AWS ORGANIZATIONS Y AWS ARTIFACT

CONTENIDO

AWS ORGANIZATIONS

Con su primera incursión en la nube de AWS, lo más probable es que comience con una cuenta de AWS y que todo resida allí. La mayoría de las personas empiezan de esta manera, pero a medida que la empresa crece o incluso comienza el traspaso a la nube, es importante separar las tareas.

Por ejemplo, quiere que los desarrolladores tengan acceso a recursos de desarrollo, que el personal de contabilidad pueda acceder a la información de facturación, o incluso tener unidades de negocio separadas para que puedan experimentar con los servicios de AWS sin afectarse mutuamente.
Así que empieza a agregar más cartas para cada persona o para quien necesite incorporarse y antes de darse cuenta, termina con un tazón enredado de espaguetis de cuentas de AWS, no tan sabrosos como uno imagina.
Por ejemplo, tendrá que hacer un seguimiento de las cuentas A, F y G, o tal vez la cuenta B tiene permisos incorrectos y la cuenta C tiene información sobre facturación y cumplimiento.

Una forma de instalar el orden y hacer cumplir a quién se le permite realizar ciertas funciones y en qué cuenta, es hacer uso de un servicio de AWS llamado AWS Organizations.
La forma más sencilla de pensar en Organizations es como ***una ubicación central para administrar varias cuentas de AWS***.
Al crear una organización, AWS Organizations crea automáticamente una raíz, que es el contenedor principal de todas las cuentas de su organización. Puede administrar el control de facturación, el acceso, el cumplimiento, la seguridad y compartir recursos entre sus cuentas de AWS.

PRINCIPALES FUNCIONES DE AWS ORGANIZATIONS

Administración centralizada de todas sus cuentas de AWS: Piense en todas esas cuentas que teníamos: A, B, C, F, G. Ahora puede combinarlas en una organización que nos permita administrar las cuentas de forma centralizada y, ahora hemos encontrado las cuentas D y E en el proceso.

Facturación unificada para todas las cuentas de miembros: Esto significa que puede usar la cuenta principal de la organización para consolidar y pagar todas las cuentas de los miembros.

Otra ventaja de la facturación unificada son los descuentos por volumen, un ahorro interesante.

Control sobre los servicios de AWS y las acciones de API a las que cada cuenta pueda acceder como administrador de la cuenta principal de una organización: Puede utilizar algo llamado políticas de control de servicio, o Service Control policies, SCP, para especificar los permisos máximos para las cuentas de los miembros de la organización.

En AWS Organizations, puede controlar de forma centralizada los permisos de las cuentas de su organización mediante las políticas de control de servicios (SCP). Las SCP le permiten imponer restricciones a los servicios, los recursos y las acciones de API individuales de AWS a los que pueden acceder los usuarios y los roles de cada cuenta.

En resumen, con las Service Control Policies puede restringir a qué servicios, recursos de AWS y acciones de API individuales pueden acceder los usuarios y roles de cada cuenta de miembros.

Implementar agrupaciones jerárquicas de cuentas para satisfacer las necesidades de seguridad, cumplimiento o de presupuesto: Esto significa que puede agrupar cuentas en unidades organizativas, o OU, algo similar a las unidades de negocio, o Business Unity, BU. Por ejemplo, si tiene cuentas que solo deben acceder a los servicios de AWS que cumplen ciertos requisitos normativos, puede colocar esas cuentas en una OU, Unidad Organizativa, o si tiene cuentas incluidas en la unidad organizativa del desarrollador, puede agruparlas en consecuencia.

UNIDADES ORGANIZATIVAS

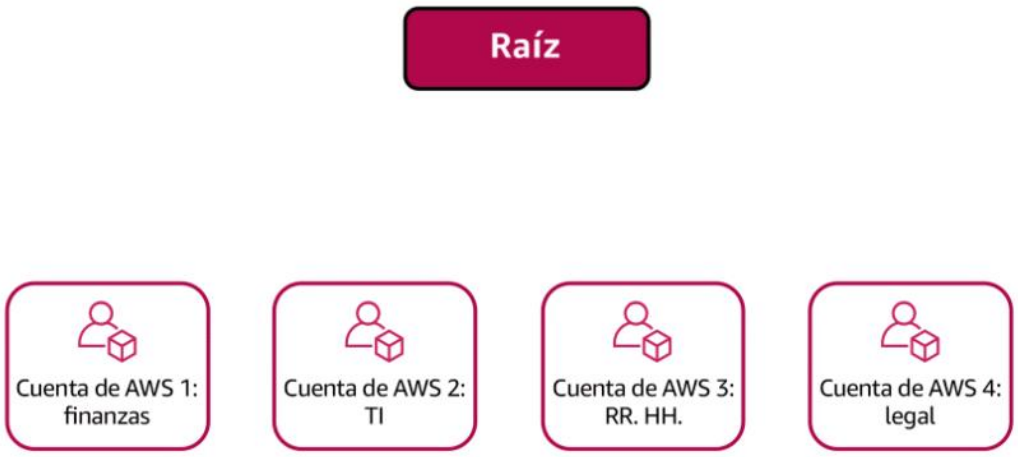
En AWS Organizations, puede agrupar las cuentas en unidades organizativas (OU) para facilitar la administración de cuentas con requisitos empresariales o de seguridad similares. Al aplicar una política a una unidad organizacional, todas las cuentas de la unidad organizacional heredan automáticamente los permisos especificados en la política.

Al organizar cuentas independientes en las OU, puede aislar con más facilidad las cargas de trabajo o las aplicaciones que tienen requisitos de seguridad específicos. Por ejemplo, si su empresa tiene cuentas que solo pueden acceder a los servicios de AWS que cumplen determinados requisitos reglamentarios, puede colocar estas cuentas en una unidad organizacional. Luego, puede adjuntar una política a la OU que bloquea el acceso a todos los demás servicios de AWS que no cumplen con los requisitos normativos.

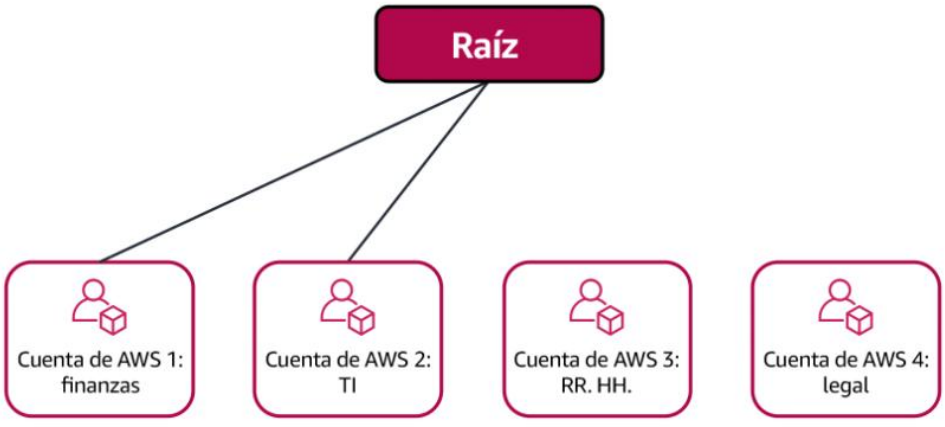
Ejemplo de cómo una empresa puede utilizar AWS Organizations

Paso 1: Imagine que su empresa tiene cuentas de AWS independientes para los departamentos de finanzas, tecnología de la información (TI), recursos humanos (RR HH) y legal. Decide consolidar estas cuentas en una sola organización para poder administrarlas desde una ubicación central. Al momento de crear la organización, se establece la raíz.

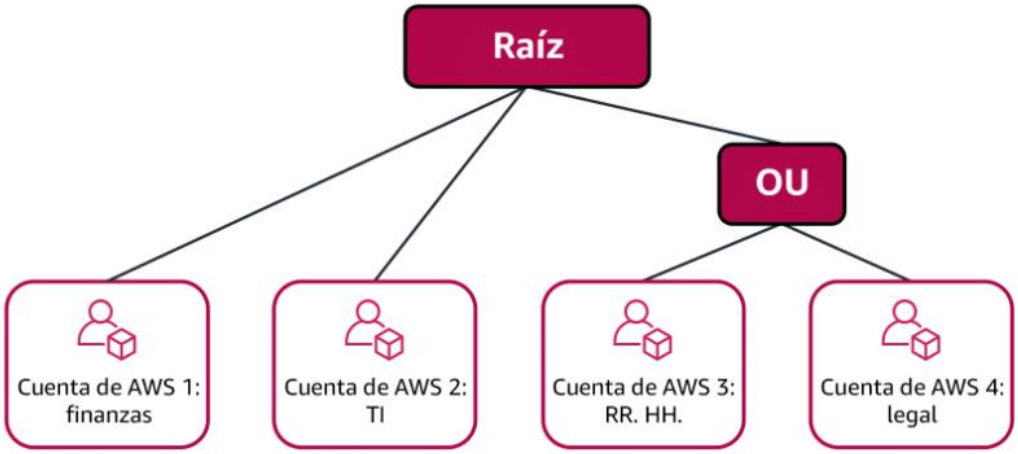
Con el diseño de su organización, debe considerar las necesidades empresariales, de seguridad y normativas de cada departamento. Esta información se utiliza para decidir qué departamentos se agrupan en unidades organizacionales.



Paso 2: Los departamentos de Finanzas y TI tienen requisitos que no se superponen con los de ningún otro departamento. Incorpora estas cuentas a su organización para aprovechar beneficios como la facturación unificada, pero no las coloca en ninguna unidad organizacional.

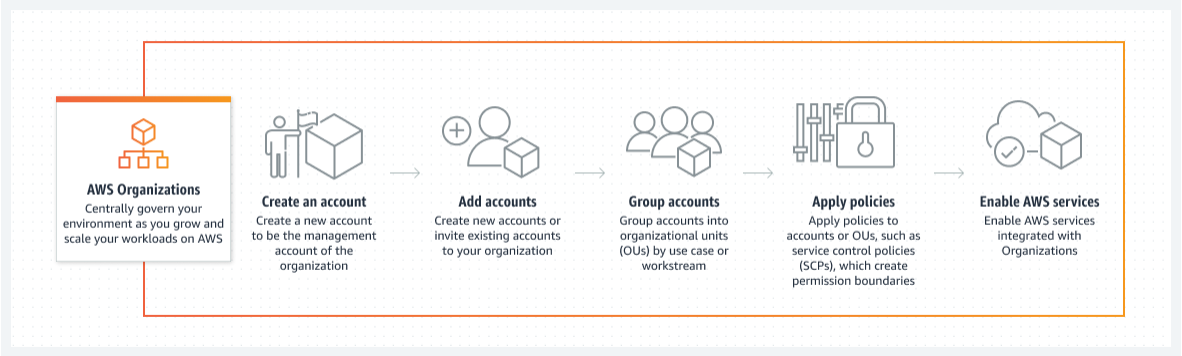


Paso 3: Los departamentos de Recursos Humanos y Legales necesitan acceder a los mismos servicios y recursos de AWS, de modo que los puede colocar juntos en una OU. Colocarlos en una OU le permite adjuntar políticas que se aplican tanto a las cuentas de AWS de los departamentos de Recursos Humanos como de los departamentos Legales.



FUNCIONAMIENTO DE AWS ORGANIZATIONS

AWS Organizations le permite crear cuentas nuevas de AWS sin costo adicional. Con cuentas en la organización, puede asignar recursos, agrupar cuentas y aplicar políticas de gobernanza a cuentas o grupos fácilmente.



BENEFICIOS DE AWS ORGANIZATIONS

AWS le permite experimentar, innovar y escalar con más rapidez, todo ello a la vez que le brinda el entorno en la nube más flexible y seguro. Un medio importante a través del cual AWS garantiza la seguridad de sus aplicaciones es la cuenta de AWS. Una cuenta de AWS brinda seguridad natural, acceso y límites de facturación para sus recursos de AWS, y le permite lograr la independencia y el aislamiento de los recursos. Por ejemplos, los usuarios ajenos a su cuenta no tienen acceso a sus recursos de forma predeterminada. De manera similar, el costo de los recursos de AWS que consume está asignado a su cuenta. Aunque puede comenzar su viaje con AWS desde una sola cuenta, AWS le recomienda que configure varias cuentas a medida que sus cargas de trabajo aumentan de tamaño y complejidad. Utilizar un entorno de varias cuentas es una práctica recomendada por AWS que ofrece diferentes beneficios:

- **Innovación rápida con diferentes requisitos**: Puede asignar cuentas de AWS a diferentes equipos, proyectos o productos dentro de su compañía de manera que asegura que todos pueden innovar con rapidez a la vez que se tienen en cuenta sus propios requisitos de seguridad.

- **Facturación simplificada**: El uso de varias cuentas de AWS simplifica la asignación de su costo de AWS puesto que ayuda a identificar qué línea de productos o servicios es la responsable de un cargo de AWS.

- **Controles de seguridad flexibles**: Puede utilizar varias cuentas de AWS para aislar cargas de trabajo o aplicaciones con requisitos de seguridad específicos, o que necesitan cumplir con normativas estrictas de conformidad, como HIPAA o PCI.

- **Fácil adaptación a procesos empresariales**: Puede organizar con facilidad varias cuentas de AWS de la manera que mejor refleje las diversas necesidades de los procesos empresariales de su compañía que cuentan con diferentes requisitos operativos, normativos y de presupuesto.

CASOS DE USO DE AWS ORGANIZATIONS

Automatice la creación de cuentas de AWS: Cree cuentas de AWS y agréguelas a grupos definidos por los usuarios para poder aplicar políticas de seguridad, desplegar una infraestructura sin contacto e inspeccionar de manera instantánea.

Habilite una protección proactiva con un grupo de seguridad dedicado: Cree un grupo de seguridad y brinde a sus clientes acceso de solo lectura a todos sus recursos a fin de supervisar, identificar y mitigar los problemas de seguridad de forma activa.

Asegure el acceso del usuario a los recursos designados: Habilite un acceso de inicio de sesión único y aplique políticas de control de servicio para permitir únicamente las acciones de los usuarios que cumplan con sus requisitos de seguridad y conformidad.

Comparta recursos comunes entre cuentas: Comparta recursos centrales, aplicaciones de software, directorios y servicios con más facilidad dentro de su organización.

CUMPLIMIENTO

Para cada industria hay estándares específicos que deben respetarse y usted será auditado o inspeccionado para garantizar que los haya cumplido.
Por ejemplo, para una cafetería, el inspector de salud pasará y comprobará que todo está en regla y cumpla con las condiciones sanitarias adecuadas. Del mismo modo, podría ser auditado por impuestos para ver que haya gestionado correctamente el área administrativa y que haya cumplido con la ley. Para poder pasar esas auditorías y comprobaciones de cumplimiento a medida que se presentan, cuenta con documentación, registros e inspecciones.

Tendría que idear una forma similar para satisfacer los requisitos de cumplimiento y las auditorías en AWS, dependiendo del tipo de soluciones que usted aloje en AWS, tendría que asegurarse de cumplir con los estándares y las normas específicos a las que su empresa está sujeta.
Si ejecuta un software que trata con datos de los consumidores en la Unión Europea, tendría que asegurarse de cumplir con el RGPD (Reglamento General de Protección de Datos), o si ejecuta aplicaciones sanitarias en Estados Unidos, tendría que diseñar las arquitecturas para satisfacer los requisitos del cumplimiento de la HIPAA (Ley de Portabilidad y Responsabilidad de los Seguros Médicos).
Cualquiera que sea su necesidad de cumplimiento, necesitará algunas herramientas para poder recopilar documentos, registros e inspeccionar su entorno de AWS para comprobar si satisface las normas de cumplimiento a los que se encuentra sujeto.

Lo primero hay que tener en cuenta es que AWS ya desarrolló la infraestructura y las redes de los centros de datos siguiendo las prácticas recomendadas de seguridad, y como cliente de AWS, usted hereda todas esas prácticas recomendadas de las políticas, la arquitectura, y los procesos operativos de AWS.

AWS cumple con una larga lista de programas de garantía que puede encontrar en línea. Esto significa que hay segmentos del cumplimiento que ya se completaron y que puede centrarse en cumplir con las normas dentro de sus propias arquitecturas que usted desarrolla utilizando AWS.

Lo siguiente que debe saber con respecto al cumplimiento y AWS, es que la región en la que elija operar podría ayudar a cumplir con las normas de cumplimiento. Si solo puede almacenar datos legalmente en el país del que estos proceden, puede elegir una región que le sea conveniente y AWS no replicará los datos en las regiones de forma automática.

También debe estar muy consciente del hecho de que usted es el propietario de sus datos en AWS. Como se muestra en el modelo de responsabilidad compartida, tiene control total sobre los datos que almacena dentro de AWS, puede emplear varios mecanismos de cifrado para mantener los datos seguros y eso varía de un servicio a otro.
Por lo tanto, si necesita estándares específicos para el almacenamiento de datos, puede idear una forma de alcanzar estos requisitos construyéndolo usted mismo a partir de AWS o utilizando las funciones que ya existen en muchos servicios. Para la mayoría de los servicios, habilitar la protección de datos es una opción más de configuración del recurso.

AWS también ofrece varios documentos técnicos e informes que puede descargar y utilizar para informes de cumplimiento. Dado que no está ejecutando el centro de datos usted mismo, puede solicitar a AWS que le proporcione la documentación que demuestre que se están siguiendo las prácticas recomendadas para la seguridad y el cumplimiento.

Un lugar desde el que puede acceder a estos documentos es a través de un servicio llamado AWS Artifact.

AWS ARTIFACT

Con AWS Artifact, puede obtener acceso a los informes de cumplimiento realizados por terceros, que validaron una amplia gama de estándares de cumplimiento.
Allí encontrará servicios de habilitación de cumplimiento, así como documentación, como, por ejemplo, el documento técnico de seguridad y riesgos de AWS, que debe leer para asegurarse de comprender la seguridad y el cumplimiento con AWS. Para saber si cumple con AWS, recuerde que se sigue el modelo de responsabilidad compartida.

La plataforma subyacente es segura y AWS puede proporcionar documentación sobre los tipos de requisitos de cumplimiento que ya satisfacen, a través de servicios como AWS

Artifact e informes de conformidad. Pero, más allá de eso, lo que cree en AWS depende de usted.
Usted controla la arquitectura de las aplicaciones y las soluciones que crea, y deben crearse con el cumplimiento, la seguridad y con el modelo de responsabilidad compartida en mente.

A continuación, se indican algunos de los informes y reglamentos de cumplimiento que puede encontrar en AWS Artifact. Cada informe incluye una descripción de su contenido y del periodo de referencia para el que el documento es válido.

AWS Artifact brinda acceso a los documentos de seguridad y cumplimiento de AWS, como las certificaciones ISO de AWS, los informes del sector de pagos con tarjeta (PCI) y los informes de control de organización y servicio (SOC).

AWS Artifact es un servicio que proporciona acceso bajo demanda a los informes de seguridad y cumplimiento de AWS y a determinados acuerdos en línea. AWS Artifact consta de dos secciones principales: Acuerdos de AWS Artifact e Informes de AWS Artifact.

ACUERDOS DE AWS ARTIFACT

Supongamos que su empresa necesita firmar un acuerdo con AWS en relación con el uso de determinados tipos de información en los servicios de AWS. Lo puede hacer a través de Acuerdos de AWS Artifact.

En los acuerdos de AWS Artifact, puede revisar, aceptar y administrar los acuerdos de una cuenta individual y de todas sus cuentas de AWS Organizations. Se ofrecen diferentes tipos de acuerdos para atender las necesidades de los clientes que están sujetos a regulaciones

específicas, como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

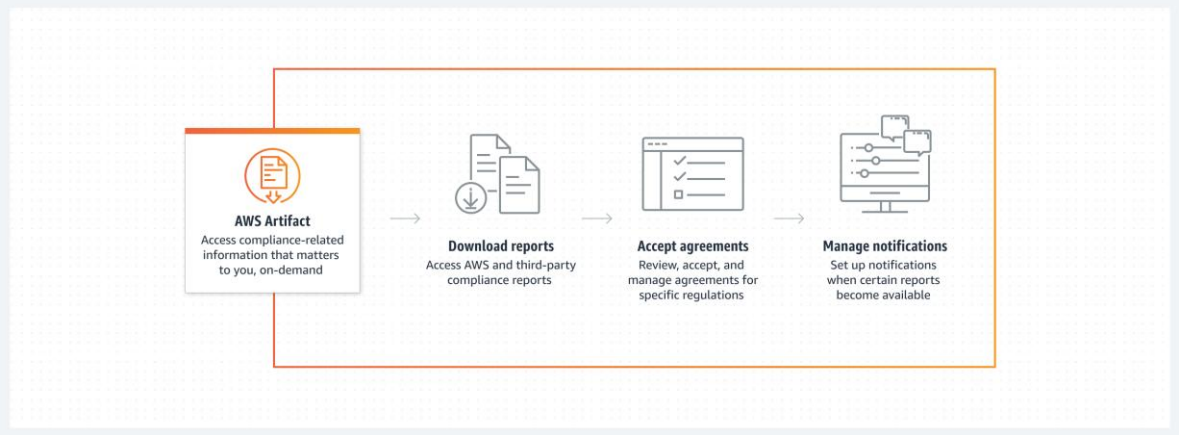
INFORMES DE AWS ARTIFACT

A continuación, imagine que un miembro del equipo de desarrollo de su empresa está creando una aplicación y necesita más información sobre su responsabilidad de cumplir con ciertos estándares regulatorios. Puede aconsejarle que acceda a esta información en Informes de AWS Artifact.

Los informes de AWS Artifact proporcionan informes de cumplimiento de auditores terceros. Estos auditores han probado y verificado que AWS cumple con una variedad de estándares y normativas de seguridad globales, regionales y específicas del sector. AWS Artifact Reports se mantiene actualizado con los últimos informes publicados. Puede proporcionar los artefactos de auditoría de AWS a sus auditores o reguladores como prueba de los controles de seguridad de AWS.

FUNCIONAMIENTO DE AWS ARTIFACT

AWS Artifact es el mejor recurso central para obtener información relacionada con el cumplimiento relevante para usted. Proporciona acceso bajo demanda a informes de seguridad y cumplimiento de AWS e ISV que venden sus productos en AWS Marketplace.



BENEFICIOS DE AWS ARTIFACT

Ahorre tiempo: Ahorre tiempo con el acceso bajo demanda a los informes de conformidad de AWS y de los proveedores de software independientes (ISV) en un portal de autoservicio.

Administre a escala: Acepte, anule o invalide y descargue bajo demanda contratos de conformidad con AWS.

Implemente con más confianza: Mejore su confianza en el despliegue de cargas de trabajo al comprender la postura de conformidad y seguridad de AWS.

CASOS DE USO DE AWS ARTIFACT

Comprenda la posición de seguridad y cumplimiento de AWS: Encuentre todos los informes, certificaciones, acreditaciones emitidas por el auditor de AWS y otras acreditaciones independientes en un recurso completo.

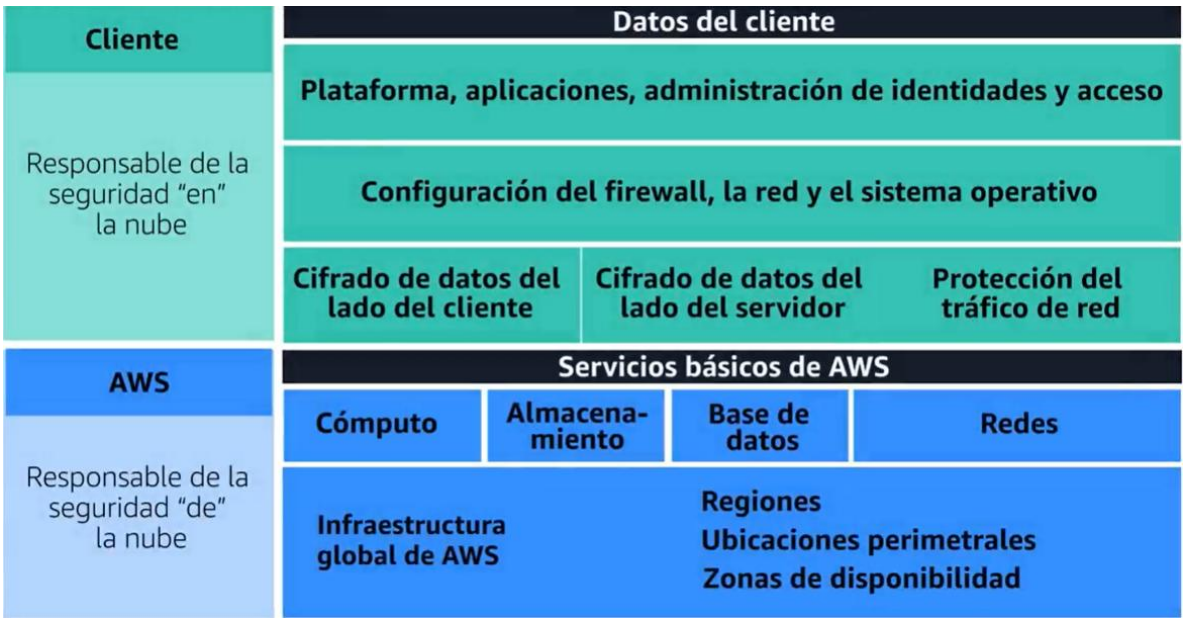
Administre acuerdos en línea seleccionados: Revise, acepte y administre sus acuerdos con AWS y aplíquelos a cuentas actuales y futuras dentro de su organización.

Evalúe la seguridad y cumplimiento de terceros: Realice la diligencia debida de los ISV que venden productos en AWS Marketplace, con acceso bajo demanda a informes de seguridad y cumplimiento.

RESUMEN SEGURIDAD EN AWS

Es hora de resumir el tema de seguridad que acabamos de estudiar.

Primero, AWS sigue un ***modelo de responsabilidad compartida***. AWS es responsable de la seguridad de la nube, y usted es responsable de la seguridad en la nube.



Con ***IAM*** tiene usuarios, grupos, roles y políticas. Los ***usuarios*** inician sesión con un nombre de usuario y contraseña y de forma predeterminada no tienen permisos. Los ***grupos*** son agrupaciones de usuarios y los ***roles*** son identidades que puede asumir para obtener acceso a credenciales temporales y permisos por una cantidad de tiempo configurable.
Para conceder permisos a una identidad, es necesario crear ***políticas*** que permitan o denieguen explícitamente una acción específica en AWS.
Con IAM también viene la ***identidad federada***. Si tiene un almacén de identidades corporativas existentes, puede federar esos usuarios a AWS, mediante el acceso basado en roles que permite a los usuarios usar un acceso tanto para sus sistemas corporativos como para AWS.
Un último punto a recordar acerca de IAM es que debe asegurarse de activar la ***autenticación multifactor*** para los usuarios, pero especialmente para el ***usuario raíz*** que tiene todos los permisos de forma predeterminada y no se puede restringir.

Hablamos sobre ***AWS Organizations***. Con AWS, es probable que tenga varias cuentas.
Las cuentas se utilizan habitualmente para aislar cargas de trabajo, entornos, equipos o aplicaciones. AWS Organizations le ayuda a administrar varias cuentas de forma jerárquica.

Analizamos temas de conformidad AWS utiliza auditores externos para demostrar que cumple con una amplia variedad de programas de conformidad.
Puede utilizar ***AWS Artifact*** para obtener acceso a los documentos de conformidad. Los requisitos de conformidad que tiene cambiarán de una aplicación a otra y entre las áreas de operación.

También hablamos de ataques de denegación de servicio distribuidos o ***ataques DDoS***, y cómo combatirlos con AWS mediante herramientas como ***AWS Shield*** y ***AWS WAF***.

Además, hablamos de ***cifrado***. En AWS, usted es el propietario de sus datos y es responsable de la seguridad. Eso significa que debe prestar atención al cifrado en tránsito y en reposo.

Hay muchas consideraciones cuando se trata de la seguridad en AWS. La seguridad es la máxima prioridad de AWS y seguirá siéndolo.

Utilice el ***principio de mínimo privilegio*** cuando defina el alcance de los permisos de usuarios y roles en IAM, y cifre los datos en cada capa, tanto en tránsito como en reposo.

Por último, asegúrese de utilizar los servicios de AWS para proteger su entorno.