ACUERDO DE ENCARGO DE TRATAMIENTO

El presente Acuerdo de Encargo de Tratamiento, forma parte de las CGC y de las CONDICIONES ESPECÍFICAS (de forma conjunta "Contrato") mediante el cual SESAME HR actuará en calidad de Encargado del Tratamiento y el CLIENTE en calidad de Responsable del Tratamiento.

ACUERDO DE ENCARGO DE TRATAMIENTO SUJECIÓN RGPD

El presente ACUERDO DE ENCARGO DE TRATAMIENTO solo será de aplicación si el CLIENTE y/o SESAME HR estén sujetos al RGPD.

CLÁUSULAS

1. **Objeto.**

Para ejecutar las prestaciones derivadas del Contrato, el Encargado del Tratamiento podrá tener acceso a datos de carácter personal responsabilidad del Responsable del Tratamiento.

2. **Identificación de la información afectada y tratamientos a realizar.**

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este Acuerdo de Encargo de Tratamiento, el Responsable del Tratamiento pone a disposición del Encargado del tratamiento una serie de datos de carácter personal mediante su incorporación a cualquiera de los SERVICIOS.

Es el Responsable del Tratamiento quien determine mediante sus acciones o la de los USUARIOS AUTORIZADOS las categorías de datos e interesados que serán tratados por el Encargado del Tratamiento.

Los tratamientos autorizados serán todos aquellos necesarios para la ejecución del Contrato

3. Duración.

El presente Acuerdo de Encargo de Tratamiento entrará en vigor en la fecha de aceptación del Contrato. Este Acuerdo de Encargo de Tratamiento es accesorio al contrato, por lo que su duración viene ligada a la duración del mismo.

4. Obligaciones del Responsable del Tratamiento.

Corresponde al Responsable del Tratamiento, además del cumplimiento de cuantas obligaciones se le atribuyan a lo largo del presente Acuerdo de Encargo de Tratamiento, la realización de las siguientes tareas:

a) Cumplir con todas las medidas técnicas y organizativas necesarias para garantizar la seguridad del tratamiento, los locales, equipos, sistemas, programas y las personas que intervengan en la actividad del tratamiento de los datos de carácter personal referidos, que se estipulen en la normativa vigente y de aplicación en cada momento.

b) Entregar al Encargado los datos a que se refiere la cláusula 2 de este documento, así como las instrucciones necesarias para llevar a cabo el tratamiento de los datos en los términos establecidos por el Responsable.

c) Responder a los derechos de los individuos afectados por el tratamiento, como son los derechos de acceso, rectificación, supresión y oposición, limitación al tratamiento, portabilidad de los datos y a no ser objeto de decisiones individuales automatizadas, en colaboración con el Encargado.

d) Realizar, en su caso, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el Encargado.

e) Velar, de forma previa y durante el tratamiento, por el cumplimiento de la normativa aplicable en materia de protección de datos por parte del Encargado.

f) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

g) Comunicar al Encargado cualquier variación que se produzca de los datos personales facilitados, para que se proceda a su actualización.

5. Deber de información y base legítima

El Responsable garantiza que ha cumplido con el deber de facilitar toda la información a los

interesados en el momento de la recogida de los datos objeto del tratamiento, cumpliendo con lo previsto en el art. 12, 13 y 14 del RGPD, según corresponda.

El Responsable del Tratamiento garantiza que dispone de una base legítima para el tratamiento de los datos personales apropiada que se ajuste a los principios de eficacia, necesidad y proporcionalidad, atendiendo a la existencia de otras medidas de protección que puedan resultar menos invasivas, evitando efectos discriminatorios y estableciendo las garantías adecuadas.

El Encargado del Tratamiento no será en ningún caso responsable de la falta de cumplimiento o cumplimiento defectuoso del deber de información o de aplicación de una base de legitimación apropiada.

6. Obligaciones del Encargado del Tratamiento.

El Encargado del Tratamiento declara y garantiza frente al Responsable del Tratamiento lo siguiente:

1. Que utilizará los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios;
2. Que tratará y utilizará los datos de carácter personal a los que tenga acceso, únicamente según las instrucciones del Responsable del Tratamiento, y de conformidad a las finalidades reguladas en el Contrato.

   Las instrucciones en relación con el tratamiento de los datos y acciones encargadas al Encargado deberán comunicarse al Encargado por escrito.

   Si el Encargado del Tratamiento considerara que el cumplimiento de una determinada instrucción del Responsable pudiese suponer un incumplimiento de la normativa sobre protección de datos, lo comunicará inmediatamente al Responsable. El Encargado en esta comunicación solicitará al Responsable que enmiende, retire o confirme la instrucción facilitada y podrá suspender su cumplimiento a la espera de una decisión por el Responsable.
3. Que, si corresponde, llevará, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga toda la información prevista en el art. 30 RGPD.
4. Que mantendrá confidencialidad y secreto sobre los datos de carácter personal a los que tenga acceso con motivo de la prestación de los Servicios.

5. Que no comunicará a terceros salvo que cuente con la autorización expresa del responsable del tratamiento, y en los supuestos legalmente admisibles.

   El Encargado podrá comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones de este último. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

6. Que facilitará al Responsable del Tratamiento la información necesaria para evidenciar el cumplimiento de las obligaciones establecidas en el Contrato.

7. Que prestará la asistencia que sea requerida por el Responsable para la realización de auditorías o inspecciones, realizadas por el Responsable del Tratamiento o por otro auditor autorizado por el Responsable. Las auditorías podrán realizarse de forma periódica, de forma planificada o "ad hoc", previa notificación al Encargado con un plazo de preaviso razonable, en el horario laboral habitual del Encargado.

8. Que garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa y por escrito, a cumplir las medidas de seguridad establecidas, y a respetar la confidencialidad de los datos. El cumplimiento de esta obligación deberá quedar documentado por el Encargado y a disposición del Responsable del Tratamiento.

9. Que ha designado un delegado de protección de datos ("DPO") cuyos datos de contacto son los siguientes: legal@sesametime.com

10. Que colaborará en el cumplimiento de obligaciones del Responsable, y ofrecerá apoyo al mismo, cuando proceda y así lo solicite el Responsable, en la realización de (i) evaluaciones de impacto relativas a los datos de carácter personal que tenga acceso; (ii) consultas previas a la autoridad de control.

7. Destino de los Datos.

Al finalizar la prestación de los Servicios, el Encargado del Tratamiento devolverá los datos personales a los que haya tenido acceso y cualquier copia existente, según le indique el Responsable del Tratamiento de conformidad con el apartado 13.2 del Acuerdo.

El Encargado del Tratamiento podrá conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación de los Servicios.

8. Notificación de violaciones de la seguridad de los datos.

El Encargado notificará al Responsable, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, cualquier incidente, sospechado o confirmado, relativo a la protección de datos, dentro de su área de responsabilidad. Entre otros, deberá comunicar al Responsable cualquier tratamiento que pueda considerarse ilícito o no autorizado, cualquier pérdida, destrucción o daño en los datos y cualquier incidente considerado una vulneración de seguridad de los datos. La notificación deberá ir acompañada de toda la información relevante para la documentación y comunicación de la incidencia a autoridades pertinentes o interesados afectados.

El Encargado del Tratamiento, adicionalmente, prestará asistencia al Responsable en relación a las obligaciones de notificación de acuerdo con el RGPD (en particular, arts. 33 y 34 del RGPD) y a cualquier otra norma aplicable, presente o futura, que modifique o complemente dichas obligaciones.

9. Ejercicio de derechos por parte de los interesados

El Encargado del Tratamiento facilitará la información y/o documentación que el Responsable le solicite para dar respuesta a las solicitudes de ejercicio de derechos que pudiera recibir el Responsable de los interesados cuyos datos se tratan. El Encargado del Tratamiento deberá facilitar dicha información en plazos razonables y, en cualquier caso, con antelación suficiente para que el Responsable pueda cumplir con los plazos legalmente aplicables para la respuesta al ejercicio de estos derechos.

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación al tratamiento, portabilidad de los datos y a no ser objeto de decisiones individuales automatizadas, ante el Encargado del Tratamiento, lo comunicará por correo electrónico a la dirección legal@sesametime.com. La comunicación deberá realizarse de forma inmediata con objeto de atenderla en los plazos legales establecidos, y en ningún caso más allá de dos días laborables a la recepción de la solicitud, presentándo la Responsable junto a toda información que pueda ser relevante para su resolución.

10. Seguridad

En relación con las medidas técnicas y organizativas de seguridad, el Encargado del Tratamiento, deberá implementar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d) Seudonimizar y cifrar los datos personales, en su caso.

En particular, las Partes han convenido una relación de medidas que el Encargado del Tratamiento debe implementar, indicadas en el **Apéndice A** a este Acuerdo de Encargo de Tratamiento.

Si el Responsable, con posterioridad a la formalización del Contrato, exige al Encargado adoptar o mantener medidas de seguridad distintas a las pactadas en este Anexo I, o bien fueran obligatorias por cualquier norma futura, y esto afectase de forma significativa a los costes de prestación de los Servicios, el Encargado y el Responsable del Tratamiento acordarán las medidas contractuales oportunas para afrontar el efecto que tales modificaciones puedan tener en el precio de los Servicios.

11. Subcontratación

El Responsable del Tratamiento concede una autorización general para que el Encargado del Tratamiento pueda subcontratar parte de los Servicios con terceras entidades o subcontratistas (el "**Subencargado**"). El Encargado del Tratamiento informará al Responsable del Tratamiento de los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 15 días.

El Encargado del Tratamiento aplicará la diligencia debida para elegir solo aquellos subencargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que los tratamientos subcontratados sean conformes con los requisitos del RGPD y quede garantizada la protección de los derechos de los interesados sujetos al tratamiento.

El Subencargado, que también tendrá la condición de encargado del tratamiento, estará obligado igualmente a cumplir las obligaciones impuestas al Encargado del Tratamiento y las instrucciones que dicte el Responsable, según lo dictado en el presente Acuerdo de Encargo de Tratamiento. Corresponde al Encargado del Tratamiento regular la nueva relación en un contrato firmado por Encargado y Subencargado, de forma que el Subencargado quede

sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que el Encargado inicial, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del Subencargado, el Encargado del Tratamiento seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones incluidas en el presente Acuerdo de Encargo de Tratamiento.

El listado de subencargados autorizados por el Responsable del Tratamiento se encuentra adjunto al presente Acuerdo de Encargo de Tratamiento como **Apéndice B**.

12. Transferencias internacionales de datos

El Encargado del Tratamiento no llevará a cabo transferencias internacionales de datos de carácter personal a los que tenga acceso, responsabilidad del Responsable del Tratamiento, salvo que cuente con autorización previa del Responsable del Tratamiento o se encuentren debidamente regularizadas según lo contenido en los artículos 45, 46 o 47 del RGPD. Sin perjuicio de los sub encargados de tratamiento autorizados referenciados en el Apéndice B que realizan ciertos tratamientos por cuenta del encargado del tratamientos en territorios fuera del Espacio Económico Europeo, los cuales cumplen con alguna de las condiciones del Capítulo V del RGPD.

13. Responsabilidad.

El Encargado será considerado responsable del tratamiento en caso de que destine los datos objeto del presente Acuerdo de Encargo a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del presente Acuerdo de Encargo, respondiendo de las infracciones en que hubiera incurrido personalmente.

El Responsable deberá informar al Encargado inmediatamente de los procedimientos sancionadores iniciados contra el Responsable del Tratamiento por la AEPD o cualquier otra autoridad competente, por tales incumplimientos o cumplimientos defectuosos, para que el Encargado pueda asumir a su cargo la defensa legal, debiendo actuar, en todo momento, de forma coordinada con el Responsable y preservando su imagen pública y reputación.

Cada Parte mantendrá indemne a la otra frente a reclamaciones, indemnizaciones, acciones y gastos derivados de reclamaciones que la Parte venga obligada a satisfacer por sentencia firme o laudo dictados por un tribunal competente, o en virtud de un acuerdo alcanzado entre una Parte y terceros reclamantes, que fueren consecuencia del incumplimiento o

cumplimiento defectuoso de la normativa aplicable.

ACUERDO DE ENCARGO DE TRATAMIENTO

El presente ACUERDO DE ENCARGO DE TRATAMIENTO solo será de aplicación si el CLIENTE y/o SESAME HR estén sujetos a la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE MEXICO

Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este Acuerdo de Encargo de Tratamiento, el Responsable del Tratamiento pone a disposición del Encargado del tratamiento determinados datos de carácter personal

Duración

El presente Acuerdo de Encargo de Tratamiento entrará en vigor en la fecha de aceptación de las condiciones del Contrato. Este Acuerdo de Encargo de Tratamiento es accesorio al contrato principal de prestación de servicios, por lo que su duración viene ligada a la duración del mismo.

Obligaciones del Responsable del Tratamiento.

Corresponde al Responsable del Tratamiento, además del cumplimiento de cuantas obligaciones se le atribuyan a lo largo del presente Acuerdo de Encargo de Tratamiento, la realización de las siguientes tareas:

- Cumplir con todas las medidas de seguridad técnicas, físicas y administrativas necesarias para garantizar la seguridad del tratamiento, los locales, equipos, sistemas, programas y las personas que intervengan en la actividad del tratamiento de los datos de carácter personal referidos, que se estipulen en la normativa vigente y de aplicación en cada momento.
- Entregar al Encargado los datos a que se refiere la cláusula 2 de este documento, así como las instrucciones necesarias para llevar a cabo el tratamiento de los datos en los términos establecidos por el Responsable.
- Responder a los derechos de los individuos afectados por el tratamiento, como son los derechos de acceso, rectificación, cancelación y oposición, en colaboración con el Encargado

- Velar, de forma previa y durante el tratamiento, por el cumplimiento de la normativa aplicable en materia de protección de datos por parte del Encargado.
- Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- Comunicar al Encargado cualquier variación que se produzca de los datos personales facilitados, para que se proceda a su actualización.

Deber de información y base legítima

El Responsable garantiza que ha cumplido con el deber de facilitar toda la información a los interesados en el momento de la recogida de los datos objeto del tratamiento, cumpliendo con lo previsto en el Capítulo Segundo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

El Responsable del Tratamiento garantiza que dispone de una base legítima para el tratamiento de los datos personales apropiada que se ajuste a los principios de eficacia, necesidad y proporcionalidad, atendiendo a la existencia de otras medidas de protección que puedan resultar menos invasivas, evitando efectos discriminatorios y estableciendo las garantías adecuadas.

El Encargado del Tratamiento no será en ningún caso responsable de la falta de cumplimiento o cumplimiento defectuoso del deber de información o de aplicación de una base de legitimación apropiada.

Obligaciones del Encargado del Tratamiento.

El Encargado del Tratamiento declara y garantiza frente al Responsable del Tratamiento lo siguiente:

- Tratar únicamente los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares y las demás disposiciones aplicables;
- Guardar confidencialidad respecto de los datos personales tratados;
- Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo

requiera la autoridad competente,sin perjuicio del listado de sub encargados del apéndice B.

Al tratarse de un servicio de computo en la nube, el encargado del tratamiento declara y garantiza frente al Responsable del Tratamiento lo siguiente:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley Federal de Protección de Datos Personales en Posesión de Particulares y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Ofrecer información transparente sobre los subcontratistas que participan en el tratamiento de datos.
- En ningún caso el encargado del tratamiento asumirá la titularidad o propiedad de la información titularidad del responsable que haya incorporado a SESAME HR.
- Cuenta con mecanismos, al menos, para:
    - Comunicar al responsable del tratamiento sobre cambios en la política de privacidad del encargado del tratamiento y en el presente Acuerdo de Encargo del Tratamiento.
    - Permitir al responsable limitar el tipo de tratamiento de los datos personales.
    - Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales.
    - Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable mediante la eliminación de manual por parte del responsable o la solicitud del mismo
    - Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

Destino de los Datos.

Al finalizar la prestación de los Servicios, el Encargado del Tratamiento devolverá los datos personales a los que haya tenido acceso y cualquier copia existente, según le indique el Responsable del Tratamiento de conformidad con el apartado 13.2 del Acuerdo.

El Encargado del Tratamiento podrá conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación de los Servicios.

Notificación de violaciónes de la seguridad de los datos.

El Encargado notificará al Responsable, sin dilación indebida, cualquier incidente,

sospechado o confirmado, relativo a la protección de datos, dentro de su área de responsabilidad. Dicha vulneración de la seguridad deberá materializarse en la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

Ejercicio de derechos por parte de los interesados

El Encargado del Tratamiento facilitará la información y/o documentación que el Responsable le solicite para dar respuesta a las solicitudes de ejercicio de derechos que pudiera recibir el Responsable de los interesados cuyos datos se tratan. El Encargado del Tratamiento deberá facilitar dicha información en plazos razonables y, en cualquier caso, con antelación suficiente para que el Responsable pueda cumplir con los plazos legalmente aplicables para la respuesta al ejercicio de estos derechos.

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, ante el Encargado del Tratamiento, lo comunicará por correo electrónico a la dirección legal@sesametime.com. La comunicación deberá realizarse de forma inmediata con objeto de atenderla en los plazos legales establecidos, y en ningún caso más allá de dos días laborables a la recepción de la solicitud, presentándose al Responsable junto a toda información que pueda ser relevante para su resolución.

Seguridad

En relación con las medidas técnicas, administrativas y físicas de seguridad, el Encargado del Tratamiento, deberá implementar mecanismos para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas, físicas y administrativas implantadas para garantizar la seguridad del tratamiento
- Seudonimizar y cifrar los datos personales, en su caso.

En particular, las Partes han convenido una relación de medidas que el Encargado del Tratamiento debe implementar, indicadas en el Apéndice A a este Acuerdo de Encargo de Tratamiento.

Si el Responsable, con posterioridad a la formalización del Contrato, exige al Encargado adoptar o mantener medidas de seguridad distintas a las pactadas en este Anexo II, o bien fueran obligatorias por cualquier norma futura, y esto afectase de forma significativa a los costes de prestación de los Servicios, el Encargado y el Responsable del Tratamiento

acordarán las medidas contractuales oportunas para afrontar el efecto que tales modificaciones puedan tener en el precio de los Servicios.

Subcontratación

El Responsable del Tratamiento concede una autorización general para que el Encargado del Tratamiento pueda subcontratar parte de los Servicios con terceras entidades o subcontratistas (el "Subencargado"). El Encargado del Tratamiento informará al Responsable del Tratamiento de los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 15 días.

El Encargado del Tratamiento aplicará la diligencia debida para elegir solo aquellos subencargados que ofrezcan garantías suficientes para aplicar medidas técnicas, fisicas y administrativas apropiadas, de manera que los tratamientos subcontratados sean conformes con los requisitos del Ley Federal de protección de datos personales en posesión de particulares y quede garantizada la protección de los derechos de los interesados sujetos al tratamiento.

El Subencargado, que también tendrá la condición de encargado del tratamiento, estará obligado igualmente a cumplir las obligaciones impuestas al Encargado del Tratamiento y las instrucciones que dicte el Responsable, según lo dictado en el presente Acuerdo de Encargo de Tratamiento. Corresponde al Encargado del Tratamiento regular la nueva relación en un contrato firmado por Encargado y Subencargado, de forma que el Subencargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que el Encargado inicial, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del Subencargado, el Encargado del Tratamiento seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones incluidas en el presente Acuerdo de Encargo de Tratamiento.

El listado de subencargados autorizados por el Responsable del Tratamiento se encuentra adjunto al presente Acuerdo de Encargo de Tratamiento como Apéndice B.

Transferencias internacionales de datos

El Encargado del Tratamiento podrá realizar transferencia internacional de datos de carácter personal los subcontratistas autorizados que se encuentren fuera del territorio nacional de México que proporcionen las garantías suficientes en lo relativo a medidas físicas, técnicas y administrativa

Responsabilidad.

El Encargado será considerado responsable del tratamiento en caso de que destine los datos objeto del presente Acuerdo de Encargo a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del presente Acuerdo de Encargo, respondiendo de las infracciones en que hubiera incurrido personalmente.

Cada Parte mantendrá indemne a la otra frente a reclamaciones, indemnizaciones, acciones y gastos derivados de reclamaciones que la Parte venga obligada a satisfacer por sentencia firme o laudo dictados por un tribunal competente, o en virtud de un acuerdo alcanzado entre una Parte y terceros reclamantes, que fueren consecuencia del incumplimiento o cumplimiento defectuoso de la normativa aplicable.

APÉNDICE A.- MEDIDAS DE SEGURIDAD

Nuestra infraestructura está basada principalmente en Cloud, utilizamos varios proveedores, para mayor tolerancia a fallos, y constantemente está en proceso de mejora.

Nuestra aplicación tiene una arquitectura distribuida, lo que nos permite tener separados front, api y otros servicios necesarios para el funcionamiento de la aplicación. Además, nos permite una mejor escalabilidad del servicio, ya que podemos controlar de forma separada qué parte de la infraestructura necesita soportar mayor carga.

Por otro lado contamos con un entorno de desarrollo virtualizado que permite a nuestro equipo realizar todos los cambios de forma paralela y controlado mediante el sistema de control de versiones GIT lo que nos permite asegurar la integridad del sistema. Así como un flujo de integración continua con Gitlab

Metodologías de desarrollo

- SOLID
- DDD (Domain Driven Design)
- Tests Unitarios
- Arquitectura Hexagonal.
- Multiple authentication
- CI/CD con Gitlab.

Lenguajes de programación

- Backend
    - Symfony 4
    - PHP 7.x.x
    - MySQL / MariaDB.
    - Redis. o SQS (o Beanstalk)
    - S3
    - SQS
- Frontend
    - VueJS
    - Tailwind
    - Librería de componentes de lógica propia.
- Apps
    - VueJS

    - Capacitor
    - Typescript
- Sockets
    - NodeJS
    - Express
    - Typescript
    - SocketIO.

Infraestructura

Para procesar toda la información disponemos de las siguientes tecnologías en infraestructura.

- Debian 10
- Docker
- K8S
- AWS
- Google Cloud
- OVH Cloud
- Proxmox
- HAProxy
- Cloudflare

Nuestro departamento de sistemas se encargará de asegurar que los servidores cuenten con la paquetería necesaria para el funcionamiento correcto de la aplicación.

Proveedores

- OVH Cloud
- So You Start
- AWS
- Google Cloud
- Cloudflare
- Dockerhub

Servidor de Base de datos

- Relacional (sql): Para las bases de datos relacionales utilizaremos MaríaDB
- La base de datos tiene que tener una codificación utf8.
- Contaremos con un usuario con los siguientes permisos:
    - Esquema (Create objects): Si (crear, modificar y borrar tablas)
    - Escritura (SUDI Select, Update, Delete e Insert): Si
    - Lectura (SELECT): Si

Las copias de seguridad se realizan semanales completas e incrementales diarias. De nuestro servidor de base de datos guardamos una copia de las copias de forma mensual, semanal y

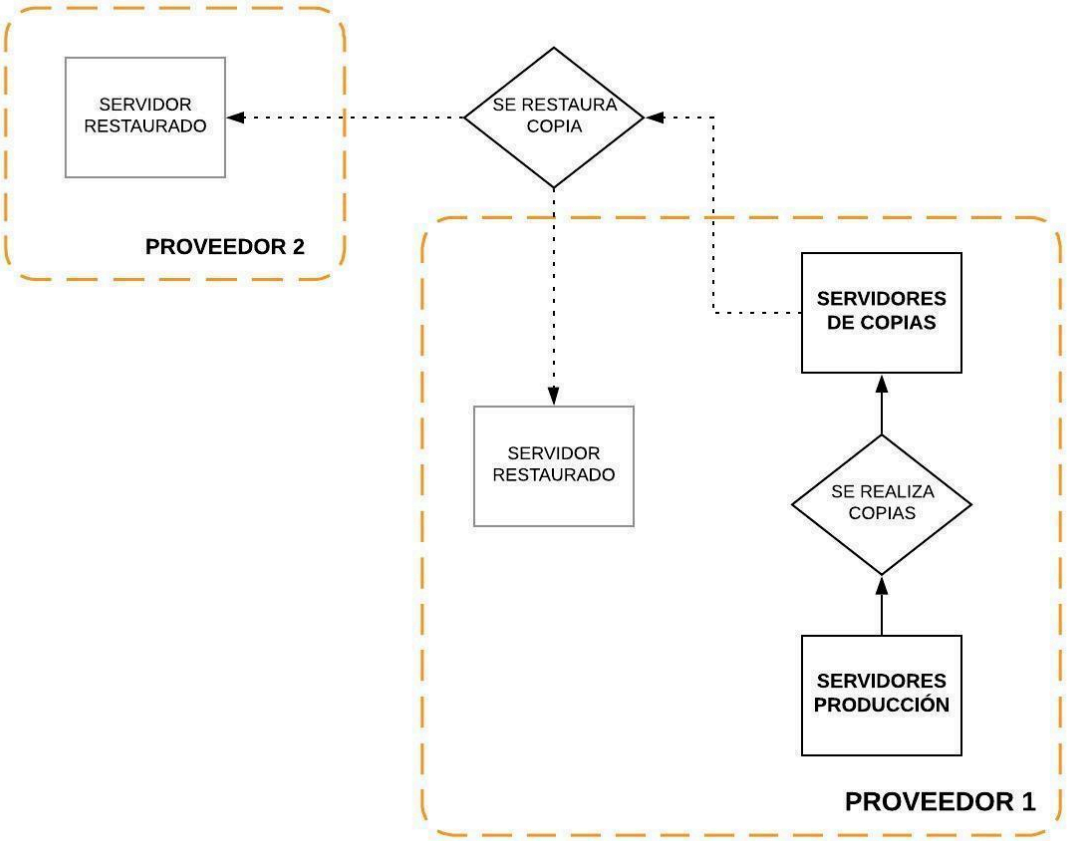
diaria, almacenadas en nuestro servidor esclavo. Además también se hacen copias cada hora de nuestra base de datos del servidor principal.

Guardamos copia de todo el contenido del servidor web, y copias de archivos de configuración de servicios críticos.

Utilizamos un servidores de copias de seguridad en Francia que se encuentra redundado en Polonia para asegurarnos la disponibilidad de las copias en caso de desastre.

El administrador del departamento de sistemas de información o Informática o la que haga sus veces es el responsable designado elaborará un procedimiento para probar las copias de seguridad y pruebas de restauración de las copias de seguridad sobre una base mensual.

En caso de recuperación de una copia, se seguirá el siguiente procedimiento:



Medidas de seguridad sobre la infraestructura
Datacenter

Contamos con servidores que se encuentran contratados en OVH, número uno en Europa y tercero mundial del alojamiento web, que tiene más de 150.000 servidores físicos. El éxito de OVH radica en el control total que ejerce sobre la cadena de alojamiento, incluyendo la producción de sus servidores. OVH es conocido por la especial atención que presta a la selección de los componentes de sus máquinas, exigiendo la máxima calidad.

Cada servidor es sometido sistemáticamente a una serie de pruebas para verificar su conformidad técnica y su buen comportamiento en cualquier circunstancia. En cuanto la máquina sale de producción, se instala y se conecta en los datacenters de OVH. A continuación, un robot comprueba que el hardware sea el que ha pedido el cliente y que sus prestaciones se ajusten a las especificaciones.

Los puntos de control son los siguientes:
- procesadores: conformidad, prueba de carga, temperatura;
- memoria RAM: tamaño, memtest;
- BIOS: versión de la BIOS, virtualización;
- discos: velocidad, prueba SMART, versión del firmware, etc.

También contamos con servicios contratados en AWS. En AWS fueron pioneros de computación en la nube desde 2006, creando una infraestructura de nube que permite a crear de manera segura e innovar más rápido. Sus centros de datos se encuentran diseñados para protegerlos de los riesgos naturales y provocados por el hombre. Se implementan controles, desarrollan sistemas automatizados y se someten a auditorías de terceros para confirmar la seguridad y la conformidad.

Los centros de datos están diseñados para prever y tolerar errores mientras se mantienen los niveles de servicio. En caso de error, los procesos automatizados desvían el tráfico de la zona afectada. Las aplicaciones principales se implementan en un estándar N+1, de forma que en caso de que se produzca un error en un centro de datos, haya capacidad suficiente para poder equilibrar la carga del tráfico entre los demás sitios.

AWS monitorea y realiza un mantenimiento preventivo del equipo eléctrico y mecánico para mantener el funcionamiento constante de los sistemas instalados en los centros de datos de AWS. A los procedimientos de mantenimiento del equipo los realizan personas cualificadas y se llevan a cabo de acuerdo con un programa de mantenimiento documentado.

Protección ante ataques

Nuestros servidores utilizan la infraestructura anti-DDoS desplegada por OVH para proteger los servidores durante las 24 horas del día contra cualquier tipo de ataque DDoS, independientemente de su duración y su envergadura.

El objetivo de un ataque DDoS es hacer caer un servidor, un servicio o una infraestructura, enviando múltiples peticiones simultáneas desde múltiples puntos de la red.

La intensidad de este «fuego cruzado» desestabiliza el servicio, o aún peor, lo inhabilita. Esta infraestructura permite:

- analizar todos los paquetes en tiempo real y a gran velocidad,
- aspirar el tráfico entrante del servidor,
- mitigar, es decir, identificar todos los paquetes IP ilegítimos, pero dejando pasar los paquetes IP legítimos.

Seguridad

Sesame está muy concienciado con la seguridad, tratamiento de los datos así como de la fuga de información de la misma. Es por ello que día a día trabaja para mejorar la seguridad de la misma manteniendo unos objetivos claros en materia de la misma. Es por ello que a continuación pasaremos a detallar más en profundidad los diferentes aspectos que tratamos en matería de seguridad tanto en la aplicación como en la infraestructura:

Proveedores cloud: Sesame cuenta con distintos proveedores cloud para brindar la máxima disponibilidad y escalabilidad posible en la aplicación. Todos nuestros proveedores cuentan como mínimo con las siguientes certificaciones de seguridad:

- ISO/IEC 27001, 27017 y 27018
- PCI DSS Nivel 1
- RGPD Cumplimiento del Reglamento de la UE 2016/679 relativo a la Protección General de Datos.
- SSAE 18 de Tipo 2: SOC 1, SOC 2 y SOC 3

El acceso a dichos proveedores únicamente está supeditado a empleados con un nivel de acreditación muy alto en la empresa, casi siempre por algún responsable de área o sistemas.

Servidores: El acceso a los servidores está restringido a empleados con un nivel de acreditación alto. Para el acceso al mismo se utilizarán par de claves cifradas RSA de 2048 bits e incluirá una contraseña de usuario nominal el cual permite registrar el acceso de dicho usuario así como de un movimiento detallado de los cambios o alteraciones en dichas máquinas para una posible auditoría posterior.

Herramientas de terceros: Sesame utiliza herramientas de seguridad de terceros como puede ser Tenable.io el cual se encarga de inventaríar todas nuestras máquinas así como dominios que utilizamos y lanzar periódicamente auditorias de vulnerabilidades e intrusión. Por lo tanto cada semana nuestros expertos disponen de nuevos informes los cuales indican posibles brechas de seguridad que según el algoritmo de IA de Tenable se irán parcheando con el orden de prioridad recomendado.

Acceso a la aplicación: El acceso a la plataforma se realizará siempre a través de nuestro proveedor de CDN y DNS CloudFlare el cual cuenta con un WAF integrado de última generación capaz de detectar y mitigar ataques que vayan dirigidos directamente a la aplicación

Política de parcheo

Todos los servicios, y la infraestructura que los sustentan, accesibles desde Internet, ya sean de uso interno de la empresa o para nuestros clientes, siguen una política de actualizaciones de seguridad ágil. Estos servicios son parcheados en cuanto se tenga conocimiento de un bug o vulnerabilidad importante. En el caso de actualizaciones no críticas se programa un parcheo mensual o trimestral en función de nuestras necesidades y de la aplicación.

Los servicios de carácter interno (impresoras, equipos de red local de usuarios, centralitas telefónicas, etc.) tienen una política de actualizaciones periódicas programadas (cada seis

meses, cada año, etc.) en función de las necesidades y llevada a cabo por el departamento IT de la empresa.

A su vez contamos con un sistema de alerta en caso de virus, ClamAV.

APÉNDICE B- LISTADO DE SUBENCARGADOS

OVH

Aplicación: Aplica para el necesario uso de la plataforma. Este proveedor aplica para todo el mundo salvo los países del continente americano (Salvo Estados Unidos y Canadá).
Nombre del subencargado: OVH SAS
Ubicación Actual del Tratamiento: Francia y Alemania
Enlace a la política de seguridad del subencargado:
https://www.ovh.es/proteccion-datos-personales/seguridad.xml

Amazon Web Services

Aplicación: Aplica para el necesario uso de la plataforma. Este proveedor aplica para todo el mundo salvo los países del continente americano (Salvo Estados Unidos y Canadá).
Nombre del subencargado: Amazon Web Services
Ubicación Actual del Tratamiento: Francia y Alemania
Enlace a la política de seguridad del subencargado: https://aws.amazon.com/es/compliance/

Mailchimp

Aplicación: Aplica para el necesario uso de la plataforma. Este proveedor aplica para todo el mundo.
Nombre del subencargado: The Rocket Science Group (Mailchimp)
Ubicación Actual del Tratamiento: Estados Unidos
Enlace a la política de seguridad del subencargado: https://mailchimp.com/es/gdpr/
Transferencia internacional a efectos de RGPD: El subencargado se encuentra adherido al EU-U.S. Data Privacy Framework

Signaturit

Aplicación: Aplica para el uso de la funcionalidad de la firma electrónica (solo si está activada la funcionalidad y se hace uso de ella). Este proveedor aplica para todo el mundo.
Nombre del subencargado: Signaturit Solutions S.L
Ubicación Actual del Tratamiento: España
Enlace a la política de seguridad del subencargado: https://www.signaturit.com/es/politica-de-privacidad/

OPEAN AI

Aplicación: Aplica para en caso de contratación y uso de SESAME IA
Nombre del subencargado: OPEAN AI
Ubicación Actual del Tratamiento: Estados Unidos de América
Transferencia internacional a efectos de RGPD: Conforme a la política de privacidad del Subencargado
Enlace a la política de seguridad del subencargado: https://openai.com/es-ES/policies/privacy-policy/

AUREN

Aplicación: Aplica para en caso de contratación y uso de "Gestor de nóminas"
Nombre del subencargado: AUREN LEGAL SP, S.L.P
Ubicación Actual del Tratamiento: España
Enlace a la política de seguridad del subencargado: https://auren.com/es/politica-privacidad-y-seguridad-informacion/

IPXON

Aplicación: Aplica para el necesario uso de la plataforma. Este proveedor aplica para los países del continente americano (Salvo Estados Unidos y Canadá).

Nombre del subencargado: CONEXUM INC (IPXON Networks)
Ubicación Actual del Tratamiento: Brasil (Solo para Clientes registrados en países del continente americano salvo Estados Unidos y Canadá)
Enlace a la política de seguridad del subencargado: https://www.ipxon.com/es-br/privacidad

SWAN

Aplicación: Aplica para en caso de contratación y uso de Control de gastos y Adelanto de nómina

Nombre del subencargado: SWAN SAS
Ubicación Actual del Tratamiento: Francia
Enlace a la política de seguridad del subencargado: https://cdn.prod.website-files.com/609a39f33751ff4530c610e2/65cc87d03aff83bcc2c1f0a3_2024-PP-ES.pdf