DESCRIPCIÓN SAAS HOPEX

LOS SERVICIOS AQUÍ DESCRITOS SÓLO SON APLICABLES A LA VERSIÓN ESTÁNDAR DE HOPEX. SI EL CLIENTE DESEA QUE SEAN APLICABLES A DESARROLLOS Y PERSONALIZACIONES ESPECÍFICAS, DEBERÁ SUSCRIBIRSE A LA OPCIÓN DE MANTENIMIENTO PREMIUM.

SE ADVIERTE AL CLIENTE DE QUE NEGARSE A MIGRAR A UNA VERSIÓN SOPORTADA, ADEMÁS DE NO BENEFICIARSE DE LOS SERVICIOS DE MANTENIMIENTO, INCLUIDA LA ENTREGA DE PARCHES, LE EXPONE A PROBLEMAS DE SEGURIDAD. MEGA NO SERÁ RESPONSABLE DE LAS CONSECUENCIAS QUE PODRÍAN HABERSE EVITADO SI EL CLIENTE HUBIERA MIGRADO A UNA VERSIÓN SOPORTADA O ACEPTADO LA INSTALACIÓN DE UN PAQUETE CORRECTOR O HOTFIX.

1. DEFINICIONES

PLAZO	DEFINICIÓN
Desarrollo específico / Personalización	Cualquier desarrollo específico o parametrización del producto HOPEX que modifique las funcionalidades de acuerdo con los requisitos funcionales específicos del Cliente. Las modificaciones pueden referirse a la estructura de los datos, las pantallas, los flujos de trabajo, las reglas de acceso a los datos, las interfaces que requieren desarrollo, las exportaciones específicas como un sitio web de intranet o los informes complejos que requieren programación. La gestión de usuarios y las configuraciones realizadas por los usuarios finales (como las preferencias de visualización, las consultas o las funciones estándar de elaboración de informes) no se consideran personalizaciones, sino únicamente la configuración básica del producto estándar.
Error	Comportamiento del Servicio no conforme con la Documentación. Cualquier error debe ser reproducible, tener síntomas claramente identificables y generar consecuencias funcionales en el servicio estándar.
Solución	Modo de funcionamiento alternativo para superar un Error.
Incidente	Comportamientos que no forman parte del funcionamiento estándar de los servicios, y que interrumpen el Servicio en producción o disminuyen la calidad del Servicio.
Caso	Instancia utilizada por el soporte técnico de MEGA para el seguimiento de una incidencia planteada por el Cliente.
Periodo de indisponibilidad o interrupción del servicio	Intervalo de tiempo dentro del periodo de aplicabilidad del Acuerdo de Nivel de Servicio durante el cual el Servicio no está disponible para los usuarios.
Lanzamiento o nueva versión	Nueva versión del programa, con nuevas funciones.
Fijar	Modificación del Servicio, desarrollado por MEGA para solucionar un Error. Las correcciones suelen incluirse en un parche correctivo o, a veces, en una revisión.
Paquetes Correctivos de CP o Versión Menor	Significa actualizaciones para que HOPEX sea más fiable. CP proporciona un conjunto coherente de correcciones, así como mejoras de seguridad y rendimiento aplicables a una versión de soporte a largo plazo.
Hotfix	Fijación establecida y proporcionada por MEGA fuera del contexto de una Publicación o un CP. Los Hotfixes suelen responder a Errores Críticos y sólo pueden instalarse en el último CP de una Release.

2. ACCESO AL SERVICIO

El acceso al servicio está limitado a las direcciones IP predefinidas proporcionadas por el Cliente. Las direcciones IP deben ser públicas (enrutables), estáticas y listadas.
Los usuarios itinerantes se conectarán primero al sitio de retransmisión de un Cliente, que les proporcionará una dirección IP a la que MEGA permite el acceso, y después se conectarán al Servicio.
Además, el Cliente informa inmediatamente a MEGA de cualquier incidente relacionado con el acceso al Servicio. El Cliente tiene que no interferir ni interrumpir el servicio, incluidos los servidores del proveedor de alojamiento de MEGA o de MEGA, y cumple las recomendaciones, procedimientos y normas comunicados por MEGA de vez en cuando para el uso adecuado del Servicio.

3. CREDENCIALES DE USUARIO

MEGA proporcionará las credenciales de usuario para permitir que el administrador del cliente, el responsable de configurar las credenciales para otros usuarios.

El cliente debe tomar todas las medidas necesarias para garantizar la confidencialidad de las credenciales del usuario. MEGA no será responsable de ningún daño resultante del uso del servicio por un tercero no autorizado. En caso de pérdida o divulgación por parte de un usuario de su información de inicio de sesión a un tercero no autorizado, el Cliente deberá notificarlo a MEGA por escrito sin demora. Por motivos de seguridad, MEGA puede exigir en cualquier momento al Cliente que cambie una contraseña o elimine un ID de usuario sin consentimiento previo.

4. DISPONIBILIDAD DEL SERVICIO

MEGA hará todos los esfuerzos razonables para que los servicios estén disponibles tal y como se establece en el mismo, excepto:

- Durante los periodos de mantenimiento. El mantenimiento programado está sujeto a un preaviso razonable, mientras que el mantenimiento no planificado estará sujeto a un preaviso de 1 día laborable (excepto en caso de Incidentes de Seguridad);
- Como resultado de cualquier circunstancia fuera del control de MEGA, como interrupciones de Internet y cualquier otro caso de Fuerza Mayor;
- En caso de cualquier problema de seguridad, como un uso anormal, fraudulento o abusivo de los servicios, cualquier intrusión, acceso fraudulento a los servicios por parte de un tercero, o extracción ilegal de la totalidad o parte de los datos, etc., el Cliente será responsable de pagar los costes ocasionados por los servicios.

MEGA hará todo lo posible por minimizar las consecuencias y restablecer el Servicio una vez hayan cesado las causas mencionadas.

DISPONIBILIDAD DEL SERVICIO	DESARROLLO	PRODUCCIÓN
Duración máxima de la interrupción no programada	1 día laborable	3 horas laborables
Máxima interrupción mensual no programada	1 día laborable	4 horas laborables

Todos los periodos de indisponibilidad se computan en el cálculo de la interrupción establecido anteriormente, excepto:

- Períodos de indisponibilidad programados, como los períodos autorizados previamente por el Cliente en el marco de operaciones de gestión de cambios.
- Períodos de indisponibilidad no programados resultantes de la exención de responsabilidad establecida en esta sección.

La interrupción se computa desde el momento en que el Cliente se pone en contacto con MEGA: declaración de *No Acceso* desde la sección de Soporte de nuestra Comunidad (https://community.mega.com).

En caso de incumplimiento de los compromisos de disponibilidad, el Cliente podrá solicitar un crédito de servicio. Un crédito de servicio representa el número de días adicionales de Servicio (además del periodo de suscripción actual) concedidos al Cliente por interrupción. Todo crédito de servicio debe solicitarse por escrito. Dicha solicitud debe realizarse dentro del periodo de 3 meses siguiente a la fecha del evento generador. El crédito de servicio es el único y exclusivo recurso del Cliente en caso de indisponibilidad del servicio.

El periodo de disponibilidad del Servicio es de 9 a 18 horas, de lunes a viernes, excluidos los días festivos bancarios.

5. LIMITACIÓN DE LA RESPONSABILIDAD DE MEGA

La responsabilidad de MEGA quedará limitada o excluida en los siguientes casos:

- El incumplimiento por parte del cliente de las instrucciones de uso del servicio establecidas en la documentación y la guía del usuario;
- Degradación del rendimiento debida a la configuración de la red del cliente y a los dispositivos de seguridad;
- Incidente debido a un producto de software instalado en el sistema informático del Cliente.
- Indisponibilidad del punto de contacto del cliente durante una interrupción.
- Negativa del Cliente a proporcionar puntualmente información (o autorización para acceder a ella) que pudiera permitir a MEGA solucionar una Incidencia o un Error.

6. GRAVEDAD DEL INCIDENTE Y TIEMPO DE RESPUESTA

SEVERIDAD	SITUACIÓN	TIEMPO DE RESPUESTA Y EXPECTATIVAS
Sin acceso	Cuestiones de seguridad Plataforma caída/No hay acceso para todos los usuarios	1 hora laborable
Crítica	Degradación significativa de una o más funcionalidades Impacto empresarial crítico	Contacto con el cliente en un plazo de 4 horas laborables. Esfuerzo continuo diario durante las horas de trabajo. Escalado rápido al soporte técnico y a los jefes de producto. Asignación rápida de los recursos adecuados. Establecimiento de un plan de reparación. Dependiendo de la complejidad del error, se puede proporcionar una solución para minimizar la interrupción operativa.
Moderado	Degradación de la funcionalidad. El trabajo puede continuar satisfactoriamente, pero deteriorado. Impacto empresarial moderado Impacto empresarial moderado.	Contacto con el cliente en el plazo de 1 día laborable. Asignación de recursos para mantener un esfuerzo constante durante las horas de trabajo. Se puede proporcionar un plan de reparación.
Menor	Degradación menor de una o más funcionalidades. Sin impacto empresarial.	Contacto con el cliente en un plazo de 2 días laborables. Haga todo lo posible durante el horario laboral.

El tiempo de respuesta se calcula a partir del día siguiente al que el Cliente notifica el Error a MEGA a través del Centro de Soporte accesible desde la Comunidad Online.
El soporte técnico de MEGA puede reducir el nivel de gravedad si el Cliente es incapaz de proporcionar los recursos o respuestas necesarios para permitir a MEGA continuar con sus esfuerzos para resolver la Incidencia.
Los servicios de soporte estándar no incluyen la asistencia in situ. En casos específicos, y tras la aprobación por parte del Cliente de los términos y condiciones de la intervención de MEGA, MEGA puede intervenir en las instalaciones del Cliente a su discreción. El Cliente proporciona a MEGA acceso a los recursos del Cliente y a personal suficientemente cualificado para dar cualquier información que pueda necesitar. El Cliente pone a disposición los datos necesarios para la asistencia y garantiza que tiene todos los derechos de propiedad intelectual sobre los elementos de terceros puestos a disposición de MEGA.

7. POLÍTICA DE CICLO DE VIDA

DEFINICIÓN	DESCRIPCIÓN
Publique (Ayuda a largo plazo)	Nueva versión de Hopex mantenida durante los siguientes periodos: en Soporte Completo durante un periodo de 27 meses, después en Soporte Limitado durante un periodo de 9 meses, y regularmente mejorada por CP. La duración específica de cada versión está disponible en la comunidad MEGA.
Soporte completo	Período durante el cual el Cliente recibe servicios de mantenimiento y soporte, incluida la mejora de las funciones existentes, la adición de nuevas funciones y productos, y los Parches.
Apoyo limitado	Periodo posterior al periodo de Soporte Completo, durante el cual sólo se podrán solucionar Incidencias Críticas del Cliente mediante Hotfixes.

8. PLAN DE COPIAS DE SEGURIDAD Y RECUPERACIÓN EN CASO DE CATÁSTROFE (DRP)

8.1. Copia de seguridad.
Como parte de los servicios de alojamiento (no opcionales), MEGA se compromete a realizar el número de copias de seguridad de datos establecido en esta sección.
En caso de desastre que afecte a sus servidores de alojamiento, MEGA se compromete a restaurar los Servicios en el plazo definido en este documento.
Por defecto, la restauración se realiza a partir de la última copia de seguridad. Todas las demás copias de seguridad conservadas de acuerdo con los términos de este documento se consideran archivos y pueden restaurarse .

RESPALDO	DIARIO	SEMANAL	MENSUAL
Período de conservación de las copias de seguridad de una copia de seguridad periódica	7 días	4 semanas	6 meses
Hora de restaurar	Última copia de seguridad: 4 horas laborables Archivo: 6 horas laborables		

8.2. Plan de recuperación en caso de catástrofe.
El Cliente se beneficia de un Plan de Recuperación de Desastres en caso de Error que afecte a la base de datos o de un problema que afecte a los servidores que alojan la Plataforma, las soluciones y/o los datos del Cliente.
MEGA se compromete a:

- Realizar copias de seguridad de los datos del Cliente según una frecuencia predefinida. Esta última se refiere a la última copia de seguridad, que utiliza para realizar su plan de recuperación (RPO),
- Restaurar los datos del Cliente a partir de la última copia de seguridad dentro del plazo definido a continuación. Este tiempo de recuperación (RTO) requerido por MEGA para restaurar los servicios.

El cliente puede suscribirse, a su entera discreción, a la opción "DRP avanzado" para beneficiarse de una mayor frecuencia de copias de seguridad y/o de un menor tiempo de recuperación.

	Objetivo de tiempo de recuperación (RTO)	Objetivo del Plan de Recuperación (OPR)
Oferta estándar	1 semana	25 horas
Con la opción DRP avanzado	24 horas	25 horas

9. PRUEBAS DE PENETRACIÓN

MEGA llevará a cabo pruebas anuales de penetración de terceros en su Servicio SaaS. Dichas pruebas se realizarán sobre las Versiones de Soporte Completo (último CP), disponibles en el mercado el día de la prueba de penetración (pen test). Cualquier otra solicitud del Cliente estará sujeta a tarifas adicionales. Previa solicitud, MEGA proporcionará al Cliente una carta de opinión y un informe ejecutivo de los resultados de dichas pruebas de penetración (pen test).

10. SOLICITUDES DE SERVICIO

Una Solicitud de Servicio es una petición formalizada de intervención en la(s) plataforma(s) SaaS del Cliente.
Las únicas personas autorizadas para realizar Servicios de solicitud son las designadas por el Cliente como "Contactos de MEGA".

10.1. Servicios incluidos en la norma.

Categoría de servicio	Nombre del departamento	Descripción del servicio	Frecuencia/cantidad máx.	Tiempo de respuesta
Gestión de versiones	Actualización de la aplicación	Despliegue de una actualización HOPEX en una de las plataformas SaaS (DEV; PRE-PROD; PROD); HotFix, Patch, Release.	4 al año	HotFix, parche correctivo 2 días laborables (PPROD primero) Versión Debe planificarse con antelación
Gestión de usuarios	Inicio de sesión de usuario	Proporcione un archivo de registro (formato TXT) que indique todas las conexiones de usuario, incluidas las licencias de usuario, los nombres de usuario, los perfiles y la disponibilidad de la plataforma.	1 al mes	1 día laborable
	Reasignar un usuario/perfil a una licencia token	Con licencias con nombre, reasigne un usuario a un modelo de licencia basado en tokens. Un usuario puede ser: usuario principal, colaborador o lector. Este servicio no se aplica a las licencias flotantes.	10 reasignaciones (todos los usuarios) al año	
Gestión de accesos	Cambiar el nombre de dominio del servicio	Cambie la URL de acceso a HOPEX Cloud de un nombre de dominio "aaa.hopexcloud.com" a "bbb.hopexcloud.com".	2 cambios al año	2 días laborables
	Declarar rangos de direcciones IP adicionales en la lista de acceso permitido	Añada hasta 5 rangos de direcciones IP adicionales a la lista de direcciones IP que pueden acceder al paquete de software HOPEX.	3 solicitudes al año	1 día laborable
Gestión de la integración	Programación de tareas	Programar tareas recurrentes con carga o descarga (si procede) hacia y desde el entorno del Cliente mediante un Protocolo Seguro de Transferencia de Archivos (SFTP). Las tareas programadas son principalmente de importación/exportación y generación de sitios web estáticos. El diseño, la fabricación y la validación de los elementos que deben planificarse siguen siendo responsabilidad del Cliente.	6 solicitudes al año	2 días laborables (PPROD primero)
	Despliegue de servicios web	Despliegue de un Servicio Web en producción. Diseñar, realizar y validar un Servicio Web sigue siendo responsabilidad del Cliente.		3 días laborables (PROD primero)
Tienda HOPEX	Despliegue de un módulo	Lista de módulos evolutivos: https://store.mega.com/modules	10 solicitudes al año	2 días laborables (PPROD primero)

Las solicitudes de servicio están sujetas al presente Acuerdo de Nivel de Servicio.
Cualquier cambio en la frecuencia y/o cantidad máxima de solicitudes de servicio está sujeto a cargos adicionales.
Además, MEGA sólo podrá comprometerse con solicitudes de servicio si:

- La solicitud de servicio se abre desde el sitio web de la Comunidad MEGA (no se tramitará ninguna solicitud de servicio enviada por correo electrónico);
- El Contacto de MEGA reconoce que ha facilitado a MEGA toda la información necesaria para llevar a cabo una solicitud de servicio. Se deducirá el tiempo necesario para recopilar información.

Para solicitudes que no figuran en el catálogo de solicitudes de servicio:

- Tiempo estimado de respuesta: 2 días laborables
- Estudio y tratamiento según la solicitud

10.2. Niveles de servicio del "Paquete Plataforma SaaS".

Niveles de servicio	Tipo de plataforma	Número de pases a producción
Inicio	Preproducción y producción	1 al año
Estándar	Desarrollo, preproducción y producción	4 al año
Avanzado	Desarrollo, preproducción y producción	12 al año

11. OPCIONES DE SERVICIOS AMPLIADOS

MEGA propone una serie de servicios opcionales en la suscripción SaaS, que incluyen mantenimiento premium, servicios de adopción y servicios de administración, como se describe a continuación. Estos servicios se denominan Servicios Ampliados y su objetivo es ofrecer a los clientes una experiencia de soporte y postimplementación premium.

11.1. Mantenimiento Premium

Objeto	Descripción
Soporte Premium	
Seguimiento mensual proactivo	Reuniones mensuales para informar sobre la resolución de casos con un único punto de contacto
Seguimiento de los indicadores sanitarios	Revisión mensual de los indicadores de salud, incluido el número de casos y los acuerdos de nivel de servicio.
Mantenimiento de las personalizaciones	
Corrección de configuraciones/personalizaciones, incluida la documentación	Apoyar y corregir las modificaciones que únicamente haya realizado MEGA. Esto también incluye las modificaciones necesarias para actualizar el servicio.
Gestión de actualizaciones	
Actualización-Validación funcional	Realice la validación funcional de la configuración después de actualizar a la última versión de HOPEX.
Gestionar el impacto de las versiones menores en los usuarios	Evaluar el impacto de cualquier cambio de actualización en la base de usuarios. Esto dará lugar a actividades como la comunicación con los usuarios y la identificación de los usuarios que requieren formación adicional.

11.2. Paquete de adopción

Objeto	Descripción
Evaluación y control de la madurez	
Talleres de evaluación de la madurez	Talleres funcionales anuales destinados a mejorar la adopción, el uso de HOPEX y la demostración de valor, basados en la metodología de evaluación de la madurez de MEGA, incluidos un experto en preventa y un CSM.
Seguimiento de las recomendaciones	Seguimiento de la adopción de HOPEX mediante indicadores clave. y aplicación de las recomendaciones de los expertos
e-Learning	
Sesiones eLearning	Sesiones de eLearning para aumentar la adopción dentro del equipo

11.3. Servicios gestionados

Objeto	Descripción
Gestión del acceso	
Gestión del modo de autenticación HOPEX	Gestionar el modo de autenticación HOPEX de los usuarios HOPEX.
Gestionar funciones empresariales	Asignar roles empresariales. Un rol empresarial define la función de una persona o un grupo de personas en la empresa. Un rol empresarial se define a nivel de repositorio.
Gestionar grupos de personas	Establecer, eliminar y configurar grupos de personas en un grupo que comparte la misma conexión. Un grupo de personas es una lista de personas que pertenecen al mismo grupo.
Acceso de usuarios/gestión de grupos	Establezca, elimine y configure usuarios, grupos de usuarios, perfiles de usuario y niveles de acceso y autorización.
Definir reglas de acceso a los datos	Establecer, eliminar y configurar estructuras de autorización de usuarios.
Restablecer la contraseña de un usuario	Establecer/restablecer la contraseña de usuario (esto sólo incluye el restablecimiento de la contraseña para los usuarios de MEGA).
Gestión de contenidos - Trabajo de los usuarios	
Gestionar objetos duplicados	Identificar los objetos duplicados (en colaboración con los propietarios de los contenidos), validar la duplicación y realizar acciones para eliminar los duplicados, es decir, fusionarlos o eliminarlos.
Gestionar objetos aislados	Identificar los objetos aislados para permitir la asignación de propiedad, la identificación para la supresión, el informe de los objetos que no figuran en los diagramas (cuando se espera que sean descritos por diagramas), el informe de los objetos no incluidos en las asociaciones.
Gestionar objetos para su eliminación	Borrar objetos, donde el usuario que modela no tiene privilegios para borrar objetos creados fuera de sus transacciones actuales. Los objetos pueden ser marcados para su eliminación por los usuarios.
Gestionar la fusión de objetos	Fusionar objetos (es decir, duplicados) dentro de un repositorio.
Gestionar el acceso a los datos	Configure y mantenga niveles de autorización de objetos que permitan/prohiban la modificación de objetos por parte de un usuario/perfil de usuario específico.
Gestionar la protección de objetos	Activar o desactivar la protección de objetos específicos dentro de un repositorio.
Gestión de contenidos - Administración	
Comparar y alinear repositorios/subconjuntos de contenidos	Comparar y promover objetos/ámbito de objetos de repositorios separados. El repositorio de destino puede alinearse con el repositorio base.
Copia de seguridad lógica del grupo de contenidos	Crear una línea de base lógica para un grupo de contenido específico (ámbito, es decir, biblioteca, proyecto, etc.), lo que permite la creación de líneas de base independientes de segmentos del contenido del repositorio.
Gestionar bibliotecas	Configurar y mantener bibliotecas y garantizar una estructura de contenidos clara dentro del repositorio. Las bibliotecas pueden utilizarse para separar lógicamente el contenido del repositorio.
Crear consultas e informes	Escribir consultas que queden registradas y disponibles para que todos los usuarios del entorno puedan reutilizarlas. Configurar informes basados en las capacidades de Report Studio.
Gestión de flujos de trabajo	Gestionar la transición de flujos de trabajo para apoyar la aprobación, autorización y movimiento de objetos. Supervisar las acciones y reasignaciones de los flujos de trabajo.
Importación de datos	Gestione la importación periódica de datos utilizando las plantillas XLS existentes.
Gestión de incidentes	
Gestionar el apoyo interno	Gestionar el primer nivel de soporte en los casos de uso funcional del cliente, en el contexto de una plataforma personalizada.
Gestionar el seguimiento de los casos	Crear, priorizar y realizar el seguimiento de los casos con el Soporte Técnico de MEGA. Proporcióneles todos los elementos necesarios para diagnosticar el problema planteado.
Formación y apoyo	
Orientación	Proporcionar mejores prácticas y orientación estándar sobre el uso de HOPEX
Transcripción de modelos	Gestionar la transcripción manual de modelos existentes (MS Word, PPT, Visio, ...) o de datos estructurados (formato XLS) a HOPEX. No aplicable a la carga en masa.
Gestionar el mantenimiento de diagramas	Actualizar los diagramas existentes basándose en una solicitud de cambio formalizada. Gestionar el impacto en los dibujos de los cambios en los conceptos de datos básicos.
Orientación	Proporcionar mejores prácticas y orientación estándar sobre el uso de HOPEX
Integración y formación de los usuarios	Integración y formación de nuevos usuarios a partir de la documentación y los materiales de formación existentes.
Modelización EA	Desde la entrevista de la PYME hasta la validación de su activo EA en los diagramas de HOPEX
Incorporación y formación de los usuarios	Incorporar e impartir formación a los nuevos usuarios finales basándose en la documentación y los cursos de formación existentes para los clientes.
Evolución continua	
Configuración	Evolución de la configuración existente.

12. CONTACTOS Y GOBERNANZA

Tras la ejecución del Contrato, el Cliente nombra un máximo de 3 contactos designados, formados en los servicios, y a los que MEGA prestará servicios de soporte. Los contactos designados deben ser capaces de realizar al menos las siguientes funciones:

- Gestionar los usuarios y su asignación a los distintos perfiles de la(s) solución(es) de MEGA que constituyen el Servicio;
- En caso de incidente:
  - Declarar un Caso en el portal MEGA recopilando y proporcionando toda la información necesaria relacionada con las circunstancias en las que se produjo el Incidente;
  - Informe inmediatamente de cualquier problema de seguridad por el medio más adecuado;
- Para una mayor eficacia operativa, participe en las reuniones de gestión y arbitraje establecidas por MEGA .

13. REVERSIBILIDAD

Los datos del Cliente se conservan durante un periodo de 3 meses a partir de la fecha de finalización o expiración de los Servicios. Durante este periodo, el Cliente ya no tendrá acceso a los servicios. El único propósito de este periodo es permitir al Cliente establecer un periodo de reversibilidad en caso de necesidad. Al final de este periodo de 3 meses, los datos se borrarán de forma permanente.

El cliente puede solicitarlo:

- Sólo se conservarán los datos durante un periodo superior a dicho plazo de 3 meses.
- O para ejecutar servicios de reversibilidad, como se define a continuación.

Cualquier prórroga del periodo de conservación y/o de los servicios de reversibilidad deberá ser recibida por MEGA a más tardar 2 meses después de la fecha efectiva de terminación o expiración de los servicios.

La ampliación de los servicios de retención y/o reversibilidad se facturará de acuerdo con la lista de precios de MEGA en vigor en la fecha en que MEGA envíe su presupuesto al Cliente.

La finalidad de los servicios de reversibilidad es la recuperación de los datos del Cliente dentro de la base de datos HOPEX.

MEGA ofrece dos tipos de servicios de reversibilidad: básica y compleja.

- Reversibilidad básica: MEGA proporciona al Cliente copias de seguridad de los datos de producción para su restauración en la misma versión de MS-SQL-Server DBMS para un uso con la misma solución HOPEX en la misma versión.
  Los datos se pondrán (i) a disposición del Cliente en un Servidor FTP de MEGA para su descarga, o (ii) se enviarán (SFTP) al servidor del Cliente o de su proveedor. Es responsabilidad exclusiva del Cliente conceder el derecho de acceso al repositorio. MEGA recomienda la formación adecuada para la administración de la solución.
- Reversibilidad compleja: estos servicios son aplicables cuando la reversibilidad básica no se ajusta a las necesidades del cliente. Pueden ser apropiados cuando los datos deben cargarse en una solución de software alternativa.
  El propósito de una Reversibilidad Compleja es proporcionar.
  - Una exportación XML codificada en UTF-8 del volcado de la base de datos;
  - Documentación sobre cómo procesar el formato XML;
  - Transferencia reconocida de competencias tanto funcionales como técnicas al equipo encargado de la toma de posesión, para la comprensión del modelo de datos de la solución, así como de las especificidades de la solución implantada, y de la exportación proporcionada.

  El cliente es responsable de que los datos transferidos sean exactos y se integren plenamente en la nueva solución.
  La Reversibilidad Compleja estará sujeta a un precio fijo.
- Otros: Si el Cliente desea solicitar servicios complementarios, deberá enviar a MEGA su requerimiento detallado por escrito. MEGA realizará un estudio de viabilidad y/o enviará un presupuesto.

14. CÁLCULO DEL TIEMPO

Cuando un periodo se indica en horas, se computa 7 días a la semana y 24 horas al día.

Cuando un periodo se indica en horas laborables, se computa para cada día laborable, de 9 de la mañana a 6 de la tarde. La zona horaria aplicable es la correspondiente a la ubicación de la filial de MEGA contratista del Cliente.

No se tiene en cuenta el momento del suceso o notificación que provoca el inicio del plazo.

Cuando un periodo se indica en días hábiles, se computa considerando únicamente los días de la semana, de lunes a viernes, excluyendo los días festivos aplicables a la filial de MEGA que es contratista del Cliente.

No se tiene en cuenta el día del acontecimiento o de la notificación que provoca el inicio del plazo.

Cuando un periodo se expresa en meses, se calcula teniendo en cuenta la fecha.

No se tiene en cuenta el día del acontecimiento o notificación que provoca el inicio del plazo.

A falta de una fecha similar, el plazo se amplía al primer día hábil siguiente, hasta medianoche.

Cuando un plazo se indica en horas, expira al final de la hora.

Cuando un plazo se indica en días o meses, expira al final del último día a las 12 de la mañana.

Un plazo expresado en días que vencería en sábado, domingo o festivo se amplía al primer día laborable siguiente, hasta medianoche.

Las notificaciones por carta certificada con acuse de recibo, se considerarán en la fecha de la primera presentación de la carta con acuse de recibo, el matasellos como prueba.

15. COMPROMISO DE SEGURIDAD DE MEGA

15.1. Seguridad mundial

Asunto	Descripción
TLS	Necesario en las plataformas HOPEX Cloud para garantizar la seguridad de las transacciones entre el front-end web y el terminal del Cliente. El certificado basado en el cifrado TLS 1.2 AES256-SHA256 está totalmente a cargo del equipo MCS (MEGA Cloud Services).
Lista blanca de IP públicas	Las direcciones IP públicas de los Clientes deben facilitarse a MEGA con antelación para poder acceder a los servicios.
Plataforma para un único inquilino	Todas las plataformas de los clientes son totalmente Singletenant. Los entornos de cada cliente se instalan en un servidor dedicado, en una VLAN dedicada totalmente segregada de los demás.
Se despliegan plataformas virtuales totalmente segregadas entre sí	Las plataformas HOPEX Cloud suelen desplegarse en modo estándar con un servidor virtual por Cliente para el entorno de Producción. Al suscribirse al nivel de servicios Estándar o Premium del "Paquete de Plataforma SaaS", se despliegan tres instancias aisladas, como : • DESARROLLO: Servidor dedicado que permite al cliente personalizar las soluciones HOPEX y probar las actualizaciones; • PRE-PRODUCCIÓN: Servidor dedicado sincronizado bajo demanda con la plataforma de Producción, que permite al Cliente validar y probar las actualizaciones antes de su implementación en Producción (por ejemplo, ajustes técnicos y funcionales, parche correctivo CP); • PRODUCCIÓN: Los contenidos desplegados en Producción son previamente probados y aprobados en la plataforma de Preproducción.
Cifrado de datos	Cifrado de almacenamiento estándar de Microsoft Azure SSE mediante cifrado AES-256 bits

15.2. Organización y gestión de la seguridad de la información .

Asunto	Descripción
Organización de la seguridad de la información y gestión del riesgo informático	MEGA ha implantado una política de seguridad de la información que incluye a todo su personal. Las principales funciones del personal de MEGA son: • La alta dirección aprueba, fomenta y apoya las medidas para mejorar la seguridad de los sistemas de información; • El Director de Seguridad de la Información (CISO) es responsable de la seguridad, disponibilidad e integridad del sistema de información; • El Director de Información (CIO) es responsable del funcionamiento y la dirección estratégica del sistema de información; • Se crean comités de seguridad para tratar todos los temas de seguridad, riesgos, incidentes y cumplimiento de la normativa.
Gestión del riesgo empresarial	MEGA ha diseñado e implantado un programa de Gestión de Riesgos Empresariales para analizar y mitigar los riesgos de forma proactiva para todas las actividades de MEGA.
Normas de garantía independientes evaluación	La oferta HOPEX Cloud Enterprise está sujeta a una auditoría anual SOC2 realizada por un tercero independiente.

15.3. Políticas de seguridad de la información .

Asunto	Descripción
Política de seguridad de los sistemas de información	Esta es la política de seguridad de los sistemas de información que ha sido aplicada y validada por la dirección de MEGA y comunicada a las partes interesadas. Este documento se revisa anualmente.
Procedimientos y políticas	Las políticas de seguridad de la información (clasificación de datos, criptografía, contraseñas, etc.), normas, procedimientos y directrices se publican en la intranet, se revisan y se comunican anualmente.
Certificación SOC 2 Tipo 2	MEGA certifica que, en la fecha de firma del presente Contrato, los servicios cumplen los criterios para la certificación SOC2 Tipo 2. En aras de la claridad, MEGA no se compromete a mantener este cumplimiento a lo largo de todo este Acuerdo.

15.4. Gestión de activos .

Asunto	Descripción
Responsabilidad de los activos	MEGA identifica los activos de la organización (inventario, propiedad, uso aceptable y devoluciones) y define las responsabilidades de protección apropiadas.
Clasificación de la información	MEGA implantó un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información
Tratamiento de los medios de comunicación	MEGA ha realizado una mejora de la política de seguridad para todos los equipos informáticos de CSM. No se permiten dispositivos de almacenamiento extraíbles en las plataformas.

15.5. Seguridad de los recursos humanos .

Asunto	Descripción
Antes de la contratación	MEGA realiza las comprobaciones y balances necesarios de todos los solicitantes de empleo de acuerdo con las leyes, reglamentos y normas éticas aplicables y de forma proporcional a las necesidades de la empresa, la clasificación de la información a la que se accede y los riesgos percibidos.
Durante el empleo	Los empleados y usuarios externos de MEGA siguen un programa de concienciación sobre seguridad. Reciben instrucción, formación y actualizaciones periódicas sobre políticas y procedimientos de seguridad según lo requiera su función laboral.
Cese y cambio de empleo	MEGA cuenta con un proceso de RRHH para gestionar cualquier rescisión o cambio de empleo.

15.6. Seguridad física y medioambiental .

Asunto	Descripción
Zonas seguras	MEGA definió perímetros de seguridad y una política física para proteger las zonas que contienen información sensible o crítica y las instalaciones de tratamiento de la información.
Equipamiento	MEGA ha implantado medidas físicas para proteger sus equipos de accesos no autorizados y cortes de electricidad. Todos los soportes de almacenamiento se escanean antes de su reutilización o desmantelamiento para garantizar que los datos confidenciales y el software con licencia se han eliminado o sobrescrito de forma segura. MEGA ha adoptado una política de seguridad de la información para los puestos de trabajo: protección de documentos en papel y soportes de almacenamiento extraíbles, bloqueo de pantalla. La oferta HOPEX Cloud Enterprise se basa en la infraestructura de Microsoft Azure, que cumple una amplia gama de normas internacionales de cumplimiento específicas del sector, como ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2, así como normas específicas de cada país, como Australia IRAP, UK G-Cloud y Singapore MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

15.7. Control de acceso.

Asunto	Descripción
Control de acceso	La política de acceso global de MEGA se basa en el principio del menor privilegio. El CISO (Chief Information Security Officer) realiza revisiones periódicas.
Gestión del acceso de los usuarios	La administración de las Plataformas en la Nube de HOPEX sólo es accesible por el equipo de MCS (MEGA Cloud Services) a través de un servidor bastión que registra (log y vídeo) todas las acciones realizadas en las plataformas del Cliente. La dirección IP pública del Cliente debe ser proporcionada al equipo MCS para conectar el servicio.
Responsabilidades de los usuarios	A cada Cliente se le concede un acceso de Administrador funcional de HOPEX que permite al Cliente gestionar todos los usuarios dentro del repositorio de HOPEX. Este administrador es también el contacto entre la empresa del Cliente y MEGA.
Control de acceso a sistemas y aplicaciones	La autenticación en el servicio HOPEX Cloud puede realizarse a través de un SSO utilizando los protocolos SAML 2.0, OpenID Connect (OIDC).

15.8. Seguridad operativa - Seguridad del sistema .

Asunto	Descripción
Procedimientos operativos y responsabilidades	MCS documentó todos los procedimientos operativos siguiendo las mejores prácticas de ITIL (CAB) para mantener las plataformas de los clientes en condiciones óptimas.
Protección frente al malware	MEGA ha implantado controles de detección, prevención y recuperación para proteger contra el malware. Estas medidas técnicas se combinan con una adecuada concienciación de los administradores.
Copia de seguridad	En las plataformas en la nube de HOPEX se realizan copias de seguridad periódicas cifradas automáticas que permiten recuperar los datos de producción del cliente en caso de incidente.
Registro y control	En las plataformas HOPEX Cloud Enterprise, además de la herramienta de supervisión HOPEX Server Supervisor integrada en todas las plataformas de los clientes, que permite al administrador de HOPEX hacer un seguimiento de todas las acciones realizadas en el sistema (por ejemplo, autenticación de usuario correcta/incorrecta, modificación del perfil/derechos del usuario, etc.), todos los registros de la plataforma se registran a través de una solución de terceros de MCS para su análisis. El equipo de MCS supervisa continuamente la disponibilidad de las plataformas de cada cliente mediante un sistema de supervisión dedicado que permite notificar a los administradores de MCS en caso de anomalía.
Control del software operativo	MCS gestiona el sistema de información según las recomendaciones de ITIL (gestión de cambios, etc.).
Gestión técnica de la vulnerabilidad	MEGA R&D utiliza la solución Coverity para escanear las vulnerabilidades del código fuente de HOPEX (comprobación diaria). En cada versión importante se realiza una auditoría de terceros. MEGA diseñó un proceso de vulnerabilidad para gestionar las amenazas y vulnerabilidades de sistemas, software y aplicaciones de forma eficaz y oportuna, mitigando el riesgo de explotación y compromiso potenciales.
Consideraciones sobre la auditoría de sistemas de información	Mantenimiento programado (sistema operativo, hardware, etc.): Los mantenimientos del sistema y del software se realizan durante el fin de semana durante un par de horas. Mantenimiento no programado: Los despliegues de parches, personalizaciones o actualizaciones críticas de HOPEX podrán realizarse fuera del horario laboral y planificarse conjuntamente con el Cliente.

15.9. Seguridad de las comunicaciones - Seguridad de las redes .

Asunto	Descripción
Gestión de la seguridad de las redes	Todas las plataformas de cliente son dedicadas (Singletenant). Cada plataforma de cliente está instalada en un servidor dedicado aislado de los demás dentro de una VLAN independiente. Cada plataforma tiene su propio cortafuegos (MS Azure Network Security Group) para reforzar y controlar el tráfico de red.
Transferencia de información	Las transacciones web deben estar encriptadas TLS para asegurar las transacciones entre el servidor o servidores web y el sitio o sitios del Cliente. El certificado TLS 1.2 basado en el cifrado AES256-SHA256 está totalmente gestionado por el servicio MCS (MEGA Cloud Services). Además, las direcciones IP públicas del Cliente deben proporcionarse a MEGA para unirse al servicio. Esta medida técnica va acompañada de una concienciación sobre la seguridad de los datos para los administradores y de un acuerdo de confidencialidad y no divulgación. En el caso de una transferencia de datos, éstos deben transmitirse mediante una transferencia de tipo SFTP.

15.10. Adquisición, desarrollo y mantenimiento del sistema .

Asunto	Descripción
Requisitos de seguridad de los sistemas de información	MEGA entrega las versiones principales cada 18 a 24 meses y las versiones secundarias cada 3 meses, incluidos todos los parches de seguridad y las evoluciones.
Seguridad en los procesos de desarrollo y soporte	El diseño de HOPEX está totalmente gestionado por MEGA. El departamento de I+D de MEGA cuenta con un SSM (Software Security Manager) encargado de: • Definición de las mejores prácticas de codificación desde el punto de vista de la seguridad; • Revisar todas las especificaciones de los proyectos de desarrollo desde el punto de vista de la seguridad; • Gestionar personalmente el desarrollo de módulos relacionados con la seguridad (autenticación, etc.); • Gestión de campañas de escaneado de códigos y seguimiento de las medidas paliativas. MEGA no recurre a la externalización del desarrollo para diseñar su solución. En caso de que los clientes necesiten personalizar su plataforma HOPEX (por ejemplo, cambios en el metamodelo), se requiere un HOPEX Cloud Workbench opcional.
Datos de la prueba	MEGA utiliza una base de datos de prueba con datos ficticios.

15.11. Aspecto de la seguridad de la información en la gestión de la continuidad de las actividades .

Asunto	Descripción
Continuidad de la seguridad de la información	La integridad de los datos está garantizada por la tecnología de almacenamiento georredundante (GRS), que permite replicar los datos de copia de seguridad en un centro de datos secundario que tiene el mismo nivel de seguridad que el centro de datos primario.
Despidos	MEGA Implantó todos los servicios de suministro de dispositivos para garantizar una alta disponibilidad
Plan de continuidad de las actividades	MEGA diseñó e implantó un Plan de Continuidad de Negocio. 9 escenarios de alto nivel que podrían poner en peligro la continuidad de la actividad, junto con respuestas predefinidas para una gestión óptima de los problemas.

15.12. Gestión de incidentes de seguridad de la información .

Asunto	Descripción
Gestión de incidentes y mejoras en la seguridad de la información	MEGA implantó un proceso de gestión de incidencias para restablecer el funcionamiento normal del servicio lo antes posible y minimizar el impacto adverso en las operaciones comerciales, garantizando así el mantenimiento de los mejores niveles posibles de calidad y disponibilidad del servicio. Este proceso incluye un procedimiento de escalada.

15.13. SOC 2 SEGURIDAD ADICIONAL

Asunto	Descripción
Almacenamiento cifrado	Las plataformas de los clientes se encuentran en almacenes cifrados.
CyberArk Bastion	Las sesiones de los administradores en las plataformas de los clientes se registran a través de bastion