

SERVICIOS DE SEGURIDAD AWS

[AWS GUARDDUTY](#)

[AWS INSPECTOR](#)

[AWS DETECTIVE](#)

[AWS SECURITY HUB](#)

[AWS TRUSTED ADVISOR](#)

[AWS WAF](#)

[AWS SHIELD](#)

[AWS MACIE](#)

[AWS FIREWALL MANAGER](#)

[RECURSOS EXTRA IMPORTANTES](#)

[AWS KMS](#)

[AWS SECRETS MANAGER:](#)

[AWS Systems Manager Parameter Store](#)

[AWS PARAMETER STORE VS AWS SECRETS MANAGER](#)

[AWS DIRECTORY SERVICES](#)

[AWS SSO](#)

AWS GUARDDUTY

- QUE ES? Servicio de detección de amenazas de AWS, monitoreo continuo de actividades maliciosas.
- FUENTES DE DATOS:
 - Eventos de CloudTrail: Registra las llamadas a las API de AWS, proporcionando información sobre las operaciones de administración realizadas en los recursos de la cuenta de AWS.
 - VPC Flow logs: Capturan información sobre el tráfico de red que entra y sale de sus interfaces de red en su VPC.
 - DNS Logs: Registros de consultas DNS que pueden ayudar a identificar actividades sospechosas como conexiones a dominios maliciosos.
 - Si se habilitan los planes de protección adicional:
 - Logs de acceso S3
 - Objetos almacenados en S3 (protección contra malware)
 - Monitoreo de clusters EKS
 - Eventos de RDS
 - Escaneo de volúmenes EBS
- 🤖 PRICING: Se basa en el volumen de registros de servicio, eventos, cargas de trabajo o datos analizados.

Detección de amenazas inteligente - Precios de Amazon GuardDuty - AWS

Los precios de Amazon GuardDuty se calculan a partir de la cantidad de eventos de AWS CloudTrail analizados y el volumen de datos de registros de DNS y registros de flujo de Amazon VPC analizados.

 <https://aws.amazon.com/es/guardduty/pricing/>



PRECIO BASICO: (OHIO)

- \$4.00 por millón de eventos de gestión CloudTrail analizados.

- \$1.00 por gigabyte (GB) de VPC flow logs.
- \$1.00 por gigabyte (GB) de logs DNS.

PRECIO DE PLANES DE PROTECCION ADICIONAL: (OHIO)

- Logs de S3: \$0.25 por 1 millón de eventos de S3.
- Objetos S3: \$0.001 por objeto analizado.
- EKS: \$0.40 por cada 1 millón de registros auditados del runtime de EKS.
- RDS: \$0.40 por cada 1 millón de eventos auditados.
- Escaneo EBS: 0,03 USD por GB
- CONCEPTOS IMPORTANTES:
 - FINDING: Evento potencialmente malicioso encontrado en la cuenta, cada uno tienen un valor asociado con la criticidad del evento.
 - INTEGRACIONES: Se puede integrar con Cloudwatch o Lambda para la mitigación automática de actividad anómala/sospechosa.
- CASOS DE USO:
 - **Monitoreo de Acceso No Autorizado:** Identificación de intentos no autorizados de acceder a recursos de AWS.
 - **Detección de Minería de Criptomonedas:** Detección de instancias de EC2 utilizadas para minería de criptomonedas sin autorización.
 - **Monitoreo de Actividades Internas:** Identificación de comportamientos inusuales o potencialmente maliciosos de usuarios internos.

AWS INSPECTOR

- QUE ES? AWS Inspector es un servicio automatizado de **evaluación de vulnerabilidades** que mejora la seguridad y conformidad de las **aplicaciones** desplegadas en AWS.
- FUENTES DE DATOS:

Evalúa instancias de EC2, funciones de Lambda e imágenes de contenedores en Amazon ECR

 - EC2: Evalúa instancias de EC2 de forma continua para detectar vulnerabilidades de software y exposición de red no deseada.
 - ECR: Analiza cada imagen de contenedor insertada en Amazon ECR para detectar vulnerabilidades de software.
 - AWS Lambda: Evalúa las funciones de Lambda de manera continua para detectar vulnerabilidades en los paquetes de software y en el código de la aplicación.
- 🗺️ PRICING: Region OHIO

Administración automatizada de vulnerabilidades - Precios de Amazon Inspector - AWS

Amazon Inspector es un servicio automatizado de administración de vulnerabilidades en el que solo paga por lo que utiliza, sin tarifas mínimas ni compromisos iniciales.

 <https://aws.amazon.com/es/inspector/pricing/>



- **Instancias de Amazon EC2:**
 - \$0.30 por instancia de EC2 evaluada por mes.

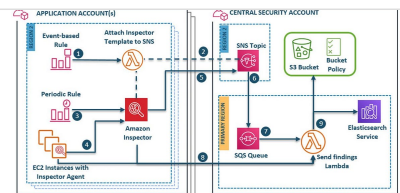
- Evaluaciones de conformidad CIS: \$0.30 por evaluación por instancia.
- **Imágenes de Contenedores en Amazon ECR:**
 - \$0.09 por imagen de contenedor evaluada (inicialmente).
 - \$0.08 por imagen de contenedor re-evaluada (mensualmente).
- **Funciones de AWS Lambda:**
 - \$0.30 por función de Lambda evaluada por mes (paquetes de software).
 - \$0.30 por función de Lambda evaluada por mes (código de la aplicación).
- **CONCEPTOS IMPORTANTES:**
 - **Findings:** Resultados de las evaluaciones que identifican vulnerabilidades y problemas de seguridad en las instancias de EC2, imágenes de contenedores y funciones de Lambda.
 - **Agente de AWS Inspector:** Un software instalado en las instancias de EC2 para recopilar datos de configuración y comportamiento.
 - **Informes:** Proporciona informes detallados de las evaluaciones con recomendaciones para la remediación.

INSPECTOR VS GUARDUTY

Use case: AWS Inspector vs GuardDuty

inb4: The official names are Amazon Inspector and Amazon GuardDuty, but I know a lot of you will be searching via the AWS name, hence the...

<https://medium.com/aws-architech/use-case-aws-inspector-vs-guardduty-3662bf80767a>



AWS Inspector	AWS Guarduty
Se enfoca en encontrar vulnerabilidades de software, configuraciones incorrectas y problemas de conformidad en instancias de EC2, imágenes de contenedores y funciones de Lambda.	Se centra en la detección de amenazas y comportamientos anómalos mediante el análisis de registros de eventos y tráfico de red.
Realiza evaluaciones basadas en políticas de seguridad y mejores prácticas de la industria, como los puntos de referencia del CIS.	Detecta accesos no autorizados, uso de credenciales comprometidas y tráfico malicioso.
Detección de problemas de seguridad específicos en el código y en los paquetes de software.	Incluye capacidades adicionales de protección para S3, análisis de malware, monitoreo de clústeres de EKS y funciones de Lambda, enfocándose en actividades anómalas y amenazas conocidas.

AWS DETECTIVE

- **QUE ES?** Servicio de ANALISIS y VISUALIZACION que facilita la investigacion de actividades sospechosas. Utiliza machine learning, análisis estadístico y teoría de gráficos para construir un modelo gráfico interactivo que ayuda a los usuarios a identificar, investigar y resolver problemas de seguridad más rápidamente.
- **TIEMPO DE RETENCION DE DATOS:** 1 año
- **FUENTES DE DATOS:**
 - Cloudtrail logs
 - VPC flow logs

- Logs de EKS
- Resultados de Security Hub
- Resultados de Guardduty
- FUNCIONES PRINCIPALES:
 - **Análisis de Datos:** Recopila automáticamente datos de AWS CloudTrail, Amazon VPC Flow Logs y Amazon GuardDuty findings.
 - **Modelado Gráfico:** Construye un modelo gráfico que permite visualizar las relaciones y actividades entre recursos de AWS.
 - **Investigación de Incidentes:** Facilita la investigación de actividades sospechosas mediante la correlación de eventos y la visualización de patrones de comportamiento.
 - **Contexto Completo:** Proporciona un contexto completo de cada actividad sospechosa, incluyendo el historial y la relación con otros eventos.
- 💰 PRICING: Se basa netamente en el volumen de datos ingeridos y almacenados, medidos en GB por mes,
 - Ingesta de datos: 2\$ x GB
 - Almacenamiento de datos: 0.25\$ x GB
- CONCEPTOS IMPORTANTES:
 - **Behavior Graph:** Modelo gráfico construido por AWS Detective que representa las relaciones y actividades entre recursos de AWS.
 - **Investigaciones:** Proceso de explorar y analizar el comportamiento de los recursos y sus interacciones para identificar la causa raíz de los incidentes de seguridad.
- CASOS DE USO:
 - **Investigación de Incidentes de Seguridad:** Exploración de actividades sospechosas y detección de patrones anómalos para identificar la causa raíz de los incidentes.
 - **Análisis Forense:** Realización de análisis forense detallado para entender cómo ocurrieron los incidentes de seguridad y prevenir futuras ocurrencias.

AWS SECURITY HUB

- QUE ES? Servicio de VISIBILIDAD INTEGRAL del estado de SEGURIDAD de AWS. Agrega, organiza y prioriza los FINDINGS de múltiples servicios de AWS.
 Básicamente permite una gestión centralizada de la postura de seguridad de la cuenta.
- FUENTES DE DATOS: (FINDINGS Y FRAMEWORKS DE SEGURIDAD)
 - Guardduty
 - Inspector
 - Macie
 - Firewall Manager
 - IAM Access Analyzer
 - Fuentes de frameworks de seguridad y conformidad (CIS, NIST, PCI, AWS Foundational Security Best Practices)
- FUNCIONALIDADES PRINCIPALES:


- **Agregación de Alertas:** Recopila findings de varios servicios de AWS como Amazon GuardDuty, AWS Inspector, AWS Macie, y soluciones de seguridad de terceros.
- **Evaluación de Conformidad:** Realiza evaluaciones de conformidad automatizadas utilizando estándares como CIS AWS Foundations Benchmark, PCI DSS, AWS Foundational Security Best Practices y más.
- **Panel de Control Centralizado:** Proporciona una vista unificada de los findings de seguridad y el estado de conformidad.
- **Automatización y Remediación:** Permite la automatización de respuestas a findings de seguridad mediante integraciones con **AWS Lambda y AWS Systems Manager**.
- 🤖 PRICING:
Se basa en la cantidad de evaluaciones de seguridad y findings procesados y reglas de automatización.
 - Eventos ingestados:
 - Primeros 10,000 eventos al mes son gratuitos.
 - Más de 10,000 eventos al mes: \$0.00003 por evento.
 - Controles de Seguridad: Evaluaciones realizadas para verificar la configuración de los recursos de AWS contra estándares de seguridad y conformidad.
 - Primeros 100,000 controles al mes: \$0.0010 por verificación.
 - Próximos 400,000 controles al mes: \$0.0008 por verificación.
 - Más de 500,000 controles al mes: \$0.0005 por verificación.
- CASOS DE USO:
 - **Gestión Centralizada de Seguridad:** Centraliza la gestión de alertas y evaluaciones de conformidad para una visión integral del estado de seguridad.
 - **Monitoreo de Conformidad:** Monitorea el cumplimiento de marcos de seguridad y conformidad reconocidos.
 - **Automatización de Respuestas:** Implementa automatización para respuestas rápidas y eficientes a findings de seguridad.
 - **Mejora Continua:** Identifica y prioriza áreas de mejora en la postura de seguridad mediante insights y evaluaciones continuas.

AWS TRUSTED ADVISOR

- QUE ES? Servicio que proporciona recomendaciones en tiempo real para ayudarte a seguir las mejores prácticas de AWS. Analiza tu entorno AWS y ofrece recomendaciones específicas en cinco categorías clave: costos, rendimiento, seguridad, tolerancia a fallos y límites de servicio.
- CATEGORIAS DE RECOMENDACIONES:
 - **Costos:** Identifica maneras de reducir costos al eliminar recursos infrautilizados o no utilizados.
 - **Rendimiento:** Ofrece sugerencias para mejorar el rendimiento de tus servicios de AWS.
 - **Seguridad:** Proporciona recomendaciones para cerrar brechas de seguridad y proteger tus datos.
 - **Tolerancia a Fallos:** Aconseja sobre cómo aumentar la disponibilidad y la recuperación ante desastres.
 - **Límites de Servicio:** Ayuda a gestionar los límites de servicio para evitar interrupciones por alcanzar los límites predefinidos.
- 🤖 PRICING:

Optimización de la nube – AWS Trusted Advisor

AWS Trusted Advisor lo ayuda a optimizar los costos y el rendimiento, mejorar la seguridad y la resiliencia, y operar a escala en la nube.

 <https://aws.amazon.com/es/premiumsupport/technology/trusted-advisor/>



- **Acceso Básico:**

- **Gratuito:** Acceso a un conjunto limitado de verificaciones y recomendaciones para todos los clientes de AWS.

- **Acceso Completo:**

- **Planes de Soporte Business y Enterprise:** Acceso a todas las verificaciones y recomendaciones. El costo está incluido en los planes de soporte Business (\$100 al mes) y Enterprise (a partir de \$15,000 al mes).


AWS WAF


- **QUE ES? AWS WAF** es un firewall de aplicaciones web que ayuda a proteger tus aplicaciones web de ataques comunes como SQL injection, cross-site scripting (XSS), y otros exploits. AWS WAF te permite crear reglas personalizadas que bloquean patrones específicos en el tráfico HTTP y HTTPS.
- **FUNCIONALIDADES PRINCIPALES:**
 - **Reglas Personalizadas:** Define reglas que filtran tráfico basado en condiciones específicas, como IPs, valores de encabezados, cuerpos de solicitud, cadenas URI, y más.
 - **Protección Contra Ataques Comunes:** Protege contra amenazas OWASP Top 10, SQL injection, cross-site scripting, y otros ataques.
 - **Managed Rules:** Utiliza conjuntos de reglas administradas proporcionadas por AWS y terceros para simplificar la configuración y el mantenimiento.
 - **Integración con AWS Services:** Se integra con Amazon CloudFront, Application Load Balancer (ALB), API Gateway, y AWS App Runner.
 - **Análisis y Visibilidad:** AWS WAF proporciona registros detallados y métricas en tiempo real para ayudarte a comprender y responder a posibles amenazas.
- **COMPONENTES PRINCIPALES:**
 - **Web ACL (Access Control List):**
 - Una colección de reglas que AWS WAF usa para filtrar tráfico hacia tus recursos web.
 - Puedes asociar una Web ACL con uno o más recursos como CloudFront distributions, ALBs, y API Gateways.
 - **Rules:**
 - **Custom Rules:** Reglas personalizadas que definen condiciones específicas para permitir, bloquear o contar solicitudes.
 - **Managed Rules:** Conjuntos de reglas administradas por AWS o proveedores de seguridad de terceros que ofrecen protección contra amenazas comunes sin necesidad de configuraciones detalladas.
 - **Rule Groups:**

- Colección de reglas que puedes reutilizar en varias Web ACLs. Puedes usar rule groups administrados o crear tus propios rule groups personalizados.
- **Conditions:**
 - **IP Match Conditions:** Filtra tráfico basado en direcciones IP.
 - **String Match Conditions:** Filtra tráfico basado en coincidencias de cadenas en las solicitudes HTTP/S.
 - **SQL Injection Match Conditions:** Detecta patrones de SQL injection.
 - **Cross-Site Scripting (XSS) Match Conditions:** Detecta patrones de XSS.
- 🤖 PRICING:

Precios – AWS WAF – Amazon Web Services (AWS)

Precios para AWS WAF – Amazon Web Services (AWS)

 <https://aws.amazon.com/es/waf/pricing/>



- **Web ACLs:**
 - \$5.00 por Web ACL creada por mes.
- **Rules:**
 - \$1.00 por regla por Web ACL por mes.
- **Rule Groups:**
 - \$1.00 por cada regla dentro del rule group por Web ACL por mes.
- **Requests:**
 - \$0.60 por millón de solicitudes revisadas por AWS WAF.
- CASOS DE USO:
 - **Protección de Aplicaciones Web:** Implementa reglas para proteger tus aplicaciones web contra ataques comunes.
 - **Conformidad con Normativas:** Asegura que las aplicaciones cumplan con las normativas de seguridad utilizando conjuntos de reglas administradas.
 - **Protección de API:** Utiliza AWS WAF para proteger APIs frente a ataques de explotación y abuso.
 - **Mitigación de DDoS:** Complementa AWS Shield para mitigar ataques de denegación de servicio distribuidos (DDoS).


AWS SHIELD


- QUE ES? AWS Shield es un servicio de protección contra ataques de denegación de servicio distribuidos (DDoS) que ayuda a proteger tus aplicaciones web y minimizar el tiempo de inactividad. AWS Shield está disponible en dos niveles: AWS Shield Standard y AWS Shield Advanced.
- NIVELES DE SEGURIDAD DE SHIELD
 - **AWS SHIELD STANDARD:** AWS Shield Standard proporciona protección automática contra ataques DDoS a todos los clientes de AWS sin costo adicional. Esta protección está habilitada por defecto y está integrada con Amazon CloudFront, Elastic Load Balancing, Amazon Route 53, y AWS Global Accelerator.

- **Protección Contra Ataques Comunes:** Protege contra los ataques DDoS más comunes, como ataques de capa de red y capa de transporte (niveles 3 y 4 del modelo OSI).
- AWS SHIELD ADVANCED: AWS Shield Advanced ofrece protección avanzada contra ataques DDoS para aplicaciones web que requieren mayor seguridad y visibilidad. Incluye capacidades adicionales y servicios de mitigación personalizados, con un costo adicional.
 - **Protección Mejorada:** Proporciona detección y mitigación avanzada para ataques DDoS a nivel de aplicación (capa 7) y protección adicional contra ataques a niveles 3 y 4.
 - **Dashboard de Seguridad:** Acceso a un panel de control en AWS Management Console con información detallada sobre ataques y métricas de tráfico.
 - **DDoS Cost Protection:** Compensación de los costos adicionales que resultan de un ataque DDoS, como picos en el uso de recursos.
 - **Asistencia Experta:** Acceso a expertos del AWS DDoS Response Team (DRT) para soporte durante y después de un ataque.
 - **Análisis y Reportes Detallados:** Reportes detallados post-ataque y análisis continuos para mejorar la postura de seguridad.
- 🏷️ PRICING:

Precios: AWS Shield: Amazon Web Services (AWS)

Precios de AWS Shield: Amazon Web Services (AWS)

 <https://aws.amazon.com/es/shield/pricing/>



- SHIELD STANDARD: Gratis
- SHIELD ADVANCED:
 - \$3,000 por mes.
 - **Costo Adicional por Data Transfer:** \$0.050 por GB para tráfico de AWS Shield Advanced.
- CONCEPTOS IMPORTANTES:
 - **Mitigación de DDoS:** Técnicas y medidas utilizadas para reducir el impacto de los ataques DDoS.
 - **Dashboard de Seguridad:** Interfaz en la consola de AWS que proporciona información detallada sobre ataques y métricas de tráfico.
 - **AWS DDoS Response Team (DRT):** Equipo de expertos en AWS que proporciona soporte y asistencia durante y después de un ataque DDoS.
- VENTAJAS:
 - **Protección Automática:** AWS Shield Standard proporciona protección básica automática sin necesidad de configuración adicional.
 - **Mitigación Avanzada:** AWS Shield Advanced ofrece capacidades avanzadas de mitigación y análisis detallado de ataques.
 - **Asistencia Experta:** Acceso a expertos del DDoS Response Team para asistencia personalizada.
 - **Compensación de Costos:** Protección contra los costos adicionales asociados a un ataque DDoS.

AWS MACIE

- QUE ES?

AWS Macie es un servicio de seguridad y privacidad de datos que utiliza machine learning y reconocimiento de patrones para descubrir, clasificar y proteger datos sensibles almacenados en Amazon S3. AWS Macie ayuda a los usuarios a cumplir con las normativas de privacidad y proteger la información personal identificable (PII) y otros datos sensibles.

- **Funcionalidades Principales:**

- **Descubrimiento y Clasificación de Datos:** Identifica y clasifica automáticamente datos sensibles, como información personal identificable (PII), información financiera, datos médicos, y más.
- **Monitorización Continua:** Monitorea continuamente los buckets de S3 para identificar cualquier acceso o actividad inusual que pueda indicar una amenaza a la seguridad.
- **Alertas y Notificaciones:** Genera alertas y notificaciones cuando se detectan datos sensibles o actividades inusuales.
- **Panel de Control Interactivo:** Proporciona un panel de control interactivo para ver y gestionar los datos sensibles y las alertas de seguridad.

- 🏷️ PRICING:

Detección de datos confidenciales - Precios de Amazon Macie - Amazon Web Services
Obtenga más información acerca de los precios de Amazon Macie.

 <https://aws.amazon.com/es/macie/pricing/>



- **Supervisión e Inventario de Buckets:**
 - \$0.10 por bucket al mes.
- **Datos Inspeccionados para Detección Automatizada y Selectiva de Datos Confidenciales:**
 - Primeros 50 TB al mes: \$1.00 por GB.
 - Sigüientes 450 TB al mes: \$0.50 por GB.
 - Más de 500 TB al mes: \$0.25 por GB.
- **Supervisión Automatizada de Objetos para Detección de Datos:**
 - \$0.010 por 100,000 objetos al mes.

- ESCENARIOS COMUNES:

- **Protección de Información Personal:** Identifica y protege información personal identificable (PII) y otros datos sensibles almacenados en S3.
- **Cumplimiento de Normativas:** Utiliza AWS Macie para cumplir con las normativas de privacidad y seguridad de datos.
- **Monitoreo de Actividades:** Monitorea continuamente los accesos y actividades en los buckets de S3 para detectar posibles amenazas.

AWS FIREWALL MANAGER

- QUES ES?

AWS Firewall Manager es un servicio de administración centralizada que permite configurar y administrar reglas de firewall en todas las cuentas y aplicaciones en tu organización de AWS. AWS Firewall Manager simplifica la configuración y mantenimiento de las reglas de seguridad y políticas de firewall, incluyendo AWS WAF, AWS Shield Advanced, y grupos de seguridad VPC.

- **FUNCIONES PRINCIPALES:**
 - **Administración Centralizada:** Gestiona y aplica reglas de firewall en todas las cuentas y aplicaciones de AWS desde un único lugar.
 - **Políticas de Seguridad:** Define y aplica políticas de seguridad consistentes en toda tu organización.
 - **Integración con AWS Services:** Se integra con AWS WAF, AWS Shield Advanced, y grupos de seguridad VPC para una protección completa.
 - **Automatización:** Automatiza la implementación y mantenimiento de reglas de firewall en todas las cuentas y aplicaciones.
- 🤖 **PRICING:**
<https://aws.amazon.com/es/firewall-manager/pricing/>
- **VENTAJAS CLAVE:**
 - **Consistencia de Seguridad:** Asegura que todas las cuentas y aplicaciones sigan políticas de seguridad consistentes.
 - **Eficiencia Operacional:** Simplifica la configuración y mantenimiento de reglas de firewall en un entorno multi-cuenta.
 - **Automatización de Políticas:** Automatiza la aplicación y mantenimiento de políticas de seguridad, reduciendo la carga administrativa.
 - **Visibilidad Centralizada:** Proporciona una vista centralizada de todas las políticas de seguridad y su estado de cumplimiento.

RECURSOS EXTRA IMPORTANTES

AWS SECURITY SERVICES CHEATSHEET

Feature/Function	AWS Security Hub	Amazon GuardDuty	Amazon Detective	Amazon Inspector	Amazon Macie
Primary Function	Centralized security and compliance management	Threat detection service for malicious activity and unauthorized behavior	Deep analysis of security data and findings to investigate incidents	Automated security assessment to find vulnerabilities and deviations from best practices	Data security and privacy service to protect sensitive information
Integration	Aggregates findings from AWS services and APN solutions	Integrates with AWS services for monitoring and logs (CloudTrail, VPC Flow Logs)	Integrates with GuardDuty, Security Hub, CloudTrail, and VPC Flow Logs	Works with AWS services to assess applications deployed on AWS	Integrates with AWS resources like S3 for data classification and protection
Key Features	- Prioritized security alerts - Compliance scores	- Anomaly detection - Machine learning for threat identification	- Visual investigation tools - Machine learning and statistical analysis	- Vulnerability scanning - Best practice checks	- Machine learning & pattern matching - Sensitive data discovery and classification
Use Cases	- Overview of security posture - Compliance monitoring	- Intrusion detection - Unusual behavior monitoring	- Security investigation - Analyzing interaction between entities	- Vulnerability management - Security assessment of EC2 instances and applications	- Data privacy compliance (GDPR, HIPAA) - Protecting against data leaks
Data Retention	N/A (aggregates and prioritizes findings from integrated services)	Continuous monitoring	Stores data for one year	N/A (provides real-time assessment and recommendations)	Continuous monitoring and alerting
Pricing	Charged based on the number of checks run and the number of findings ingested	Charged based on the amount of data analyzed	Charged based on the volume of ingested data	Charged based on the number of assessments and the types of instances assessed	Charged based on the amount of data processed
Target User	Security teams needing a comprehensive security overview and compliance reporting	Organizations looking for continuous security monitoring and threat detection	Security analysts requiring detailed investigations of security incidents	Security and compliance teams focused on application security and vulnerability management	Organizations with a need to protect sensitive data and ensure privacy compliance

PRODUCTOS DE SEGURIDAD, CLASIFICACION DE FUNCIONES

Productos de seguridad, identidad y conformidad en la nube – Amazon Web Services (AWS)

Los servicios de seguridad, identidad y conformidad de AWS le permiten asegurar sus cargas de trabajo y aplicaciones en la nube.

 <https://aws.amazon.com/es/products/security/>



AWS KMS

- **QUE ES?** AWS Key Management Service (KMS) es un servicio de gestión de claves que permite crear, controlar y administrar las claves de cifrado utilizadas para proteger los datos en AWS.

- **CONCEPTOS IMPORTANTES:**

- **CMK (Customer Managed Keys):** Creadas y gestionadas por el usuario, controla la rotaciones, eliminación y políticas.
- **AMK (AWS Managed Keys):** Creadas y gestionadas por AWS, se integra con otros servicios.
- **KEYS IMPORTADAS:** El usuario importa su material de clave para generar claves maestras CMK.

- **PRICING:**

AWS Managed Keys:

- \$0.03 por 10k solicitudes a la API
- \$1 dolar por rotación para las 2 primeras. Rotaciones posteriores GRATIS

CMK y IMPORTED KEYS:

- \$1 por clave al mes
- \$0.03 por 10k solicitudes a la API (cifrado, descifrado, generación y operaciones de firma)
- \$1 dolar por rotación para las 2 primeras. Rotaciones posteriores GRATIS

- **FUNCIONALIDADES:**

- **GESTION DE CLAVES**

- **Creación de Claves:** Permite crear claves maestras de cliente (CMKs) que pueden ser usadas para cifrar y descifrar datos.
- **Rotación de Claves:** Automatiza la rotación de claves maestras para mejorar la seguridad.
- **Importación de Claves:** Permite importar claves propias para tener un control completo sobre las claves de cifrado.
- **Control de Acceso:** Utiliza políticas de IAM y políticas de claves para controlar quién puede administrar y usar las claves.

- **CIFRADO**

- **Cifrado en reposo:** Cifra datos en reposo en varios servicios de AWS, como S3, EBS, y RDS, sin necesidad de cambiar la lógica de la aplicación.
- **Cifrado de datos** altamente sensibles en aplicaciones críticas.

AWS SECRETS MANAGER:

- **QUE ES?** Servicio que permite rotar, gestionar y recuperar credenciales, claves y otros secretos.

- **FUNCIONES PRINCIPALES**
 - **Almacenamiento Seguro:** Almacena credenciales y secretos de manera segura.
 - **Rotación Automática:** Facilita la rotación automática de credenciales y secretos según una programación definida.
 - **Recuperación de Secretos:** Proporciona una API segura para recuperar secretos cuando las aplicaciones los necesiten.
- **INTEGRACIONES DIRECTAS**
 - **Amazon RDS:** Integración directa para la rotación de credenciales de bases de datos.
 - **Amazon Redshift, Amazon DocumentDB:** Soporte para la rotación y gestión de credenciales.
 - **IAM Policies:** Control de acceso detallado utilizando políticas de AWS IAM para gestionar quién puede acceder y gestionar los secretos.
- **PRICING**
 - \$0.40 por secreto almacenado por mes.
 - \$0.05 por cada 10,000 solicitudes de API.
- **CONCEPTOS IMPORTANTES**
 - **Secretos:** Información sensible como credenciales de base de datos, claves API y certificados, que necesitan ser gestionados y protegidos.
 - **Rotación de Secretos:** Proceso de actualizar los secretos periódicamente para mantener la seguridad.
 - **Políticas de IAM:** Utilizadas para definir quién tiene acceso a gestionar y recuperar los secretos.


AWS Systems Manager Parameter Store

- **¿Qué es?**
AWS Systems Manager Parameter Store es un servicio que proporciona un almacenamiento seguro para valores de configuración y secretos simples. Permite gestionar configuraciones y parámetros a lo largo de múltiples servicios y aplicaciones.
- **Funcionalidades Principales:**
 - **Almacenamiento de Configuraciones:** Permite almacenar valores de configuración como cadenas de texto, datos cifrados y parámetros jerárquicos.
 - **Parámetros Cifrados:** Ofrece la opción de cifrar parámetros utilizando AWS KMS.
 - **Versionado:** Mantiene un historial de versiones de parámetros, permitiendo revertir a versiones anteriores.
 - **Notificaciones:** Integración con AWS CloudWatch Events para recibir notificaciones sobre cambios en los parámetros.
 - **Integración con IAM:** Controla el acceso a los parámetros mediante políticas de IAM.
- **Pricing:**
 - **Parámetros No Cifrados:** Gratis.
 - **Parámetros Cifrados:** \$0.05 por parámetro almacenado por mes.
 - **Solicitudes de API:** Gratis hasta 1 millón de solicitudes por mes, después \$0.40 por millón de solicitudes adicionales.

AWS PARAMETER STORE VS AWS SECRETS MANAGER

AWS—Difference between Secrets Manager and Parameter Store (Systems Manager)

Comparisons: AWS Secrets Manager vs Systems Manager Parameter Store

 <https://medium.com/awesome-cloud/aws-difference-between-secrets-manager-and-parameter-store-systems-manager-f02686604eae>



- **Propósito y Uso:**

- **Parameter Store:** Diseñado para almacenar valores de configuración y parámetros simples. Adecuado para configuraciones de aplicaciones y variables de entorno.
- **Secrets Manager:** Diseñado específicamente para gestionar secretos, como credenciales y claves API, y proporciona capacidades avanzadas de rotación y auditoría.

- **Rotación de Secretos:**

- **Parameter Store:** No ofrece rotación automática de secretos. La rotación debe ser manejada manualmente por el usuario.
- **Secrets Manager:** Ofrece rotación automática de secretos, integrándose con varios servicios de AWS para actualizar automáticamente las credenciales.

AWS DIRECTORY SERVICES

- QUE ES? AWS Directory Services ofrece varias soluciones de directorio para gestionar identidades y recursos dentro de la infraestructura de AWS. Estas soluciones incluyen Simple AD, AWS Managed Microsoft AD y AD Connector. Cada una de estas opciones está diseñada para satisfacer diferentes necesidades de gestión de identidades y acceso en entornos AWS
- OPCIONES
 - SIMPLE AD: Opción de directorio administrado económica que soporta características básicas de Active Directory. Es ideal para organizaciones que no necesitan todas las capacidades avanzadas de Microsoft AD y buscan una solución simple y de bajo costo.
 - Autenticación
 - Gestión de usuarios, grupos y recursos dentro de AWS
 - Soporta integración con LDAP
 - AWS MANAGED MICROSOFT AD: Es un servicio de directorio administrado que ejecuta Microsoft Active Directory (AD) en AWS. Ofrece todas las características avanzadas de AD sin la necesidad de gestionar la infraestructura subyacente.
 - Sistema totalmente gestionado, soporta federación con otros AD.
 - AD CONNECTOR: AD Connector es un **proxy de directorio** que permite a las aplicaciones de AWS utilizar un directorio existente en Microsoft AD sin necesidad de sincronizar o duplicar identidades en la nube.
 - No requiere sincronización de datos.
 - Permite autenticación y autorización usando un AD ya existente

Característica	Simple AD	AWS Managed Microsoft AD	AD Connector
Descripción	Directorio básico y económico	Directorio avanzado de AD	Proxy para directorio de AD
Totalmente Administrado	Sí	Sí	No
Federación de Identidades	No	Sí	No
Integración con AD Existente	No	Sí	Sí
Costo	Económico	Alto	Depende del uso
Uso Común	PYMES	Grandes empresas	Empresas con AD on-premises

AWS SSO

- **QUE ES?** servicio que permite gestionar el acceso a múltiples cuentas y aplicaciones de AWS mediante un inicio de sesión único.
- **FUNCIONES**
 - **Inicio de Sesión Único:** Permite a los usuarios iniciar sesión una vez para acceder a múltiples aplicaciones y cuentas de AWS.
 - **Integración con Directorios:** Se integra con AWS Managed Microsoft AD y otros directorios compatibles para gestionar identidades.