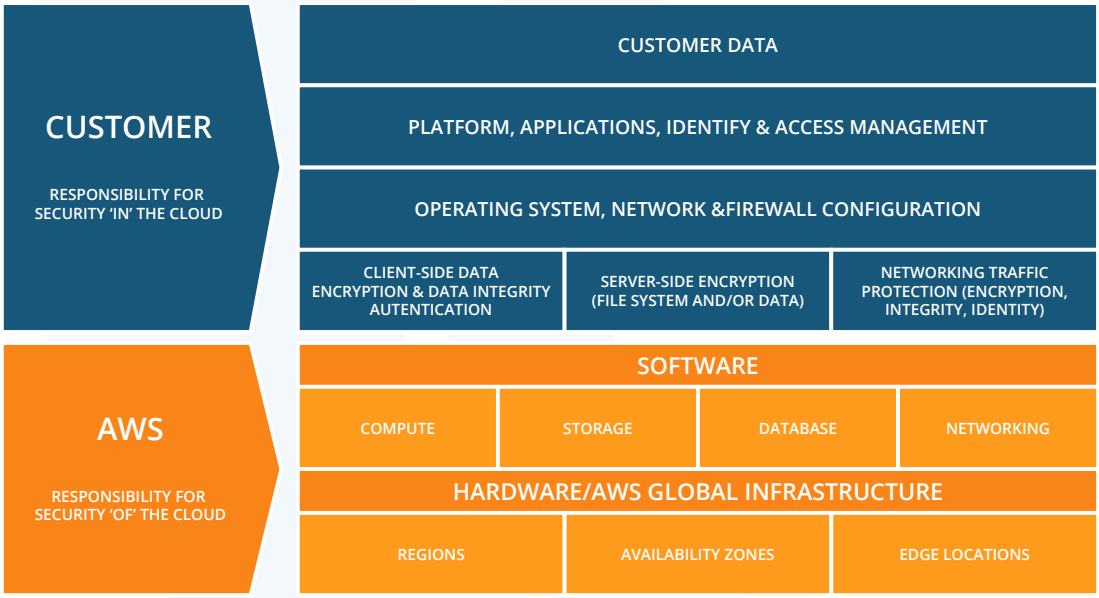

# Securización de entornos cloud AWS

En este artículo analizaremos el modelo de seguridad compartida de Amazon Web Services y las distintas herramientas que este proveedor de cloud ofrece a sus clientes para facilitar la implementación de buenas prácticas de seguridad en lo concerniente a la provisión, operación y evolución de infraestructuras en este tipo de entornos.

# Modelo de seguridad compartida

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS y el cliente. Este modelo compartido **permite aliviar la carga operativa del cliente**, ya que AWS opera, administra y controla los componentes del sistema operativo host, la capa de virtualización y la seguridad física de las instalaciones en las que funcionan los servicios. **El cliente asume la responsabilidad y la administración de los sistemas operativos huésped** (incluidas las actualizaciones y los parches de seguridad), **así como de cualquier otro software de aplicaciones asociado y la configuración del firewall ofrecido por AWS**. Como se muestra a continuación, 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 clasificados como software como servicio (SaaS), 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 consumir el servicio. **Los clientes son responsables de administrar sus datos** (incluidas las opciones de cifrado)**, clasificar sus recursos y utilizar las herramientas de gestión de identidades (IAM) para solicitar los permisos correspondientes.**

# Servicios de seguridad

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.

Para facilitar a los clientes la correcta ejecución de buenas prácticas de seguridad y cumplimiento de normativas concretas, AWS pone a disposición de sus clientes numerosos servicios de propósito específico especialmente ideados para cubrir necesidades concretas en este ámbito.

## Gestión de Identidades

Amazon Web Services ofrece múltiples opciones para el gobierno de identidades y los potenciales permisos que dichas identidades pueden llegar a obtener. A continuación, se detallan los principales servicios dentro de esta categoría y los casos de uso que cubren:

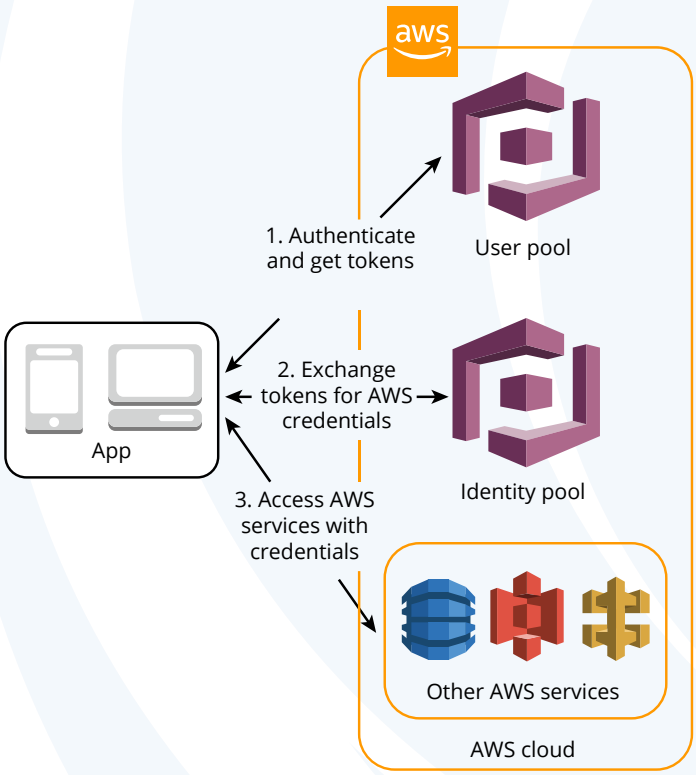
**AWS Identity & Access Management (IAM)** es el principal servicio de gestión de identidades que utilizarán la inmensa mayoría de usuarios de AWS, ya que es aquí donde se gestionan los distintos usuarios, grupos, roles y políticas de permisos requeridos para la correcta operación y funcionamiento de los recursos de infraestructura.

AWS proporciona numerosas políticas de seguridad predefinidas para facilitar la implementación de políticas de otorgación de permisos mínimos. Todas estas políticas se actualizan periódicamente para dar soporte a las nuevas APIs y servicios. Las políticas de seguridad predefinidas se agrupan en 2 categorías:

- Políticas de servicio. Para cada uno de los distintos servicios de AWS se proporcionan políticas de permiso con sets de permisos concretos.

- Políticas por función de trabajo. Útiles para otorgar rápidamente permisos para los roles de trabajo más habituales: Administradores globales, sólo lectura, operadores de redes, operadores de bases de datos, etc.

**Amazon Cognito** ofrece autenticación, autorización y administración de usuarios para sus aplicaciones móviles y web. Los dos componentes principales de Amazon Cognito son los grupos de usuarios y los grupos de identidades.




Los grupos de usuarios proporcionan, entre otras funcionalidades:

- Servicios de inscripción e inicio de sesión.

- Una interfaz de usuario web personalizable integrada para que los usuarios inicien sesión.

- Inicio de sesión a través de redes sociales con Facebook, Google, Login with Amazon e Inicio de sesión con Apple, o por medio de proveedores de identidad SAML y OIDC desde su grupo de usuarios.

- Administración de directorios de usuarios y perfiles de usuario.

- Características de seguridad como la autenticación multifactor (MFA), comprobaciones de credenciales filtradas, protección de posesión de cuenta y verificación de correo electrónico y teléfono.

Con un grupo de identidades, los usuarios pueden obtener credenciales temporales para acceder directamente a servicios de AWS como Amazon S3 y DynamoDB. Los grupos de identidades admiten usuarios invitados anónimos, así como los múltiples proveedores de identidad que puede utilizar para autenticar a los usuarios para grupos de identidades:

- Grupos de usuarios de Amazon Cognito
- Inicio de sesión a través de redes sociales con Facebook, Google, Login with Amazon e Inicio de sesión con Apple
- Proveedores de OpenID Connect (OIDC)
- Proveedores de identidad SAML

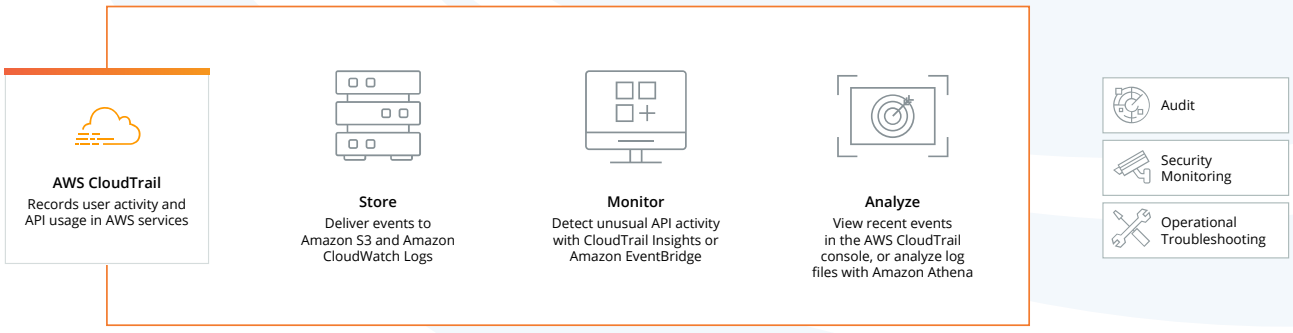
**AWS Directory Service** facilita la implementación de servicios de directorio y puntos de enlace para la integración con servicios de AWS:

- Microsoft Active Directory. Esta opción de despliegue proporciona un directorio de Microsoft Active Directory totalmente administrado. Ofrece todas las características habituales de este servicio: Identidades, DNS, políticas de grupo, relaciones de confianza, etc. y es la opción recomendada para la mayoría de casos de uso empresariales. Los directorios de este tipo no pueden pertenecer a un dominio existente, con lo que la integración con dominios corporativos existentes pasa por el establecimiento de relaciones de confianza.
- AD Connector. Pasarela administrada para la redirección de peticiones a un directorio de Microsoft Active Directory en instalaciones OnPremise. Esta forma de trabajar permite extender el dominio corporativo en vigor a AWS con un esfuerzo mínimo.
- Simple AD. Esta opción de despliegue implementa un directorio basado en Samba 4 que ofrece una funcionalidad básica de autenticación y administración de identidades mediante LDAP; se trata de una opción de bajo coste para aplicaciones que no requieran funcionalidad de directorio avanzada.

## Detección

Dada la naturaleza flexible de este tipo de entornos, Amazon proporciona a los clientes finales diversos servicios para facilitar las labores de detección y notificación de hallazgos de seguridad.

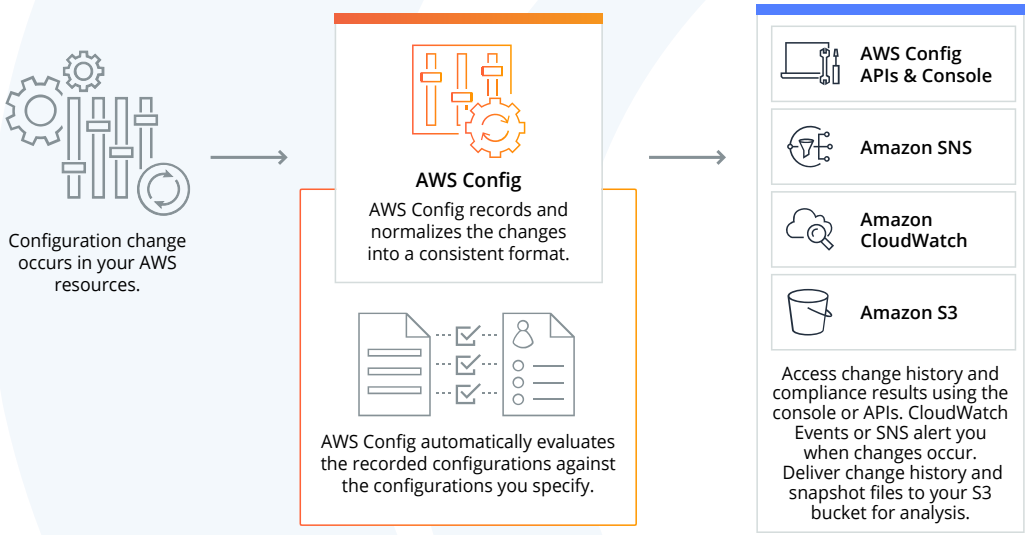
**AWS Cloudtrail** es el servicio de auditoría de APIs y actividad de usuarios AWS. De forma gratuita permite realizar búsquedas simples en el registro de los últimos 90 días. Con pago adicional, Cloudtrail permite la integración con organizaciones multi-cuenta, exportación de datos a S3 o la integración con Cloudwatch Insights para la realización de análisis complejos.



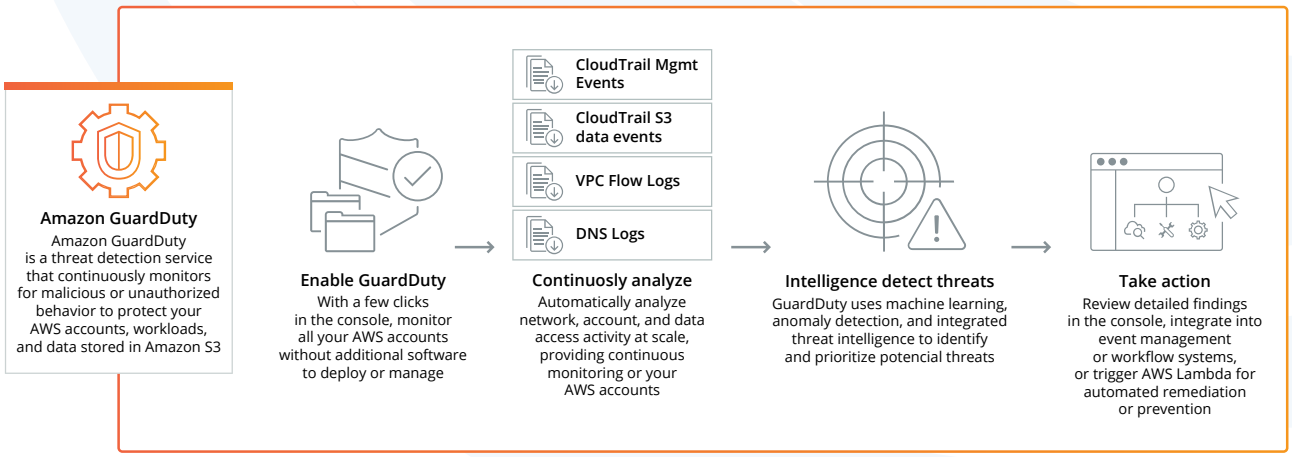
**AWS Config** es el servicio de auditoría de control de cambios y evaluación contínua de la configuración de recursos de infraestructura. Este servicio habilita la implementación de múltiples funcionalidades de control como por ejemplo:

- Automatizar la evaluación de las configuraciones registradas con respecto a las configuraciones deseadas.
- Revisar los cambios en las configuraciones y las relaciones entre los recursos de AWS.
- Determinar la conformidad general con respecto a las configuraciones especificadas.

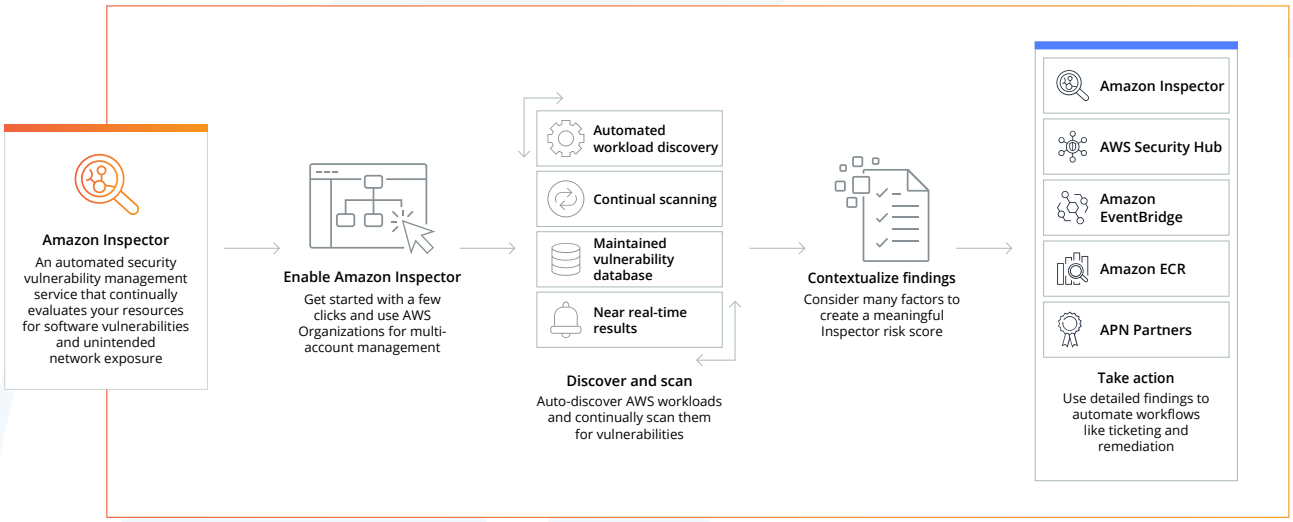
Config se integra con otros servicios más avanzados como SecurityHub o AWS Organizations para ayudar en la gobernabilidad, monitorización e implementación de políticas y estándares de seguridad.




**Amazon GuardDuty** es un servicio de detección de amenazas que monitoriza de manera continua las cargas de trabajo en AWS para detectar actividades maliciosas y envía hallazgos detallados de seguridad para su visibilidad y resolución. GuardDuty analiza de forma continua la información generada por AWS Cloudtrail logs, registros de flujo de VPC y logs de acceso de DNS; toda esta información se correlaciona y evalúa para emitir hallazgos de diversas categorías: Desde consultas DNS a dominios sospechosos hasta eventos de actividad del usuario raíz de la cuenta.



**Amazon Inspector** es el servicio de análisis de vulnerabiblidad de aplicaciones de AWS. Gracias a su integración con el servicio de administración de servidores AWS Systems Manager, Inspector permite autodescubrir las instancias EC2 de su cuenta y ejecutar sobre ellas análisis de vulnerabilidades cuyos resultados se pueden consultar fácilmente desde la consola o programáticamente.



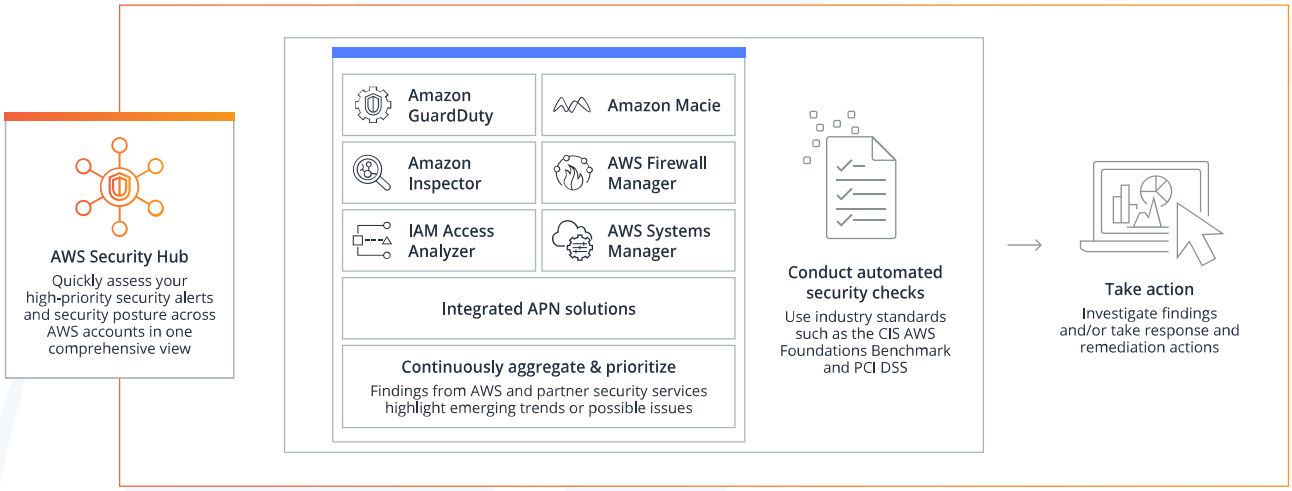

Inspector también permite realizar análisis de seguridad sobre imágenes Docker alojadas en Elastic Container Registry. Cada vez que se suba una nueva imagen, esta es analizada automáticamente por Inspector para recopilar los problemas de seguridad conocidos y vulnerabilidades pendientes de corrección.

**Systems Manager Patch Manager** proporciona un sistema de administración centralizada para la detección y aplicación de parches sobre una flota de instancias Windows y Linux de Amazon EC2 o servidores OnPremise.

**AWS Security Hub** es un servicio para la administración de su postura de seguridad en la nube. Realiza comprobaciones de las prácticas recomendadas de seguridad, agrega alertas y permite la corrección automática. Para ello, SecurityHub se integra con las siguientes fuentes de datos:

- Amazon GuardDuty
- Amazon Inspector
- IAM Access Analyzer
- Amazon Macie
- AWS Firewall Manager
- AWS Systems Manager
- AWS Config

SecurityHub proporciona también conjuntos de evaluaciones de AWS Config para validar el cumplimiento de diversos estándares de seguridad con el fin de disponer de un informe actualizado del estado de su infraestructura:




## Protección de infraestructuras

Aunque AWS proporciona diversas herramientas de propósito específico para la protección de cargas de trabajo, siempre es recomendable hacer un correcto diseño de redes privadas con **AWS Virtual Private Cloud (VPC)**. Por defecto, todas las cuentas de AWS implementan una VPC por defecto que cuenta con tantas subredes públicas como zonas de disponibilidad disponga la región donde se hospede. Esto significa que cualquier instancia EC2 o servicio con integración para VPC obtendrá automáticamente una IP pública y acceso a Internet sin restricciones, lo que puede derivar en una superficie de ataque elevada si no se tiene el debido cuidado a la hora de configurar los grupos de seguridad que conforman el firewall dentro del ecosistema de VPC.

La recomendación es siempre realizar una implementación de redes privadas en la que existan subredes públicas (donde se hospedarán servicios e instancias EC2 expuestas al tráfico externo proveniente de Internet) y subredes internas, donde el acceso externo no sea posible y el acceso a Internet desde dichas subredes requiera del uso de la pasarela correspondiente de alguna subred pública. AWS proporciona todo tipo de herramientas para la correcta implementación de este tipo de diseños de red:

- Internet Gateway: Elemento que habilita el acceso directo a Internet desde subredes públicas
- NAT Gateway: Pasarela NAT gestionada y altamente disponible
- Egress Only Gateway: Específicamente pensada para entornos de red con IPv6, este tipo de pasarela permite implementar de forma sencilla redes privadas que implementen el protocolo IPv6, en el que todas las IPs son de ámbito global.
- Tablas de rutas que facilitan la implementación de reglas de control de flujo
- ACLs de red para la implementación de reglas de firewall sin estado
- Grupos de seguridad para la implementación de reglas de firewall con estado

Para complementar y extender las capacidades de seguridad intrínsecas de VPC, AWS proporciona servicios de propósito específico para cubrir ciertas necesidades:

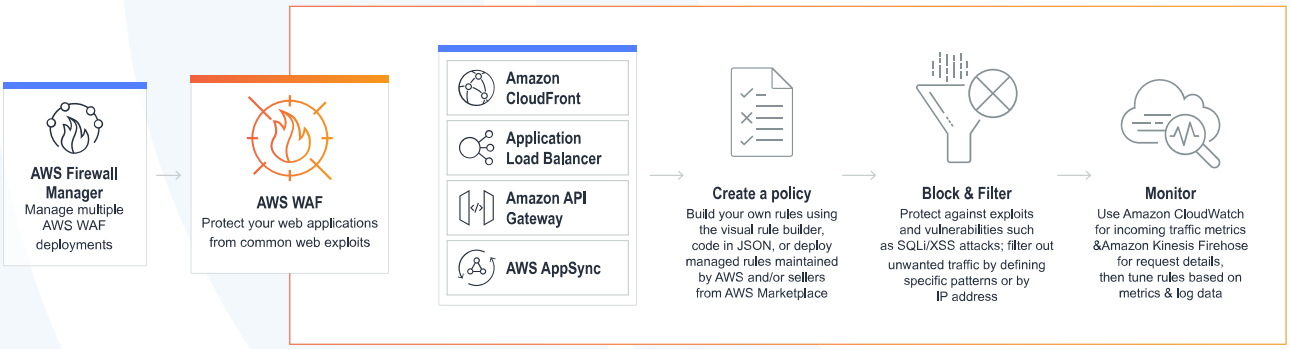
**AWS Network Firewall** es un firewall de red avanzado que permite la implementación de reglas con inspección de tráfico que habilitan la realización de seguimiento e identificación de conexiones, detección de vulnerabilidades mediante detección de firmas, y filtrado de tráfico web saliente en función del dominio de destino, entre otras.

**AWS DNS Firewall** es un sistema de filtrado de peticiones DNS que permite interceptar peticiones para su autorización en función de reglas de negocio.

**AWS WAF** es un firewall para aplicaciones web que ayuda a proteger sus aplicaciones web o API contra ataques web y bots comunes que pueden afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos.

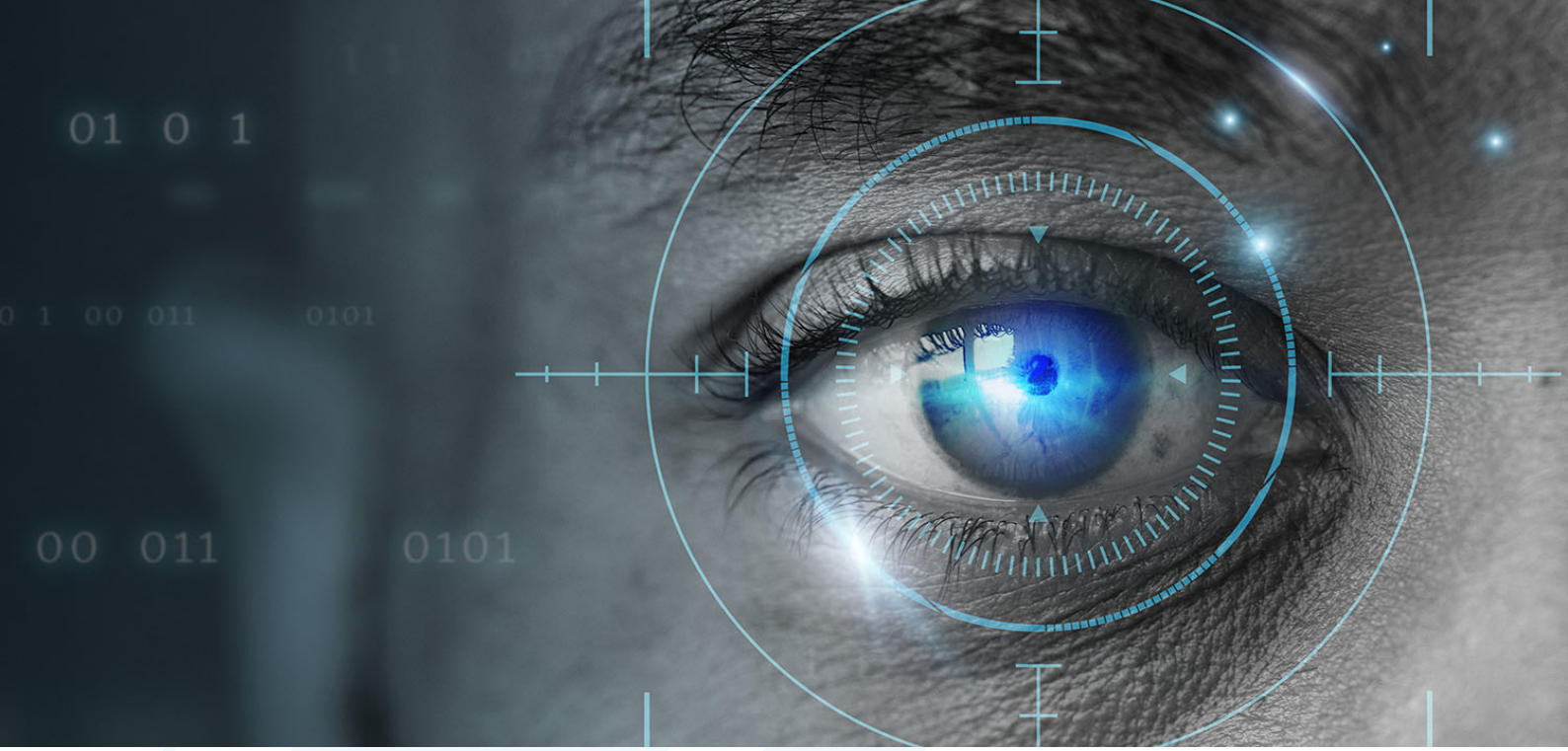
Para facilitar la implementación de protecciones ante ataques comunes, AWS WAF proporciona conjuntos de reglas administrados para los casos de uso más habituales y abre la opción a la implementación de conjuntos de reglas administrados por proveedores especializados como F5 o Fortigate.

AWS WAF se integra con múltiples servicios para evaluar las reglas de protección antes de reenviar el tráfico a sus servidores si esto fuera necesario.




**AWS Shield** es el servicio de protección frente a ataques DDoS de AWS.

En su capa gratuita, ofrece protecciones básicas en capa de red sobre toda la infraestructura y servicios en AWS con integración específica para Cloudfront (CDN) y Route53 (DNS). Si se desea un nivel de protección superior, la versión avanzada de Shield proporciona un conjunto mayor de protecciones con integraciones para Cloudfront, Route53, Elastic Load Balancer y ElasticIP, además de proporcionar acceso directo al equipo de soporte de AWS Shield para la remediación ante ataques.




## Protección de datos

Todos los servicios gestionados de AWS ofrecen opciones para el encriptado de datos, tanto en tránsito como en reposo. Es responsabilidad de los usuarios el hacer un correcto uso de estas funcionalidades en caso de que lo consideren necesario.

Para una correcta gestión de claves de encriptación, AWS pone a disposición de los usuarios el servicio **AWS Key Management Service (KMS)**, el cual se integra con prácticamente todos los servicios de almacenamiento de AWS. Con este servicio, los usuarios tienen la posibilidad de controlar mediante políticas de baja granularidad qué usuarios, cuentas o servicios AWS tienen el acceso necesario a las claves de encriptación necesarias para la recuperación o encriptación de datos en los distintos servicios de almacenamiento de AWS.

Para aquellas organizaciones que tengan requisitos elevados de cumplimiento de normativa, AWS permite la disposición de appliances hardware de propósito específico para el almacenamiento y custodia de claves de encriptación a través de su servicio **AWS CloudHSM**. Este servicio no está tan integrado con servicios de almacenamiento de AWS y está más orientado a su uso por parte de aplicaciones para la realización de operaciones de encriptado en el lado cliente, antes de que el dato se deposite en el servicio de almacenamiento correspondiente.

**AWS Certificate Manager** es un servicio gestionado para la emisión y distribución de certificados. Se ofrecen tanto certificados emitidos por la CA pública de AWS como la provisión de entidades de certificación privadas.

Con los certificados emitidos por la entidad certificadora pública de Amazon se habilita la posibilidad de utilizar certificados SSL con dominio personalizado en Cloudfront y Elastic Load Balancer sin coste adicional. El servicio ser encarga de instalar automáticamente el certificado en los recursos que se solicite y realizará la rotación del mismo de forma automática cuando el vencimiento del certificado esté próximo.

Las entidades de certificación privadas tienen como caso de uso principal la emisión de certificados de autenticación para usuarios y dispositivos; sin embargo, gracias a este servicio la carga de operar y mantener este tipo de infraestructura queda minimizada y basta con consumir el servicio cuando se necesite.

**AWS Secrets Manager** es un servicio especialmente diseñado para el almacenamiento, distribución, auditoría y rotación de secretos para aplicaciones tales como credenciales de bases de datos o APIs de terceros. Tiene una fuerte integración con el servicio de bases de datos Amazon RDS, Redshift y DocumentDB, así como con el servicio de orquestación de contenedores Elastic Container Service, que permite la distribución de secretos a los contenedores como variables de entorno.

**Tanto si eres una empresa como un profesional del sector y te interesan estos contenidos, servicios y soluciones, te invitamos a seguirnos en nuestros canales habituales de publicación o ponerte en contacto con nuestro equipo.**

**Síguenos en nuestras redes sociales para no perderte nada**

**Visita nuestra web y descubre nuestro blog**


**Qualoom Expertise Technology**

Correo de contacto: **contacto@qualoom.es**

Teléfono: (+34) 91 236 4808