emburse captio

Seguridad en entornos SaaS

8 claves a tener en cuenta antes de elegir una herramienta cloud

Cada vez más la digitalización está presente en las empresas y se amplía la oferta de servicios de software en modo SaaS (Software as a Service). Como cliente, debes saber que un contrato SaaS bien redactado y negociado adecuadamente es la base para garantizar un servicio con total seguridad.

Para elegir un proveedor en la nube, primero, debes definir cuáles son los objetivos de seguridad. Con estos objetivos claros, tendrás bien evaluado a tus proveedores con el fin de ver cuál entiende tus necesidades en este aspecto.

1. ¿El software aplica medidas de seguridad en referencia a la conservación de los datos?

Globalmente, las medidas de seguridad de datos se aplican para proteger la **privacidad digital** y así evitar el acceso no autorizado a los datos que pueden permanecer en ordenadores, bases de datos, sitios web, etc. Es decir, para protegerlos de una posible corrupción.

En caso de pérdida de datos, lo ideal es tener bien definida y documentada una **política de backup**, con copias frecuentes e incrementales, así como un proceso de restauración de datos originales claro y probado.

No basta con tener instalado un antivirus, las medidas de protección físicas y las medidas de protección contra ataques informáticos se basan en mantener la vigilancia de nuestros equipos, establecer protecciones contra el acceso a la información por parte de terceros, proteger los dispositivos periféricos (discos duros, USB) y el hardware, y proteger la transmisión y almacenamiento de datos.

En seguridad informática, destaca una de las técnicas más útiles: el **pentesting**[1]. Ha nacido a consecuencia de los fraudes y robos de datos e información de muchas empresas.

[1]PENTESTING:

El término está formado por dos palabras, **penetration y testing**, el también llamado **test de penetración** es una práctica diseñada para determinar el **alcance de los fallos de seguridad de un sistema. Gracias a la aplicación de** pentests por parte de tus proveedores, podrás tener la seguridad que el software contratado ha sido puesto a prueba y se han localizado sus vulnerabilidades de seguridad, para corregirse posteriormente.

2. ¿Cumple con las regulaciones de seguridad y privacidad de datos según el Reglamento General de Protección de Datos?

El nuevo Reglamento General de Protección de Datos (GDPR) obliga a cumplir las regulaciones de protección de datos para que sea una constante en las empresas, con acciones como la encriptación de la información y comunicaciones, la implementación de medidas físicas y lógicas de control de acceso, la localización física de los datos, formación a los empleados sobre privacidad de datos y sobre actualizaciones relevantes de términos contractuales.

3. ¿Dispone de seguridad aplicada en las transferencias de datos?

Para garantizar la seguridad del servicio contratado y de los datos de los clientes, se debe firmar un compromiso que vele por el respeto por la integridad de los datos, la protección de la confidencialidad de los datos utilizados y almacenados, la disponibilidad y la trazabilidad de éstos. Para cumplir con este punto, algunas medidas son la encriptación de los datos o el uso de protocolos seguros de transferencia.

4. ¿Tiene garantías de que tus datos no son accesibles para otros clientes?

El proveedor de servicios debe aplicar medidas que limiten el uso fraudulento de los datos e impidan su pérdida o corrupción. Para evitarlo, existen procesos como el **bastionado de sistemas**, cuya finalidad es garantizar la máxima seguridad posible de los equipos, redes o sistemas informáticos. Algunas de sus acciones son la implementación de antivirus, la fortificación de contraseñas, la autenticación de doble factor o los cortafuegos.

5. ¿Asegura garantías de alta disponibilidad de tus datos?

La alta disponibilidad o HA (high availability) es la capacidad de un proveedor de asegurar que los sistemas siguen disponibles para su uso ante posibles fallos. Más el grado con el que los recursos de los sistemas están activos o disponibles para que el usuario final pueda utilizarlos.

La redundancia de hardware o tener los sistemas redundados significa duplicar los sistemas, y sirve para mover virtualmente las máquinas a aquellos sitios donde ha habido un fallo, algo que no debe repercutir a los usuarios y las empresas que tienen contratados los servicios de cloud.

6. ¿El sistema dispone de flexibilidad y capacidad de escalabilidad según las necesidades?

¿El uso de los recursos se puede escalar en función de tus necesidades? La flexibilidad y evolución de producto es indispensable para tu empresa, por si en otro contexto determinado necesitas expandir características técnicas y que el producto se adapte a tu crecimiento, a todos los cambios del negocio, y a todas las áreas. Una solución SaaS flexible y escalable responde sin limitación para llevar a cabo cualquier iniciativa, y te ofrece la posibilidad de invertir en aquellas soluciones, módulos y opciones que tu empresa necesita, adaptándose al ritmo de crecimiento de tu negocio.

7. ¿Tiene medidas para extraer todos tus datos en caso de finalización de contrato u otras necesidades que lo requieran?

Hay que garantizar el cumplimiento de la normativa vigente en materia de recogida y tratamiento de datos personales, en caso de finalización de contrato u otras situaciones que lo requieran. Los datos introducidos son del cliente, y por tanto el SaaS tiene que ofrecer facilidades para la gestión y portabilidad de los datos; ya sean herramientas de exportación de datos o mecanismos para la eliminación de datos personales.

En caso de finalización de contrato así como otras necesidades que requieran la portabilidad de dichos datos, hay que garantizar lo dispuesto por la normativa vigente en materia de protección de datos. En este sentido, los datos introducidos son titularidad del cliente, y por tanto el SaaS tiene que ofrecer mecanismos para la gestión de dichos datos una vez finalizada la prestación de los servicios, ya sean herramientas que permitan la portabilidad de dichos datos, la eliminación de los mismos, o en su caso, si aplica legalmente, la conservación de los mismos debidamente bloqueados como establece la ley.

8. ¿Dispone del sistema de gestión de los sistemas de información implementado y en funcionamiento?

El estándar internacional de seguridad ISO/IEC 27001 es una certificación que asegura el cumplimiento de los criterios para una gestión de la información correcta y segura, y permite trasladar la garantía de que los datos de los clientes se tratan con total seguridad, con medidas como la implementación de una política efectiva para la gestión de la seguridad de la información, etc.

La seguridad de tus datos es una de nuestras prioridades.

Con Emburse Captio, disfrutarás de un entorno seguro y estable que te permitirá centrarte en lo importante, tu negocio.

En Emburse Captio desde siempre adoptamos una política de seguridad de la información propia, que nos permita establecer un modelo de actuación para desarrollar una cultura de empresa, una forma de trabajar y de tomar decisiones en Captio, así como lograr que la seguridad de la información y el respeto a los datos personales sean una constante.

Y, además te garantizamos:

- **Cumplimiento de la Ley GDPR**
- **Certificado Bureau Veritas**
- Alojamiento en el cloud de Microsoft Azure
- 100 % de cumplimiento del servicio SLA basado en la metodología ITIL
- **Certificación bajo el estándar internacional de seguridad ISO/IEC 27001**

Puedes encontrar más información sobre nuestra garantía y seguridad **aquí.**

emburse captio