança e Supervisão/Aplicação. A IBM executa auditorias SSAE 16 padrão de indústria (ou seu equivalente) anualmente nos datacenters de produção. A IBM revisa atividades relacionadas a segurança e privacidade para o cumprimento dos requisitos de negócios da IBM. Avaliações e auditorias são realizadas regularmente pela IBM para confirmar a conformidade com suas políticas de segurança de informações. Um treinamento da força de trabalho sobre educação e conscientização de segurança é feito pelos funcionários da IBM e por funcionários de fornecedores anualmente. A equipe é lembrada de seus objetivos de cargo e de sua responsabilidade de atender à conduta ética de negócios, confidencialidade, e às obrigações de segurança da IBM anualmente.

3. Compromisso de Nível de Serviço

A IBM fornece o acordo de nível de serviço ("SLA") de disponibilidade a seguir para o Serviço em Nuvem. O Cliente entende que o SLA não constitui uma garantia.

3.1 Definições

- a. "Contato Autorizado" significa o(s) indivíduo(s) que o Cliente especificou para a IBM que está(ão) autorizado(S) a submeter Reivindicações sob este SLA.
- b. "Crédito de Disponibilidade" significa a solução que a IBM fornecerá para uma Reivindicação validada. O Crédito de Disponibilidade será aplicado no formato de um crédito ou desconto com relação a uma futura fatura de encargos de subscrição do Serviço em Nuvem.
- c. "Reivindicação" significa uma reclamação que o Cliente envia para a IBM conforme o SLA de que um Nível de Serviço não foi atendido durante um Mês Contratado.
- d. "Cliente" significa uma entidade assinando o Serviço diretamente da IBM, e a qual não tem quaisquer obrigações materiais, incluindo obrigações de pagamento, de acordo com seu contrato com a IBM para o Serviço.
- e. "Mês Contratado" significa cada mês completo durante o prazo medido das 12h - horário padrão do leste dos EUA - no primeiro dia do mês até às 23h59 - horário padrão do leste dos EUA - no último dia do mês.

- f. "Tempo de inatividade" significa um período de tempo durante o qual o processamento do sistema de produção para o Serviço em Nuvem foi interrompido e seus usuários não podem usar todos os aspectos do Serviço em Nuvem para o qual eles têm permissões. Tempo de inatividade não inclui o período de tempo quando o Serviço em Nuvem não está disponível devido a:
- (1) uma indisponibilidade de manutenção planejada ou anunciada;
 - (2) Eventos ou causas além do controle da IBM (por exemplo, desastre natural, indisponibilidades da internet, manutenção de emergência, etc.);
 - (3) problemas com os aplicativos do Cliente, equipamento ou dados, ou aplicativos, equipamento ou dados de um terceiro;
 - (4) falha do Cliente em aderir às configurações requeridas do sistema e às plataformas suportadas para acessar o Serviço em Nuvem; ou
 - (5) A conformidade da IBM com qualquer designs, especificações ou instruções que o Cliente fornece à IBM ou que um terceiro fornece à IBM em nome do cliente.
- g. "Evento" significa uma circunstância ou conjunto de circunstâncias reunidas, que resultam em uma falha em atingir o Nível de Serviço.
- h. "Nível de Serviço" significa o padrão apresentado abaixo pelo qual a IBM mede o nível de serviço que ela fornece neste SLA.

3.2 Créditos de Disponibilidade

- a. Para submeter uma Reivindicação, o Cliente deve registrar um chamado de suporte de Gravidade 1 (conforme definido abaixo na seção Suporte Técnico) para cada Evento com o help desk de suporte técnico IBM, dentro de 24 horas da primeira vez que o Cliente tomou conhecimento que o Evento causou impacto em seu uso do Serviço em Nuvem. O Cliente deve fornecer todas as informações necessárias sobre o Evento e razoavelmente ajudar a IBM com o diagnóstico e a resolução do Evento.
- b. O Cliente deve submeter sua Reivindicação de um Crédito de Disponibilidade não mais do que três (3) dia úteis após o término do Mês Contratado no qual a Reivindicação surgiu.
- c. Os Créditos de Disponibilidade são baseados na duração do Tempo de Inatividade medido a partir do momento que o Cliente relata que foi impactado pela primeira vez pelo Tempo de Inatividade. Para cada Reivindicação válida, a IBM irá aplicar o Crédito de Disponibilidade mais alto aplicável com base no Nível de Serviço atingido durante cada Mês Contratado, conforme mostrado na tabela abaixo. A IBM não será responsabilizada por diversos Créditos de Disponibilidade para o mesmo Evento no mesmo Mês Contratado.
- d. Os Créditos de Disponibilidade totais concedidos com relação a qualquer Mês Contratado não deverão, sob nenhuma circunstância, exceder a 10 por cento (10%) de um doze avos (1/12) do encargo anual pago pelo Cliente para IBM para o Serviço em Nuvem.

3.3 Níveis de Serviço

Disponibilidade do Serviço em Nuvem durante um Mês Contratado

Disponibilidade durante um Mês Contratado	Crédito de Disponibilidade (% do Encargo de Subscrição Mensal para o Mês Contratado que é objeto de uma Reivindicação)
99% – 99,75%	2%
95% – 98,99%	5%
Menor que 95.0%	10%

A disponibilidade, expressa como uma porcentagem é calculada como: (a) o número total de minutos em um Mês Contratado menos (b) o número total de minutos de Tempo de Inatividade em um Mês Contratado, dividido pelo (c) número total de minutos em um Mês Contratado.

Exemplo: 476 minutos totais de Tempo de Inatividade durante o Mês Contratado

Total de 43.200 minutos em um Mês Contratado de 30 dias - 476 minutos de Tempo de Inatividade = 42.724 minutos	= 5% de Crédito de Disponibilidade para 98,9% de Disponibilidade durante o Mês Contratado
Total de 43.200 minutos em um Mês Contratado de 30 dias	

3.4 Outras informações sobre este SLA

Este SLA é disponibilizado apenas para clientes da IBM e não se aplica a reivindicações feitas por seus usuários, convidados, participantes e guests permitidos do Serviço em Nuvem ou para quaisquer serviços beta ou de avaliação que a IBM fornece. O SLA somente se aplica aos Serviços em Nuvem que estão no uso da produção. Ele não se aplica a ambientes de não produção, incluindo, mas não se limitando a, de testes, recuperação de desastre, garantia de qualidade ou desenvolvimento.

4. Informações de Autorização e Faturamento

4.1 Métricas de Encargos

Os Serviços em Nuvem são disponibilizados sob uma das métricas de encargos a seguir, conforme especificado no Documento de Transação:

- a. c. "Instância" é uma unidade de medida pela qual o IBM SaaS pode ser obtido. Uma Instância é o acesso a uma configuração específica do IBM SaaS. Devem ser obtidas autorizações suficientes para cada Instância do Serviço em Nuvem disponibilizadas para acesso e uso durante o período de medida especificado no Documento de Transação.
- b. Usuário Autorizado é uma unidade de medida pela qual o Serviço em Nuvem pode ser obtido. Um Usuário Autorizado é uma pessoa exclusiva a quem é concedido acesso ao Serviço em Nuvem. O Cliente deve obter autorizações separadas dedicadas para cada Usuário Autorizado que acessa a oferta de Serviço em Nuvem de qualquer maneira direta ou indiretamente (por exemplo: por meio de um programa de multiplexação, dispositivo ou servidor de aplicativos) por qualquer meio durante o período de medida especificado no Documento de Transação. Uma autorização para um Usuário Autorizado é exclusiva para esse Usuário Autorizado e não pode ser compartilhada ou redesignada a não ser por transferência permanente da autorização do Usuário Autorizado para outra pessoa. Para os fins do Serviço na Nuvem, é possível fornecer acesso aos usuários que estejam fora de sua Empresa. Tais usuários devem ser considerados como Usuários do Autorizados e devem ser autorizados apropriadamente.
- c. Consultoria é uma unidade de medida pela qual os serviços podem ser obtidos. Um Compromisso consiste em serviços profissionais e/ou de treinamento relacionados ao Serviço em Nuvem. Devem ser obtidas autorizações suficientes para cobrir cada Compromisso.

4.2 Encargos e Faturamento

A quantia a pagar pelo Serviço em Nuvem é especificada em um Documento de Transação.

4.3 Encargos de Configuração

Encargos de configuração serão especificados em um Documento de Transação.

4.4 Encargos Mensais Parciais

O encargo mensal parcial é um encargo mensal rateado. Os encargos mensais parciais são calculados com base nos dias restantes do mês parcial iniciando na data em que o Cliente é notificado pela IBM que o seu acesso à oferta de Serviço em Nuvem está disponível.

4.5 Encargos On Demand

Opções On-Demand incluídas no Documento de Transação não serão faturadas até que o cliente solicite a ativação da parte On-Demand. Quando ativado, o Cliente será faturado de acordo com o encargo definido no Documento de Transação.

5. Opções de Vigência e Renovação

5.1 Prazo

A vigência do Serviço em Nuvem inicia na data em que a IBM notifica o Cliente que ele tem acesso ao Serviço em Nuvem, conforme descrito no Documento de Transação. A parte de PoE do Documento de Transação confirmará a data exata do início e término da vigência. O Cliente tem permissão de aumentar seu nível de uso do Serviço em Nuvem durante o prazo ao entrar em contato com a IBM ou seu Parceiro de Negócios IBM. A IBM confirmará o nível aumentado de uso no Documento de Transação.

5.2 Opções de Renovação da Vigência dos Serviços em Nuvem

O Documento de Transação do Cliente indicará se o Serviço em Nuvem será renovado no final da vigência, designando a vigência como um dos seguintes:

5.2.1 Renovação Automática

Caso o Documento de Transação indique que a renovação é automática, o Cliente poderá rescindir a vigência do Serviço em Nuvem a ser expirado por solicitação escrita, pelo menos noventa (90) dias antes da data de expiração do prazo apresentada no Documento de Transação. Se a IBM ou seu Parceiro de Negócios IBM não receber tal aviso de rescisão até a data de expiração, a vigência de expiração será automaticamente renovada pelo prazo de um ano ou pela mesma duração que a vigência original, conforme definido no PoE.

5.2.2 Faturamento Contínuo

Quando o Documento de Transação declarar que seu faturamento é contínuo, o cliente continuará tendo acesso ao Serviço em Nuvem após o término da vigência e será faturado pelo uso do Serviço em Nuvem em uma base contínua. Para descontinuar o uso do Serviço em Nuvem e parar o processo de faturamento contínuo, o Cliente deve fornecer à IBM ou seu Parceiro de Negócios IBM um aviso por escrito com noventa (90) dias de antecedência, solicitando que seu Serviço em Nuvem seja cancelado. Mediante o cancelamento do acesso do Cliente, ele será faturado por quaisquer encargos de acesso pendentes até o mês em que o cancelamento entrou em vigor.

5.2.3 Renovação Obrigatória

Quando o Documento de Transação indica que o seu tipo de renovação é "rescindir", o Serviço em Nuvem será rescindido no término da vigência e seu acesso ao Serviço em Nuvem será removido. Para continuar a usar o Serviço em Nuvem além da data de encerramento, o cliente deve fazer o pedido com seu representante de vendas IBM ou Parceiro de Negócios IBM para adquirir um novo período de subscrição.

6. Suporte Técnico

O suporte técnico para o Serviço em Nuvem fica disponível durante o período de subscrição.

Horas de Operação de Suporte por Telefone e E-mail Regular são como a seguir:

Chamado de Suporte ou Email: A qualquer momento, chamados são processados de acordo com os níveis de gravidade designados. Os níveis de gravidade entre 2 e 4 serão manipulados durante o horário comercial.

Telefone: Segunda a sexta-feira, 9h – 17h no horário local (excluindo feriados reconhecidos pela IBM).

Suporte após o Horário de Expediente:

Suporte após o Horário de Expediente (fora das horas operacionais regulares declaradas acima) está disponível para problemas de Gravidade 1 em dias úteis, fins de semana e feriados.

Linha Direta de Suporte: 1-877-465-5444.

Email: vsupport@ca.ibm.com

Para criação de log de um chamado via email, os clientes devem usar o endereço temporário da Varicent/IBM.

Portal da web de suporte: <http://support.varicent.com>

Veja o link em anexo para obter o guia de suporte técnico: <http://www-1.ibm.com/software/analytics/varicent/customercenter/saas.html>.

Gravidade	Definição de Gravidade	Objetivos de Tempo de Resposta	Cobertura do Tempo de Resposta
1	Impacto crítico nos negócios/inatividade do serviço incluem: Funcionalidades críticas para os negócios ficam inoperáveis ou ocorre falha na interface crítica. Geralmente, se aplica a um ambiente de produção e indica uma incapacidade de acessar serviços que resulta em um impacto crítico nas operações. Essa condição requer uma solução imediata.	Dentro de 1 hora	24x7
2	Impacto de negócios significativo: O uso de um recurso de negócios de serviço ou de uma função do serviço fica gravemente restringido ou o Cliente corre o risco de perder prazos finais de negócios.	Dentro de 2 horas em horário comercial	Horário comercial de segunda a sexta-feira
3	Impacto de negócios menor: Indica que o serviço ou a funcionalidade está utilizável e não há um impacto crítico nas operações.	Dentro de 4 horas em horário comercial	Horário comercial de segunda a sexta-feira
4	Impacto de negócios mínimo: Uma solicitação de consulta ou não técnica	Dentro de 1 hora em horário comercial	Horário comercial de segunda a sexta-feira

7. Conformidade com o Safe Harbor

A IBM não determinou a conformidade deste Serviço em Nuvem com o US-EU and US-Swiss Safe Harbor Frameworks.

8. Informações Adicionais

8.1 Locais de Benefícios Derivados

Onde aplicável, os tributos são baseados no(s) local(is) que o Cliente identifica como os que recebem os benefícios dos Serviços em Nuvem. A IBM aplicará tributos com base no endereço de negócios listado ao solicitar um Serviço em Nuvem como o local de benefício primário, a menos que o Cliente forneça informações adicionais à IBM. O Cliente é responsável por manter tais informações atualizadas e por fornecer quaisquer mudanças à IBM.

8.2 Sem Informações de Saúde Pessoal

O Serviço em Nuvem não foi projetado para conformidade com o HIPAA e não pode ser usado para a transmissão ou armazenamento de quaisquer Informações de Saúde Pessoal.

8.3 Cookies

O cliente está ciente e concorda que a IBM pode, como parte da operação e suporte normais do Serviço em Nuvem, coletar suas informações pessoais (seus funcionários e fornecedores) relacionadas ao uso do Serviço em Nuvem, por meio de rastreamento e de outras tecnologias. A IBM faz isso para reunir estatísticas e informações de uso sobre a efetividade de nosso Serviço em Nuvem para o propósito de melhorar a experiência do usuário e/ou customizar interações com o cliente. O Cliente confirma que obterá ou obteve consentimento para permitir que a IBM processe as informações pessoais coletadas para o propósito acima na IBM, outras empresas IBM e suas subcontratadas, onde quer que a IBM ou seus subcontratados façam negócios, em conformidade com a lei aplicável. A IBM irá cumprir com as solicitações dos funcionários e contratados do Cliente para acessar, atualizar, corrigir ou excluir suas informações pessoais coletadas.

8.4 Recuperação de Desastre e Backup de Conteúdo

Este Serviço em Nuvem também inclui os seguintes serviços de recuperação de desastre e backup de conteúdo:

Caso ocorra uma condição catastrófica, catastrófico é definido como "Força Maior", o que significa atos de Deus, terrorismo, ação trabalhista, incêndio, enchente, terremoto, motim, guerra, atos governamentais, ordens ou restrições, vírus, ataques de recusa de serviço e outras condutas mal-intencionadas, falhas dos serviços públicos e de conectividade de rede ou qualquer outra causa de indisponibilidade do Serviço em Nuvem que esteja fora do controle razoável da IBM, a IBM irá trabalhar para restaurar o acesso do Cliente ao Serviço em Nuvem conforme a seguir:

- a. Opção Padrão – a IBM deve fornecer a infraestrutura de hardware, software e rede na rede do datacenter da IBM que ativará o Cliente para continuar o acesso ao IBM SaaS dentro de 14 dias.
- b. Opção Premium – a IBM deve fornecer a infraestrutura de hardware, software e rede na rede do datacenter da IBM que ativará o Cliente para continuar o acesso ao IBM SaaS dentro de 5 dias.

O ambiente será restaurado usando o backup de Conteúdo mais recente, conforme descrito abaixo, com menos de 24 horas de perda de Conteúdo do conjunto de dados de Conteúdo restaurado.

Os backups são efetuados diariamente e copiados para um local externo no evento de um evento Força Maior na localização primária. A IBM mantém backups, em uma base contínua: a cada 7 dias, um backup de banco de dados completo é feito e a cada dia subsequente dentro de uma semana, é feito um backup diferencial comparativo. A IBM reterá os últimos 7 dias de backups diferenciados diários e os 4 backups completos anteriores (cobrindo um período de 28 dias de atividade). Conforme um novo backup completo é criado, a versão mais antiga é descartada. Os backups são criptografados at rest em um sistema de backup baseado em disco e durante a transmissão para o local externo.