# 1. OBJETO

**ASAC COMUNICACIONES, S.L.** (en adelante "ASAC"), con domicilio social en Llanera (Asturias), Parque Tecnológico – Parcela 29, C.I.F. B-33490426, presenta a su Cliente el siguiente contrato de servicios Cloud.

# 2. PUNTOS DE CONTACTO

Nuestros servicios Cloud son diferentes e implican diferentes prestaciones. Es importante lea detenidamente la información que se presenta a continuación.

Si tuviera cualquier duda, no olvide que dispone de un punto de contacto con nosotros, y puede plantear todas las dudas que tuviera.

Puede ponerse en contacto con nosotros:

| Como ponerse en contacto con ASAC Comunicaciones para gestiones del servicio | |
|---|---|
| Soporte servicios en modo Cloud | Atención telefónica: 902 265 041<br>Correo electrónico: soporte@asac.as<br>HelpDesk: Canal Xperta: https://asac.xperta.es<br>Resolución según niveles de servicio. |
| Consultas sobre el servicio | Responsable de cliente<br>Canal Xperta<br>Correo electrónico |
| Consultas sobre facturación | Acceso mediante Cloud 4b |
| Realizar una sugerencia, comentario, queja o reclamación sobre el servicio. | Envió de correo electrónico reclamaciones@asac.as |
| Como ponerse en contacto con el Delegado de Protección de Datos de ASAC Comunicaciones | |
| Para consultas sobre las medidas de diligencia en ASAC Comunicaciones | Envió de correo electrónico a rgpd@asac.as indicando en el asunto "Diligencia Proveedor". |
| Para consultas relacionadas con la seguridad del servicio | Envío de correo electrónico a rgpd@asac.asindicando en el asunto "Medidas de Seguridad". |
| Realizar una consulta o reclamación relativa a protección de datos | Envío de correo electrónico a rgpd@asac.asindicando en el asunto "Reclamación protección de datos". |

# 3. POLÍTICA DE SEGURIDAD DE ASAC COMUNICACIONES

| | |
|---|---|
| Política de Seguridad de ASAC | En ASAC Comunicaciones creemos en la seguridad como principio transversal de todos nuestros servicios. Disponemos de diferentes certificaciones que nos ayudan a seguir mejorando cada día: Esquema Nacional de Seguridad Cat. Alta, ISO 27001, ISO 27017, ISO 27018, ISO 22301; ISO 20000-1, ISO 9001, ISO 14001. |
| Principios de seguridad de nuestros servicios Cloud | |
| Ciclo completo | La seguridad de la información forma parte de todo el ciclo de los servicios de ASAC Comunicaciones, desde la fase más temprana de diseño y análisis hasta la propia implementación del servicio. |
| Gestión del riesgo | ASAC Comunicaciones mantiene una evaluación de riesgos que le permite mejorar todas las medidas de seguridad desplegadas. Además, mantenemos un análisis detallado de las amenazas Cloud que se declaran año a año. |
| Aislamiento | Nuestros servicios Cloud mantienen un aislamiento seguro sin menoscabar los recursos propios de los servicios. Nuestros entornos disponen de medidas para evitar accesos de otros usuarios ajenos. |

| | |
|---|---|
| Elasticidad y escalabilidad | Nuestros servicios pueden ser ampliados a medida que crecen las necesidades de nuestros clientes. Mantenemos mediciones constantes y nuestros clientes pueden acceder a la información de sus servicios en tiempo real o solicitarnos informes detallados. |
| Seguridad | Disponemos de medidas de seguridad desplegadas que aseguran nuestra infraestructura y servicios, incluyéndose, controles en los accesos, trazabilidad de acciones, monitorizaciones… |

## 4. SERVICIOS CLOUD PRESTADOS POR ASAC

El desglose de los productos y servicios incluidos dentro del alcance del presente contrato son:

| | | |
|---|---|---|
| IaaS | Infrastructure as a Service. | Incluye infraestructura (servidores, almacenamiento y redes). |
| PaaS | *Platform as a Service*. | Incluye infraestructura (servidores, almacenamiento y redes). También middleware, herramientas de desarrollo, sistemas de administración de bases de datos, etc. |
| SaaS | *Software as a Service*. | Asociado a gestión de incidencias ( Xperta), y nuestro canal de denuncias. |
| DaaS | *Desktop as a Service.* | Puesto de trabajo accesible desde cualquier ubicación y dispositivo, con accesos a información y servicios, en mismo modo que en local. |
| BaaS | *Backup as a Service* | Gestión de conservación de copias ante desastres e incidencias. |
| STaaS | *Storage as a Service* | Almacenamiento cloud de información, sobre una infraestructura securizada y redundada, y con protocolos de segregación que evitan accesos no consentidos en entornos no dedicados. |
| DRaaS | *Disaster Recovery as a Service* . | Apoyo en procesos de respaldo en la nube, y servicio de contingencia en caso de necesitar un centro operativo como recuperación ante desastres y reanudación de servicios, bajo el protocolo dado por la ISO 22301. |

Todos nuestros servicios incluyen una serie de actividades como valor añadido que detallamos a continuación. Algunas actividades no se incluyen en la prestación de servicio, aunque puede consultarnos como incluirla en su contrato.

Todos los servicios son desarrollados en el idioma declarado: español

## 5. ACTIVIDADES INCLUIDAS EN LOS SERVICIOS CLOUD

Se indican a continuación el precio de las ampliaciones disponibles en este servicio:

| | Que incluye | Que no incluye |
|---|---|---|
| IaaS | - Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Sistemas de alojamiento (hipervisor, cortafuego virtual, etc.)<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Mantenimiento del sistema de gestión de identidad<br>- Gestión del sistema de gestión de identidad<br>- Gestión de la plataforma de autenticación (incluida política de contraseñas)<br>- Gestión de parches del sistema operativo de invitado y procedimientos de refuerzo (también verificación de cualquier conflicto entre el cliente y la política de seguridad del proveedor)<br>- Configuración de seguridad (cortafuegos, IDS/IPS, etc.)<br>- Supervisión de los sistemas de invitado<br>- Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes)<br>- Recogida de registros y control de la seguridad |
| PaaS | - Infraestructura de soporte físico (instalaciones, espacio, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Gestión de soporte, parches y mantenimiento (también verificación de cualquier conflicto entre el cliente y la política de seguridad del proveedor)<br>- Configuración de seguridad (cortafuegos, IDS/IPS, etc.)<br>- Supervisión de los sistemas<br>- Mantenimiento de la plataforma de seguridad (cortafuegos, IDS/IPS de alojamiento, antivirus, filtrado de paquetes)<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Mantenimiento del sistema de gestión de identidad<br>- Gestión del sistema de gestión de identidad<br>- Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas) |
| SaaS | - Infraestructura de soporte físico (instalaciones, espacio, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Gestión de soporte, parches y mantenimiento (también verificación de cualquier conflicto entre el cliente y la política de seguridad del proveedor)<br>- Configuración de seguridad (cortafuegos, IDS/IPS, etc.)<br>- Supervisión del sistema<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Cumplimiento de la normativa de protección de protección de datos con respecto a los datos implicados en el servicio.<br>- Política interna y mantenimiento del sistema de gestión de identidad y acceso.<br>- Gestión del sistema de gestión de identidad<br>- Gestión de la plataforma de autenticación (incluido el cumplimiento de la política de contraseñas)<br>- Comunicar incidencias |
| DaaS | - Infraestructura de soporte físico (instalaciones, espacio, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Gestión de la plataforma de escritorio | - Cumplimiento de la normativa de protección de protección de datos y normas laborales y de privacidad.<br>- Política interna y mantenimiento del sistema de gestión de identidad y acceso. |

| | | |
|---|---|---|
| | - Gestión de soporte, parches y mantenimiento (también verificación de cualquier conflicto entre el cliente y la política de seguridad del proveedor)<br>- Configuración de seguridad (cortafuegos, IDS/IPS, etc.)<br>- Supervisión del sistema<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Comunicar incidencias |
| BaaS | - Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Sistemas de alojamiento asociados al almacenamiento (hipervisor, cortafuegos virtual, etc.)<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Cumplimiento de la normativa de protección de protección de datos con respecto a los datos implicados en el servicio.<br>- Mantenimiento del sistema de gestión de identidad<br>- Recogida de registros y control de la seguridad |
| STaaS | - Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Sistemas de alojamiento asociados al almacenamiento (hipervisor, cortafuegos virtual, etc.)<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Cumplimiento de la normativa de protección de protección de datos con respecto a los datos implicados en el servicio.<br>- Mantenimiento del sistema de gestión de identidad<br>- Recogida de registros y control de la seguridad |
| DRaaS | - Infraestructura de soporte físico (instalaciones, espacio en bastidor, potencia, refrigeración, cableado, etc.)<br>- Disponibilidad y seguridad de la infraestructura física (servidores, almacenamiento, red, ancho de banda, etc.)<br>- Sistemas de alojamiento (hipervisor, cortafuegos virtuales, etc.)<br>- Ejecución de pruebas bajo instrucciones (reporte de informes)<br>- Gestionar incidencias de seguridad comunicadas o detectadas proactivamente.<br>- Recogida de registros y control de la seguridad | - Mantenimiento del sistema de gestión de identidad<br>- Gestión del sistema de gestión de identidad<br>- Gestión de la plataforma de autenticación (incluida política de contraseñas)<br>- Gestión de parches del sistema operativo de invitado y procedimientos de refuerzo (también verificación de cualquier conflicto entre el cliente y la política de seguridad del proveedor)<br>- Configuración y mantenimiento de seguridad (cortafuegos, IDS/IPS, etc.)<br>- Plan de continuidad<br>- Pruebas de contingencia<br>- Supervisión de los sistemas de invitado<br>- Recogida de registros y control de la seguridad |

*ASAC proveerá de herramientas para la gestión de servicios, relacionadas con la gestión de los servidores virtuales del cliente y la plataforma de monitorización.

Es posible que como cliente haya contratado el servicio con más inclusiones. Por favor consulte con nosotros en caso de dudas.

## 6. CARACTERÍSTICAS DE NUESTROS SERVICIO CLOUD

| | |
|---|---|
| Migración a nuestro servicio | ASAC Comunicaciones ayuda a sus clientes para poder migrar su información y servicios a nuestras plataformas. Recomendamos y ponemos a su disposición el uso de medios de migración securizados. Nuestros servicios se adaptan a las diferentes tecnologías. |
| Bastionados | Salvo que forme parte del servicio ASAC Comunicaciones no se encargará del bastionado de las máquinas y otros elementos gestionados directamente por el cliente.<br>ASAC Comunicaciones se encargará de mantener el correcto bastionado de las maquinas físicas y plataformas de virtualización (VMWare / Citrix) así como de la infraestructura de red que debe dar soporte al servicio. Mantenemos bastionados de elementos de red, firewall, hipervisores VMWare y elementos Citrix<br>El cliente debe asegurarse de gestionar adecuadamente, todos los elementos de configuración de su servicio y especialmente la creación, mantenimiento y eliminación de máquinas y otros elementos (bases de datos, ...)<br>El cliente es el encargado de la gestión de las maquinas virtualizadas (servicios, protocolos y puertos). Es recomendable que el cliente realice un despliegue de servicios de seguridad conforme a los estándares de seguridad más reconocidos. |
| Política de acceso e identificación | ASAC Comunicaciones mantiene un estricto control de las medidas de acceso a su sistema, y dispone de una política de identificación y autenticación de sus usuarios.<br>Para la gestión de sus propios servicios, nuestros clientes deben desarrollar o modificar sus políticas de identificación y derechos de acceso. Es importante que mantenga un control sobre los accesos, autorizando las acciones de los usuarios, y que mantenga vigilancia sobre los permisos privilegiados que conceda.<br>Es importante que se mantenga una adecuada gestión de las credenciales. Recomendamos que haga uso de un gestor de claves. No se deben reutilizar identificadores, redistribuir accesos, crear accesos genéricos no individuales y por defecto, mantener usuarios permanentemente.<br>El cliente es responsable del control de los accesos concedidos, del almacenamiento de información, de las aplicaciones ejecutadas o interconexiones cuando el tipo de servicio lo permita.<br>Se recomienda que su política de identificación y acceso considere, quien debe acceder, como podrán acceder, que permisos le debe entregar, permitir los accesos solo el tiempo necesario, gestionar las trazas de los accesos y acciones, y reducir al máximo los privilegios.<br>ASAC Comunicaciones seguirá todas las instrucciones de nuestros clientes, incluyendo cuando sea necesario, gestionar los accesos de terceros para gestionar los servicios de nuestros clientes. |
| Usuarios de ASAC | Para realizar las acciones de mantenimiento y de soporte algunos usuarios de ASAC podrán acceder al sistema y servicio de los clientes. Se mantendrán trazas completas de sus acciones y una gestión de las acciones privilegiadas en base a las necesidades. |
| Doble factor | Algunos de los servicios de ASAC Comunicaciones pueden aceptar una autenticación mediante doble factor, empleando elementos de Token o factores de contraseña fuera de banda. Debe consultar la compatibilidad de esta función con su servicio. |
| Copias | ASAC Comunicaciones mantiene un proceso completo de copias de seguridad, bajo petición y contratación del cliente:<br>a) Copias diarias incrementales con un periodo de retención de 7 días.<br>b) Copias semanales completas con una retención de 4 semanas.<br>c) Opcional previa contratación: copias mensuales completas a cinta con cifrado y con una retención de 12 meses. Cinta custodia bajo medidas de seguridad.<br>d) Programa de copias particularizado para el cliente. Siempre bajo demanda se adaptará el sistema de copias.<br>ASAC no considera los snapshots como copias de seguridad y solo se ejecutan bajo demanda de los clientes que no pueden ejecutarlas directamente.<br>ASAC Comunicaciones realiza procesos de eliminación de las copias de seguridad conforme la ISO 27040. |
| Restauraciones | Mantenemos diferentes procesos de pruebas de restauración que junto con las pruebas de contingencia de ASAC nos permiten asegurar el proceso de continuidad de ASAC y de sus servicios<br>Cuando un cliente necesita una restauración, puede solicitarlo como una petición de servicio y nuestro personal procederá a su ejecución. Solo se permitirán restauraciones cuando sean solicitadas por un interlocutor validado de nuestro cliente. |
| Cifrado | ASAC Comunicaciones puede ofrecer la posibilidad bajo demanda de un cliente y como servicio añadido, el cifrado de sus almacenamientos o de información específica. Cuando un cliente nos solicite esta protección, |

| | |
|---|---|
| | se estudiarán las diferentes opciones para escoger junto con nuestro cliente la que se puede ajustar mas a sus necesidades.<br>Por defecto todas nuestras cintas de copia están cifradas. |
| Incidencias | ASAC dispone de un proceso completo para gestionar las incidencias de seguridad, incluidas aquellas que pueden afectar a datos personales. Todas las incidencias son registradas y constan las acciones para su tratamiento<br>Nuestros clientes pueden informarnos de cualquier incidencia que pudiera afectar a sus servicios mediante los puntos de contacto definidos.<br>Nuestros clientes pueden solicitarnos evidencias que requieran para justificar determinadas actividades no autorizadas o ilícitas en sus servicios.<br>Cuando ASAC detecte alguna incidencia que puede afectar a los clientes o a sus servicios o información, realizará una notificación mediante su canal de comunicación, informando de la incidencia, impacto y posibles notificaciones a organismos cuando sea pertinente. .<br>Se recomienda a nuestros clientes que mantengan control sobre las operaciones que requieren privilegios para evitar pérdidas o fallos del sistema, como borrados o apagados de máquinas, eliminación de información y otros, que puedan generar incidencias significativas. |
| Monitorización | ASAC Comunicaciones dispone de registros operativos, de actividades de sus usuarios, excepciones, fallos y eventos de seguridad que son tratados y gestionados, de manera automatizada por un SIEM. Disponemos de alertas que nos avisan de actividades anómalas en el sistema y en la red y que son gestionada por nuestro personal de seguridad. ASAC no es responsable de la monitorización de los servicios del cliente. Este servicio es extensible a los clientes que lo consideren necesario como un servicio complementario bajo petición y contratación, en modo compartido o modo dedicado. Consulte con nosotros en caso de necesidad.<br>Se recomienda que mantenga activados los registros de eventos de sus máquinas y de otros elementos de sus servicios.<br>Los clientes solo acceden a sus servicios, infraestructuras y máquinas y por tanto a sus logs, mediante Cloud4B y la propia configuración y características de la virtualización de VMware y segmentación de redes.<br>Los servicios SaaS por defecto disponen de Logs que pueden ser consultados por los usuarios.<br>En ASAC Comunicaciones, y así lo recomendamos a nuestros clientes, los logs con información personal, son tratados conforme a la normativa de protección de datos. |
| Segregación | ASAC Comunicaciones utiliza diferentes tecnologías que permiten mantener entornos segregados para ASAC y para sus clientes. ASAC mantiene la segregación lógica de sistemas, aplicaciones, almacenamiento y redes, manteniendo un adecuado aislamiento de los clientes y de los servicios.<br>Se mantienen controles sobre los hipervisores, sobre los recursos implicados, y sobre la red.<br>Segregación del servicio<br>Se mantienen el aislamiento del entorno virtual compartido, por lo que cada cliente accede exclusivamente a sus servicios. Por defecto no se incorporan más de un servicio crítico a una LUN.<br>Segregación de la red<br>Se mantiene una segregación de la red a nivel de firewall, bien en modo dedicado o en modo compartido (según requisito del cliente y servicio contratado). |
| Reutilización | Nuestros entornos virtuales de multicliente son sanitizados para evitar que un cliente pueda acceder a información que previamente hubiera sido almacenada, conforme a la ISO 27040.<br>Los sistemas asociados a virtualización no son reutilizables sin una previa sanitización, conforme con el procedimiento derivado de la ISO 27040. |
| Sanitización | Cuando un recurso se retira del servicio y antes de la reutilización o eliminación, procedemos a un completo proceso de sanitización. Esto incluye también los espacios de almacenamiento previamente utilizados. |
| Devolución de información | ASAC adoptara un proceso de devolución de la información, según las indicaciones del cliente, siendo recomendable un método securizado.<br>Si los recursos deben ser transferidos a otro proveedor, ASAC facilitara su acceso o transferencia. Las migraciones se realizan siempre en un formato estándar y compatible con la mayoría de las tecnologías de virtualización.<br>Si un cliente requiere un proceso determinado por motivos de portabilidad, se podrá considerar como un servicio diferente e incluirá estudio previo de requisitos de accesibilidad, posibles necesidades de integración, y securizacion del proceso<br>La información no necesaria asociada a copias de seguridad o registros, será eliminada salvo que ASAC deba mantenerla por cuestiones legales. |

## 7. NIVELES DE SERVICIO

ASAC Comunicaciones dispone de una declaración de niveles de servicio según servicio Cloud. Por defecto nuestra disponibilidad es de un 95%.

| Tiempos | Prioridades | |
|---|---|---|
| | Urgente | Normal |
| Tiempo de Respuesta | 4 horas | 8 horas |
| Tiempo de Resolución | 8 horas | 16 horas |
| % Cumplimiento | 95 % | 95 % |

## 8. SOPORTE

Los soportes disponibles para nuestros clientes contratables son:

| | |
|---|---|
| Nivel 1 | Horario 24x7.<br>*Incluye servicio de mantenimiento de condiciones físicas para el normal funcionamiento del servicio (disponibilidad de CPD, alimentación eléctrica, climatización, seguridad física, disponibilidad de elementos de comunicaciones y del equipamiento hardware de base, disponibilidad de la plataforma de virtualización de servidores y aplicaciones.). |
| Nivel 2 | Horario: lunes a jueves 8:30 a 14:30 y 16:00 a 19:00. Viernes de 8:00-14:00 / Julio y agosto 8:00-15:00<br>*Incluye servicio de mantenimiento de los sistemas software de base necesarios para el funcionamiento de los aplicativos: sistemas operativos, base de datos y a sistemas virtuales. |

## 9. NORMATIVA APLICABLE

| | |
|---|---|
| Legislación aplicable | Se considera normativa aplicable la legislación española y europea directamente aplicable. |
| Protección de datos | ASAC Comunicaciones como prestador de servicios de un Estado Miembro queda sometido a la normativa de protección de datos vigente; Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales<br>Ubicación: todos los datos son almacenados en España.<br>Transferencias: ASAC no realiza transferencias internacionales<br>Encargo de tratamiento: El cliente dispone de un contrato especifico relacionado con el tratamiento de datos personales en su servicio. Si es necesario puede considerase un modelo propio del cliente.<br>Medidas de diligencia. ASAC Comunicaciones adopta las medidas de seguridad, técnicas y organizativas necesarias para garantizar su seguridad, conforme a los riesgos declarados y la tecnología empleada en sus servicios. Cuando es preciso ASAC desarrolla evaluaciones de impacto de protección de datos e implementa medidas concretas para mejorar la seguridad.<br>En aquellos servicios en los que ASAC no gestiona la configuración de los elementos del servicio (creación, mantenimiento y eliminación de máquinas y otros elementos como antivirus o bases de datos) el cliente debe extremar las medidas de seguridad para evitar brechas de seguridad.<br>ASAC Comunicaciones pone a disposición de los clientes, evidencias de cumplimiento.<br>Notificación: ASAC Comunicaciones comunicará a sus clientes, solicitudes legalmente vinculantes, relacionadas con accesos a datos personales, salvo que la normativa prohíba dicho acceso. |
| Subcontrataciones | En la prestación de servicios, ASAC Comunicaciones no realiza subcontrataciones. Excepcionalmente pueden existir servicios complementarios y accesorios, que pueden ser realizados por una entidad subcontratada. En estos casos, ASAC realizará una comunicación al cliente indicándole, servicio subcontratado, entidad ejecutante y personal asignado al servicio.<br>Todas las entidades que pudiéramos subcontratar deberán cumplir con la normativa en vigor y disponer de medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos. Nuestro Delegado de Protección de Datos velará por mantener proveedores diligentes. |

| | |
|---|---|
| | ASAC no subcontrata servicios de alojamiento, salvo que nuestros clientes lo exijan expresamente. |
| Confidencialidad | Toda la información, incluidos los datos personales, implicada en la prestación del servicio, será considerada confidencial y nuestro personal la tratará con las máximas garantías de sigilo y seguridad. Todas las personas que intervienen en el servicio, estarán sometidas al deber de confidencialidad del artículo 5.1 letra f) del Reglamento (UE) 2016/679.<br>Toda la información, estará sometida a secreto y no podrá ser revelada a terceros, incluso más allá de finalizado el servicio. |
| Propiedad intelectual | ASAC Comunicaciones es propietaria en régimen de propiedad o de licenciamiento, de toda la tecnología, plataforma y software implicado en el servicio. El hecho de que sean empleables para los servicios, no genera derecho al cliente, más allá del uso permitido durante la vigencia del contrato.<br>El cliente es responsable de las aplicaciones que implemente en su infraestructura y plataforma y de la propiedad o licencia de uso de las mismas, así como de la información gestionada.<br>ASAC reconoce la propiedad de toda información implicada en el servicio y de las licencias de los diferentes recursos que el cliente pueda emplear en sus servicios. |
| Modificaciones | Cualquier modificación de estas características será notificada a los clientes |

## 10. SEGURIDAD EN EL ENTORNO CLOUD

| | |
|---|---|
| Arquitectura e infraestructura: | Gestión de toda la arquitectura y tecnología subyacente, incluidos los controles técnicos de seguridad y privacidad, durante todo el ciclo de vida de todos los componentes del sistema.<br>Configuración de seguridad para hipervisores, contenedores y redes. |
| Tecnología actualizada | Nuestro sistema de virtualización esta actualizado y se mantiene conforme a las pautas de uno de los más reconocidos fabricantes.<br>Controles de configuración respecto a hipervisores para reducir drásticamente la exposición ante vectores de ataque. |
| Roles y permisos | Grupo diferenciados y permisos específicos con acceso a la plataforma y máquinas con restricciones del empleo del programa de virtualización sin elevación de privilegios no relacionadas con el uso de las máquinas virtuales. |
| Capacidad | Planificación de los servicios para dimensionar las necesidades del cliente y la escalabilidad del servicio. |
| Seguridad perimetral | Mediante firewalll correctamente actualizado. |
| Aprendizaje | Sistema de aprendizaje constante mediante boletines e información de vulnerabilidades y eventos de seguridad en el entorno cloud. |
| Continuidad | Política de continuidad asociada a la ISO 22301 |