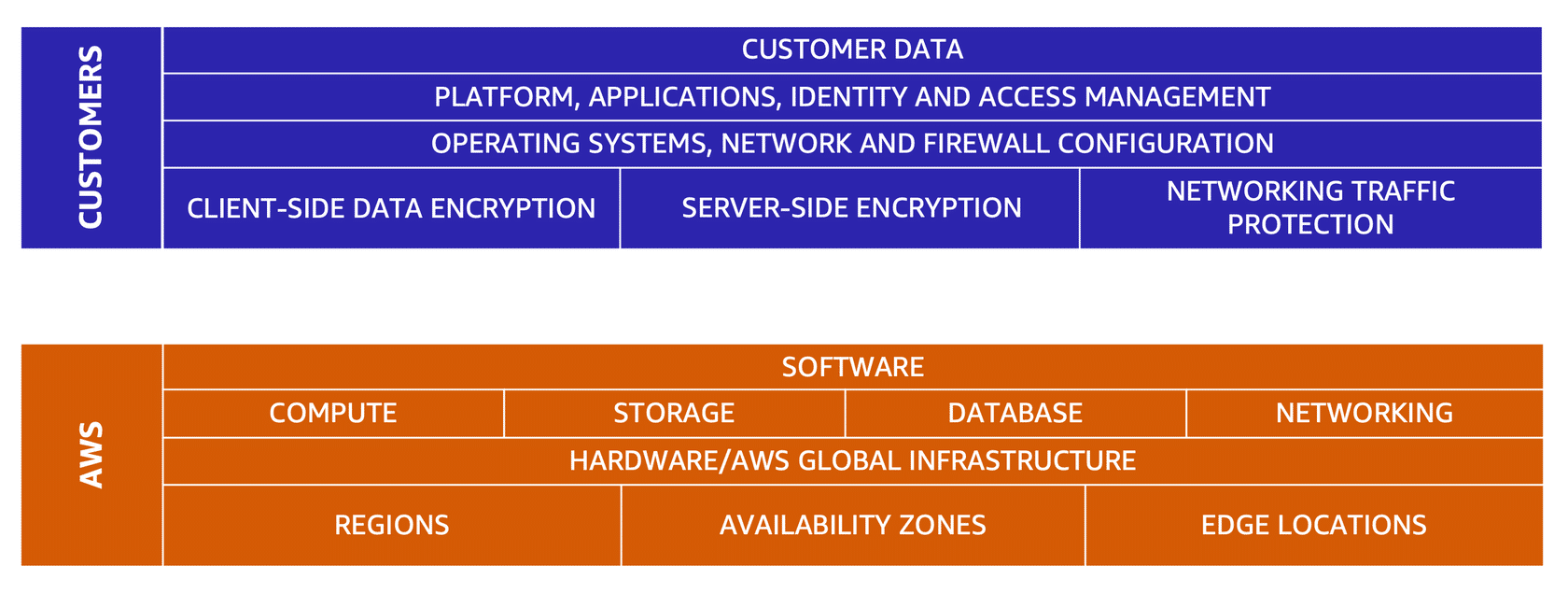
**Shared Responsibility Model**

**The AWS Shared Responsibility Model**

Throughout this course, you have learned about a variety of resources that you can create in the AWS Cloud. These resources include Amazon EC2 instances, Amazon S3 buckets, and Amazon RDS databases. Who is responsible for keeping these resources secure: you (the customer) or AWS?

The answer is both. The reason is that you do not treat your AWS environment as a single object. Rather, you treat the environment as a collection of parts that build upon each other. AWS is responsible for some parts of your environment and you (the customer) are responsible for other parts. This concept is known as the **[shared responsibility model](https://aws.amazon.com/compliance/shared-responsibility-model/" \t "_blank)**.

The shared responsibility model divides into customer responsibilities (commonly referred to as “security in the cloud”) and AWS responsibilities (commonly referred to as “security of the cloud”).



You can think of this model as being similar to the division of responsibilities between a homeowner and a homebuilder. The builder (AWS) is responsible for constructing your house and ensuring that it is solidly built. As the homeowner (the customer), it is your responsibility to secure everything in the house by ensuring that the doors are closed and locked.

**Customers: Security in the Cloud**

Customers are responsible for the security of everything that they create and put *in*the AWS Cloud.

When using AWS services, you, the customer, maintain complete control over your content. You are responsible for managing security requirements for your content, including which content you choose to store on AWS, which AWS services you use, and who has access to that content. You also control how access rights are granted, managed, and revoked.

The security steps that you take will depend on factors such as the services that you use, the complexity of your systems, and your company’s specific operational and security needs. Steps include selecting, configuring, and patching the operating systems that will run on Amazon EC2 instances, configuring security groups, and managing user accounts.

**AWS: Security of the Cloud**

AWS is responsible for security *of*the cloud.

AWS operates, manages, and controls the components at all layers of infrastructure. This includes areas such as the host operating system, the virtualization layer, and even the physical security of the data centers from which services operate.

AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure includes AWS Regions, Availability Zones, and edge locations.

AWS manages the security of the cloud, specifically the physical infrastructure that hosts your resources, which include:

* Physical security of data centers
* Hardware and software infrastructure
* Network infrastructure
* Virtualization infrastructure

Although you cannot visit AWS data centers to see this protection firsthand, AWS provides several reports from third-party auditors. These auditors have verified its compliance with a variety of computer security standards and regulations.

==================== ESPAÑOL =====================

**Modelo de Responsabilidad Compartida de AWS**

A lo largo de este curso, has aprendido acerca de una variedad de recursos que puedes crear en la nube de AWS. Estos recursos incluyen instancias de Amazon EC2, buckets de Amazon S3 y bases de datos de Amazon RDS. ¿Quién es responsable de mantener seguros estos recursos: tú (el cliente) o AWS?

La respuesta es ambos. La razón es que no consideras tu entorno de AWS como un objeto único. Más bien, tratas el entorno como una colección de partes que se construyen una sobre la otra. AWS es responsable de algunas partes de tu entorno y tú (el cliente) eres responsable de otras partes. Este concepto se conoce como el modelo de responsabilidad compartida.

El modelo de responsabilidad compartida se divide en responsabilidades del cliente (comúnmente conocidas como "seguridad en la nube") y responsabilidades de AWS (comúnmente conocidas como "seguridad de la nube").

Puedes pensar en este modelo como similar a la división de responsabilidades entre un propietario de vivienda y un constructor de viviendas. El constructor (AWS) es responsable de construir tu casa y asegurarse de que esté sólidamente construida. Como propietario (el cliente), es tu responsabilidad asegurar todo en la casa asegurándote de que las puertas estén cerradas y con llave.

Clientes: Seguridad en la Nube

Los clientes son responsables de la seguridad de todo lo que crean y ponen en la nube de AWS.

Cuando utilizas los servicios de AWS, tú, el cliente, mantienes un control completo sobre tu contenido. Eres responsable de administrar los requisitos de seguridad de tu contenido, incluido qué contenido eliges almacenar en AWS, qué servicios de AWS utilizas y quién tiene acceso a ese contenido. También controlas cómo se otorgan, administran y revocan los derechos de acceso.

Los pasos de seguridad que tomas dependerán de factores como los servicios que utilizas, la complejidad de tus sistemas y las necesidades específicas de operación y seguridad de tu empresa. Los pasos incluyen la selección, configuración y parcheo de los sistemas operativos que se ejecutarán en las instancias de Amazon EC2, la configuración de grupos de seguridad y la administración de cuentas de usuario.

AWS: Seguridad de la Nube

AWS es responsable de la seguridad de la nube.

AWS opera, administra y controla los componentes en todas las capas de la infraestructura. Esto incluye áreas como el sistema operativo del host, la capa de virtualización e incluso la seguridad física de los centros de datos desde los cuales funcionan los servicios.

AWS es responsable de proteger la infraestructura global que ejecuta todos los servicios ofrecidos en la nube de AWS. Esta infraestructura incluye Regiones de AWS, Zonas de Disponibilidad y ubicaciones periféricas.

AWS gestiona la seguridad de la nube, específicamente la infraestructura física que aloja tus recursos, que incluye:

Seguridad física de los centros de datos

Infraestructura de hardware y software

Infraestructura de red

Infraestructura de virtualización

Aunque no puedes visitar los centros de datos de AWS para ver esta protección de primera mano, AWS proporciona varios informes de auditores externos. Estos auditores han verificado su cumplimiento con una variedad de normas y regulaciones de seguridad informática.