

AWS CAF Y WAF



Programa

1.

TITULO

2.

INDICE

3.

¿QUÉ ES AWS CAF?

4.

FUNCIONAMIENTO

5.

PERSPECTIVA DE
NEGOCIOS

6.

PERSPECTIVA DE
PERSONAS

7.

PERSPECTIVA DE
GOBERNANZA

8.

PERSPECTIVA DE
PLATAFORMA

9.

PERSPECTIVA DE
SEGURIDAD

10.

PERSPECTIVA DE
SEGURIDAD

11.

PERSPECTIVA DE
OPERACIONES

12.

¿QUÉ ES AWS WAF?

13.

PILARES DE WAF

14.

AREAS DE PRACTICAS
RECOMENDADAS DE LOS
PILARES

15.

MODELO DE
RESPONSABILIDAD
COMPARTIDA(15,16,17)

16.


17.

¿QUÉ ES AWS CAF?

AWS Cloud Adoption Framework (AWS CAF) aprovecha la experiencia y las prácticas recomendadas de AWS para contribuir a la transformación digital y a la aceleración de los resultados empresariales a través del uso innovador de AWS. AWS CAF identifica las capacidades organizativas específicas que dan lugar a transformaciones en la nube con éxito. Dichas capacidades brindan orientación sobre prácticas recomendadas que le ayudan a mejorar su preparación para la nube. AWS CAF agrupa sus capacidades en seis perspectivas: Comercial, Personas, Gobernanza, Plataforma, Seguridad y Operaciones. Cada perspectiva abarca un conjunto de capacidades que las partes interesadas relacionadas de manera funcional poseen o administran en el viaje de transformación en la nube. Utilice AWS CAF para identificar y dar prioridad a oportunidades de transformación, evaluar y mejorar su preparación para la nube y evolucionar de manera iterativa su plan de desarrollo.

Capacidades y perspectivas

Las capacidades de AWS CAF le brindan orientación sobre prácticas recomendadas que le ayudan a mejorar su preparación para la nube. Cada perspectiva de AWS CAF abarca diferentes capacidades que las partes interesadas relacionadas de manera funcional poseen o administran en su viaje de transformación a la nube.



¿QUÉ ES AWS CAF?

Funcionamiento:

Visualización:

Identifique y priorice oportunidades de transformación que están en consonancia con sus objetivos estratégicos. Asociar sus iniciativas de transformación con partes interesadas clave y resultados empresariales medibles lo ayudará a demostrar valor a medida que progresa en su viaje de transformación.

Alineación:

Identifique brechas de capacidad y dependencias entre organizaciones. Lo ayudará a crear estrategias para mejorar su preparación para la nube, garantizar la alineación de las partes interesadas y facilitar actividades de administración de cambios organizativos relevantes.

Lanzamiento:

Entregue pilotos en producción y demuestre un valor empresarial que aumenta de manera progresiva. Los pilotos deben tener un impacto muy alto y, en caso de que sean adecuados, influenciarán en la futura dirección. Aprender de los pilotos lo ayudará a ajustar su enfoque antes de escalar a la producción completa.

Escalado:

Amplíe los pilotos y el valor empresarial a la escala deseada y asegúrese de que los beneficios comerciales asociados a sus inversiones en la nube se produzcan y mantengan.

Perspectiva Negocios

La perspectiva empresarial ayuda a garantizar que sus inversiones en la nube aceleren sus ambiciones de transformación digital y sus resultados empresariales alineados. Comprende ocho capacidades que se muestran en la siguiente figura. Las partes interesadas más habituales son **el director general (CEO), el director financiero (CFO), el director de operaciones (COO), el director de información (CIO), el director de marketing (CMO), el director de producto (CPO) y el director de tecnología (CTO).**

La transformación digital de la empresa ya no es una cuestión de «si» o «cuándo», sino de «cómo». Aunque la tecnología es a la vez un motor crítico y un facilitador de la transformación empresarial digital, para aumentar las probabilidades de éxito, su transformación debe estar impulsada por el negocio más que por la tecnología. La aplicación de las ocho capacidades identificadas en este documento puede ayudarle a garantizar que sus inversiones en la nube aceleren sus ambiciones de transformación digital y los resultados empresariales.

Capacidades de la perspectiva de Negocios:

Gestión de estrategias: Aproveche la nube para acelerar sus resultados empresariales

Gestión de productos: Gestionar datos y ofertas en la nube como productos

Información empresarial: Obtenga información en tiempo real y responda a preguntas sobre su negocio

Gestión de la cartera: Priorizar la entrega de productos e iniciativas de nube de alto valor

Asociación estratégica: Construya o haga crecer su negocio a través de una asociación estratégica con su proveedor de nube

Ciencia de datos: aproveche los análisis avanzados y el aprendizaje automático para resolver problemas empresariales complejos

Gestión de la innovación: Desarrollar nuevos procesos, productos y experiencias y mejorar los existentes

Monetización de datos: Aprovechar los datos para obtener un beneficio empresarial cuantificable

Perspectiva Personas

La perspectiva de las personas sirve de puente entre la tecnología y la empresa, acelerando el viaje a la nube para ayudar a las organizaciones a evolucionar más rápidamente hacia una cultura de crecimiento continuo, aprendizaje y un entorno en el que el cambio se convierta en algo normal, centrándose en la cultura, la estructura organizativa, el liderazgo y el personal. Comprende siete capacidades que se muestran en la siguiente figura. Las partes interesadas habituales son los directores de información (CIO), los directores de operaciones (COO), los directores de tecnología (CTO), los directores de recursos humanos (CHRO), los directores de la nube y los líderes interfuncionales y de toda la empresa.

Las personas son el alma de cualquier esfuerzo de transformación en la nube que tenga éxito. Contar con una plantilla cualificada, motivada, comprometida e impulsada por un equipo directivo comprometido con el valor y el rendimiento de la inversión en la nube tendrá un efecto multiplicador en su organización. A medida que los líderes se sientan más inspirados por los clientes y deseen que su empresa innove, impulsarán a sus empleados a aprender y desarrollar más tecnologías basadas en la nube. Esto dará lugar a una cultura en continuo aprendizaje, innovación y apertura en sus comunicaciones, lecciones aprendidas e incluso fracasos.

Capacidades de la perspectiva de Personas:

Evolución de la cultura: Evaluar, evolucionar gradualmente y codificar la cultura organizativa con aspiraciones de transformación digital

Transformación de la plantilla: Habilitar el talento y modernizar las funciones para atraer, desarrollar y retener una fuerza laboral digitalmente fluida y de alto rendimiento.

Liderazgo transformacional : Fortalecer la capacidad de liderazgo y movilizar a los líderes para impulsar el cambio transformacional

Aceleración del cambio: Acelerar la adopción de las nuevas formas de trabajar aplicando un marco programático de aceleración del cambio

Alineación organizativa: Establecer una asociación continua entre las estructuras organizativas las operaciones empresariales, el talento y la cultura

Fluidez en la nube: Desarrollar la perspicacia digital para aprovechar con confianza y eficacia la nube para acelerar los resultados empresariales

Diseño organizativo: Evaluar y evolucionar el diseño organizativo para alinearlos con las nuevas formas de trabajar en la nube

Perspectiva Gobernanza



la perspectiva de Gobernanza se centra en ayudar orquestas tus iniciativas en la nube mientras maximizas beneficios organizacionales y minimización de riesgos relacionados con la transformación. Comprende siete capacidades, como se muestra en la siguiente figura. Las partes interesadas comunes incluyen director de transformación, jefe oficial de información (CIO), director de tecnología (CTO), jefe oficial financiero (CFO), director de datos (CDO) y jefe de riesgo oficial (CRO).

La transformación digital impulsada por la nube es un esfuerzo continuo respaldado por numerosas iniciativas multifuncionales que deben ser cuidadosamente orquestado y administrado como un programa cohesivo a largo plazo. Al mismo tiempo, demasiada gobernanza, supervisión y Red Tape pueden ralentizar, o incluso detener programas de transformación complejos, si bien la falta de gobernanza puede conducir a un aumento en los negocios y riesgos tecnológicos. Una función de gobernanza efectiva ayuda las organizaciones identifican y eliminan los bloqueadores, alcanzan la alineación metas, progreso y logros, y finalmente acelerar cambio organizacional.

Capacidades de la perspectiva de Gobernanza:

Gestión de programas y proyectos: Llevar a cabo iniciativas interdependientes en la nube de forma flexible y flexible y coordinada

Gestión financiera en la nube: Planifique, mida y optimice su gasto en la nube

Gestión de beneficios: Garantice que los beneficios empresariales de sus inversiones en la nube se realizadas y sostenidas

Gestión de la cartera de aplicaciones: Gestione y optimice su cartera de aplicaciones en apoyo de su estrategia empresarial

Curación de datos: Organice un inventario de productos de datos en un catálogo de datos

Gestión de riesgos: Aproveche la nube para reducir su perfil de riesgo

Gobierno de datos: Ejercer autoridad y control sobre sus datos para satisfacer las expectativas de las partes interesadas



Perspectiva Plataforma

La perspectiva de plataforma es una pieza fundamental de AWS CAF. Es el nexo en el que convergen las decisiones tomadas en todas las demás perspectivas para proporcionar agilidad y valor empresarial. Las decisiones tomadas aquí ayudan o dificultan sus objetivos empresariales a un nivel fundamental. La perspectiva de la plataforma de AWS CAF **facilita la creación de un entorno en la nube escalable y de nivel empresarial que sustenta la transformación de su organización. A través de esta perspectiva, AWS CAF le guía en el establecimiento de una plataforma sólida que puede permitir su viaje a la nube, lo que en última instancia conduce a la transformación y el crecimiento empresarial significativo.**

Mientras trabaja en la perspectiva de la plataforma, tenga en cuenta las conexiones interfuncionales con los líderes empresariales que deben desarrollarse y el valor que aportan a sus equipos y organización. Preste más atención a los cambios en el modelo operativo y las topologías de los equipos para garantizar que se cumplen los requisitos. Además, procure desarrollar las habilidades que sus equipos necesitan para construir la plataforma y permitir su uso en todos los equipos de aplicación. Al tomar estas decisiones, tenga en cuenta los objetivos de su organización en materia de personal, negocio, gobernanza, seguridad y operaciones, ya que son fundamentales para garantizar la adopción de la plataforma y el éxito de sus esfuerzos.

Capacidades de la perspectiva de Plataforma

Arquitectura de plataformas: Establecer directrices, principios, patrones y guardarraíles para su entorno de nube

Ingeniería de datos: Automatice y orqueste los flujos de datos en toda su organización

Arquitectura de datos: Diseñe y desarrolle una arquitectura de datos y análisis y arquitectura de datos

Aprovisionamiento y orquestación: **Creación, gestión y distribución de productos en nube a los usuarios finales**

Integración y entrega continuas: **Evolución y mejora rápidas de aplicaciones y servicios**

Ingeniería de plataformas: Cree un entorno de nube que cumpla las normativas con seguridad mejoradas y productos empaquetados y reutilizables

Desarrollo de aplicaciones modernas: Cree aplicaciones nativas de la nube bien diseñadas


Perspectiva Seguridad



El objetivo de la perspectiva de seguridad es ayudarle a lograr la confidencialidad, integridad y disponibilidad de sus datos y cargas de trabajo en la nube de AWS, al tiempo que mejora su postura de seguridad. Este documento técnico organiza los principios de las nueve capacidades que le ayudarán a impulsar la transformación de la cultura de seguridad de su organización. Para cada capacidad, discutiremos acciones específicas que puede tomar y métodos para medir el progreso.

La seguridad es una prioridad máxima para AWS. A medida que las organizaciones adoptan la escalabilidad y flexibilidad de la nube, AWS les ayuda a evolucionar su seguridad, identidad y conformidad aprovechando este nuevo entorno. AWS incorpora la seguridad en el núcleo de la infraestructura de la nube de AWS. Ofrece servicios básicos para ayudarle a cumplir sus requisitos de seguridad exclusivos en la nube de AWS.

El objetivo de su programa de seguridad sigue siendo el mismo, ya sea en las instalaciones, en la nube o en un entorno híbrido. AWS CAF le ayuda a aumentar la madurez y eficacia del programa, al tiempo que acorta los plazos y reduce los costes. La diferencia al utilizar la nube es fundamental e impactante: usted ya no administra la seguridad física de sus centros de datos, ni el diseño, la implementación, la capacitación, la implementación o el mantenimiento relacionados con ellos. AWS proporciona y asegura los centros de datos y gestiona todas las actualizaciones físicas y el mantenimiento. Puede utilizar herramientas de seguridad basadas en software para monitorizar y proteger el flujo de información que entra y sale de sus recursos en la nube. Como cliente de AWS, se beneficia de todas las prácticas recomendadas de las políticas, la arquitectura y los procesos operativos de AWS que satisfacen los requisitos de nuestros clientes más sensibles a la seguridad.

La conformidad de AWS describe los sólidos controles existentes en AWS para la seguridad y la protección de datos en la nube de AWS. AWS obtiene regularmente la validación de terceros para miles de requisitos de conformidad globales que supervisamos continuamente para ayudarle a satisfacer las necesidades de seguridad y conformidad. **La seguridad y la conformidad es una responsabilidad compartida entre usted y AWS, siendo AWS responsable de la «Seguridad de la nube» mientras que usted sigue siendo responsable de la «Seguridad en la nube».**



Capacidades de la perspectiva de Seguridad

Gobernanza de la seguridad: Desarrollar y comunicar las funciones de seguridad responsabilidades, políticas, procesos y procedimientos de seguridad

Detección de amenazas: Comprender e identificar posibles seguridad, amenazas o comportamientos inesperados.

Protección de datos: Mantener la visibilidad y el control sobre los datos y cómo se accede a ellos y se utilizan en su organización

Garantía de seguridad: Supervisar, evaluar, gestionar y mejorar la eficacia de sus programas de seguridad y privacidad

Gestión de vulnerabilidades: Identificar, clasificar, remediar y mitigar continuamente vulnerabilidades de seguridad

Seguridad de las aplicaciones: Detectar y abordar las vulnerabilidades de seguridad durante el proceso de desarrollo de software

Gestión de identidades y accesos: Gestione identidades y permisos a escala

Protección de infraestructuras: Valide que los sistemas y servicios de su carga de trabajo están protegidos

Respuesta a incidentes: Reduzca el daño potencial respondiendo eficazmente a los incidentes de seguridad



Perspectiva de Operaciones

La perspectiva de operaciones se centra en garantizar que los servicios en la nube se prestan al nivel acordado con las partes interesadas de su negocio. Comprende nueve capacidades, como se muestra en la siguiente figura (Capacidades de la perspectiva de operaciones de AWS CAF). Entre las partes interesadas comunes se incluyen los líderes de infraestructura y operaciones, los ingenieros de fiabilidad del sitio y los administradores de servicios de tecnología de la información.

Este documento técnico proporciona una visión general de los beneficios de operar en la nube de AWS y le presenta los servicios de operaciones en la nube y la orientación prescriptiva que le ayudarán a operar de manera eficiente y eficaz a escala.

Las operaciones son fundamentales para el éxito de toda organización y su transformación digital. La excelencia operativa es necesaria para garantizar que su transformación logre su propósito y que las aplicaciones cumplan constantemente sus resultados empresariales y las expectativas de sus usuarios.

Capacidades de la perspectiva de Operaciones

Observabilidad: Obtenga información práctica de su infraestructura y aplicaciones

Gestión de eventos (AIOps): Detecte eventos, evalúe su impacto potencial y determine la acción de control adecuada

Gestión de incidentes y problemas: Restablecer rápidamente las operaciones de servicio y minimizar el impacto adverso en el negocio

Gestión de cambios y publicaciones: Introducir y modificar cargas de trabajo minimizando el riesgo para los entornos de producción

Rendimiento y capacidad: Supervisar el rendimiento de la carga de trabajo y garantizar que la capacidad satisfaga las demandas actuales y futuras

Gestión de la configuración: Mantener un registro de las cargas de trabajo en la nube, sus relaciones y los cambios de configuración a lo largo del tiempo

Gestión de parches: Distribuir y aplicar sistemáticamente actualizaciones de software

Disponibilidad y continuidad: Garantizar la disponibilidad de la información crítica para el negocio, aplicaciones y servicios críticos para la empresa

Gestión de aplicaciones: investigue y corrija los problemas de las aplicaciones en un solo panel

¿QUÉ ES AWS WAF?

AWS Well-Architected Framework le ayuda a comprender las ventajas y desventajas de las decisiones que toma al crear sistemas en AWS. Mediante el uso del marco, podrá conocer las prácticas recomendadas de arquitectura para diseñar y operar cargas de trabajo en la Nube de AWS que sean seguras, fiables, eficaces, rentables y sostenibles. Proporciona una forma de medir sus arquitecturas de forma constante en función de las prácticas recomendadas y de identificar áreas que se puedan mejorar. El proceso para revisar una arquitectura representa una conversación constructiva sobre decisiones arquitectónicas y no se trata de un mecanismo de auditoría. Creemos que contar con sistemas de buena arquitectura aumenta en gran medida la probabilidad de éxito empresarial.

AWS Well-Architected Framework documenta un conjunto de cuestiones fundamentales que le permiten comprender si una arquitectura específica se corresponde con las prácticas recomendadas de la nube. El marco proporciona un enfoque coherente para evaluar los sistemas frente a las cualidades que espera de los sistemas modernos basados en la nube y la solución necesaria para lograr dichas cualidades.

AWS también proporciona un servicio para revisar sus cargas de trabajo de forma gratuita. La herramienta de AWS Well-Architected (AWS WA Tool) es un servicio en la nube que proporciona un proceso coherente para que revise y mida su arquitectura con AWS Well-Architected Framework. AWS WA Tool proporciona recomendaciones para lograr que sus cargas de trabajo sean más fiables, seguras, eficientes y rentables.

conclusión: AWS Well-Architected Framework proporciona prácticas recomendadas sobre arquitectura en los seis pilares para diseñar y utilizar sistemas en la nube fiables, seguros, eficaces, rentables y sostenibles. El marco proporciona un conjunto de preguntas que le permiten revisar una arquitectura existente o propuesta. También proporciona un conjunto de prácticas recomendadas de AWS para cada pilar. El uso del marco de trabajo en su arquitectura le ayudará a producir sistemas estables y eficaces, lo que le permite centrarse en sus requisitos funcionales.

Los 6 pilares de AWS Well-Architected Framework

Excelencia operativa	Capacidad de apoyar el desarrollo y ejecutar cargas de trabajo eficazmente, conocer sus operaciones y mejorar continuamente los procesos y procedimientos de soporte para ofrecer valor empresarial.
Seguridad	El pilar de seguridad describe cómo sacar partido de las tecnologías de nube para proteger datos, sistemas y recursos de una forma que pueda mejorar su nivel de seguridad.
Fiabilidad	El pilar de fiabilidad <u>abarca la capacidad de una carga de trabajo para realizar su función prevista de forma correcta y coherente cuando se espera que lo haga. Esto incluye la capacidad de utilizar y probar la carga de trabajo a lo largo de todo su ciclo de vida.</u> En este documento se incluye orientación de prácticas recomendadas para la implementación de cargas de trabajo fiables en AWS.
Eficiencia del rendimiento	Es la capacidad de utilizar de forma eficaz los recursos informáticos para satisfacer los requisitos del sistema, así como de mantener la eficiencia a medida que la demanda cambia y las tecnologías evolucionan.
Optimización de costes	Capacidad de ejecutar sistemas para ofrecer valor empresarial al menor precio posible.
Sostenibilidad	Es la capacidad de mejorar constantemente el impacto en la sostenibilidad mediante la reducción del consumo de energía y el aumento de la eficiencia en todos los componentes de una carga de trabajo, maximizando los beneficios de los recursos aprovisionados y minimizando el número total de recursos necesarios.



Hay cuatro áreas de prácticas recomendadas para la **excelencia operativa** en la nube:

- Organización
- Prepárese
- Operación
- Evolución

Existen cuatro áreas de prácticas recomendadas para la **fiabilidad** en la nube:

- Fundamentos
- Arquitectura de la carga de trabajo
- Administración de cambios
- Administración de errores

Existen cinco áreas de prácticas recomendadas para la **optimización de costes** en la nube:

- Práctica de administración financiera en la nube
 - Conciencia del gasto y del uso
 - Recursos rentables
- Administración de la demanda y suministro de recursos
- Optimización a lo largo del tiempo

Existen seis áreas de prácticas recomendadas para la **seguridad** en la nube:

- Seguridad
- Identity and Access Management
- Detección
- Protección de la infraestructura
 - Protección de los datos
- respuesta frente a incidencias

Existen cinco áreas de prácticas recomendadas para la **eficiencia del rendimiento** en la nube:

- Selección de la arquitectura
- Computación y hardware
- Administración de datos
- Redes y entrega de contenido
- Proceso y cultura

Existen seis áreas de prácticas recomendadas para la **sostenibilidad** en la nube:

- Selección de regiones
- Patrones de comportamiento de los usuarios
- Patrones de software y arquitectura
 - Patrones de datos
 - Patrones de hardware
- Proceso de desarrollo e implementación



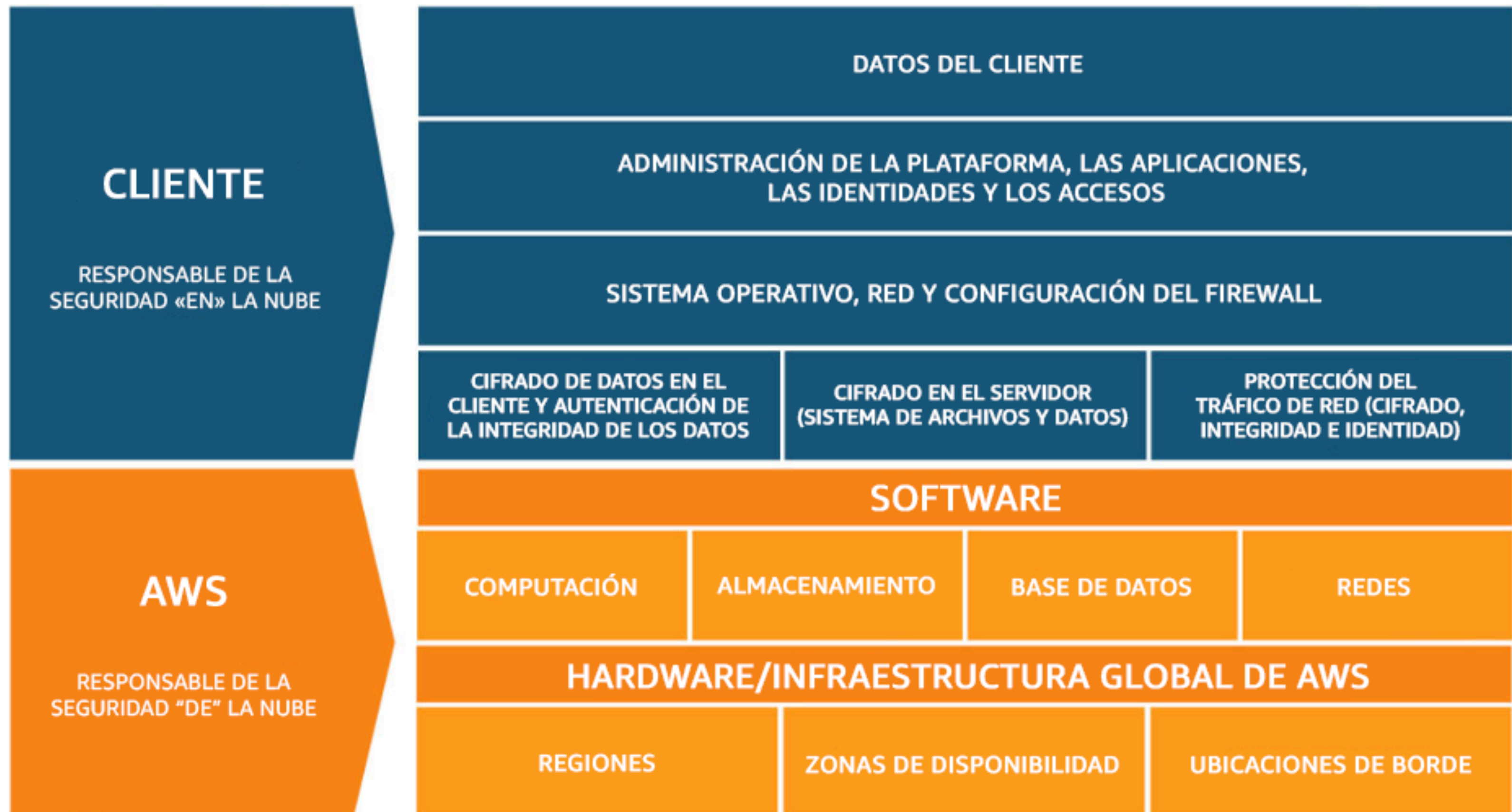
Modelo de responsabilidad compartida

La seguridad y la conformidad constituyen 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 con el fin de ofrecer seguridad física en las instalaciones en las que operan los servicios**. Por otra parte, 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 asociadas 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, la integración de estos en su entorno de TI, y la legislación y los reglamentos aplicables. La naturaleza de esta responsabilidad compartida también ofrece la flexibilidad y la posibilidad de que el cliente pueda controlar el despliegue. Tal y como se muestra en el siguiente gráfico, esta diferenciación de responsabilidad suele denominarse Seguridad «de» la nube en comparación con Seguridad «en» la nube.

Responsabilidad de AWS: «Seguridad de la nube» – AWS es responsable de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la nube de AWS. Esta infraestructura está compuesta por hardware, software, redes e instalaciones que ejecutan servicios en la nube de AWS.

Responsabilidad del cliente: «Seguridad en la nube» – La responsabilidad del cliente variará en función de los servicios en la nube de AWS que seleccione. Esto determina la cantidad de trabajo de configuración que el cliente debe realizar como parte de sus responsabilidades de seguridad. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se categoriza como infraestructura como servicio (IaaS) y, como tal, requiere que el cliente realice todas las tareas necesarias de administración y configuración de seguridad. Los clientes que despliegan una instancia de Amazon EC2 son responsables de administrar el sistema operativo invitado (incluidas las actualizaciones y los parches de seguridad), todo el software de la aplicación o las utilidades que instale el cliente en las instancias y la configuración del firewall proporcionado por AWS (conocido como grupo de seguridad) en cada instancia. En el caso de los servicios abstractos, como Amazon S3 y Amazon DynamoDB, AWS se encarga de gestionar la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes acceden a los puntos de conexión para guardar y recuperar información. Los clientes son responsables de administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y utilizar herramientas de IAM para aplicar los permisos adecuados.

Modelo de responsabilidad compartida



Este modelo de responsabilidad compartida entre clientes y AWS también abarca los controles de TI. De la misma forma que AWS y sus clientes comparten la responsabilidad de operar el entorno de TI, también la comparten en lo referente a la administración, operación y verificación de los controles de TI. AWS puede ayudar a aliviar la carga que supone para los clientes operar los controles, administrando los controles asociados con la infraestructura física desplegada en el entorno de AWS, de cuya administración se encargaba el cliente anteriormente. Como el despliegue 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 así obtener un entorno de control distribuido (nuevo). Los clientes pueden utilizar la documentación de conformidad y control de AWS disponible para realizar sus procedimientos de evaluación y verificación de control según sea necesario. Los siguientes son ejemplos de controles administrados por AWS, los clientes de AWS o por ambos.

Controles heredados – Controles que un cliente hereda completamente de AWS.

- Controles ambientales y físicos

Controles compartidos – Controles que se aplican tanto a la capa de infraestructura como a la del cliente, pero en perspectivas o contextos distintos. En un control compartido, AWS proporciona los requisitos para la infraestructura y el cliente debe proporcionar su propia implementación de control en el uso que se haga de los servicios de AWS. Entre los ejemplos se incluyen:

- Administración de parches: AWS es responsable de la aplicación de parches y de la solución de defectos en la infraestructura, pero los clientes son responsables de la aplicación de parches en las aplicaciones y el sistema operativo invitado.
-
- Administración de la configuración: AWS mantiene la configuración de sus dispositivos de infraestructura, pero los clientes son responsables de la configuración de sus propios sistemas operativos invitados, bases de datos y aplicaciones.
-
- Concienciación y formación: AWS imparte formación a los empleados de AWS, pero los clientes deben formar a sus propios empleados.

Específicos del cliente – Controles que son responsabilidad exclusiva del cliente en función de la aplicación que esté desplegando en los servicios de AWS. Entre los ejemplos se incluyen:

- Protección de comunicaciones y servicios o seguridad de zona, que pueden requerir que un cliente enrute o especifique datos de zona en entornos de seguridad específicos.