IBM Security Verify

Esta Descripción del Servicio describe el Servicio de Cloud. Los documentos de pedidos aplicables proporcionan precios y detalles adicionales sobre el pedido del Cliente.

1. Servicio de Cloud

IBM Cloud Identity proporciona un inicio de sesión único (SSO), autenticación de multifactores y controles del ciclo de vida de las identidades para los tipos de usuario internos (empleados) y externos.

1.1 Ofertas

El Cliente puede seleccionar entre las siguientes ofertas disponibles.

1.1.1 IBM Security Verify

IBM Security Verify ayuda a los Clientes a proteger la productividad del usuario con suministros en cloud, inicio de sesión único, autenticación de multifactores, gestión de ciclo de vida, autenticación adaptativa, análisis de identidad y gobierno de identidades en un único número de pieza. Este Servicio de Cloud también da soporte a miles de conectores integrados previamente para facilitar el suministro; acceso a conocidas aplicaciones de servicio de cloud y plantillas integradas previamente para ayudar a integrar aplicaciones internas.

- Inicio de sesión único

  Este Servicio de Cloud proporciona un inicio de sesión único (SSO) y Open ID Connect (OIDC), Autenticación como Servicio para la autorización de APIs basadas en cloud, un launchpad de aplicaciones, informes de administrador y un dashboard de analíticas. Este Servicio de Cloud conecta los usuarios a las aplicaciones utilizando una autenticación basada en estándares modernos y protocolos de federación, incluidos cientos de conectores a aplicaciones comunes. Este Servicio de Cloud se integra perfectamente con el programa de software IBM Security Access software y con el programa de software IBM Security Verify Application Gateway, que se incluye como software de habilitación, para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud.

- Autenticación de multifactores

  Este Servicio de Cloud proporciona autenticación de multifactores para las aplicaciones protegidas por Cloud Identity Connect, o mediante la invocación de API directa, y para otros puntos de aplicación, incluidos los clientes RADIUS, los servidores PAM de Unix/Linux y los servidores de Windows, para verificar sus identidades cuando acceden a un servicio digital. Esto incluye mecanismos como, por ejemplo, el correo electrónico, SMS y contraseñas puntuales (software de software) con caducidad, así como la autenticación biométrica móvil basada en IBM Verify con notificaciones push. Este Servicio de Cloud se integra con el programa de software IBM Security Verify Access local para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud.

- Acceso adaptativo

  Este Servicio de Cloud utiliza una combinación de Inteligencia frente a amenazas e Inteligencia Artificial (AI) para ayudar a las organizaciones a diferenciar de forma precisa entre usuarios auténticos y maliciosos, cuando un usuario intenta acceder a una aplicación protegida por el servicio. El servicio consume perspectivas sobre los usuarios, sus dispositivos y patrones de comportamiento para determinar en tiempo real una acción de reducción del riesgo: permitir acceso, obligar a realizar la autenticación o bloquear el acceso. El servicio utiliza cientos de puntos de datos e información contextual recopilada del dispositivo del usuario final para tomar impresiones dactilares del dispositivo y calcular el nivel de riesgo global de la sesión. Las reglas de acceso basadas en riesgo definidas en la política de acceso utilizan el nivel de riesgo de la sesión con parámetros adicionales para determinar la acción del sistema. Este servicio está estrechamente relacionado con los informes de administrador de Security Verify, el editor de reglas de políticas de acceso y el servicio de autenticación de multifactores.

- Lifecycle Management and Governance

  Este Servicio de Cloud se integra perfectamente con el programa de software IBM Security Identity Governance and Intelligence (IGI) y con el programa de software IBM Security Identity Manager (ISIM), que se incluye como software de habilitación, para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para el gobierno de identidades tanto en sus aplicaciones locales como en entornos cloud. Este Servicio de Cloud proporciona a las empresas prestaciones avanzadas de gestión del ciclo de vida de identidades dentro de cloud e incluye la sincronización de cuentas, un flujo de trabajo de solicitud de acceso, la certificación de acceso y el suministro de aplicaciones de cloud y local. Los Clientes pueden incluir IBM Security Verify Account Synchronization como servicio complementario.

- Analítica

  Este Servicio de Cloud complementa las soluciones existentes de IBM, como IBM Security Identity Governance and Intelligence (IGI) e IBM Security Identity Manager (ISIM), para proporcionar un perfil de riesgo holístico de los usuarios gestionados. Este Servicio de Cloud incluye un motor de análisis multipropósito local que procesa datos de actividad y derechos de titularidad de una variedad de orígenes, lo cual proporciona una vista integral de los riesgos de acceso con capacidad de tomar medidas en base a estas perspectivas de riesgo.

1.1.2 IBM Cloud Identity Connect

Este Servicio de Cloud proporciona un inicio de sesión único (SSO) y Open ID Connect (OIDC), Autenticación como Servicio para la autorización de APIs basadas en cloud, un launchpad de aplicaciones, informes de administrador y un dashboard de analíticas. Este Servicio de Cloud conecta los usuarios a las aplicaciones utilizando una autenticación basada en estándares modernos y protocolos de federación, incluidos cientos de conectores a aplicaciones comunes. Este Servicio de Cloud se integra perfectamente con el programa de software IBM Security Access Management (ISAM) local, que se incluye como software de habilitación, para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud.

1.1.3 IBM Cloud Identity Connect for ISAM

Este Servicio de Cloud se integra perfectamente con el programa de software IBM Security Access Management (ISAM) local para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud. Este Servicio de Cloud requiere que el Cliente tenga un derecho de titularidad de Suscripción y Soporte de Software (S&S) para el programa IBM Security Access Management (ISAM), y el S&S debe permanecer activo durante el plazo de la suscripción del Servicio de Cloud del Cliente. El derecho de titularidad del Cliente para este Servicio de Cloud debe ser equivalente al derecho de titularidad de licencia ISAM local del Cliente. La interrupción del servicio de S&S del Cliente también interrumpirá este Servicio de Cloud. El acceso al software de habilitación definido en el apartado 5.2 no se incluye con este Servicio de Cloud.

1.1.4 IBM Cloud Identity Essentials

Este Servicio de Cloud proporciona a los Clientes prestaciones de Inicio de Sesión Único (SSO) para las distintas aplicaciones de IBM y de cloud público que utilizan. Este Servicio de Cloud puede combinarse con MaaS360 de IBM para proporcionar niveles adicionales de controles de seguridad, como el acceso condicional.

1.1.5 IBM Cloud Identity Verify

Este Servicio de Cloud proporciona autenticación de multifactores para las aplicaciones protegidas por Cloud Identity Connect, o mediante la invocación de API directa, y para otros puntos de aplicación, incluidos los clientes RADIUS, los servidores PAM de Unix/Linux y los servidores de Windows, para verificar sus identidades cuando acceden a un servicio digital. Esto incluye mecanismos como, por ejemplo, el correo electrónico, SMS y contraseñas puntuales (software de software) con caducidad, así como la autenticación biométrica móvil basada en IBM Verify con notificaciones push. Este Servicio de Cloud se integra con el programa de software IBM Security Access Management (ISAM) local para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud. Está disponible de manera

autónoma o para complementar Cloud Identity Connect, Cloud Identity Connect for ISAM y Cloud Identity Essentials.

1.1.6 IBM Cloud Identity Govern

Este Servicio de Cloud se integra perfectamente con el programa de software IBM Security Identity Governance and Intelligence (IGI) y con el programa de software IBM Security Identity Manager (ISIM), que se incluye como software de habilitación, para proporcionar una solución para que los Clientes soporten sus demandas de línea de negocio para la gestión de acceso tanto en sus aplicaciones locales como en entornos cloud. Este Servicio de Cloud proporciona a las empresas prestaciones avanzadas de gestión del ciclo de vida de identidades dentro de cloud e incluye un flujo de trabajo de solicitud de acceso.

1.1.7 IBM Cloud Identity Connect and Verify

Este Servicio de Cloud proporciona al Cliente la funcionalidad de IBM Cloud Identity Connect e IBM Cloud Identity Verify como una sola oferta.

1.1.8 IBM Cloud Identity Analyze

Este Servicio de Cloud complementa las soluciones existentes de IBM, como IBM Security Identity Governance and Intelligence (IGI) e IBM Security Identity Manager (ISIM), para proporcionar un perfil de riesgo holístico de los usuarios gestionados. Este Servicio de Cloud incluye un motor de análisis multipropósito local que procesa datos de actividad y derechos de titularidad de una variedad de orígenes, lo cual proporciona una vista integral de los riesgos de acceso con capacidad de tomar medidas en base a estas perspectivas de riesgo.

1.1.9 IBM Cloud Identity Adaptive Access

Este Servicio de Cloud utiliza perspectivas contextuales basadas en Inteligencia Artificial (IA) sobre los usuarios, sus dispositivos y patrones de comportamiento, para ayudar a las organizaciones a aplicar las políticas de autenticación correctas.

1.1.10 IBM Cloud Identity Connect Verify and Govern

Este Servicio de Cloud proporciona al Cliente la funcionalidad de IBM Cloud Identity Connect, IBM Cloud Identity Verify e IBM Cloud Identity Govern como una sola oferta.

1.2 Servicios Opcionales

1.2.1 IBM Security Verify Non-Production

IBM Security Verify Non-Production Environment on Cloud es una instancia independiente de la plataforma IBM Security Verify que el Cliente sólo podrá utilizar para actividades internas no productivas 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 Servicio de Cloud mediante interfaces de programación de aplicaciones publicadas. Este Servicio de Cloud tiene la opción de incluir un acuerdo de nivel de servicio de disponibilidad (SLA), sujeto a los términos del apartado 3, Niveles de Servicio y Soporte Técnico. Este Servicio de Cloud tiene una capacidad de 100 Eventos por segundo.

1.2.2 IBM Security Verify Vanity Domain

Un dominio Vanity (un dominio) permite que el Cliente use un dominio de su propiedad, y más relevante para su organización, en lugar de usar el dominio de tenant predeterminado que proporciona directamente la plataforma. IBM mantendrá un certificado SSL para este dominio, que se renovará anualmente.

1.2.3 IBM Security Verify Application Gateway Hosted

La puerta de enlace de aplicaciones proporciona un dispositivo ligero gestionado y alojado por IBM para los Clientes que buscan soporte para mecanismos de autenticación no estándar o heredados. Estos mecanismos incluyen autenticación basada en encabezados LTPA y HTTP. El mantenimiento y la monitorización continuados los gestiona IBM.

1.2.4 IBM Security Verify SMS and Email One-time Password

Este servicio proporciona contraseñas únicas entregadas por correo electrónico o SMS, como mecanismo de autenticación de segundo factor.

1.2.5 IBM Security Verify Account Synchronization

La Sincronización de cuentas es el proceso a través del cual las cuentas de las aplicaciones de destino configuradas para el suministro se obtienen y se introducen en Security Verify. El proceso valida la información de la cuenta existente y aplica las políticas de adopción y corrección para mantener la coherencia entre el sistema y la aplicación de destino.

1.2.6 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud s una instancia independiente de la plataforma IBM Cloud Identity que el Cliente sólo podrá utilizar para actividades internas no productivas 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 Servicio de Cloud mediante interfaces de programación de aplicaciones publicadas. Este Servicio de Cloud tiene la opción de incluir un acuerdo de nivel de servicio de disponibilidad (SLA), sujeto a los términos del apartado 3, Niveles de Servicio y Soporte Técnico. Este Servicio de Cloud tiene una capacidad de 100 Eventos por segundo.

1.2.7 IBM Cloud Identity Vanity Domain

Un dominio Vanity (un dominio) permite que el Cliente use un dominio de su propiedad, y más relevante para su organización, en lugar de usar el dominio de tenant predeterminado que proporciona directamente la plataforma. IBM mantendrá un certificado SSL para este dominio, que se renovará anualmente.

1.2.8 IBM Cloud Identity Application Gateway Hosted

La puerta de enlace de aplicaciones proporciona un dispositivo ligero gestionado y alojado por IBM para los Clientes que buscan soporte para mecanismos de autenticación no estándar o heredados. Estos mecanismos incluyen autenticación basada en encabezados LTPA y HTTP. El mantenimiento y la monitorización continuados los gestiona IBM.

1.3 Servicios de Aceleración

1.3.1 IBM Security Verify Solution Planning

Este servicio ofrece una (1) semana de servicios profesionales durante los cuales IBM realizará algunos o todos los puntos siguientes:

- Establecer un inicio de sesión único para aplicaciones SaaS basadas en cloud
- Configurar una plataforma de lanzamiento para facilitar la ubicación de la aplicación
- Conectar aplicaciones con conectores listos para usar
- Planificación, arquitectura y orientación de soluciones
- Enfoque y prácticas recomendadas por IBM

1.3.2 IBM Security Verify Workshop for Multi-Factor Authentication

Este servicio ofrece un taller de servicios profesionales de tres (3) días, centrado en los desafíos de autenticación de múltiples factores y en la protección de las aplicaciones de un Cliente mediante IBM Cloud Identify Verify. El taller cubrirá algunos o todos los aspectos siguientes:

- Integrar la autenticación familiar en todas las interacciones digitales y personales en las que se requiere autenticación.
- Habilitar una aplicación para reforzar la autenticación sólida utilizando un API REST compatible con el desarrollador
- Proporcionar recomendaciones de mejores prácticas del sector sobre la seguridad de la identidad
- Experiencia de usuario optimizada y adopción en todos los factores de forma: teléfonos, tabletas y portátiles

1.3.3 IBM Security Verify Strategy and Planning

Este servicio proporciona un taller de servicios profesionales de tres (3) semanas sobre cómo aplicar las mejores prácticas de seguridad en cloud, con un enfoque en la seguridad de la infraestructura y las aplicaciones. El taller cubrirá algunos o todos los aspectos siguientes:

- Establecer un inicio de sesión único para aplicaciones SaaS basadas en cloud
- Configurar una plataforma de lanzamiento para facilitar la ubicación de la aplicación
- Conectar aplicaciones con conectores listos para usar
- Planificación, arquitectura y orientación de soluciones
- Información sobre las nuevas tendencias en materia de ciberseguridad
- Enfoque y prácticas recomendadas por IBM

1.3.4 IBM Security Verify Expert On Demand

Este servicio proporciona veinte (20) horas de servicios profesionales, entregados en dos (2) sesiones de una hora dentro de los treinta (30) días del inicio. Los servicios proporcionarán un arquitecto de IBM Security Verify para responder preguntas y proporcionar orientación y recomendaciones, pero no limitado a:

- Conocimientos técnicos para aumentar la implementación de una solución de Cliente
- Preguntas sobre arquitectura e implementación en la solución de un Cliente
- Orientación sobre la solución y/o estrategia de un Cliente

1.3.5 IBM Cloud Identity Connect Solution Planning

Este servicio ofrece una (1) semana de servicios profesionales durante los cuales IBM realizará algunos o todos los puntos siguientes:

- Establecer un inicio de sesión único para aplicaciones SaaS basadas en cloud
- Configurar una plataforma de lanzamiento para facilitar la ubicación de la aplicación
- Conectar aplicaciones con conectores listos para usar
- Planificación, arquitectura y orientación de soluciones
- Enfoque y prácticas recomendadas por IBM

1.3.6 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Este servicio ofrece un taller de servicios profesionales de tres (3) días, centrado en los desafíos de autenticación de múltiples factores y en la protección de las aplicaciones de un Cliente mediante IBM Cloud Identify Verify. El taller cubrirá algunos o todos los aspectos siguientes:

- Integrar la autenticación familiar en todas las interacciones digitales y personales en las que se requiere autenticación.
- Habilitar una aplicación para reforzar la autenticación sólida utilizando un API REST compatible con el desarrollador
- Proporcionar recomendaciones de mejores prácticas del sector sobre la seguridad de la identidad
- Experiencia de usuario optimizada y adopción en todos los factores de forma: teléfonos, tabletas y portátiles

1.3.7 IBM Cloud Security Strategy and Planning

Este servicio proporciona un taller de servicios profesionales de tres (3) semanas sobre cómo aplicar las mejores prácticas de seguridad en cloud, con un enfoque en la seguridad de la infraestructura y las aplicaciones. El taller cubrirá algunos o todos los aspectos siguientes:

- Establecer un inicio de sesión único para aplicaciones SaaS basadas en cloud
- Configurar una plataforma de lanzamiento para facilitar la ubicación de la aplicación
- Conectar aplicaciones con conectores listos para usar
- Planificación, arquitectura y orientación de soluciones
- Información sobre las nuevas tendencias en materia de ciberseguridad
- Enfoque y prácticas recomendadas por IBM

1.3.8 IBM Cloud Identity Expert On Demand

Este servicio proporciona veinte (20) horas de servicios profesionales, entregados en dos (2) sesiones de una hora dentro de los treinta (30) días del inicio. Los servicios proporcionarán un arquitecto de Identidad en Cloud para responder preguntas y proporcionar orientación y recomendaciones, pero no limitado a:

- Conocimientos técnicos para aumentar la implementación de una solución de Identidad en el Cloud de un Cliente
- Preguntas sobre arquitectura e implementación en la solución de identidad en el Cloud de un Cliente
- Orientación sobre la solución y/o estrategia de Identidad en el Cloud de un Cliente

2. Fichas de Características de Protección y Tratamiento de Datos

El Anexo de Tratamiento de Datos (DPA) de IBM, en http://ibm.com/dpa, y las Fichas de Características de Protección y Tratamiento de Datos (referidas como fichas de datos o Suplementos del DPA) en los enlaces siguientes proporcionan información adicional de protección de datos para los Servicios de Cloud y sus opciones sobre los tipos de Contenido que pueden tratarse, las actividades de tratamiento involucradas, las características de protección de datos y detalles específicos sobre la retención y la devolución de Contenido. El DPA se aplica a los datos personales contenidos en el Contenido, siempre y cuando: i) se cumpla el Reglamento General de Protección de Datos de la Unión Europea (EU/2016/679) (GDPR); o ii) se aplique otra legislación sobre protección de datos identificada en http://ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

3. Nivel de Servicio y Soporte Técnico

3.1 Acuerdo de Nivel de Servicio (SLA)

IBM proporciona al Cliente el siguiente acuerdo de nivel de servicio (SLA) de disponibilidad. IBM aplicará la compensación aplicable más alta en función de la disponibilidad acumulativa del Servicio de Cloud, como se muestra en la tabla siguiente. El porcentaje de disponibilidad se calcula como el número total de minutos en un mes contratado, menos el número total de minutos de Inactividad del Servicio en un mes contratado, dividido por el número total de minutos en un mes contratado, y es específico para la región afectada y el número de usuarios inscritos en dicha región. La definición de Inactividad del Servicio, el proceso de reclamación y la información acerca de cómo ponerse en contacto con IBM con respecto a los problemas de disponibilidad del servicio se encuentran en la descripción general de soporte de SaaS de IBM, en la dirección https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilidad	Crédito (% de la tarifa de suscripción mensual*)
Menos del 99,9%	10%

* La tarifa de suscripción es el precio contratado para el mes que está sujeto a la reclamación.

3.1.1 Información Adicional acerca de este SLA

Durante los primeros sesenta (60) días de plazo del Cliente ("Período de Adaptación"), el Cliente no tendrá derecho de titularidad sobre ningún crédito debido a una anomalía del entorno del Servicio de Cloud que suponga no alcanzar el mínimo de 99,9% de Porcentaje de Tiempo de Actividad en virtud del presente Contrato. Si antes del Periodo de Adaptación, o durante el mismo, IBM identifica configuraciones, políticas, datos o código existentes del Cliente ("Componentes Preexistentes") destinados a su migración al Servicio de Cloud que pudieran evitar que el Servicio de Cloud consiguiera con éxito el porcentaje de Porcentaje de Tiempo de Actividad dentro de este Contrato, IBM se reserva el derecho de notificar al Cliente la existencia de dichos Componentes Preexistentes y eximirlos a discreción exclusiva de IBM, según lo dispuesto en el SLA. En caso de que IBM notifique al Cliente la existencia de Componentes Preexistentes exentos, IBM será responsable de presentar al Cliente un plan de remediación, en la medida posible, que permita que tales componentes exentos cumplan el Porcentaje de Tiempo de Actividad de este Contrato. El Cliente será el único responsable por el coste de tal remediación a menos que sea acordado de otra manera por ambas partes.

3.2 Soporte Técnico

El Soporte Técnico para el Servicio de Cloud, incluyendo detalles de contacto de soporte, niveles de gravedad, horas de disponibilidad de soporte, tiempos de respuesta y otros procesos e información de soporte, se encuentra seleccionando el Servicio de Cloud en la guía de soporte de IBM disponible en la dirección https://www.ibm.com/support/home/pages/support-guide/.

4. Cargos

4.1 Métricas de Cargo

Las métricas de cargo por el Servicio de Cloud se especifican en el Documento Transaccional.

Se aplican a este Servicio de Cloud las métricas de cargo siguientes:

- Una Instancia es cada acceso a una configuración específica de los Servicios de Cloud.
- Un Compromiso es un servicio profesional o de formación relacionado con los Servicios de Cloud.
- Un Evento es una aparición de evento específico procesado por, o relacionado con el uso de, los Servicios de Cloud.
  - Para Security Verify SMS and One-Time Password, un Evento es una contraseña única enviada por correo electrónico o SMS.
  - Para Cloud Identity Connect, un Evento es una solicitud http en el Servicio de Cloud.
- Para Cloud Identity Verify, un Evento es un método de varios factores que se invoca a través del Servicio de Cloud. Un Usuario Autorizado es un usuario exclusivo a quien se ha concedido acceso a los Servicios de Cloud de forma directa o indirecta (por ejemplo, a través de un programa, dispositivo o servidor de aplicaciones multiplexor) mediante cualquier método.
- Un Empleado es una única persona empleada por, pagada por o que actúa en nombre de la Empresa del Cliente, ya sea que tenga o no acceso a los Servicios de Cloud.
- Un Participante Elegible es un individuo o una entidad elegible para participar en un programa de prestación de servicios gestionados o monitorizados por los Servicios de Cloud.
- Una Unidad de Recurso es una medida independiente de un recurso gestionado por, o relacionado con, el uso del Servicio de Cloud.

  El uso de cada capacidad funcional requiere el número especificado de autorizaciones de Unidad de Recurso para esta suscripción de Servicio de Cloud:

		Capacidad Funcional en Unidades de Recurso ponderadas necesarias por Usuario				
Nivel Graduado	**Máximo de Usuarios Activos Mensuales**	**Inicio de sesión único**	**Autenticación de multifactores**	**Acceso adaptativo**	**Lifecycle Management and Governance**	**Analítica**
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5,000	0,0800	0,0800	0,0800	0,0750	0,1000
3	10.000	0,0600	0,0600	0,0600	0,0500	0,0750
4	100.000	0,0080	0,0080	0,0080	0,0050	0,0200
5	500,000	0,0025	0,0025	0,0025	0,0020	0,0150
6	1.000.000	0,0020	0,0020	0,0020	0,0010	0,0010
7	5.000.000	0,0015	0,0015	0,0015	0,0005	0,0005
8	10.000.000	0,0015	0,0015	0,0015	0,0002	0,0002
9	50.000.000	0,0010	0,0010	0,0010	0,0001	0,0001
10	999.999.999	0,0005	0,0005	0,0005	0,0001	0,0001

Nota: todos los cálculos se redondearán a un número entero.

5. Términos Adicionales

Para los Contratos de Servicio de Cloud (o contratos de cloud base equivalentes) firmados antes del 1 de enero de 2019, se aplican las condiciones disponibles en https://www.ibm.com/acs.

5.1 Referencia del Cliente

El Cliente acepta que IBM puede referirse públicamente al Cliente como suscriptor a los Servicios de Cloud en un comunicado de marketing o publicitario.

5.2 Software de Habilitación

El Servicio de Cloud contiene el Software de Habilitación siguiente:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login
- IBM Security Verify Gateway for PAM (en AIX)
- IBM Security Verify Gateway for PAM
- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials

El siguiente software de habilitación puede utilizarse únicamente con los Servicios de Cloud IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify e IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

EL siguiente software de habilitación puede utilizarse únicamente con los Servicios de Cloud IBM Security Verify e IBM Cloud Identity Govern e IBM Cloud Identity Connect Verify and Govern:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager