

CONTRATO DE LICENCIA DE USUARIO FINAL DE SESAME HR

Al leer y aceptar el presente Contrato de Licencia de Usuario Final (en adelante, el CLUF) se concede a su aceptante una licencia sobre la solución tecnológica SESAME HR, la cual se regirá por los presentes términos. Este CLUF es de exclusiva aplicación para aquellos aceptantes que hayan adquirido SESAME a través de los fabricantes autorizados del fabricante.

La licencia concedida por el fabricante al aceptante y el presente CLUF es independiente de la relación contractual entre el aceptante y el distribuidor de SESAME HR.

El distribuidor con el que el aceptante mantenga una relación comercial está autorizado a la distribución de SESAME HR.

1. Definiciones

Distribuidor: Persona física o jurídica que mantiene una relación con el fabricante para la distribución autorizada de SESAME HR

SESAME HR: Solución tecnológica desarrollada por el fabricante y de la cual ostenta la propiedad intelectual.

Aceptante: Persona física o jurídica que mantiene una relación comercial con el distribuidor.

Fabricante: La sociedad mercantil SESAME LABS S.L con CIF B98719818, la cual ostenta la titularidad sobre la solución SESAME HR.

Servicio de Apoyo Técnico: Soporte en relación con el uso, la identificación y la resolución de errores relativos a SESAME HR.

Bases de Datos: Conjunto integrado de datos de titularidad del aceptante incluido dentro de SESAME durante la duración del CLUF. En caso de tratamiento de datos personales incluidos como parte de la Base de Datos les será de aplicación el Acuerdo de Subencargado del Tratamiento.

Usuario(s) Autorizado(s): Usuarios que mantienen una relación contractual con el aceptante y que utilizan SESAME HR.

Las partes: Referencia conjunta al fabricante y aceptante.

La parte: Referencia indistinta al fabricante o el aceptante.

2. Ámbito de aplicación y duración.

Se concede al aceptante una licencia sobre SESAME HR, la cual es no sublicenciable, no

exclusiva, de ámbito mundial y con una duración ligada a la relación comercial entre el aceptante y el distribuidor.

3. Condiciones de Uso

Derechos de Uso. Se concede al aceptante y a los Usuarios Autorizados el derecho personal, no exclusivo, intransferible y no sublicenciable de utilizar SESAME HR, a nivel mundial, durante la duración del presente CLUF.

Restricciones de Uso. El aceptante no podrá: (a) realizar ingeniería inversa, descompilar, desensamblar o tratar de obtener o derivar el código fuente, las ideas subyacentes, los algoritmos, los formatos de archivo o las API no públicas de los Servicios, así como traducir, modificar o crear obras derivadas de SESAME HR o cualquier parte de los mismos, salvo en la medida en que lo permita la legislación aplicable; (b) copiar/reproducir, prestar, vender, alquilar, sublicenciar, emitir, distribuir, editar, transferir a terceros o facilitar el acceso a SESAME HR, así como adaptar lo o cualquier parte de los mismos de cualquier manera; (c) utilizar SESAME HR en beneficio de cualquier tercero; (d) utilizar SESAME HR para cualquier fin comercial o en un producto o servicio que el aceptante proporcione a terceros; (e) eludir, modificar, eliminar, borrar, alterar o manipular de otro modo cualquier tecnología o programa de seguridad, encriptación o de otro tipo que forme parte de SESAME HR; (f) acceder o utilizar SESAME HR con el fin de realizar un análisis de la competencia o crear un producto o servicio similar o competitivo; (g) usar SESAME HR para ningún propósito ilegal o no autorizado por el fabricante, incluida la publicidad no solicitada y el spam; (h) crear, recopilar, transmitir, almacenar, utilizar o procesar cualquier dato a través de SESAME HR que viole cualquier ley aplicable, o infrinja los derechos de propiedad intelectual u otros derechos de cualquier tercero; (i) introducir o difundir contenido o software (virus y malware) que pueda causar daños a los sistemas informáticos del fabricante, sus proveedores de servicios tecnológicos o los usuarios de terceros; o (j) alentar, permitir o ayudar a cualquier tercero a hacer cualquiera de los anteriores

Actualizaciones y nuevas versiones. Las actualizaciones, versiones sucesivas de SESAME HR que se proporcionen al aceptante durante la vigencia del CLUF, estarán sujetas a los mismos términos.

4. Servicio de Apoyo técnico y disponibilidad

Servicios de Apoyo Técnico. El fabricante proporcionará al aceptante soporte durante el horario de trabajo del fabricante para ayudar al aceptante a resolver dudas, localizar y corregir problemas en relación con SESAME HR. El aceptante autoriza que el fabricante, a través de su personal, y con previa solicitud del aceptante, a poder acceder a las cuentas de los Usuario Autorizados para llevar a cabo las actuaciones oportunas para solventar las dudas o incidencias acaecidas con SESAME HR.

Disponibilidad. El fabricante empleará los esfuerzos comercialmente razonables para que SESAME HR tenga una disponibilidad del 98% y hará esfuerzos comercialmente razonables para avisar al aceptante con, al menos, 48 horas de antelación de los mantenimientos programados dentro del horario comercial habitual.

5. Uso de la cuenta

Acceso a la Cuenta. El aceptante y los Usuarios Autorizados deberán mantener la seguridad de las claves de acceso a las cuentas de Usuario Autorizado en SESAME HR (“Cuenta”). El fabricante no será responsable en ningún caso de cualquier pérdida de información o daño producido por el incumplimiento de esta obligación de seguridad.

Restricciones. No está permitido: (i) compartir una (1) cuenta entre varios Usuarios Autorizados; y (ii) la creación de cuentas por “bots” u otros métodos automatizados. El aceptante será responsable de todas las acciones realizadas y de todos los datos cargados por los Usuarios Autorizados en SESAME HR.

Gestión de las Cuentas. El aceptante se compromete a bloquear o desactivar la cuenta a un Usuario Autorizado de inmediato en el caso de que: (i) se suspenda o termine la relación entre el aceptante y el Usuario Autorizado; o (ii) considere que un Usuario ha efectuado un mal uso de sus claves de acceso a SESAME HR. Si el fabricante tiene constancia de que un Usuario Autorizado se encuentra en uno de los supuestos previstos en la presente Cláusula, el fabricante podrá suspender el acceso a la Cuenta infractora de forma temporal o indefinida, debiendo el fabricante, en dicho supuesto, notificar al aceptante sobre la infracción detectada y la medida tomada respecto a dicha Cuenta.

6. Usuarios Autorizados

Activación de Cuentas de Usuario Autorizado. Únicamente podrán tener cuentas de Usuario Autorizado en SESAME HR (“Cuenta”) las personas que tengan la edad mínima legal para poder trabajar.

Acceso a la Cuenta. El aceptante reconoce que, cuando un Usuario Autorizado accede por primera vez a SESAME HR, dicho Usuario Autorizado estará obligado a (i) leer y mostrar su aceptación en línea a determinadas condiciones y restricciones de conformidad con las condiciones del presente CLUF, y (ii) proporcionar sus claves de acceso para fines de identificación y verificación de su identidad como Usuario Autorizado; (iii) mantener la seguridad de sus claves de acceso a su Cuenta. El fabricante no será responsable en ningún caso de cualquier pérdida de información o daño producido por el incumplimiento de esta obligación de seguridad.

Restricciones. No está permitido: (i) compartir una (1) cuenta entre varios Usuarios Autorizados. Cada cuenta es de uso personal e intransferible; (ii) la creación de cuentas por “bots” u otros métodos automatizados; (iii) usar SESAME HR para ningún propósito ilegal o no autorizado por el fabricante. El aceptante será responsable de todas las acciones realizadas y de todos los datos cargados por los Usuarios Autorizados en SESAME HR.

Desactivación de Cuentas. El aceptante se compromete a bloquear o desactivar la cuenta a un Usuario Autorizado de inmediato en el caso de que: **(i)** se suspenda o termine la relación entre el aceptante y el Usuario Autorizado; o **(ii)** si el aceptante reconoce o considera que un Usuario ha efectuado un mal uso de sus claves de acceso a SESAME HR.

En el caso de que el fabricante considerará que un Usuario Autorizado pueda haber infringido alguno de los términos indicados, efectúe un mal uso de sus claves de acceso, el fabricante podrá, según su propio criterio, suspender el uso de dicha cuenta indefinidamente, además de cualquier otro derecho o recursos previstos según el presente CLUF o en virtud de la ley.

La desactivación de una cuenta de Usuario Autorizado conllevará la posibilidad, pero no obligación del fabricante, de conservar y el almacenar los datos que integran dicha Cuenta, en todo caso durante un período máximo de un (1) año con el único fin de proporcionar al aceptante una copia de la información contenida en la misma o su futuro uso o reactivación. Tras este período, los datos serán totalmente suprimidos y no será posible recuperar la información.

7. Propiedad Intelectual

Propiedad Intelectual e Industrial en relación con SESAME HR. El fabricante conservará su posición como titular de todos los derechos de propiedad intelectual e industrial relacionados con todos los componentes de SESAME HR y cualquier otro desarrollo, mejora, actualización u obra derivada del presente CLUF. Los derechos de propiedad intelectual e industrial abarcarán todos datos, código fuente y objeto, scripts, diseños, conceptos, aplicaciones, textos, imágenes, cualquier documentación relacionada, copias, modificaciones y documentos o documentación derivados de lo anterior (en su totalidad o en parte) y todos los derechos de autor relacionados, patentes, marcas, secretos comerciales y otros derechos de propiedad, son y seguirán siendo de la exclusiva propiedad del fabricante y/o sus titulares de licencia.

Propiedad Intelectual e Industrial del aceptante. Todos los derechos, títulos e intereses en relación con la Base de Datos, marcas, nombres comerciales, y logos del aceptante, así como los que puedan existir en su propio sistema informático, seguirán siendo propiedad del aceptante.

8. Confidencialidad

Definición de Información Confidencial. Se entiende por “Información Confidencial”, cualquier material o información revelada verbalmente o por escrito etiquetada o calificada como confidencial o que, por su naturaleza, razonablemente se entienda como confidencial que haya sido entregada o proporcionada por cualquiera de las Partes a la otra con motivo del presente CLUF, incluyendo información relacionada con los sistemas informáticos y la arquitectura de los sistemas previstos o existentes de las Partes, incluido el hardware, el software, el propio SAAS, la Documentación, la Base de Datos, los métodos de procesamiento y métodos operativos.

Excepciones. La Información Confidencial no incluirá información que (i) era de dominio público en el momento en que se divulgó a la Parte receptora; (ii) entró en el dominio público mediante uso, publicación o similares, con posterioridad a la revelación a la Parte receptora, sin que mediara culpa o acto alguno de la Parte receptora; (iii) estaba en posesión de la Parte receptora de forma legítima y libre de cualquier obligación de confidencialidad en el momento en que fue revelada a la Parte receptora; (iv) es comunicada legítimamente a la Parte receptora por un tercero con derecho a revelar dicha Información Confidencial, con posterioridad al momento en que fue revelada a la Parte receptora.

Deber de confidencialidad. Las Partes se comprometen a no utilizar, revelar, copiar, publicar, utilizar, explotar, difundir o distribuir la Información Confidencial de la otra Parte, ni permitir que la Información Confidencial recibida sea explotada o distribuida por terceros, sin el previo consentimiento por escrito de la Parte reveladora, salvo en la medida en que sea necesario para cumplir con sus obligaciones o ejercer sus derechos en virtud del CLUF. Las Partes se comprometen a tratar la Información Confidencial con el mismo grado de cuidado que utilizan para proteger su propia Información Confidencial, y en ningún caso con un grado de cuidado inferior al razonable. La obligación de confidencialidad se mantendrá en vigor de forma indefinida y se extiende igualmente a los empleados y representantes de las Partes, así como también a los asesores externos que cualquiera de las Partes haya contratado en conexión con este CLUF.

Divulgación de la Información Confidencial. Las Partes solo podrán divulgar la Información Confidencial en los siguientes supuestos: (i) en respuesta a una orden de un tribunal u otro organismo gubernamental, o según lo exija la ley, (en este caso se notificará previamente por escrito a la Parte reveladora sobre dicha divulgación potencial y se limitará lo máximo posible dicha divulgación); (ii) cuando la Parte receptora de dicha Información Confidencial deba revelarla a sus empleados, representantes o a sus asesores externos (si existen) que haya contratado, con el objeto de cumplir con sus obligaciones bajo el presente CLUF y sólo dándoles acceso a la misma en la medida de lo necesario; (iii) cuando una Parte haya recibido autorización expresa y por escrito de la otra Parte para divulgar su Información Confidencial (o una parte de esta).

Incumplimiento del deber de confidencialidad. El incumplimiento de las obligaciones de confidencialidad plasmadas en este CLUF, o las actuaciones dolosas o culposas llevadas a cabo por cualquiera de las Partes, sus empleados o directivos, facultará a la Parte no incumplidora a reclamar por la vía legal, las responsabilidades, directas o indirectas o frente a terceros, incluidos gastos judiciales, extrajudiciales y costes que la defensa que la Parte incumplidora ocasionara, así como a indemnizar los daños y perjuicios que tal incumplimiento hubiera ocasionado a la Parte no incumplidora.

9. Protección de datos

Datos de las partes. Las Partes se informan mutuamente de que los datos personales de las personas que trabajen para las respectivas Partes, y los datos de contacto indicados a efectos de notificaciones, serán objeto de tratamiento por la otra Parte con la única finalidad de gestionar y ejecutar el CLUF. Los datos se conservarán mientras se mantenga vigente la relación y una vez finalizada ésta, se conservarán únicamente durante el tiempo que sea

necesario para satisfacer el cumplimiento de obligaciones fiscales, legales y administrativas a las que las Partes vengán obligadas.

La base que legitima este tratamiento es la necesidad de ejecutar el presente CLUF. Los datos no serán comunicados ni cedidos a terceros con excepción de aquellos que sean imprescindibles para la propia ejecución del CLUF (proveedores de servicios necesarios) y para el cumplimiento de las obligaciones legales (Administraciones Públicas, Auditoras, entidades financieras, Compañías aseguradoras cuando proceda, entre otras).

En el caso de proveedores de servicios necesarios, es posible que tengan su sede fuera de la UE y se produzca una transferencia internacional de datos. En dicho supuesto, las Partes se comprometen a velar porque sus proveedores internacionales cuenten con las garantías adecuadas según la normativa aplicable.

Las Partes podrán solicitar el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad en el domicilio designado en el presente CLUF o en la dirección electrónica, indicando claramente el derecho que desean ejercitar. Igualmente, las Partes quedan mutuamente informadas de que tienen derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es). No obstante las Partes pondrán sus mejores medios y tratarán de resolver cualquier cuestión relativa a los datos personales de forma amistosa.

Base de Datos incluida por el aceptante. El tratamiento de los datos personales contenidos en la Base de Datos que se llevará a cabo por parte del fabricante como consecuencia de la licencia concedida en virtud del CLUF estará regulada por el Acuerdo de Subencargado del tratamiento.

10. Garantías

Garantía de titularidad. El fabricante garantiza al aceptante que es el propietario o titular legítimo de todos los derechos de propiedad intelectual necesarios para proporcionar SESAME HR.

Exclusiones. SESAME HR se suministra “TAL CUAL” y “según esté disponible” y el fabricante excluye cualquier otro tipo de garantía, incluidas, entre otras, las garantías implícitas de disponibilidad, rendimiento, no infracción, comerciabilidad o idoneidad para un fin determinado, sin perjuicio, en su caso, de las garantías exigidas por la ley. El aceptante acepta que es el único responsable de los resultados obtenidos por el uso de SESAME HR y de sus funcionalidades. No se aceptarán reclamaciones por supuestas especificaciones que, en opinión del aceptante, SESAME HR deba reunir.

11. Responsabilidad

Limitación de Responsabilidades. El aceptante acepta indemnizar y mantener indemne al

fabricante por cualquier reclamación, acción o demanda directa, indirecta, incidental o consecuente de terceros, así como por cualquier gasto, responsabilidad, daño, acuerdo o cuota que surja del mal uso de SESAME HR por parte del aceptante, o de la violación de cualquiera de los términos del presente CLUF. El fabricante tampoco asumirá responsabilidad alguna por cualesquiera reclamaciones, pérdidas o daños que se deriven del uso por parte del aceptante o de algún Usuario de cualquier producto de terceros, servicios, software o sitios web a los que se acceda a través de enlaces o links desde SESAME HR

Daños Indirectos. El fabricante no será responsable (salvo que la ley disponga lo contrario) ante el aceptante por ningún daño, compensación o indemnización basada en daños indirectos (incluyendo, pero limitándose al daño emergente, la pérdida de uso, la pérdida o inexactitud de los datos, el lucro cesante, el fallo de los mecanismos de seguridad, la interrupción del negocio, los costos de la demora) o cualquier daños especial, incidental o consecuente de cualquier tipo, incluso si se le informa de la posibilidad de tales daños con antelación.

Nada de lo dispuesto en el presente CLUF limitará o excluirá la responsabilidad de una Parte que no pueda ser excluida o limitada en términos de la legislación aplicable.

Fuerza Mayor. Ninguna de las partes será responsable ante la otra por el incumplimiento de los obligaciones contraídas en virtud del CLUF en la medida en que dicho incumplimiento o demora sea resultado de una causa o circunstancia que escape del control razonable de la Parte afectada y que no haya podido evitarse o superarse actuando de manera razonable y prudente (como por ejemplo, pero sin limitarse a ello, incendios, inundaciones, huelgas, conflictos laborales u otros disturbios industriales, guerra – declarada o no-, embargos, bloqueos, restricciones legales, disturbios, insurrecciones, reglamentos gubernamentales).

Cumplimiento normativo. El aceptante será el único responsable del pleno cumplimiento de todas las leyes aplicables a su negocio en su jurisdicción. El uso de SESAME HR no equivale ni garantiza en modo alguno el cumplimiento de la normativa aplicable a la gestión de la jornada laboral. SESAME HR es una herramienta sujeta al uso del aceptante, que es el responsable del cumplimiento de sus obligaciones.

12. Resolución

Si el aceptante incumple alguna disposición del presente CLUF, el fabricante podrá dar por rescindido de inmediato.

Como excepción a lo anterior, el fabricante se reserva el derecho de rescindir el CLUF de pleno derecho, sin aviso previo ni indemnización, en caso de que el aceptante o un Usuario Autorizado comprometa de alguna manera la integridad de SESAME HR, los derechos de propiedad intelectual e industrial del fabricante sobre SESAME HR o la reputación de las marcas o productos del fabricante.

Efectos de la resolución. Al vencimiento del CLUF o a su rescisión por cualquier motivo: (i) a petición del aceptante, el fabricante se compromete a proporcionar al aceptante una copia de la Base de Datos en un formato técnico estándar. Dicha petición deberá realizarse en el plazo de un mes desde la terminación del CLUF; (ii) todas las disposiciones del mismo dejarán de

tener efecto, salvo las disposiciones del presente CLUF que, por su naturaleza, deba permanecer en vigor, aunque el CLUF se dé por terminado, incluyendo las disposiciones en materia de confidencialidad, propiedad intelectual y protección de datos.

13. Miscelánea

Cesión. El aceptante no podrá ceder o transferir este CLUF sin el consentimiento previo y por escrito del fabricante. Sin embargo, el CLUF sí podrá ser cedido o transferido por el fabricante sin necesidad de consentimiento del aceptante, bastando la notificación previa y por escrito de la cesión al aceptante para que dicha cesión sea efectiva. Una vez formalizada la cesión, cualquier referencia a la Parte cedente contenida en el presente Acuerdo deberá entenderse como una referencia a la entidad o entidades cesionarias.

Renuncia. Ningún retraso en el ejercicio de un derecho se considerará una renuncia al mismo, ni la renuncia a un derecho o recurso en un caso concreto constituirá una renuncia a dicho derecho o recurso en general.

Modificaciones. El fabricante podrá modificar el presente CLUF sin necesidad de previa comunicación al aceptante el cual acepta la modificación mientras se continúa haciendo uso de la licencia.

Invalidez parcial. Si se determina que alguna de las disposiciones del presente CLUF es inaplicable o inválida, las restantes disposiciones del presente CLUF no se verán afectadas y permanecerán en pleno vigor y efecto.

14.Ley aplicable y jurisdicción

Legislación aplicable. Los términos del presente CLUF se regirán e interpretarán en todos los aspectos de acuerdo con la legislación española.

Fuero aplicable. Las Partes declaran conjuntamente que, en la medida de lo razonable, toda controversia que surja en relación con el presente CLUF o que se derive del mismo se resolverá mediante negociaciones y consultas mutuas. En caso de que no se llegue a una solución satisfactoria, dicha controversia se someterá a los tribunales de la ciudad de Valencia.

ANEXO I.- ACUERDO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Los datos personales del aceptante, en calidad de responsable del tratamiento de datos de carácter personales , serán tratados por el fabricante en calidad de encargado del tratamiento de datos de carácter personal.

Las obligaciones y derechos establecidos en el presente Anexo serán de aplicación independientemente respecto del acuerdo que en materia de protección de datos personales puedan haber celebrado el aceptante y el distribuidor; el fabricante no estará sujeto, bajo ningún concepto, al acuerdo alcanzado por el distribuidor y aceptante en materia de protección de datos, salvo lo establecido en el presente Anexo y en su caso de los contratos y acuerdos que el fabricante haya suscrito con el distribuidor.

1. Objeto e información afectada.

Para ejecutar las prestaciones derivadas del CLUF, el fabricante tendrá acceso a los datos de carácter personal que el aceptante haya introducido en SESAME HR.

2. Obligaciones del Aceptante.

Corresponde al Aceptante 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) 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.
- c) Realizar, en su caso, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento.
- d) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

3. Deber de información y base legítima

El Aceptante 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 Aceptante 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.

Ni el fabricante ni el distribuidor serán en ningún caso responsables de la falta de cumplimiento o cumplimiento defectuoso del deber de información o de aplicación de una base de legitimación apropiada.

4. Seguridad, Subcontratación y Transferencias internacionales de datos.

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

- a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente 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 indicadas en el **Apéndice A**

El fabricante podrá subcontratar con terceras entidades todos aquellos servicios necesarios para la ejecución del CLUF.

El listado de subencargados del fabricante se encuentran en el **Apéndice B**.

El fabricante podrá llevar a cabo transferencias internacionales de datos de carácter personal a los que tenga acceso siempre que se encuentren debidamente regularizadas según lo contenido en los artículos 45, 46 o 47 del RGPD.

5. Responsabilidad.

El aceptante mantendrá indemne al fabricante frente a reclamaciones, indemnizaciones, acciones y gastos derivados de reclamaciones que el fabricante 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

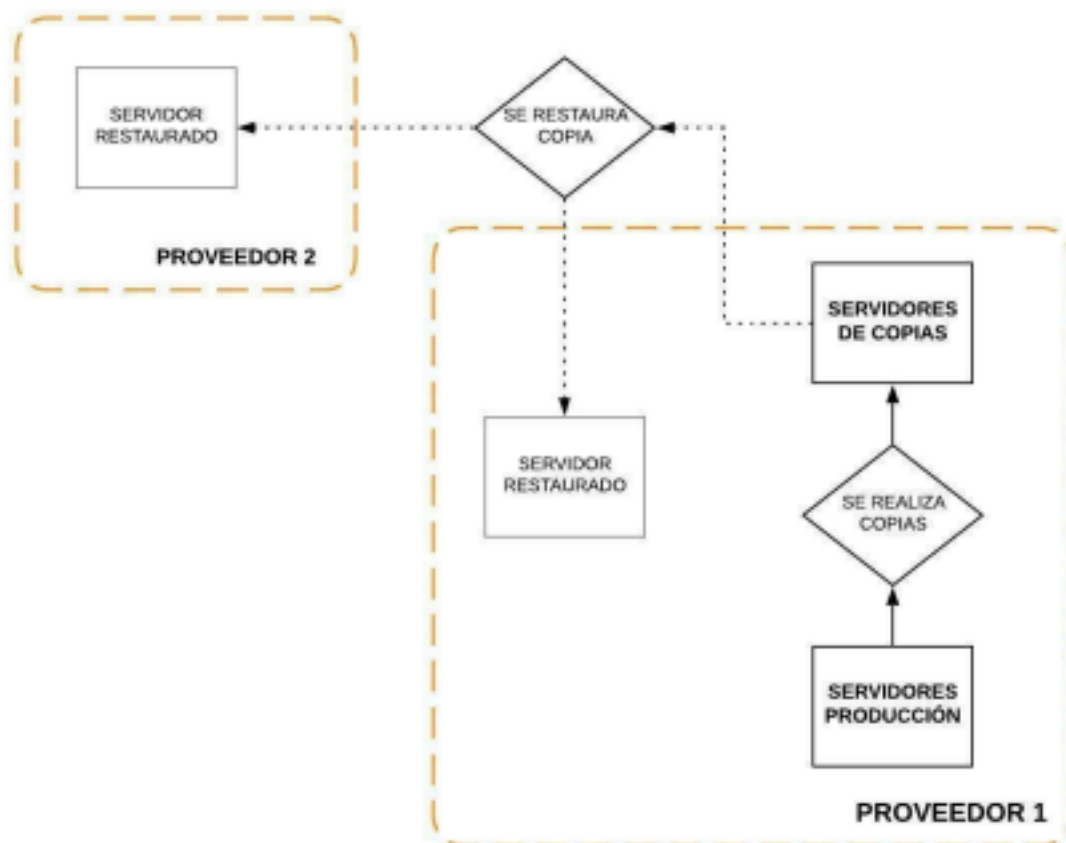
Las copias de seguridad se realizan semanales completas e incrementales diarias. De nuestro servidor de base de datos guardamos una copia de las copias de forma mensual, semanal y diaria, almacenadas en nuestro servidor esclavo. Además también se hacen copias cada hora de nuestra base de datos del servidor 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 materia de seguridad tanto en la aplicación como en la infraestructura:

Sesame: Sesame cuenta con la siguiente certificación de seguridad:

- ISO 27001

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](https://tenable.io) el cual se encarga de inventariar todas nuestras máquinas así como dominios que utilizamos y lanzar periódicamente auditorías 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

NOMBRE DE SUBENCARGADO	DIRECCIÓN COMERCIAL REGISTRADA	UBICACIÓN ACTUAL DEL TRATAMIENTO	ENLACE A LA POLÍTICA DE SEGURIDAD DEL SUBENCARGADO
OVH SAS	2 rue Kellermann 59100 Roubaix, (Francia)	Francia (OVH Cloud Gravelines (GRA3) Rte de la Frm Masson 59820 Gravelinas)	https://www.ovh.es/proteccion-datos-personales/seguridad.xml
Amazon Web Services	410 Terry Avenue North, Seattle, WA 98109-5210, ATTN	Francia (Amazon Brétigny-sur-Orge 91220 Brétigny-sur-Orge)	https://aws.amazon.com/es/compliance/
The Rocket Science Group (Mailchimp)	675 Ponce De Leon Ave NE, Atlanta, Georgia 30308, US	Estados Unidos	https://mailchimp.com/about/security/
Signaturit Solutions S.L	C/ d'Àvila, 29, Sant Martí, 08005 Barcelona	C/ d'Àvila, 29, Sant Martí, 08005 Barcelona	https://www.signaturit.com/es/politica-de-privacidad/