Condiciones de Uso de IBM – Condiciones Específicas de la Oferta SaaS

IBM Watson Health Core

Las Condiciones de Uso ("CDU") constan de estas Condiciones de Uso de IBM – Condiciones Específicas de la Oferta SaaS ("Condiciones Específicas de la Oferta SaaS") y un documento con el título Condiciones de Uso de IBM – Condiciones Generales ("Condiciones Generales") disponible en el URL siguiente: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

En caso de conflicto, los Términos de Oferta específicos de SaaS prevalecen sobre las Condiciones Generales. Al hacer un pedido, acceder o utilizar SaaS IBM, el Cliente acepta las Condiciones de Uso.

Las Condiciones de Uso se rigen por el Acuerdo Internacional Passport Advantage de IBM, el Acuerdo Internacional Passport Advantage Express de IBM o el Acuerdo Internacional de IBM para Ofertas Seleccionadas de SaaS IBM, según proceda ("Acuerdo") y conjuntamente con las Condiciones de Uso conforman el acuerdo completo.

1. SaaS IBM

Las siguientes ofertas de SaaS IBM están cubiertas por estas Condiciones Específicas de la Oferta de SaaS:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Métricas de Cargo

SaaS IBM se vende bajo una de las siguientes métricas de cargo según se especifica en el Documento Transaccional:

a. **Acceso**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un Acceso son los derechos para utilizar SaaS IBM. El Cliente debe obtener un único derecho de titularidad de Acceso para poder utilizar SaaS IBM durante el período de medida especificado en el Documento de Titularidad (POE) o el Documento Transaccional del Cliente.

b. **Individuo**: es una unidad de medida con la que se puede adquirir SaaS IBM. Un individuo es una persona o un elemento. Deben adquirirse derechos de titularidad suficientes para cubrir los Individuos procesados o gestionados por el SaaS IBM durante el período de medida especificado en el POE o el Documento Transaccional del Cliente.

   A los efectos de este SaaS IBM, un Individuo es una persona, un dispositivo o una aplicación móvil cuyos datos son gestionados por el SaaS IBM.

c. **Instancia**: es una unidad de medida con la que se puede adquirir SaaS IBM. Una Instancia es el acceso a una configuración específica de SaaS IBM. Deben adquirirse derechos de titularidad suficientes para cada Instancia de SaaS IBM disponible para su acceso y uso durante el período de medida especificado en el Documento Transaccional del Cliente.

3. Cargos y Facturación

El importe que se debe abonar para SaaS IBM se especifica en un Documento Transaccional.

3.1 Cargo Mensual Parcial

Puede evaluarse un cargo mensual parcial, según lo especificado en el Documento Transaccional, sobre una base prorrateada.

3.2 Cargo por Uso en Exceso

Si el uso actual del SaaS IBM por parte del Cliente durante el período de medida supera los derechos de titularidad especificados en el Documento de Titularidad (POE), se facturará al Cliente por el uso en exceso, según se establece en el Documento Transaccional.

4. Opciones de Vigencia y Renovación

La vigencia del SaaS IBM empezará en la fecha en la que IBM notifique al Cliente que éste tiene acceso al entorno operativo de Prueba Piloto del SaaS IBM, según se describe en el Documento Transaccional. El periodo de suscripción para los derechos de titularidad de Individuo empieza cuando IBM notifica al Cliente el acceso del Cliente al entorno operativo de Producción. El Documento de Pedido especificará si el SaaS IBM se renueva automáticamente, sigue bajo una base de uso continuado o termina al finalizar la vigencia.

En relación con la renovación automática, a menos que el Cliente notifique su voluntad de no renovar como mínimo 90 días antes de la fecha de vencimiento, el SaaS IBM se renovará automáticamente por el plazo especificado en el POE.

En relación con el uso continuado, el SaaS IBM seguirá estando disponible mensualmente, hasta que el Cliente notifique por escrito su voluntad de terminación con 90 días de antelación. El SaaS IBM seguirá estando disponible hasta el final del mes natural tras este período de 90 días.

5. Soporte Técnico

IBM pondrá a disposición el manual IBM Software as a Service Support Handbook, que proporciona información de contacto de soporte técnico, las horas de mantenimiento y otro tipo de información y procesos. Se puede encontrar información de contacto de soporte técnico y otros detalles relacionados con las operaciones de soporte en el manual IBM SaaS Support Handbook: https://support.ibmcloud.com.

El soporte técnico y las solicitudes de configuración sencilla para el SaaS IBM se proporcionan a través de envío electrónico. El soporte técnico se ofrece en SaaS IBM y no está disponible como oferta independiente.

No puede incluirse ningún tipo de Información Personal (IP), incluyendo información personal sensible (IPS) o Información Médica Protegida (IMP) en ninguna documentación o información para informar acerca de una incidencia.

6. Definiciones

Leyes Aplicables: significa cualquier ley, estatuto o acto legislativo, normas, reglamentos, directivas, mandatos, decretos u otros requisitos emitidos por una autoridad gubernamental o cualquier estándar del sector reconocido de forma generalizada que sea aplicable a la realización de estas Condiciones de Uso.

API: interfaz de programación de aplicaciones, que es un conjunto de rutinas, protocolos y herramientas para la creación de aplicaciones de software. La API especifica cómo deben interactuar los componentes de software, y las API se utilizan en la programación de componentes de interfaz gráfica de usuario (GUI).

Administrador Autorizado: cualquier empleado del Cliente, contratista aprobado del Cliente, individuo o grupo responsable de la gestión del mantenimiento y el funcionamiento fiable de la plataforma. Las responsabilidades pueden incluir configuración, soporte y gestión de usuarios y cuentas. El administrador también puede ser un investigador clínico responsable de la definición de un estudio en el sistema Watson Health.

Individuo Autorizado: cualquier persona autenticada, aplicación móvil o dispositivo al cual se ha dado acceso a los derechos de acceso para enviar datos a Watson Health Core. Esto puede incluir el Cliente; o los participantes del estudio, los clientes respectivos o los pacientes del Cliente.

Leyes de Datos Aplicables del Cliente: las Leyes de Datos aplicables al cumplimiento de las obligaciones del Cliente en virtud del Acuerdo, los Documentos Asociados y las Descripciones de Servicios aplicables, Documentos de Pedido y Especificaciones de Trabajo entre las Partes.

Datos del Cliente: cualquier entrada de datos en el SaaS IBM por parte de o para el Cliente, ya sean los propios datos del Cliente o los datos introducidos por o en nombre del cliente respectivo del Cliente o por terceros, e incluyendo todos los datos de dispositivos médicos de bienestar de terceros.

Leyes de Datos: Leyes Aplicables que se relacionan con la protección de datos personales, la privacidad o la seguridad de los datos.

Sujeto de los Datos: persona física identificada o identificable con quien se relacionan los Datos Personales.

Centro de Datos Designado: el centro (o los centros) de datos especificado como centro de datos principal y de recuperación tras desastre en el Documento Transaccional que ejecuta la instancia del Cliente del SaaS IBM, si es aplicable.

Datos Médicos: cualquier dato o información, incluyendo imágenes, que sea Información Personal relacionada con la salud.

Datos Médicos Habilitados en relación con el SaaS IBM, la capacidad del SaaS IBM para cumplir con los estándares aplicables de seguridad y privacidad, leyes y regulaciones en Jurisdicciones Dentro de Alcance para los datos médicos, incluyendo las especificaciones de implementación establecidas en la Parte 164, Subpartes A y C, de los reglamentos de aplicación de la ley HIPAA (según la modificación de la Ley de alta tecnología, HITECH Act) y otras Leyes Aplicables en materia de Datos Médicos, pero no significa que IBM esté actuando en virtud de Socio Empresarial o Responsable del Tratamiento de Datos.

HIPAA: Health Insurance Portability and Accountability Act de 1996, en sus versiones modificadas, incluyendo la Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), determinados reglamentos promulgados bajo la HIPAA por el Department of Health and Human Services de los EE.UU. en C.F.R. 45 Partes 160 y 164 y determinadas leyes promulgadas en conformidad con la HITECH Act.

Leyes de Datos Aplicables de IBM: Leyes de Datos Aplicables a la ejecución de las obligaciones de IBM en virtud del Acuerdo, Documentos Asociados y Descripciones de Servicios aplicables, Documentos de Pedido y Especificaciones de Trabajo entre las partes.

Personal de IBM: (a) IBM, sus Afiliados y sus subcontratistas, y con respecto a cada uno de los anteriores, sus empleados; y (b) todos los proveedores terceros; en cada caso, que realiza servicios en nombre de IBM de conformidad con el Acuerdo y los Documentos Asociados aplicables, o a quien IBM autoriza el acceso a los Datos Personales del Cliente.

Países Dentro de Alcance: los 28 Estados miembros de la Unión Europea y Suiza, así como aquellos países que IBM pueda añadir a esta lista de vez en cuando.

Datos Personales o **Información Personal**: información en cualquier soporte o formato, incluidos los registros electrónicos y en papel, que se refiere a una persona física identificada o identificable, siendo un "individuo identificable" alguien que pueda ser identificado, directa o indirectamente, en especial haciendo referencia a un número de identificación o a uno o más factores específicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Proceso y las variantes del término, como **procesamiento** (en mayúsculas o no), significa cualquier operación o conjunto de operaciones que se llevan a cabo en los datos, sea o no mediante procedimientos automatizados, como la recogida, el registro, la organización, el almacenamiento, la adaptación o alternación, la recuperación, la consulta, la utilización, la divulgación por transmisión, la difusión o cualquier otra forma de puesta a disposición, alineación o combinación, bloqueo, supresión o destrucción.

Datos Procesados: cualquier dato, información o material confidencial o privado, incluyendo Datos Médicos y Datos Personales, es decir procesados por IBM en aplicación del Acuerdo, un Documento Asociado y/o una Descripción de Servicios, Documento de Pedido y/o Especificación de Trabajo.

Incidente de Seguridad: tiene el significado que se establece en el SBCA.

7. Gestión de Cuentas

El SaaS IBM es accesible para los usuarios autorizados del Cliente (solo los "**Administradores autorizados**" o los "**Individuos Autorizados**"). El Cliente controlará las cuentas autorizadas para acceder al SaaS IBM, lo cual puede incluir las aplicaciones autorizadas, el personal del Cliente, los contratistas y proveedores de servicios terceros del Cliente, y es el responsable exclusivo de (i) controlar a todos los usuarios autorizados, incluyendo, sin limitación, la verificación de la identidad de cualquier usuario autorizado; y (ii) garantizar que únicamente los usuarios autorizados acceden al SaaS IBM.

Los Individuos Autorizados que son clientes, pacientes o participantes en el estudio del Cliente pueden tener acceso solamente con el fin de cargar información en el SaaS IBM, en cuyo caso dichos Individuos Autorizados no tendrán otro acceso al SaaS IBM.

8. Privacidad

8.1 Requisitos Generales

Entre las Partes, el Cliente es el responsable exclusivo de todos los Datos Personales del Cliente, y el Cliente designa a IBM como encargado del tratamiento de datos. De acuerdo con las Leyes de Datos Aplicables, el Cliente tiene el derecho a dar instrucciones a IBM en relación con el procesamiento de los Datos Personales del Cliente por parte de IBM.

En la medida en que IBM procese los Datos Personales del Cliente, IBM deberá:

a. cumplir lo establecido en las Leyes de Datos Aplicables de IBM; y

b. no mezclar Datos Personales del Cliente con datos de otros orígenes, excepto:

- según sea necesario para proporcionar el SaaS IBM y posteriormente no para ningún otro propósito, a menos que reciba instrucciones concretas del Cliente para hacerlo; o
- de conformidad con los términos de estas Condiciones de Uso y del Apéndice de Seguridad y Continuidad Empresarial.

En la medida en que IBM procese los Datos Personales del Cliente, el Cliente deberá:

a. cumplir lo establecido en las Leyes de Datos Aplicables del Cliente;

b. responsabilizarse de todas las comunicaciones por parte del Cliente con Afiliados del Cliente, pacientes, usuarios finales, Sujetos de los Datos y/o terceros del Cliente;

c. cerrar acuerdos de procesamiento de datos con los responsables que sean necesarios para permitir a IBM como encargado del tratamiento de datos y a sus subprocesadores procesar los Datos Personales del Cliente; y

d. servir como única persona de contacto para IBM y ser el único responsable de la coordinación interna, la revisión y el envío de instrucciones o solicitudes de los Afiliados del Cliente que son otros responsables de IBM. IBM quedará liberado de su obligación de informar o notificar a cualquier Afiliado del Cliente que constituye un responsable cuando se haya proporcionado dicha información o aviso al Cliente. IBM tiene derecho de titularidad para rechazar cualquier instrucción proporcionada directamente por cualquier Afiliado del Cliente que constituye un controlador que no es Cliente.

No se requerirá a ninguna de las partes actuar infringiendo las Leyes de Datos Aplicables de la parte.

8.2 Derechos de Datos del Cliente

El Cliente declara y garantiza que (a) es propietario de los datos que introducirá en el SaaS IBM, o (b) ha obtenido, y es responsable de su mantenimiento, todos los derechos, permisos, consentimientos y autorizaciones necesarios para garantizar a IBM los derechos de acceso, uso y divulgación de los Datos del Cliente, de acuerdo con los términos establecidos en las presentes Condiciones de Uso o el Acuerdo o según sea necesario para que IBM proporcione el SaaS IBM. El Cliente declara y garantiza adicionalmente que los Datos del Cliente solo estarán o bien (a) en relación con los individuos que residen en los Estados Unidos y posteriormente sólo se podrán introducir en el SaaS IBM en el centro de datos de Estados Unidos o (b) en relación con los individuos que residen en uno o más países Dentro de Alcance y posteriormente sólo se podrán introducir en el SaaS IBM en los Centros de Datos Designados.

8.3 Responsabilidades y Servicios de Datos

a. El Cliente acepta que sólo llevará a cabo análisis o solicitará que IBM realice análisis sobre los Datos del Cliente en relación con las actividades que constituyen las "operaciones de cuidado médico" o "investigación" del Cliente, como se define bajo el HIPAA y/o términos similares bajo otras Leyes de Datos Aplicables y que el Cliente utilizará los Datos del Cliente o indicará a IBM que utilice los Datos del Cliente solamente de acuerdo con todos los requisitos pertinentes (por ejemplo, la determinación o la renuncia de la Junta de Revisión Institucional, cuando se requiera) bajo estas y otras Leyes de Datos Aplicables del Cliente.

b. El Cliente es el único responsable de la obtención de todos los posibles registros, consentimientos, autorizaciones y permisos según lo requieran las Leyes Aplicables del Cliente en cada País Dentro de Alcance, incluyendo, sin limitación, la HIPAA y cualquier otra ley de privacidad y seguridad de los datos, reglas y reglamentos, a fin de que los Datos del Cliente que se introducen en el SaaS IBM se utilicen y divulguen como se contempla en estas Condiciones de Uso y el Acuerdo por parte del Cliente y de IBM y los subcontratistas autorizados de IBM. IBM no tendrá ninguna

responsabilidad por la monitorización cuando dichos registros, consentimientos, autorizaciones y permisos se reciban o se requieran.

c. El Cliente es el único responsable de garantizar que todos los Datos del Cliente introducidos en el SaaS IBM se limiten a los datos relativos a los individuos que residen en los Estados Unidos o en un país Dentro de Alcance.

d. IBM tendrá centros de soporte con personal formado sobre la HIPAA y otras Leyes de Datos Aplicables de IBM respecto a los datos de los países Dentro de Alcance.

8.4 Medidas de Seguridad e Incidentes de Seguridad

a. IBM deberá implementar, mantener y cumplir las medidas técnicas y organizativas (incluidos los procesos y procedimientos organizativos, y en particular las obligaciones de seguridad específicas definidas o mencionadas en estas Condiciones de Uso y el SBCA para proteger los Datos Personales del Cliente frente a uso o acceso no autorizado, pérdida accidental, daño, modificación, destrucción, robo o divulgación no autorizada.

b. En el caso de que IBM tenga conocimiento de un Incidente de Seguridad (tal como se define en el SBCA) que implique a Datos Procesados del Cliente, IBM deberá informar al Cliente de acuerdo con los términos del SBCA y las Leyes de Datos Aplicables de IBM, y dicha notificación incluirá información sobre cualquier impacto conocido en el Cliente o cualesquiera Sujetos de los Datos (si existen) afectados por dicho Incidente de Seguridad y las medidas correctivas adoptadas o propuestas para ser tomadas por parte de IBM.

8.5 Recepción de Consultas y Quejas

IBM deberá notificar al Cliente por escrito con prontitud y, en la medida permitida por las Leyes de Datos Aplicables de IBM, antes de que transcurran cinco (5) días laborables tras la recepción por parte del Representante de Privacidad de los Datos de IBM Watson Health de cualquier investigación, comunicación o denuncia recibida por parte de IBM en relación con los Datos Personales del Cliente en:

a. cualquier Sujeto de los Datos, en relación con Datos Personales acerca de este Sujeto de los Datos Procesados por IBM. El Cliente deberá responder a dichas solicitudes de los Sujetos de los Datos e IBM cumplirá con las instrucciones razonables del Cliente para ayudar al Cliente a responder a tales peticiones. Si lo requieren las leyes aplicables de IBM, IBM puede responder directamente a dichas solicitudes, siempre que IBM notifique por anticipado al Cliente dichas respuestas y se coordine razonablemente con el Cliente con respecto a la forma y el contenido de las respuestas, cuando lo permitan las Leyes Aplicables de IBM o de otro modo sea posible;

b. cualquier autoridad legal o reglamentaria, en relación con el Procesamiento por parte de IBM de los Datos Personales del Cliente, siempre que IBM pueda responder a dichas solicitudes recibidas de una agencia gubernamental con una resolución o un documento legal similar que obligue a la divulgación por parte de IBM o según lo requiera de otro modo la Ley Aplicable de Datos, siempre que IBM notifique al Cliente anticipadamente dicha divulgación y se cooordine razonablemente con el Cliente con respecto a la forma y el contenido de dicha respuesta, cuando lo permita la ley o sea de otro modo posible.

8.6 Procesamiento de los Datos Personales del Cliente

IBM restringirá la divulgación de los Datos Personales del Cliente al Personal de IBM que pueda ser necesario para colaborar en la prestación de los Servicios.

IBM deberá atender cualquier solicitud razonable del Cliente que requiera a IBM modificar, corregir o suprimir o bloquear Datos Personales del Cliente de acuerdo con la Ley Aplicable.

A petición de cualquiera de las Partes, IBM, el Cliente o sus respectivos Afiliados cerrarán los acuerdos estándar requeridos por la ley para la protección de Datos Personales del Cliente. Las Partes aceptan (y procurarán que sus respectivos afiliados acepten) que tales acuerdos estarán sujetos a las limitaciones y exclusiones de responsabilidad en este Acuerdo a efectos de reclamaciones entre las Partes. Las Partes deberán cooperar para cerrar (o procurar que los Afiliados de dichas Parte cierren) y cumplir las condiciones o los acuerdos mutuamente aceptados según lo requieran las Leyes de Datos Aplicables.

8.7 Devolución de Datos Personales del Cliente

Al vencer o terminar el Acuerdo, IBM deberá cesar, y hará que todo el Personal de IBM cese, el uso o el procesamiento de cualquier Información Propiedad del Cliente y de cualesquiera Datos Personales del Cliente y deberá, a decisión y solicitud del Cliente:

a. devolver con celeridad en un formato y en unos soportes de almacenamiento que el Cliente pueda solicitar razonablemente toda la Información Propiedad del Cliente y los Datos Personales del Cliente que IBM esté almacenando electrónicamente y, tras confirmación de recepción por parte del Cliente, suprimir, destruir o de otra forma hacer que sea permanentemente ilegible o indescifrable la Información Propiedad del Cliente y los Datos Personales del Cliente, incluidas las copias y las copias de seguridad. IBM podrá cobrar por el coste/costo de los soportes de almacenamiento y por ciertas actividades llevadas a cabo a petición del Cliente (como entregar Información Propiedad del Cliente y Datos Personales del Cliente en un formato específico o destruir la Información Propiedad del Cliente o los Datos Personales del Cliente de una forma determinada); y

b. directamente destruir o de otra forma hacer que sea permanentemente ilegible o indescifrable la Información Propiedad del Cliente y los Datos Personales del Cliente, incluidas las copias y las copias de seguridad.

8.8 Acuerdo de Asociado de Negocio

En la medida en que sea adecuado y requerido por la ley HIPAA, IBM y el Cliente cerrarán un Acuerdo de Asociado Empresarial ("BAA"), que regirá las obligaciones de IBM como Asociado Empresarial del Cliente en la provisión del SaaS IBM. Sin limitar las obligaciones expresas de IBM en virtud del Acuerdo y el BAA si es aplicable, el Cliente reconoce y acepta que es responsable de determinar la aplicabilidad, y el cumplimiento, de todas las Leyes Aplicables y los requisitos de licencia que se apliquen al uso del Cliente u otras actividades con respecto al SaaS IBM (incluyendo el uso u otras actividades por parte de los Usuarios Autorizados).

8.9 Anexo de Procesamiento de Datos en la Unión Europea

Si el Cliente implica a IBM en el procesamiento de Datos Personales de la Unión Europea, IBM y el Cliente firmarán un Anexo de Procesamiento de Datos, incluyendo, según corresponda, Cláusulas Tipo de la UE, con las cláusulas opcionales eliminadas.

9. Condiciones Adicionales de la Oferta de SaaS IBM

9.1 Seguridad

Este SaaS IBM cumple los principios de privacidad y seguridad de los datos de IBM para SaaS IBM que están disponibles en http://www.ibm.com/cloud/data-security y los términos adicionales que se proporcionan a continuación y en el Apéndice de Seguridad y Continuidad Empresarial de estas Condiciones de Uso. Cualquier cambio en los principios de privacidad y seguridad de los datos de IBM no significará una disminución de la seguridad del SaaS IBM.

IBM Watson Health Core implementa políticas de seguridad, normas y procesos basados en el marco ISO 27001, según se describe con más detalle en la Descripción de Seguridad. Entre sus prestaciones de seguridad, la solución implementa lo siguiente:

a. Zonas de Operación Segura

   IBM Watson Health Core implementa una estrategia de defensa en profundidad, utilizando múltiples zonas de seguridad para la gestión de puntos de integración de entornos cloud, como la incorporación de datos y el desarrollo de aplicaciones personalizadas.

b. Cifrado

   Todos los Datos del Cliente se cifran en reposo y durante la actividad. Todos los datos en tránsito hacia y desde IBM Watson Health Core son cifrados. Un servicio compartido proporciona gestión de claves de cifrado. El Cliente es responsable de toda la calidad y la conectividad de la red entre el servidor proxy del Cliente y el Servicio IBM Watson Health.

c. Monitorización de Eventos de Seguridad

   IBM aprovecha su plataforma de inteligencia de seguridad para información de seguridad y gestión de eventos, gestión de registros, análisis forense de incidentes, detección de amenazas y gestión de vulnerabilidades.

d. Gestión de identidades

- Watson Health Core da soporte a los proveedores de identidad de estándares abiertos para poblaciones de usuarios y pacientes a gran escala mediante OpenID Connect.
- Para las poblaciones de usuarios en las cuales IBM es el proveedor de identidad, Watson Health Core aprovecha las capacidades adecuadas de servicios de directorio y gestión de identidad para manejar la autenticación.

e. Autenticación Segura y Acceso Basado en Roles

- Watson Health Core da soporte a la autenticación a través de SAML como mecanismo para los Clientes de cara a integrar sus servicios de directorio o Inicio de Sesión Único (SSO).
- Watson Health Core aprovecha una solución de gestión de acceso y los componentes relacionados para gestionar las políticas de seguridad, cuando sea necesario.
- Watson Health Core es compatible con la autenticación de dos factores basada en software.
- Watson Health Core proporciona un control básico de acceso basado en roles, según sea necesario; Watson Health Core admite la configuración de estudios, perfiles de usuario, roles y grupos de usuarios a través de interfaces de programación de aplicaciones ("API") que permiten el acceso basado en roles.

9.2 Cookies

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

9.3 Ubicaciones con Ventajas Derivadas

Cuando sea aplicable, los impuestos se basan en las ubicaciones que el Cliente identifica como receptoras de los servicios SaaS IBM. IBM aplicará los tributos en base a las direcciones de facturación enumeradas a la hora de solicitar SaaS IBM 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.

9.4 Prestación Continua

El Cliente tiene derecho de titularidad a capacidades y mejoras realizadas en la solución y desplegadas por IBM en un modelo de prestación en cloud continua.

9.5 Copias de Seguridad-Respaldo y su Restauración

IBM Watson Health Core proporciona copia de seguridad de los Datos del Cliente en el entorno productivo (incluyendo los repositorios Laguna de Datos y Depósito de Datos) en el último estado correcto conocido con el propósito de recuperar el servicio en caso de fallo del sistema.

9.6 Alta Disponibilidad

Los componentes de IBM Watson Health Core en el entorno productivo se implementan en configuraciones de alta disponibilidad, con servidores de BD agrupados en clúster para redundancia de cara a proporcionar una distribución de la carga de trabajo y eliminar los puntos únicos de fallo.

9.7 Recuperación Tras Desastre

El enfoque de IBM para la recuperación tras desastre consiste en múltiples centros de datos en áreas geográficamente dispersas para lograr sus objetivos de continuidad del negocio de la siguiente manera para su entorno productivo:

- RTO – dentro de las primeras 36 horas tras la declaración de desastre
- RPO – transcurridas no más de 24 horas tras la pérdida de contenido del Cliente

9.8 Herramientas de Medida

El SaaS IBM utiliza una solución de monitorización sintética para monitorizar, medir e informar sobre la disponibilidad o las interrupciones en relación con los niveles de servicio comprometidos. Esta solución simula y realiza un seguimiento de la respuesta del usuario y la experiencia del usuario a nivel mundial, para las transacciones y la disponibilidad estática.

El SaaS IBM también utiliza un sistema de monitorización interno para métricas, eventos y alertas a lo largo de toda la solución.

9.9 Publicidad

El Cliente acepta que IBM puede referirse públicamente al Cliente como suscriptor al SaaS IBM en una publicidad o un comunicado de prensa.

Apéndice A

1. IBM Watson Health Core

IBM Watson Health Core es una plataforma como servicio (PaaS) Compatible con Datos Médicos, la plataforma de desarrollo y el subsistema operativo para almacenar, supervisar y procesar Información Médica Protegida (PHI), tal como define la ley HIPAA, y otros Datos Médicos de conformidad con Ley de Datos Aplicable de IBM, que se encuentren en un centro de datos bajo la propiedad o el control de IBM. El Cliente debe adquirir los derechos de titularidad correspondientes a IBM Watson Health Core e IBM Watson Health Core Access para habilitar las características y capacidades que se describen a continuación.

1.1 Entornos Operativos de Watson Health Core

El derecho de titularidad de Watson Health Core abarca tres entornos operativos en cloud Compatibles con Datos Médicos para procesar Datos Médicos:

- Prueba Piloto

  Proporciona un entorno de pruebas donde los Clientes pueden desarrollar y probar aplicaciones creadas mediante el SaaS IBM. El entorno piloto implementa todos los controles de seguridad de HIPAA a excepción de la Recuperación Tras Desastre, la alta disponibilidad y la seguridad de los sistemas de registro.

- Entorno Productivo

  Proporciona el entorno a gran escala donde los Clientes pueden desplegar cargas de trabajo de Datos Médicos. El entorno productivo es un entorno de carga equilibrada y alta disponibilidad, y es capaz de conmutar por error a una ubicación de Recuperación Tras Desastre.

- Recuperación Tras Desastre

  Proporciona una duplicación del Entorno Productivo; este entorno se encuentra en una ubicación de centro de datos independiente.

1.2 Desarrollo de Aplicaciones

IBM Watson Health Core permite el desarrollo de aplicaciones y la recopilación de datos segura de dispositivos del Cliente o dispositivos de los usuarios autorizados del Cliente. Las API proporcionan la documentación y las interfaces de programa que los usuarios autorizados del Cliente, incluidos los proveedores de servicio terceros del Cliente, pueden utilizar para desarrollar aplicaciones e intercambiar datos con el SaaS IBM. El uso de las API por parte del Cliente o de los desarrolladores del Cliente está sujeto al cumplimiento de los Requisitos del Desarrollador de API.

- API de REST

  Watson Health Core ofrece una serie de API de REST y servicios para la plataforma Watson Health Core. Entre las capacidades de la API se incluyen, a título enunciativo pero no limitativo, los mecanismos de acceso a los repositorios de datos, el servicio de supervisión de datos, la gestión de usuarios y los registros de auditoría.

- Apple HealthKit y Apple ResearchKit

  Watson Health Core es compatible con la integración con el marco de la API de Apple ResearchKit para los estudios de investigación basados en iOS, y con Apple HealthKit para capturar datos relacionados con la salud.

1.3 Gobierno de Datos

- Gestión de Consentimientos

  Watson Health Core proporciona el marco para capturar el consentimiento proporcionado por los pacientes o los participantes en estudios y puede almacenar de forma segura un registro de los consentimientos, además de la carga útil de datos, cuando el individuo se inscribe a través de una aplicación del Cliente compatible con los consentimientos.

- Enmascaramiento de Datos

  Watson Health Core proporciona la capacidad de separar los identificadores de nombres de las cargas útiles de datos estructurados. Watson Health Core recibe datos en cloud a través de las API del programa. Las API permiten la separación de los identificadores de nombre de individuos o pacientes del resto de la carga útil de datos, para almacenarlos en un almacén de datos cifrado independiente. A la carga útil de datos se le asigna un token anonimizado que se puede utilizar en el seguimiento de procedencias futuro.

1.4 Servicios de Datos Médicos

Watson Health Core ofrece recogida, almacenamiento, sincronización de datos, incluyendo Datos Médicos de procedencia externa y otra Información Personal, tanto estructurados como no estructurados.

- Consumo de Datos

  Watson Health Core proporciona la capacidad de consumir datos de dispositivos o aplicaciones de paciente a través de API de programa. Watson Health Core concede derecho de titularidad a cada uno de los Individuos Autorizados del Cliente para cargar hasta 25 MB de datos en Health Core cada año de vigencia del contrato. El servicio tiene una capacidad para un máximo de 10 cargas por Individuo por día.

- Laguna de Datos Operativa

  Los Datos Sin Formato del Cliente o del paciente se almacenan en Watson Health Core en su formato nativo hasta que se necesite para el análisis y el modelado.

- Extract Transform Load (ETL)

  Los datos se transforman en un formato normalizado dentro del subsistema operativo. Un Bus de Servicio Empresarial (ESB) basado en estándares del sector para recursos de atención sanitaria permite la integración a través de diferentes aplicaciones y protocolos del Cliente.

- Depósito de Datos

  Una vez supervisados, los datos se mueven al Depósito de Datos. Watson Health Core utiliza aspectos del Modelo de Datos Unificado de IBM para Atención Sanitaria (IBM Unified Data Model for Healthcare) para normalizar los datos médicos empresariales y técnicos para su uso en las analíticas.

- Índice de Personas Maestro

  Watson Health proporciona herramientas de Gestión de Datos Maestros para consolidar los datos de diversos orígenes para crear un Registro Longitudinal de Personas (LPR).

2. Características Opcionales

2.1 IBM Watson Health Core Terminology Service

Este servicio complementario facilita la integración de los datos y la interoperabilidad entre sistemas médicos dispares, proporcionando un uso de terminología clínica coherente a través de todas las aplicaciones de Watson Health Cloud. Este servicio ofrece la plataforma funcional para todas las tareas que implican terminologías, sistemas de código y contenido estructurado, tales como:

- creación de nuevos sistemas de codificación;
- traducción de sistemas de codificación internacionales; y
- asignaciones entre listas de codificación locales y los estándares internacionales.

Apéndice B

IBM proporciona el siguiente acuerdo de Nivel de Servicio ("SLA") de disponibilidad para el SaaS IBM según lo especificado en un POE. El SLA no es una garantía. El SLA está disponible solamente para el Cliente y se aplica sólo para su uso en entornos productivos.

1. Créditos de Disponibilidad

Las rebajas de disponibilidad solo son aplicables a las tarifas de suscripción para los derechos de titularidad de Individuo.

El Cliente debe registrar un ticket de soporte de Severidad 1 en el help desk del servicio de asistencia técnica de IBM, en un período de veinticuatro (24) horas desde que el Cliente tuvo conocimiento en primera instancia de un evento que ha afectado la disponibilidad del SaaS IBM. El Cliente debe ayudar razonablemente a IBM en relación con cualquier diagnóstico y terminación de los posibles problemas.

Debe enviarse un ticket de soporte en caso de incumplimiento de un SLA, a más tardar tres (3) días laborables después del último día del mes contratado. La compensación por una reclamación válida de SLA será un crédito aplicable en una factura futura para el SaaS IBM, basado en el plazo temporal durante el cual el procesamiento en el sistema productivo para el SaaS IBM no haya estado disponible ("Tiempo de Inactividad"). El Tiempo de Inactividad se mide desde el momento en que el Cliente notifica el evento hasta el momento en que el SaaS IBM se restaura y no incluye: tiempo relacionado con un corte de mantenimiento planificado o anunciado; causas que queden fuera del control de IBM; problemas con contenido/tecnología, diseños o instrucciones del Cliente o un tercero; plataformas o configuraciones del sistema no compatibles, u otros errores del Cliente; o incidencias de seguridad o pruebas de seguridad del Cliente. IBM aplicará la compensación correspondiente más alta en función de la disponibilidad acumulativa del SaaS IBM durante cada mes contratado, como se muestra en la tabla siguiente. La compensación total concedida en relación con cualquier mes contratado no puede superar el 20 por ciento de una doceava parte (1/12) del cargo anual por el SaaS IBM.

2. Niveles de Servicio

Disponibilidad del SaaS IBM durante un mes contratado

Disponibilidad durante un mes contratado	**Compensación (% de la cuota de suscripción Individual mensual* para el mes contratado que es objeto de una reclamación)**
< 99,95%	10%
< 99,0%	20 %

* Si el Cliente ha adquirido el SaaS IBM a un Business Partner de IBM, la tarifa de suscripción mensual se calculará según el precio según catálogo actualizado del SaaS IBM en vigor para el mes contratado que es sujeto de la reclamación, con un descuento del 50%. IBM proporcionará una rebaja directamente el Cliente.

La Disponibilidad, expresada como porcentaje, se calcula de este modo: el número total de minutos en un mes contratado, menos el número total de minutos de Tiempo de Inactividad en un mes contratado, dividido por el número total de minutos en un mes contratado.

Ejemplo: 108 minutos de Tiempo de Inactividad total durante un mes contratado

43.200 minutos en total en un mes contratado de 30 días - 108 minutos de Tiempo de Inactividad = 43.092 minutos _____ 43.200 minutos en total	= 10% de crédito de Disponibilidad para un 99,75% de disponibilidad durante el mes contratado

3. Exclusiones

Este SLA no se aplica en los siguientes casos:

- Además de la monitorización del servidor, el SLA no se aplica a las máquinas virtuales alojadas para soportar aplicaciones personalizadas o del Cliente.
- Si el Cliente ha incumplido alguna obligación correspondiente a las obligaciones del presente acuerdo.

Apéndice C

Este Apéndice de Seguridad y Continuidad Empresarial (este "SBCA") establece ciertos requisitos y obligaciones de IBM en la prestación del SaaS IBM al Cliente. Los requisitos y las obligaciones establecidos en este documento son adicionales a los establecidos en la descripción de los principios de seguridad de los datos para SaaS IBM que están disponibles en http://www.ibm.com/cloud/data-security. Los términos en mayúsculas que no están definidos en el presente documento tendrán los significados establecidos en el Acuerdo o las Condiciones de Uso.

1. Programa de Seguridad de la Información

IBM cuenta con políticas internas de seguridad, normas y procesos basadosen el marco de la norma ISO 27001 y las áreas de control. Además del gobierno de la Organización de Seguridad Corporativa de IBM, estas políticas, normas y procesos son regularmente objeto de auditorías internas.

IBM mantiene un programa de seguridad de la información sobre las protecciones organizativas, operativas, administrativas, físicas y técnicas que regulan que el procesamiento, el almacenamiento y la transmisión de contenido del Cliente sean como mínimo coherentes con los requisitos del presente SBCA.

IBM compartirá con el Cliente, a petición del Cliente, información sobre el programa de seguridad de la información de IBM Watson Health para que el Cliente pueda determinar razonablemente su conveniencia, adecuación y eficacia continuadas. El programa de seguridad de la información de IBM Watson Health deberá actualizarse de vez en cuando, para mantenerse actualizado con las prácticas generalmente aceptadas del sector y las Leyes Aplicables de IBM.

2. Controles de Acceso

IBM divulgará el contenido del Cliente sólo a sus empleados, subcontratistas o terceros que tengan una necesidad comercial legítima para acceder a dicho contenido del Cliente con el fin de ayudar a IBM a llevar a cabo sus obligaciones con el Cliente o con otras personas según sea necesario para proporcionar el SaaS IBM, de conformidad con las Leyes Aplicables, el Acuerdo o un Documento Asociado, según sea aplicable. En caso de que IBM sea un Asociado Empresarial del Cliente, IBM y el Cliente divulgarán la Información Médica Personal solamente de acuerdo con las condiciones de un Acuerdo de Asociado Empresarial aplicable entre las Partes.

IBM cuenta con un proceso formal e interno de gestión de accesos de usuario, mediante el cual se solicita formalmente el acceso de los usuarios, se aprueba tras la verificación de identidad y se concede en función de la necesidad de conocimiento por parte del usuario, mediante la utilización del concepto de privilegio mínimo. El acceso a los contenidos del Cliente se limitará sólo a los usuarios activos y las cuentas de usuario activas. IBM cuenta con un proceso formal para la revalidación periódica del acceso interno de las cuentas de usuario activas.

IBM utiliza protocolos seguros de autenticación de usuario, incluyendo la asignación de identificaciones y contraseñas seguras para las cuentas de usuario activas en los sistemas utilizados para proporcionar servicios al Cliente de conformidad con las políticas y las normas de seguridad corporativas de IBM:

a. Las contraseñas no deben ser contraseñas predeterminadas suministradas por un proveedor, y se mantendrán en un lugar y/o formato que no ponga en peligro la seguridad de los datos que protegen.

b. La visualización y la impresión de las contraseñas deben enmascararse, suprimirse o de otro modo ocultarse de tal forma que terceros no autorizados no puedan verlas o en consecuencia recuperarlas. Las contraseñas no deben registrarse o capturarse mientras se introducen. Las contraseñas de usuario no deben almacenarse en un formato de texto evidente.

c. Las contraseñas para cada tecnología que comprende el SaaS IBM se seleccionan para mitigar los riesgos asociados a las vulnerabilidades conocidas de longitud de contraseña y deben documentarse.

d. Cuando se requiere el uso de ID funcionales internos, privilegiados y compartidos, por razones operativas, IBM gestiona los ID compartidos, funcionales y/o del Sistema que requieran la creación de contraseñas para mantener la responsabilidad individual.

Se establecen tiempos de espera de inactividad para todos los sistemas y aplicaciones que almacenan contenido del Cliente.

Si es necesario, el acceso remoto a redes, sistemas y aplicaciones de IBM que almacenan contenido del Cliente se establecerá a petición del Cliente y con la aprobación formal de IBM, y todas esas conexiones remotas deberán asegurarse mediante protocolos seguros de autenticación y cifrado. La actividad de acceso remoto deberá registrarse y monitorizarse.

En la medida en que la prestación del SaaS IBM requiera que IBM acceda de forma remota a cualquier Sistema incluido en las redes internas del Cliente, todo el acceso remoto se realizará exclusivamente utilizando protocolos y sistemas de acceso remoto seguro del Cliente y mediante el uso de credenciales de acceso proporcionadas a IBM por el Cliente. El acceso remoto a la red del Cliente se establecerá solamente a petición de IBM y tras aprobación por parte del Cliente, y de acuerdo con las políticas vigentes en ese momento del Cliente, que serán proporcionadas a IBM por adelantado. El uso por parte de IBM de las redes internas del Cliente estará sujeto a las políticas de uso y seguridad de las TI del Cliente, que serán proporcionadas a IBM por adelantado.

IBM implementa la separación de funciones para la administración de la seguridad, la revisión de accesos y las investigaciones de infracciones de seguridad.

El almacenamiento, el alojamiento y el procesamiento de contenido del Cliente específico para el Cliente están lógicamente separados de los de otros Clientes atendidos por IBM. En los casos en que el uso compartido de un almacenamiento, alojamiento o área de trabajo de procesamiento sea autorizado por el Cliente, IBM debe tener procedimientos y protecciones vigentes de conformidad con los requisitos establecidos en este SBCA, que estén diseñados para evitar la divulgación no autorizada de dicho contenido del Cliente.

IBM implementa políticas de pantallas y escritorios limpios para garantizar que el contenido del Cliente no quede desatendido en cualquier lugar público en ningún momento.

3. Transferencia y Cifrado

IBM deberá tomar las precauciones adecuadas en la transmisión de contenido del Cliente (por fax, correo electrónico, mensajería, etc.) para garantizar que la información de contacto correcta se utiliza para el destinatario y llevar a cabo los arreglos previos con el destinatario previsto para asegurar la recepción de dicha información.

IBM utiliza, y hará que el Personal de IBM utilice, medios apropiados de cifrado u otras tecnologías seguras en todo momento en relación con el procesamiento de los contenidos del Cliente, incluso en relación con cualquier transferencia, comunicación, acceso remoto o almacenamiento (incluido el almacenamiento de copia de seguridad) de contenido del Cliente. Por ejemplo, IBM deberá cifrar, utilizando un cifrado estándar del sector apropiado, todos los registros y archivos que contengan contenido del Cliente:

a. almacenado en sistemas portátiles de IBM, dispositivos portátiles o medios electrónicos portátiles, incluyendo las cintas de copia de seguridad cuando están en tránsito hacia una instalación de almacenamiento externa;

b. almacenado o transportado por IBM fuera de las oficinas e instalaciones protegidas físicamente del Cliente o de IBM, con exclusión de los documentos impresos en papel;

c. durante el trayecto entre redes públicas por parte de IBM;

d. mientras se transfiere desde los sistemas de IBM al Cliente;

e. durante la transmisión inalámbrica por parte de IBM; y

f. almacenado por IBM en servidores y BD.

4. Seguridad de la Red

IBM utiliza versiones razonablemente actualizadas del software de seguridad del sistema, como firewalls, servidores proxy, firewalls de aplicaciones web e interfaces. Este tipo de software debe incluir protección de malware y parches y definiciones de virus razonablemente actualizados. De acuerdo con los estándares corporativos, el software antivirus debe estar instalado en las estaciones de trabajo, servidores y puntos finales relacionados cuando sea técnicamente factible, y el software se gestiona con la política corporativa con soluciones de gestión interna.

IBM monitoriza el SaaS IBM para detectar e identificar los incidentes de seguridad tan pronto como sea posible. IBM deberá mantener, como mínimo, las herramientas estándar del sector de detección de

intrusiones, así los como procesos de prevención, monitorización y respuesta de una manera diseñada para identificar las vulnerabilidades y los riesgos internos y externos que podrían dar lugar a acceso no autorizado, mal uso, alteración o destrucción de los sistema de información o el contenido del Cliente que se utilicen para prestar servicios al Cliente.

IBM se suscribe a servicios de inteligencia de vulnerabilidades o a consultorías de seguridad de la información y otras fuentes pertinentes que proporcionen información actualizada acerca de las vulnerabilidades del sistema. IBM lleva a cabo evaluaciones periódicas de vulnerabilidades y resolución en su red.

IBM monitoriza el SaaS IBM para detectar, identificar, contener y resolver Incidentes de Seguridad.

IBM valida la disponibilidad, la integridad y la eficacia de la infraestructura de seguridad de la red en la que el SaaS IBM se pone a disposición, a través de los procesos de gestión de versiones de IBM.

5. Gestión de Incidentes y Notificaciones

Los equipos de IBM Watson Health trabajan conjuntamente con el Equipo de Respuesta a Incidentes de Ciberseguridad de IBM, un equipo global que gestiona la recepción, la investigación y la coordinación interna de incidentes de seguridad relacionados con ofertas de IBM, y para poner en práctica las medidas preventivas necesarias para reducir los problemas de seguridad relacionados con el software. Un "Incidente de Seguridad" es cualquier acceso, uso, divulgación, modificación o interferencia sin autorización y de forma satisfactoria respecto a los datos o las operaciones del sistema en un sistema de información utilizado por IBM para prestar el SaaS IBM. Si se descubre un Incidente de Seguridad (a través de escaneos, alertas, eventos de umbral, etc.), IBM informará y notificará al Cliente:

a. cualquier Incidente de Seguridad que implique contenido del Cliente tan pronto como sea posible y en ningún caso transcurridos 2 días laborables después de la investigación y la confirmación de dicho Incidente de Seguridad;

b. con prontitud después de cualquier solicitud de acceso, o de información acerca de, cualquier contenido del Cliente de cualquier funcionario del gobierno (incluyendo cualquier agencia de protección de datos personales o agencia de aplicación de la ley) a menos que tenga prohibido hacerlo por ley u orden pertinente; y

c. a excepción de lo permitido en el apartado titulado Controles de Acceso de este SBCA, antes de cualquier divulgación o transferencia de, o acceso a, contenido del Cliente a o por parte de un tercero.

6. Registros

IBM mantiene, de conformidad con las políticas y prácticas de IBM y las prácticas del sector generalmente aceptadas, la monitorización razonable de los sistemas frente al acceso o uso no autorizado a los Datos Procesados del Cliente. Deberán registrarse las infracciones de inicio de sesión presuntas o reales y las infracciones de acceso.

IBM mantiene un registro de todas las solicitudes de acceso y registros de las actividades de acceso para todos los sistemas que almacenan, acceden, procesan y transmiten Datos Médicos y del Cliente durante el tiempo que lo exija la ley HIPAA y otras Leyes de Datos Aplicables de IBM.

Los registros y los informes incluyen, como mínimo: (i) todos los intentos de inicio de sesión, sean satisfactorios o no, incluyendo información de identificación razonable; (ii) todos los cambios en la configuración de la red y el sistema, incluyendo instalación de aplicaciones, cambios de gestión de usuarios y modificaciones de los permisos de acceso de los archivos; (iii) intentos de acceso a recursos, sean satisfactorios o no, incluidos los intentos de acceso a cualquier archivo, recurso compartido de red, registro u otros recursos; y (iv) descargas de datos, incluyendo el tipo de contenido de los datos y el protocolo de acceso utilizados para lograr la descarga.

7. Gestión de Cambios y Desarrollo de Aplicaciones de Software

IBM sigue unas prácticas de codificación y desarrollo de aplicaciones seguras que protegen la integridad de las aplicaciones de producción y el código fuente asociado frente a modificaciones no autorizadas y no probadas.

IBM sigue un proceso de gestión de cambios que incluye (a) el registro y la aprobación formal de los cambios, y una retirada de los procedimientos; y (b) la prueba adecuada de tales cambios, incluidas las pruebas de aceptación del usuario, cuando proceda, además de las pruebas de seguridad.

IBM sigue un proceso de gestión de parches que incluye parches de prueba antes de la instalación en todos los sistemas que se utilizan para almacenar, acceder y transmitir el contenido del Cliente o se utilizan para prestar servicios, incluyendo SaaS IBM, al Cliente.

IBM requiere que los administradores de sistemas mantengan una información completa, precisa y actualizada sobre la configuración de todos los sistemas de información utilizados para almacenar, acceder y transmitir contenido del Cliente.

8. Seguridad Física y del Entorno

La plataforma IBM Watson Health Core se despliega sobre la infraestructura de datos de IBM SoftLayer. IBM SoftLayer mantiene la seguridad física y del entorno, control de acceso, controles y procesos para proteger los datos del Cliente frente a impactos o infracciones humanas, técnicas y del entorno.

El acceso general a los edificios donde se aloja el SaaS IBM se controla mediante el uso de un sistema de acceso mediante tarjeta. Hay cámaras del circuito cerrado de televisión (CCTV) instaladas en las ubicaciones y monitorizadas por personal de seguridad. Determinadas puertas de acceso cuentan con sistemas de alarma y el personal de seguridad monitoriza dichas alarmas.

El acceso a áreas controladas se restringe mediante el uso de una tarjeta de acceso y/o verificación biométrica adicional. Aquellas personas que no cuenten con acceso autorizado a las áreas controladas, deberán identificarse al entrar e ir acompañadas de una persona con acceso autorizado al área controlada. Todas las salidas de emergencia del área controlada cuentan con alarmas sonoras y el personal de seguridad se encarga de la monitorización de dichas alarmas. La verificación periódica del funcionamiento de las alarmas se ejecuta, se documenta y se conserva. Los derechos de acceso a áreas controladas se revalidan trimestralmente. El acceso a áreas controladas se revoca con la terminación del contrato.

Las instalaciones están protegidas contra factores ambientales, como el fuego, el agua y el calor, mediante alarmas de incendios, extintores, detectores de humo y sistemas de extinción de incendios. Las instalaciones están protegidas contra anomalías o interrupciones del suministro eléctrico mediante sistemas de Suministro Ininterrumpido de Energía (UPS) y generadores de reserva, cuyo mantenimiento regular incluye pruebas de funcionamiento.

Los informes y la información de conformidad de IBM SoftLayer se puede encontrar información en: http://www.softlayer.com/compliance.

9. Continuidad de las Operaciones Comerciales

IBM dispone de planes de continuidad empresarial y recuperación tras desastre que están diseñados para mantener un nivel de servicio acorde con sus obligaciones en virtud del Acuerdo. Estos planes de continuidad empresarial y recuperación tras desastre deberán actualizarse y probarse periódicamente (al menos una vez al año). IBM deberá implementar todos los cambios razonables en los planes de continuidad empresarial y recuperación tras desastre necesarios para seguir en conformidad con las prácticas del sector generalmente aceptadas, en cada caso sin interferir excesivamente en el SaaS IBM o el entorno productivo en uso por parte del Cliente.

En caso de que surja un desastre que provoque la no disponibilidad del SaaS IBM para el Cliente, IBM lo notificará lo antes posible al Cliente y activará el plan de continuidad empresarial y/o recuperación tras desastre. Cuando se declara un desastre, el objetivo de continuidad empresarial del SaaS IBM es restaurar el acceso del Cliente al SaaS IBM de la siguiente manera: en caso de una interrupción, el Objetivo de Tiempo de Recuperación (RTO) para restaurar el entorno productivo de IBM Watson Health es no superar las 36 horas siguientes a la declaración del desastre. El Objetivo de Punto de Recuperación (RPO) es no superar las 24 horas de pérdida de contenido del Cliente dentro del entorno productivo. Los objetivos de continuidad empresarial de las soluciones Watson Health específicas pueden variar.

El enfoque de IBM para la recuperación tras desastre consiste en múltiples centros de datos en áreas geográficamente dispersas.

Todos los centros de datos de IBM SoftLayer mantienen diversos alimentadores de energía, enlaces de fibra, generadores dedicados y batería de reserva. Se crean a partir de hardware y equipamiento líder del sector, proporcionando el más alto nivel de rendimiento, fiabilidad e interoperabilidad. Todos los componentes del centro de datos que deben incluirse, por ejemplo n+1 recursos de alimentación y refrigeración redundantes, son inspeccionados para mantener la estabilidad dentro de los centros de datos.

10. Cumplimiento

Las prácticas de seguridad de IBM se basan en la norma ISO 27001-27002. Estas prácticas proporcionan estructuras de control para, a título enunciativo y no limitativo, Análisis de Riesgos, Seguridad Física, Planificación de Emergencia, Investigaciones, Protección de la Información, Formación, Protección de Datos Personales y Operaciones.

IBM revisa las actividades relacionadas con la seguridad y la privacidad para que cumplan con las prácticas de seguridad de IBM.

IBM cumple las Leyes de Datos Aplicables en las Jurisdicciones Dentro de Alcance.

También se requiere un manejo adecuado de la información confidencial de los Clientes en virtud de la Directrices de Conducta Empresarial de IBM, que todos los empleados deben revisar (y certificar su revisión de las mismas) una vez al año.

11. Diversos

IBM deberá garantizar que sus acuerdos con todos los subcontratistas y/o terceros que participan en la prestación del SaaS IBM tengan condiciones que sean al menos tan protectoras de los contenidos del Cliente como los que se establecen en este SBCA, y en cualquier Documento Asociado aplicable, cada uno en la medida en que dichas condiciones sean aplicables a los servicios a prestar por dichos subcontratistas y/o terceros.