Confidencialidad

AWS proporciona servicios que le ayudan a proteger sus datos, cuentas y cargas de trabajo del acceso no autorizado. Los servicios de protección de datos de AWS proporcionan cifrado y administración de claves y detección de amenazas que monitorizan y protegen continuamente sus cuentas y cargas de trabajo.

AWS te da a elegir cómo proteger su contenido. Le ofrecemos un cifrado seguro del contenido en tránsito y en reposo, y le brindamos la opción de administrar sus propias claves de cifrado. Estas características incluyen:

Funciones de cifrado de datos disponibles en los servicios de almacenamiento y base de datos de AWS, como Amazon Elastic Block Store, Amazon Simple Storage Service, Amazon Relational Database Service y Amazon Redshift.

Opciones flexibles de administración de claves, como AWS Key Management Service (KMS), que permiten a los clientes elegir si AWS administra las claves de cifrado o si quiere mantener el control total sobre ellas.

Los clientes de AWS pueden implementar el Cifrado del lado del servidor (SSE) con las claves gestionadas de Amazon S3 (SSE-S3), SSE con las claves gestionadas de AWS KMW (SSE-KMS) o SSE con claves de cifrado provistas por el cliente (SSE-C).

Integridad

AWS identifica las amenazas mediante el monitoreo continuo de la actividad de la red y del comportamiento de la cuenta dentro del entorno de su nube.

A nivel de integridad y confidencialidad de estos, proporciona privacidad y seguridad de extremo a extremo, aspecto que lo hace ideal para realizar backup de nuestros archivos personales y empresariales.

Para lograr esos niveles de seguridad, los centros de datos de esta reconocida empresa cuentan con varias capas de seguridad TI, tanto física como operativa. Además, Amazon realiza auditorías de manera recurrente a los fines de garantizar la seguridad física de su infraestructura.

Disponibilidad

AWS ofrece la disponibilidad de red más alta que cualquier proveedor de nube, con 7 veces menos horas de inactividad que el siguiente proveedor de nube más grande.Cada región está completamente aislada y compuesta de múltiples AZ, que son particiones completamente aisladas de nuestra infraestructura. Para aislar mejor cualquier problema y lograr un nivel de disponibilidad alto, puede dividir las aplicaciones en varias AZ en la misma región. Además, los planos de control de AWS y la consola de administración de AWS se distribuyen en regiones e incluyen puntos de enlace de API regionales, que están diseñados para funcionar de forma segura durante por lo menos 24 horas en caso de quedar aislados de las funciones del plano de control global sin necesidad de que los clientes accedan a la región o a sus puntos de enlace de API mediante redes externas durante cualquier aislamiento.

Control de acceso

Como cliente, mantiene el control completo de su contenido y la responsabilidad de configurar el acceso a los servicios y recursos de AWS. Proporcionamos un conjunto avanzado de características de acceso, cifrado y registro que le ayudarán a llevar esto a cabo de forma eficaz (por ejemplo: AWS Identity and Access Management, AWS Organizations y AWS CloudTrail). Proporcionamos API para que configure los permisos de control de acceso para cualquier dispositivo que desarrolle o implemente en un entorno de AWS. No accedemos a su contenido ni lo usamos para ningún otro fin sin su consentimiento. En ningún momento utilizamos su contenido ni extraemos información para marketing o publicidad.