EL MODELO DE RESPONSABILIDAD COMPARTIDA DE AWS

CONTENIDO

EL MODELO DE RESPONSABILIDAD COMPARTIDA

En el modelo tradicional on-premises (en las instalaciones), el cliente tiene su propio centro de datos, sus servidores y su infraestructura localmente en su empresa. A diferencia de la computación en la nube, los clientes de on-premises obtienen todo el control de sus recursos y también asumen todos los riesgos bajo su responsabilidad.

Responsabilidades del cliente en un modelo tradicional local:

Control absoluto: El cliente tiene control sobre todos los recursos y los datos y decide quiénes pueden acceder a ellos.

Operación y mantenimiento: El cliente es responsable de mantener y gestionar la infraestructura, incluyendo servidores, almacenamiento y redes, así como de implementar y actualizar el software localmente.

Costos: Además de los riesgos, el cliente asume los costos generados por la utilización de los recursos, como tasas de mantenimiento y costos de funcionamiento de hardware y software.

Es decir, el cliente tiene la responsabilidad de operar y mantener el software y el hardware en su propio entorno informático, lo que le brinda mayor control, pero también implica más carga operativa y mayores costos.

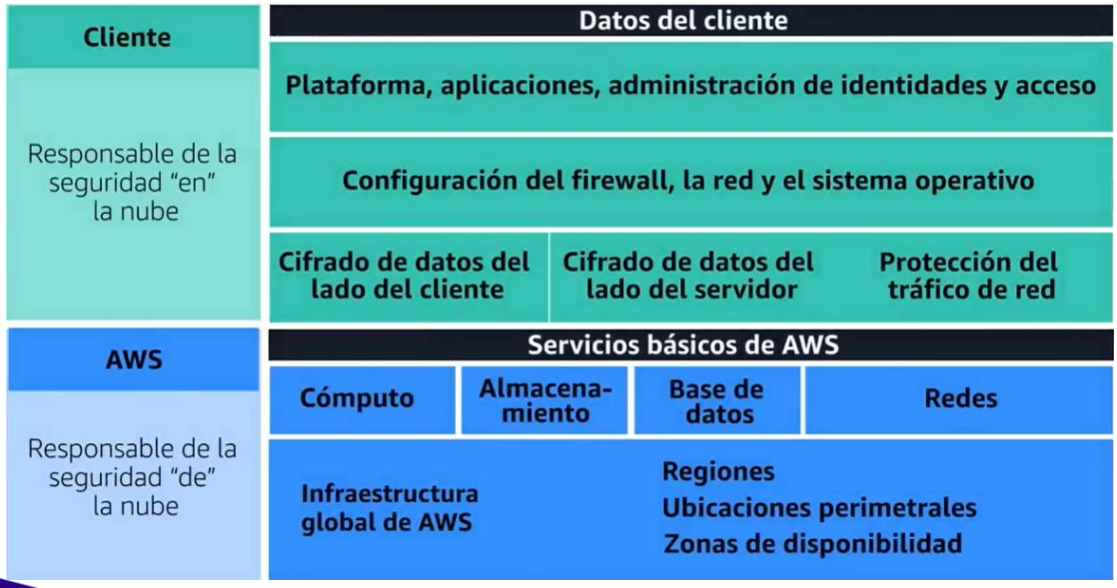
Recordemos el ejemplo de la pizza como servicio, este modelo sería el tipo de pizza casera desde cero en el que somos responsables de todo el proceso, desde comprar los ingredientes y hacer la preparación, hasta la limpieza de los platos.
Tener nuestro propio datacenter es igual que cocinar en casa, se deben conseguir todos los ingredientes por separado, tener toda la infraestructura disponible y los conocimientos para la preparación.

EL MODELO DE RESPONSABILIDAD COMPARTIDA DE AWS

A lo largo de este bootcamp, ha aprendido sobre una variedad de recursos que puede crear en la nube de AWS. Estos recursos incluyen instancias de Amazon EC2, buckets de Amazon S3 y bases de datos de Amazon RDS. Por lo que es importante preguntarse ¿Quién es responsable de mantener la seguridad de estos recursos: ¿Usted (el cliente) o AWS? Y la respuesta es ambos.

Ambos son responsables de asegurarse de estar protegidos. Ahora, si hay algún experto en seguridad en este bootcamp tal vez esté negando con la cabeza diciendo que no puede haber dos entidades diferentes con la responsabilidad final sobre un solo objeto, que eso no es seguridad y que es una ilusión. En AWS, están totalmente de acuerdo con eso, pero AWS no considera el entorno como un solo objeto, sino que lo ve como una colección de piezas que se basan unas en otras.

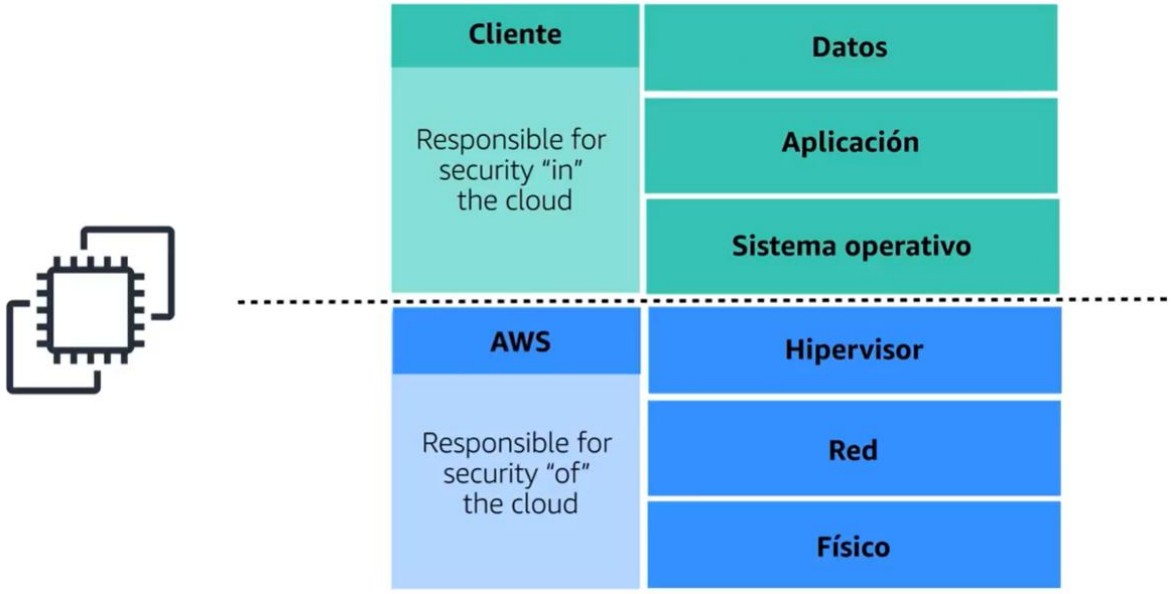
AWS es responsable de algunas partes de su entorno y usted (el cliente) es responsable de otras partes. Esto es lo que se conoce como el modelo de responsabilidad compartida.



No es diferente a asegurar una casa. El constructor construyó la casa con cuatro paredes y una puerta, por lo tanto, es su responsabilidad asegurarse de que las paredes sean fuertes y que las puertas sean sólidas. Como propietario, usted tiene la responsabilidad de cerrar y bloquear las puertas. Realmente es así de sencillo en AWS también.

Ejemplo del modelo de responsabilidad compartida en una EC2

EC2 vive en un edificio físico, en un centro de datos que debe protegerse.
Tiene una red y un hipervisor que admiten las instancias con sus sistemas operativos individuales. Además del sistema operativo tiene su aplicación que admite sus datos. Así que para EC2 y todos los servicios que ofrece AWS, hay una pila similar de partes que se construyen unas sobre otras. AWS es 100 % responsable de algunas, mientras que usted es responsable de las demás.



Entonces empecemos por la capa física. Esto es hierro, concreto, vallas y guardas de seguridad. Alguien tiene que poseer el concreto; alguien tiene que controlar el perímetro físico, todos los días, las 24 horas. Esto es AWS.

Sobre la capa física tenemos nuestra red y nuestro hipervisor. No vamos a entrar en detalles sobre cómo todo esto está asegurado, pero básicamente AWS reinventa esas tecnologías para hacerlas más rápidas, más fuertes y a prueba de manipulaciones.
Pero no tenemos que creer en la palabra de AWS, AWS tiene numerosos auditores externos que han revisado el código y la forma en que construyen su infraestructura y pueden

proporcionar la documentación adecuada que necesitamos para las estructuras de cumplimiento de seguridad.

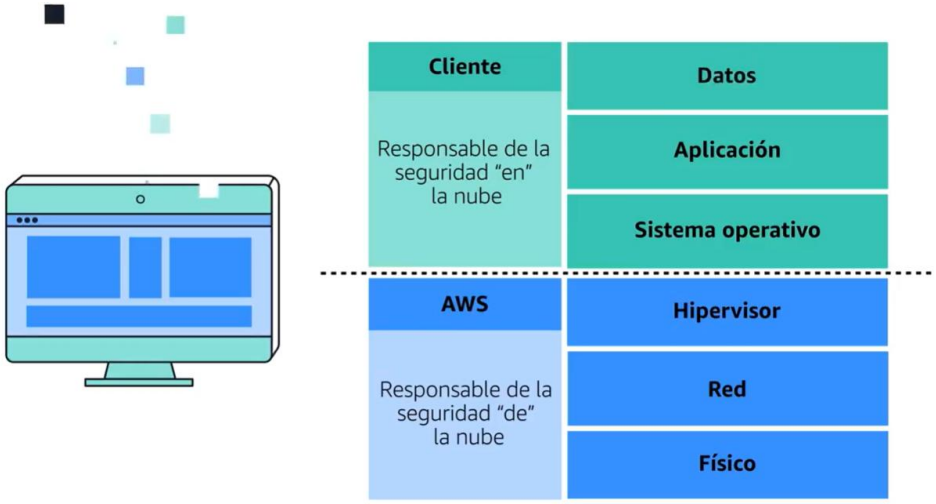
Ahora, además de todo eso, en EC2, ahora podemos elegir qué sistema operativo queremos ejecutar. Esta es la línea divisoria mágica que separa nuestra responsabilidad. La responsabilidad de AWS y la del cliente. Este es el sistema operativo, el cliente está 100% a cargo de esto.

AWS no tiene ninguna puerta trasera en su sistema aquí, usted y solo usted tiene la clave única de cifrado para iniciar sesión en la raíz de este sistema operativo o para crear cualquier cuenta de usuario allí. Es decir, así como una empresa constructora no guardaría copias de la llave de la puerta principal de una casa, AWS no puede entrar en nuestro sistema operativo.
Y aquí hay una sugerencia: Si alguien de AWS llama y le pide la clave de su sistema operativo, no es AWS.

Eso significa que su equipo de operaciones es 100% responsable de mantener el sistema operativo parchado. Si AWS descubre que hay algunas vulnerabilidades nuevas en su versión de Windows, por ejemplo, pueden notificar al propietario de la cuenta, pero no pueden implementar un parche. Esto es realmente bueno para su seguridad, significa que nadie puede implementar nada que pueda romper su sistema sin que su equipo sea el que lo haga.

Ahora, sobre ese sistema operativo, puede ejecutar las aplicaciones que desee, son suyas, usted las mantiene. Lo que nos lleva a la parte más importante de la pila: Sus datos. Este es siempre el dominio que usted debe controlar y a veces es posible que desee tener sus datos abiertos para que todos los vean, como imágenes en un sitio web minorista. Otras veces, como en el sector bancario o de salud, no debe tenerlos tan al alcance.

AWS proporciona a sus clientes el conjunto de herramientas que necesitan para que los datos se compartan a algunas personas autorizadas, a todos, a una sola persona en condiciones específicas, o incluso brinda la posibilidad de bloquearlos para que nadie pueda acceder a ellos.
Además, proporciona la capacidad de tener un cifrado ubicuo, es decir, un cifrado de manera generalizada y constante en todos los datos, de esa manera, incluso si accidentalmente dejó la puerta abierta, todo lo que alguien vería es contenido cifrado ilegible.



El modelo de responsabilidad compartida de AWS trata de asegurarse de que ambas partes entiendan exactamente cuáles son las tareas que le pertenecen.

Básicamente, AWS es responsable **de** la seguridad de la nube y el cliente es responsable de la seguridad **en** la nube. Juntos tienen un entorno en el que podemos confiar.

CLIENTES: Seguridad EN la nube

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

Al utilizar los servicios de AWS, usted, el cliente, mantiene un control total sobre su contenido. Usted es responsable de administrar los requisitos de seguridad del contenido, incluido qué contenido decide almacenar en AWS, qué servicios de AWS utiliza y quién tiene acceso a ese contenido. También puede controlar el modo en que se conceden, administran y revocan los permisos de acceso.

Los pasos de seguridad que realice dependerán de algunos factores, como los servicios que utilice, la complejidad de los sistemas y las necesidades operativas y de seguridad específicas de su empresa. Los pasos incluyen la selección, configuración y aplicación de parches en los sistemas operativos que se ejecutarán en instancias de Amazon EC2, configuración de grupos de seguridad y administración de cuentas de usuario.

AWS: 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 host, la capa de virtualización e incluso la seguridad física de los centros de datos desde los que operan los servicios.

AWS tiene la responsabilidad de proteger la infraestructura mundial que ejecuta todos los servicios ofrecidos en la nube de AWS. Esa infraestructura incluye las regiones de AWS, las zonas de disponibilidad y las ubicaciones perimetrales.

AWS administra la seguridad **DE** la nube, en especial la infraestructura física que aloja los recursos, que incluye lo siguiente:

- Seguridad física de los centros de datos
- Infraestructura de hardware y software
- Infraestructura de red
- Infraestructura de virtualización

Aunque los clientes no pueden visitar los centros de datos de AWS para ver esta protección de primera mano, AWS proporciona varios informes de auditores terceros. Estos auditores han verificado la conformidad con una variedad de normas y reglamentos de seguridad informática.

Entidad responsable	Parte del entorno de AWS
Cliente	Datos del cliente
	Plataforma, aplicaciones e Identity and Access Management (IAM)
	Sistemas operativos y configuración de red y firewall
	Cifrado de datos del lado del cliente, cifrado de datos del lado del servidor y protección de tráfico de redes
Amazon Web Services (AWS)	**Software:** cómputo, almacenamiento, base de datos y redes
	Hardware: región, zona de disponibilidad y ubicación perimetral

Entendiendo a detalle el modelo de responsabilidad compartida de AWS

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, administra y controla los componentes del sistema operativo host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios.
El cliente asume la responsabilidad y la administración del sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), de cualquier otro software de aplicaciones asociado y de la configuración del firewall del grupo de seguridad que ofrece AWS.

Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en su entorno de TI y de la legislación y los reglamentos correspondientes. La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y el control por parte del cliente que permite concretar la implementación.

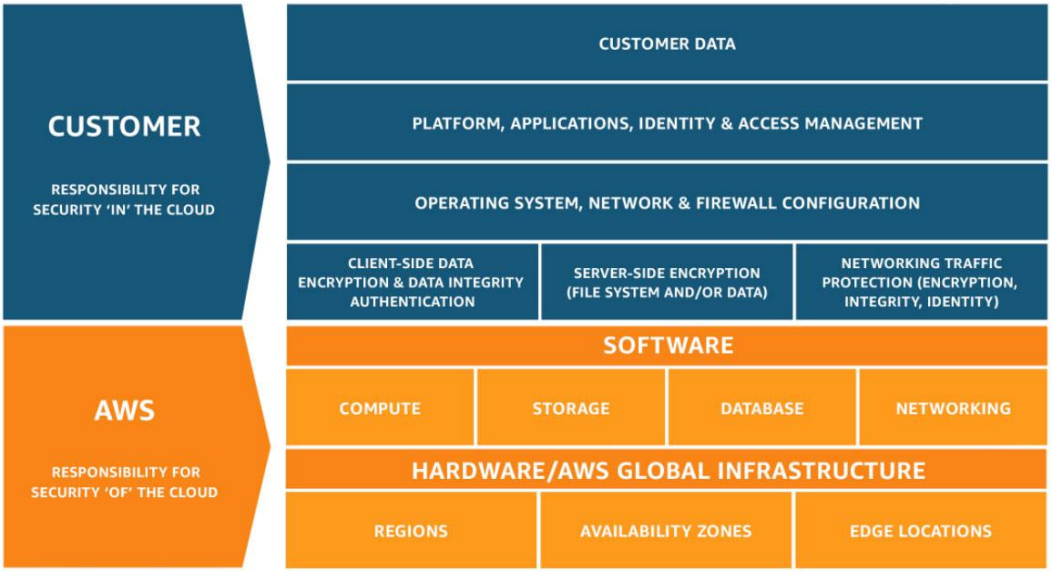
La diferenciación de responsabilidades se conoce normalmente como seguridad "de" la nube y seguridad "en" la nube.

Responsabilidad de AWS en relación con la "seguridad de la nube": AWS es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Responsabilidad del cliente en relación con la "seguridad en la nube": La responsabilidad del cliente estará determinada por los servicios de la nube de AWS que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como Infraestructura como servicio (IaaS) y, como tal, requiere que el cliente realice todas las tareas de administración y configuración de seguridad necesarias. Los clientes que implementan una instancia de Amazon EC2 son responsables de la administración del sistema operativo huésped (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por AWS (llamado grupo de seguridad) en cada instancia.

En el caso de los servicios administrados, como Amazon S3 y Amazon DynamoDB, AWS maneja la capa de infraestructura, el sistema operativo y las plataformas, mientras que los

clientes acceden a los puntos de enlace para recuperar y almacenar los datos. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar las herramientas de IAM para solicitar los permisos correspondientes.



Este modelo de responsabilidad compartida entre los clientes y AWS también abarca los controles de TI. De la misma forma que AWS y sus clientes comparten la responsabilidad del funcionamiento del entorno de TI, también comparten la administración, el funcionamiento y la verificación de los controles de TI. AWS puede ayudar a aliviar la carga que supone para los clientes operar los controles, para lo que administra los controles asociados con la infraestructura física implementada en el entorno de AWS de cuya administración se encargaba anteriormente el cliente.

Dado que la implementación de cada cliente se realiza de manera diferente en AWS, los clientes tienen la oportunidad de migrar a AWS la administración de determinados controles de TI para obtener un nuevo entorno de control distribuido. Los clientes pueden usar la documentación de conformidad y control de AWS disponible para ejecutar sus procedimientos de verificación y evaluación de controles según sea necesario.

A continuación, presentaremos ejemplos de controles cuya administración está a cargo de AWS, de los clientes de AWS o de ambos.

Controles heredados: Controles que un cliente hereda totalmente de AWS.

- Controles físicos y de entorno

Controles compartidos: Controles que se aplican tanto a la capa de la infraestructura como a las capas de los clientes, pero en contextos o perspectivas completamente independientes. En un control compartido, AWS suministra los requisitos para la infraestructura y el cliente debe proveer su propia implementación de controles en el uso que haga de los servicios de AWS. Entre los ejemplos se incluyen:

- *Administración de parches*: AWS es responsable de implementar parches y de corregir imperfecciones en el interior de la infraestructura, pero los clientes son responsables de implementar parches en sus aplicaciones y sistemas operativos huésped.

- *Administración de configuración*: AWS mantiene la configuración de sus dispositivos de infraestructura, pero el cliente es responsable de configurar sus aplicaciones, bases de datos y sistemas operativos huésped.

- *Información y formación técnica*: AWS capacita a los empleados de AWS, pero el cliente debe capacitar a sus propios empleados.

Controles específicos del cliente: Controles que son de absoluta responsabilidad del cliente en función de la aplicación que implementa dentro de los servicios de AWS. Entre los ejemplos se incluyen:

- Seguridad de zona o protección de comunicaciones y servicios, que podrían necesitar que el cliente direccione o separe en zonas datos en entornos de seguridad específicos.

Aplicación del modelo de responsabilidad compartida de AWS en la práctica

Una vez que un cliente entiende el modelo de responsabilidad compartida de AWS y cómo se aplica en general a la operación en la nube, debe determinar cómo se aplica a su caso de uso.
La responsabilidad del cliente varía en función de muchos factores, como los servicios de AWS y las regiones que elija, la integración de dichos servicios en su entorno de TI y las leyes y normativas aplicables a su organización y carga de trabajo.