BUENAS PRÁCTICAS DE SEGURIDAD PARA APLICACIONES WEB DESPLEGADAS EN UN MODELO DE INFRAESTRUCTURA TIPO IAAS EN LA NUBE DE AWS

ELKIN MAURICIO RIVERA MEJÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

BUENAS PRÁCTICAS DE SEGURIDAD PARA APLICACIONES WEB DESPLEGADAS EN UN MODELO DE INFRAESTRUCTURA TIPO IAAS EN LA NUBE DE AWS

ELKIN MAURICIO RIVERA MEJÍA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:
KATERINE MÁRCELES VILLALBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 2023

AGRADECIMIENTOS

Agradezco a Dios por darme la oportunidad de realizar y culminar esta etapa de mi formación profesional, a mi familia por la paciencia y apoyo incondicional durante el desarrollo de mis estudios.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

GLOSARIO

ANCHO DE BANDA: Capacidad de transferir información en una red a otra incluyendo la salida a internet.

BACKUP: Copia que se realiza a la información y se encuentra almacenada en una ubicación diferente y funciona como respaldo ante cualquier tipo de incidente.

BALANCE DE CARGA: Consiste en dividir la capacidad de procesamiento entre varios dispositivos.

CAPEX: Define “Gastos de Capital”, asociado a los bienes que son adquiríos por una organización, en el cual tiene en cuenta el pago único y definición de la vida útil de un producto.

CENTRO DE DATOS: También conocidos como (CPD), ubicaciones físicas donde se encuentran los recursos e infraestructura.

CLOUD PÚBLICO: Servicios ofrecidos por una empresa la cual alquila su infraestructura y son alcanzados a través de una red pública.

COMPUTACIÓN EN LA NUBE: Despliegue de recursos informáticos y consultados a través de redes públicas como el internet, los servicios varían dependiendo del proveedor.

DIRECCIÓN IP: Identificador de un dispositivo conectado a una red informática, existen dos tipos de direcciones IP, las IP públicas que se encuentran enrutadas en internet y las IP privadas que son usadas en redes LAN.

DNS: Sistema de nombres de dominio, mediante el uso de este protocolo los nombres de los sitios web o dominios son convertidos en direcciones IP, lo que ocasiona que los usuarios puedan acceder a los recursos de manera práctica.

DoS: Ataque de denegación de servicios, consiste en generar miles de sesiones simultaneas con el fin de ocasionar que los dispositivos no tengan la capacidad de responder a cada una de estas, ocasionando fallas en la prestación de servicios.

FIREWALL: Este equipo realiza la inspección del tráfico entrante como saliente de una red y de acuerdo a sus políticas lo permite o restringe.

FRAMEWORK: Conjunto de estándares que contiene prácticas y conceptos para enfocase en un tipo especifico de problemática.

HIPERVISOR: Proceso mediante el cual es posible crear y ejecutar máquinas virtuales, permitiendo aprovechar las funciones de virtualización y ofreciendo recursos de cómputo**.**

IPSEC: Seguridad del protocolo de internet, mediante el uso de este protocolo es posible garantizar la confidencialidad de los datos ya que a estos se le aplica una capa de cifrado y requiere de una llave para poder acceder.

INTERNET: Es la red informática mundial que permite realizar la interconexión de diferentes dispositivos, ofreciendo gran variedad de servicios y recursos con el fin de facilitar la comunicación entre usuarios.

ISP: Proveedor de servicios de internet. Empresa encargada de prestar conectividad para consumir recursos que se encuentran en nube pública al igual que la navegación de los usuarios.

LAN: Red de área local, permite la comunicación entre dispositivos conectados a nivel local o en el mismo dominio de broadcast.

NTP: (Network Time Protocol), este protocolo es utilizado para sincronizar la hora en los relojes de los sistemas informáticos.

MÁQUINA VIRTUAL: Software que permite simular y ejecutar sistemas operativos.

OPEX: Define “Gastos de operacionales”, asociado a los costos generados por la contratación de servicios que garantizan la operación de un servicio.

PAY AS-YOU-GO: modelo de pago para servicios adquiridos en la nube, en el que únicamente se paga por los servicios que son consumidos en el desarrollo de determinada actividad.

SEGURIDAD INFORMÁTICA: Esta área se encarga de la protección de las infraestructuras, mediante la identificación de vulnerabilidades y buenas prácticas para aplicar en la configuración de los dispositivos.

SISTEMA OPERATIVO: Conjunto de programas que permite realizar la interacción con el hardware de los equipos, adicionalmente permite la prestación de servicios y aplicaciones.

TIME TO MARKET: Reducción del tiempo que transcurre desde que un producto es seleccionado hasta que es puesto es producción

VPN: Red virtual privada permite realizar la extensión y conexión segura a una red LAN, a través de un agente o una conexión cifrada cuando la VPN es establecida con equipos que soportan el protocolo ipsec.

WAF: Este dispositivo se encarga de realizar la protección de las aplicaciones web incluidas el top 10 de Owasp.

RESUMEN

Cloud Computing, puede ser utilizada por cualquier tipo de organización independiente de su tamaño. Sin embargo, las empresas con menos recursos pueden obtener mayor beneficio ya que no requieren de grande sumas de dinero para la implementación de centros de datos; entre los beneficios que se encuentran están los relacionados con optimizar el aprovisionamiento de recursos informáticos, garantizando que las empresas puedan desplegar sus infraestructuras de manera escalable, ágil y ajustándose a sus necesidades, facilitando la administración y actualización de los componentes utilizados, lo cual permite que las empresas puedan desarrollar sus actividades y procesos del día a día, que van en pro del posicionamiento y crecimiento económico.

Se deben considerar algunos aspectos indispensables como la seguridad de la información almacenada, el tratamiento de datos y las aplicaciones web desplegadas en infraestructuras cloud tipo IaaS; teniendo en cuenta lo anterior, se han generado nuevos retos de seguridad para los administradores de estas plataformas, ya que se tiende a creer que los responsables son los Providers cloud, dejando en el olvido el aseguramiento y buenas prácticas que se deben tener en cuenta al momento de realizar la migración a infraestructuras cloud, de no seguir el correcto procedimiento, puede llevar a que se generen brechas de seguridad y posiblemente incidentes que afecten la prestación de servicios.

Palabras claves: Cloud Computing, IaaS, incidentes, incidentes

ABSTRACT

Cloud Computing can be used by any type of organization regardless of its size. However, companies with fewer resources can obtain greater benefit since they do not require large sums of money for the implementation of data centers; among the benefits that we find are those related to optimizing the provisioning of computing resources, guaranteeing that companies can deploy their infrastructures in a scalable, agile manner and adjusting to their needs, facilitating the administration and updating of the components used, which allows companies to companies can develop their day-to-day activities and processes, which are in favor of positioning and economic growth.

Some essential aspects must be considered, such as the security of stored information, data processing and web applications deployed in IaaS-type cloud infrastructures; Taking into account the above, new security challenges have been generated for the administrators of these platforms, since there is a tendency to believe that those responsible are the Cloud Providers, forgetting the assurance and good practices that must be taken into account when At the moment of migrating to cloud infrastructures, if the correct procedure is not followed, it can lead to security breaches and possibly incidents that affect the provision of services.

Keywords: Cloud Computing, IaaS, incidents, incidents

INTRODUCCIÓN

Las organizaciones deciden migrar sus infraestructuras a la nube pública, con el fin de reducir los costos de operación y administración, buscando que sus aplicaciones y datos siempre se encuentren disponibles y dar continuidad al negocio, sin embargo, es importante tener en cuenta los mecanismos disponibles para garantizar la protección de las infraestructuras implementadas, en el desarrollo del presente documento se realiza una descripción de cada uno de los mecanismos que se encuentran disponibles en AWS.

Otro de los aspectos fundamentales que es necesario tener en cuenta al momento de realizar el despliegue de infraestructuras en la nube, consiste en garantizar la seguridad de los datos que se encuentran en tránsito como en reposo, por que se hace necesario definir las herramientas que serán utilizadas para tal fin; AWS cuenta con varias alternativas que dependiendo de la capacidad monetaria de la organización pueden llegar a implementar, se mencionaran las opciones más relevantes que se encuentran disponibles y enfocadas en asegurar la información, adicionalmente se realiza una prueba de concepto donde se utilizaron los mecanismos de seguridad y de protección de datos tanto en tránsito como en reposo, describiendo las mejores prácticas que deben ser tenidas en cuenta durante el proceso de implementación.

Por último y basados en el framework NIST SP 800-53 V5, se seguirán las recomendaciones para asegurar el ciclo de vida de las entidades y roles de usuarios, siendo este un aspecto fundamental ya que estos son los que tiene visibilidad de los servicios que se encuentran desplegados y son el eslabón más débil en la cadena de seguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años se ha evidenciado un aumento significativo en la adopción de servicios cloud públicos por parte de las organizaciones, (desde pequeñas empresas, hasta multinacionales). Las empresas están realizando la migración de sus infraestructuras clásicas “on-premises” a infraestructuras cloud. Si bien, esto trae consigo muchos beneficios como:

- Time to market
- Pay as-you-go
- Capex to opex
- Business agility
- Escalabilidad y alta disponibilidad de aplicaciones y servicios
- Integración nativa con soluciones de seguridad cloud

Así mismo trae consigo nuevos riesgos de seguridad de acuerdo con enisa estos se encuentran relacionados con:

- Modelo de responsabilidad compartida,
- Pérdida de gobierno,
- Riesgos de conformidad,

Los cuales no están siendo confrontados, dejando a la deriva la seguridad de los despliegues de este tipo de infraestructura.[1]

Las infraestructuras como servicio (IaaS), desplegadas en la nube, no se encuentran exentas de los ciberdelincuentes, los ataques registrados a este tipo de infraestructuras se deben principalmente a problemas relacionados con la administración de la plataforma. [2]

Dentro de los principales riesgos de seguridad se encuentran:

[1] ENISA.EUROPA. [Sitio Web]. Beneficios, riesgos y recomendaciones para la seguridad de la información. [Consulta: 15 de octubre del 2022]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

[2] infosecuritymexico. [Sitio Web]. Nube y Ciberseguridad. [Consulta: 15 de octubre del 2022]. Disponible en: https://www.infosecuritymexico.com/es/blog/nube-y-ciberseguridad.html

- Gestión inadecuada de las entidades incluyendo credenciales débiles y por defecto.
- Acceso de usuarios con privilegios y uso de la cuenta root.
- Plataformas desactualizadas.
- Desarrollo de software sin aplicar buenas prácticas de seguridad.
- No realizar análisis periódicos de vulnerabilidades.
- Indisponibilidad de los servicios por malas configuraciones erróneas

1.2 FORMULACIÓN DEL PROBLEMA

La implementación de equipos y políticas de seguridad en las organizaciones cada vez se convierte en una de las actividades más relevantes a desarrollar, ya que se busca proteger cada uno de los activos indispensables para el buen funcionamiento de las compañías. Para garantizar la seguridad de la información, se requiere de capacitación y concientización de todo el personal, como también mantener actualizadas las guías de buenas prácticas recomendadas por los fabricantes y diferentes framework disponibles en el mercado, con el fin de prevenir incidentes de seguridad.

De acuerdo a lo anterior, con el desarrollo de la presente monografía se busca dar respuesta al siguiente interrogante: ¿Cuáles serían las características de seguridad a tener en cuenta para el despliegue de aplicaciones web en un modelo de implementación IaaS, en la nube de AWS?

2 JUSTIFICACIÓN

Con la finalidad de realizar un despliegue o implementación adecuada de los servicios que se encuentran en infraestructuras en la nube, se debe verificar y tener en cuenta algunas recomendaciones que están enfocadas con la aplicación de buenas prácticas de seguridad como, no utilizar configuraciones por defecto, no utilizar algoritmos de cifrado, no aislar o segmentar los ambientes pre productivos y de producción, entre otros, convirtiéndose en las principales falencias y aspectos a mejorar por las organizaciones que migran sus diferentes servicios.

AWS tiene a disposición de los clientes varios mecanismos enfocados en asegurar los datos e infraestructuras, el cliente es el responsable de configurar y administrar cada uno de estos componentes, por lo general se piensa que el responsable de la seguridad es el proveedor de nube y sumado el desconocimiento de las herramientas que se encuentran disponibles ocasiona que despleguemos infraestructuras poco seguras.

En el desarrollo del presente documento se darán a conocer algunos de los mecanismos de seguridad y protección de datos disponibles en AWS, y la forma en la que deben ser implementados, se indicaran recomendaciones y buenas prácticas de seguridad, enfocadas en garantizar despliegues de infraestructuras seguras, buscando que el activo más importante para cualquier organización este protegido y a través de esta guía se le permita asegurarlo.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer buenas prácticas de seguridad, teniendo como referencia el framework NIST SP 800-53 V5, para asegurar el despliegue de aplicaciones web en un modelo de implementación IaaS, en la nube de AWS.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar los servicios de seguridad nativos de AWS, a través de la caracterización de éstos, con el fin de asegurar la infraestructura y determinar las mejores prácticas de seguridad.

- Examinar los mecanismos para la protección de datos en tránsito, como en reposo para las aplicaciones web desplegadas en un modelo de implementación IaaS, con el fin de validar confidencialidad e integridad de los datos.

- Diseñar una prueba de concepto, donde se apliquen las recomendaciones y buenas prácticas que se deben tener en cuenta al momento de desplegar una aplicación web en un modelo de implementación IaaS, con el fin de validar las estrategias propuestas.

- Elaborar recomendaciones y buenas prácticas de seguridad a partir el framework NIST SP 800-53 V5 para asegurar el despliegue de aplicaciones web en un modelo de implementación IaaS, teniendo como referente la gestión del ciclo de vida de las identidades para usuarios, cuentas de servicio y roles.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

AWS provisiona mecanismos enfocados en garantizar la seguridad de las infraestructuras y servicios que se encuentran desplegadas dentro de la nube, esta postura de seguridad está orientada en proteger información, identidades, aplicaciones y dispositivos.

Mediante la implementación de los servicios de seguridad nativos de AWS se busca:

4.1.1 Seguridad de los datos

Los datos son el activo más importante para cualquier organización por lo cual es indispensable controlar en dónde se almacenan, identificar qué recursos se están consumiendo y quién está accediendo a estos, adicionalmente es necesario generar controles de acceso que permitan identificar al usuario dependiendo del rol y actividad.

Por lo tanto, es importante monitorear el tráfico que es generado hacia la aplicación con el fin de detectar eventos de seguridad que puedan ser inusuales, así como validar quien ejecuta cambios en la configuración de la aplicación y en los parámetros de seguridad.[3]

En la siguiente ilustración se muestra el ciclo de vida de los datos.

Ilustración 1. Ciclo de vida de los datos

Fuente: BLOG SMARTEKH. [Sitio Web]. TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD.

[3] AMAZON WEB SERVICES. [Sitio Web]. Seguridad en la nube de AWS. [Consulta: 15 de octubre del 2022]. Disponible en: https://aws.amazon.com/es/security/

[Consulta: 15 de octubre del 2022]. Disponible en: https://cdn2.hubspot.net/hubfs/2241716/Imported_Blog_Media/lifecycle11.png
El ciclo de vida de los datos facilitará comprender el flujo de la información a través de los diferentes actores, gestionar la información y la forma en la que se gobierna su uso.

4.1.2 Protección de los datos

La localización de la información incluye herramientas y procesos con el fin de identificar qué información está siendo almacenada y se debe garantizar la protección de los datos que se encuentran en tránsito como en reposo, la implementación de certificados TLS y el uso de VPN resuelta primordial con el fin de garantizar la confidencialidad.

La localización de contenidos es una funcionalidad de las herramientas de Data Loss Prevention; está disponible en los productos de monitorización de la actividad de bases de datos (DAM). El escaneo puede hacerse accediendo a las carpetas compartidas o mediante un agente instalado en el sistema operativo. [4]

4.1.3 Cifrado de volúmenes

En los despliegues realizados en los modelos de implementación IaaS pueden ser empleados los siguientes métodos.

- Cifrado por instancias: el cifrado se realiza dentro de la instancia y la llave se almacena dentro del volumen la protección de la llave re realiza mediante una contraseña robusta.
- Cifrado externo: el cifrado se realiza dentro de la instancia, pero las llaves son gestionadas de forma externa y se indican en el momento de realizar una consulta.
- Cifrado Proxy: en este modelo la instancia se conecta al volumen por medio de instancia cifrada que administra las llaves y operaciones criptográficas ya sea de forma remoto o interna.[5]

4.1.4 Modelo de responsabilidad compartida

Uno de los aspectos principales cuando se toma la decisión de migrar a la nube, es entender los roles y responsabilidades de cada actor (cloud provider y cliente). En función del modelo de servicio utilizado.

---

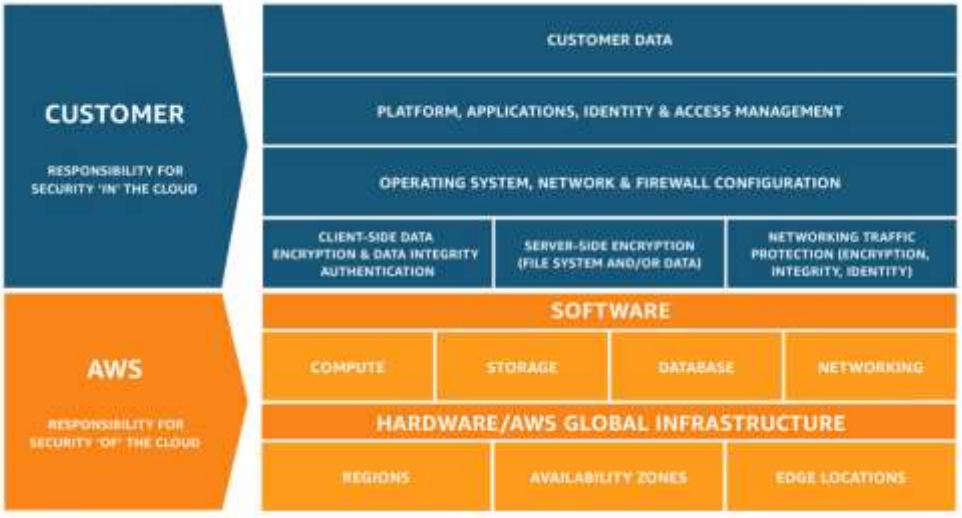
[4] MINTIC. [Sitio Web]. Seguridad y privacidad de la información. [Consulta: 15 de octubre del 2022]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf
[5] Ibit.

AWS, es responsable de garantizar la protección de la infraestructura, donde se ejecutan los servicios aprovisionados. La infraestructura está conformada por el hardware, software, redes e instalaciones que ejecutan los servicios de la nube de AWS[6].

Los clientes son responsables de la configuración de los servicios que han sido contratados, dentro de los que encuentran, sistemas operativos huéspedes que incluyen la instalación de actualizaciones y parches de seguridad; la creación de usuarios, definición de roles, responsabilidades y permisos de acceso para utilizar los recursos desplegados, al igual que agregar capas de cifrado a la información que circula y se encuentra almacenada dentro de la infraestructura.

La siguiente ilustración resume la distribución de responsabilidades entre los cloud providers y el cliente. Esta es la base para poder establecer un modelo de gobierno en la nube.

Ilustración 2. Modelo de seguridad compartida



Fuente: AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en:https://d1.awsstatic.com/security-center/Shared_Responsibility_Model_V2.59d1eccec334b366627e9295b304202faf7b899b.jpg

[6] AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en: https://aws.amazon.com/es/compliance/shared-responsibility-model/

4.2 MARCO CONCEPTUAL

A continuación, se realiza una descripción de los aspectos más relevantes que deben tener en cuenta al momento de contratar servicios cloud, con el fin de garantizar que los recursos son usados eficientemente y permitan asegurar las plataformas que sean desplegadas o implementadas.

4.2.1 Cloud computing

Conjunto de servicios tecnológicos ofrecidos a través de internet, estos se encuentran diseñados para crecer a gran escala reduciendo los costos de infraestructura, espacio y centralización de la información ajustable a las necesidades de los clientes.

Dentro de los servicios ofrecidos se encuentran:

- Computo: Cuenta con gran capacidad de procesamiento y memoria para garantizar que las aplicaciones estén soportadas y disponibles para ser utilizadas en el momento que sea requerido por cualquier tipo de usuario.
- Almacenamiento: Garantiza capacidades ilimitadas para replicar información en múltiples dispositivos y ubicaciones geográficas.
- Networking: Permite virtualizar la capa de red y la protección de la infraestructura con equipos de seguridad perimetral y protección de aplicaciones web, adicionalmente se controla la conexión entre equipos que se encuentran en el mismo segmento de red.

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[7], define cloud computing, como un modelo que busca facilitar los recursos y servicios de la computación, para que estén disponibles de forma instantánea y bajo demanda, garantizando crecimiento a escala y flexibilidad.

Para Peter Mell[8], informático del Instituto Nacional de Estándares y Tecnología de EE. UU (NIST), define cloud computing como un modelo para permitir servicios y accesos bajo demanda, en un conjunto de recursos informáticos compartidos que pueden ser aprovisionados y puestos en producción rápidamente.

[7] EUROPEAN UNION AGENCY FOR CYBERSECURITY. [Sitio Web]. Cloud Computing Risk Assessment – Spanish. [Consulta: 14 de abril del 2022]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish.

[8] Peter Mell. What's Special About Cloud Security? IT Professional (IEEE). Abril 14 2012

4.2.2 Cloud Providers

Los proveedores de servicios en la nube son organizaciones de terceros que se dedica a ofrecer diferentes servicios entre los que se encuentran[9]:

- Plataformas
- Infraestructuras
- Almacenamiento
- Aplicaciones
- Procesamiento

Los servicios que son suministrados en la nube presentan un modelo de pago por servicio, esta liquidación se realiza a partir del uso y la cantidad de recursos que son desplegados para soportar y mantener la infraestructura de los clientes, cualquier servicio que sea contratado es administrado desde internet.

Algunos de los beneficios de contratar servicios en la nube son:

- Facilidad de implementación
- Escalabilidad
- Flexibilidad
- Disponibilidad
- Accesibilidad y movilidad
- Actualizaciones tecnológicas
- Velocidad y productividad

Los cloud providers se caracterizan por ser empresas consolidadas en el mercado y con amplia experiencia, garantizando que los recursos, disponibilidad y seguridad física en los centros de datos, cumplen con estándares internacionales; así, generar confianza al momento de adquirir este tipo de servicios.

Los principales Cloud Providers son**:**

- Amazon Web Services (AWs)
- Microsoft Azure
- Google Cloud
- Alibaba Cloud

[9] MICROSOFT. [Sitio Web]. What is a cloud service provider? [Consulta: 15 de abril del 2022]. Disponible en: https://azure.microsoft.com/en-us/overview/what-is-a-cloud-provider/

- IBM Cloud
- Oracle Cloud
- Sales force
- Rackspace Cloud
- VMWare

4.2.3 Modelos de implementación de informática cloud

Es importante definir el modelo de implementación de acuerdo al tipo de organización; iniciando por el acceso a los servicios que van a ser desplegados y al presupuesto destinado para el proyecto, adicionalmente es indispensable validar las políticas para el tratamiento y protección de los datos que van a ser almacenados. A continuación, se describen los modelos de computación existentes.[10]

- Nube pública: Es un modelo de implementación en la nube, que se encuentra dentro de un catálogo de servicios ofrecido a múltiples clientes, donde la infraestructura es compartida y se accede a través de redes públicas como internet. La infraestructura es administrada por los cloud providers y se garantiza la disponibilidad de los recursos, mediante acuerdos de niveles de servicio; también se incluye la seguridad física y lógica de los centros de datos, en donde los clientes realizan el pago de acuerdo al uso de la infraestructura desplegada.
- Nube privada: Es un modelo de implementación en la nube, donde la infraestructura y servicios, se encuentran alojados de manera privada en centros de datos propios de la organización y los recursos no son compartidos con otros clientes. La organización se encarga del mantenimiento, administración, seguridad física, disponibilidad y gestión que garanticen el funcionamiento de la nube, este modelo de implementación se asemeja a las infraestructuras On premise, y los costos asociados al mantenimiento, administración y operación pueden ser elevados.[11]
- Nube híbrida: Es un conjunto de plataformas compuesta por nube pública y nube privada, con el fin de mejorar los recursos de infraestructura existentes; de esta manera es posible agregar elementos de cómputo, como almacenamiento y procesamiento de datos, de acuerdo con el tipo de demanda que sea generado.

[10] S. Gupta, A. Gupta y G. Shankar, "Cloud Computing: Services, Deployment Models and Security Challenges", 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 414-418, doi: 10.1109/ ICOSEC51865.2021.9591794.

[11] AMAZON WEB SERVICES. [Sitio Web]. Modelos de informática en la nube. [Consulta: 16 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing/

- Multiclouds: Para realizar esta implementación se requiere de dos proveedores de nube pública, siendo posible contar con réplicas de la información e infraestructura; es utilizada para realizar redundancia y planes de recuperación de desastres (DRP), algunas de sus desventajas son los costos elevados de mantener y sostener dos infraestructuras de manera simultánea. [12]

4.2.4 Modelos de servicio cloud

El modelo de servicios en la nube de AWS está compuesto por los siguientes tipos[13], como se puede ver en la siguiente ilustración:

Ilustración 3. Modelos de servicio cloud.

Fuente: AMAZON WEB SERVICES. [Sitio Web]. Modelos de informática en la nube. [Consulta: 16 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing/

- Infraestructura como Servicio (IaaS): Es un modelo de computación bajo demanda, que garantiza flexibilidad y control de los dispositivos desplegados. El cloud provider, ofrece recursos de infraestructura como servicios de virtualización, procesamiento, firewall, sistemas de almacenamiento y balanceadores; los cuales quedan bajo la responsabilidad y administración de los clientes que adquieren este tipo de servicios, en este modelo de servicio el pago es realizado de acuerdo con el uso de los recursos desplegados.

[12] REDHAT. [Sitio Web]. Tipos de cloud computing. [Consulta: 15 de abril del 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud#:~:text=Hay%20cuatro%20tipos%20principales%20de,software%20como%20servicio%20(SaaS).

[13] AMAZON WEB SERVICES. [Sitio Web]. Tipos de informática en la nube. [Consulta: 14 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing

- Plataforma como Servicio (PaaS): En este modelo de servicio el cliente accede a los recursos, a través de internet o por medio de una consola que le permite desarrollar, ejecutar y administrar sus aplicaciones de forma rápida y rentable, sin hacerse cargo del diseño y administración de la infraestructura; de igual forma se debe tener en cuenta que es el responsable de definir el aprovisionamiento y dimensionar la solución, con base a la necesidad del proyecto. Para realizar la liquidación de los pagos por consumo se utilizan herramientas de monitoreo y gestión.
- Software como Servicio (Software as a Service - SaaS): Son servicios diseñados y administrados por el cloud provider, este software está orientado para los consumidores, permitiéndoles ingresar desde una aplicación liviana o desde un navegador, donde únicamente puedan realizar configuraciones básicas. Dentro de los servicios se encuentra el correo electrónico, aplicaciones ofimáticas, aplicaciones productivas entre otras.
- Las ventajas que tiene este modelo de servicio están relacionadas con la flexibilidad para suplir requerimientos de software de manera rápida y oportuna, también se obtiene adaptación a los entornos y aplicaciones que son común mente utilizados, garantizando que la experiencia sea satisfactoria para los usuarios; los cambios y administración son sencillos por lo que no requiere dedicar esfuerzos en la administración de infraestructuras.

4.2.5 Infraestructura cloud AWS

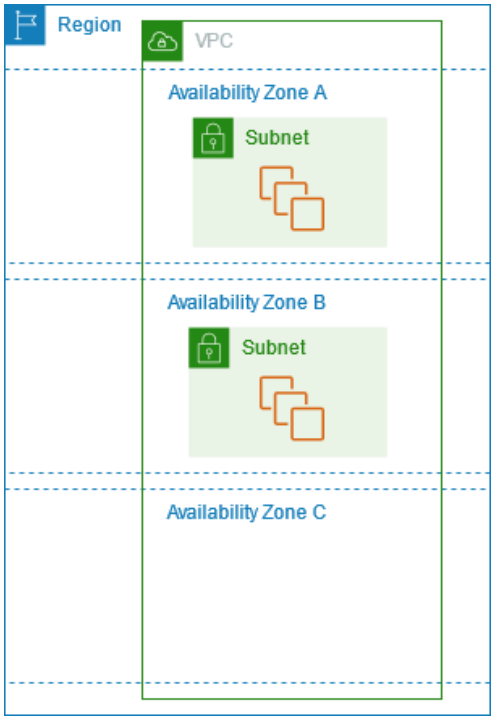
Los recursos desplegados en la nube están alojados en varias ubicaciones físicas por todo el mundo. Estas ubicaciones se componen de regiones, zonas de disponibilidad y zonas locales.

A continuación, una descripción de cada uno de estos conceptos.

- Regiones**:** Son zonas geográficas compuestas de uno o varios Data Centers. Cada región está diseñada para estar totalmente aislada de las demás, evitando así el riesgo ‘Blast Radius’ (propagación de errores a través múltiples componentes). Este diseño permite tener alto nivel de disponibilidad y una mayor tolerancia a errores.
- Zonas de disponibilidad**:** Es el lugar donde los componentes de la arquitectura son implementados (bases de datos, servidores, balanceadores, etc.). Cada zona de disponibilidad está diseñada para ser totalmente independiente.

A continuación, se muestran en la ilustración con la relación de componentes básicos y su interacción:

Ilustración 4. Relación de componentes básicos y cómo interactúan.



Fuente: AMAZON WEB SERVICES. [Sitio Web]. Relación de componentes básicos y cómo interactúan. [Consulta: 15 de marzo del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/images/region-with-azs.png

4.2.6 NIST

Instituto nacional de estándares y tecnología, es una organización creada por los Estado Unidos, con el fin de que todas las organizaciones puedan identificar y reducir los riesgos para proteger las redes y los datos[14].

Este marco está compuesto por cinco funciones, que se encuentran subdivididas en veintitrés categorías. Cada categoría define los controles de seguridad y resultados que se desean obtener luego de ajustar los procesos y procedimientos para la prevención, mitigación y recuperación de los servicios ante un posible incidente de seguridad.

[14] Fuente: NIST. [Sitio Web]. Framework Documents. [Consulta: 10 de marzo del 2022]. Disponible en https://www.nist.gov/cyberframework/framework

A continuación, en la ilustración se describen las cinco funciones:

Ilustración 5. NIST cinco funciones

Fuente: NIST. [Sitio Web]. The Five Functions. [Consulta: 10 de marzo del 2022]. Disponible en: https://www.nist.gov/sites/default/files/styles/220_x_220_limit/public/images/2018/04/12/ipdrr_circle.png?itok=qV5agiH5

Identificar: Se identifican los activos y recursos que son empleados para el desarrollo de funciones críticas y los riesgos asociados en cuanto a la ciberseguridad, para determinar la forma en que puede llegar a impactar.

Dentro de los cuales se encuentran:

- Datos: Analizar los flujos y entradas de datos con el fin de detectar tráfico inusual que pueda generar incidentes de seguridad.
- Gestión de activos: realizar y mantener actualizado el inventario de activos con el fin de identificar que se debe proteger.
- Entorno empresarial: analizar los riesgos a los que se encuentra expuesta la organización dependiendo del core de negocio.
- Evaluación de riesgo: realizar análisis de vulnerabilidades de forma periódica con el fin de mitigar brechas de seguridad.
- Gestión de riesgos de la cadena de suministro: analizar y detectar alternativas para el suministro de servicios que puedan llegar a comprometer la operación y continuidad del negocio.

Proteger: Desarrollar e implementar medidas necesarias que permitan proteger y limitar el impacto, que pueda ser generado por un evento de ciberseguridad.

Dentro de estas medidas se encuentran:

- Procesos y procedimientos de protección de la información: implementar políticas que permitan garantizar la protección de los datos en tránsito como

en reposo, se debe clasificar la información de acuerdo a la criticidad de la misma.

- Control de acceso: garantizar la seguridad física a través de la implementación de biométricos, CCTV en la organización y centro de datos como medida de protección de la información.
- Seguridad de los datos: conocer los flujos y cadenas de entrada de los diferentes sistemas con el fin de detectar comportamientos inusuales.
- Capacitación y concientización: todo el personal de la organización debe conocer los riesgos a los que se encuentra expuesto al ingresar a los diferentes sistemas de información e internet.

Detectar: Se llevan a cabo actividades que permitan identificar eventos de seguridad, a través del monitoreo continuo de las diferentes plataformas e infraestructura.

Dentro de estas medidas se encuentran:

- Anomalías y eventos: monitoreo de tráfico y notificaciones generadas por el correlacionador de eventos que permitan alertar posibles incidentes de seguridad.
- Control continuo de la seguridad: actualización periódica de las guías de buenas prácticas de seguridad y la actualización de las plataformas.
- Procesos de detección: contar con equipos destinados al monitoreo y contención de ataques IDS/IPS y plan de acción ante incidentes de seguridad.

Responder: Se realiza el despliegue de las actividades, que permitan mitigar o disminuir el impacto que pueda llegar a ocasionar un evento de ciberseguridad.

Actividades realizadas:

- Planificación: ejecutar los procesos y procedimientos que permitan dar respuesta oportuna ante un incidente de seguridad.
- Análisis: determinar las posibles causas para asegurar la repuesta adecuada y generar las actividades de recuperación.
- Mitigación: acciones que buscan prevenir, mitigar y erradicar un incidente de seguridad.
- Mejoras: actividades de respuesta que buscan corregir y aplicar las lecciones aprendidas

Recuperar: Se realizan actividades para dar continuidad a la operación después de un incidente de seguridad

Actividades realizadas:

- Planificación: ejecutar procesos y procedimientos que permitan restablecer y recuperar la operación de forma oportuna.
- Mejoras: realiza procesos de recuperación donde se incluyan actividades como actualizar periódicamente la guía de buenas practicar y realizar análisis de vulnerabilidades a las plataformas.
- Comunicaciones: coordinar los procesos de restauración de las plataformas con todo el personal involucrado ya sea interno o externo.

4.2.7 NIST SP 800-53 V5

Controles de seguridad y privacidad para Sistemas de Información y Organizaciones, los controles de seguridad son medidas utilizadas dentro de un sistema o una organización con la finalidad de proteger la confidencialidad, integridad y disponibilidad del sistema y su información, buscando gestionar y disminuir el riesgo de seguridad de la información y sus sistemas, estos controles pueden llegar a ser implementados dentro de cualquier organización y sistema que almacene, transmita y procese información.

Los controles de seguridad y privacidad descritos en la SP 800-53 V5 tienen una organización y estructura definida, donde se especifican cada selección para facilitar el uso del procedimiento descrito, los controles están descritos y agrupados en 20 familias.[15]

En la siguiente ilustración se describen los controles propuestos por NIST SP 800-53 V5.

[15] NIST Special Publication 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations", 2020 National Institute of Standards and Technology, pp. 1

Ilustración 6. Controles de seguridad y privacidad

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Fuente: NIST Special Publication 800-53 Revisión 5, "Security and Privacy Controls for Information Systems and Organizations", 2020 National Institute of Standards and Technology, pp. 8.

4.3 MARCO LEGAL

En Colombia se han promovido diferentes leyes que buscan la protección de los datos, estas buscan garantizar que los procedimientos y manejo para la trasmisión y almacenamiento de la información aseguren su protección.

4.3.1 Ley 1622 de 2008

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”[16], esta ley tiene como objetivo que todas las personas conozcan, actualicen y ratifiquen la información que ha sido suministrada a las entidades bancarias y demás entes, que de una forma u otra hayan captado y contengan información personal.

4.3.2 Ley 1273 de 2009

Es denominada “de la protección de la información y de los datos”[17], también es conocida como la ley de delitos informáticos en Colombia, por medio de esta, se tipificaron los delitos informáticos, para garantizar la protección y conservar de forma íntegra los sistemas que empleen tecnologías de la información y de las telecomunicaciones.

[16] SECRETARIA SENADO. [Sitio Web]. LEY ESTATUTARIA 1266 DE 2008. [Consulta: 16 de abril del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
[17] SECRETARIA SENADO. [Sitio Web]. LEY 1273 DE 2009. [Consulta: 16 de abril del 2022]. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

4.3.3 Ley 1581 de 2012

“Por la cual se dictan disposiciones generales para la protección de datos personales.[18]”. Las personas tienen derecho a conocer, actualizar y verificar los datos suministrados, los cuales se encuentren en bases de datos; también regula que los cuidadnos puedan conocer el uso y disposición que se realizan a sus datos.

[18] SECRETARIA SENADO. [Sitio Web]. LEY ESTATUTARIA 1581 DE 2012. [Consulta: 16 de abril del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

5 DESCRIPCIÓN DE LOS MECANISMOS DE SEGURIDAD UTILIZADOS EN INFRAESTRUCTURAS DESPLEGADAS EN AWS.

Existen múltiples herramientas disponibles en el mercado que son adquiridas por las organizaciones con el fin de proteger las infraestructuras desplegadas en la nube, esta diversidad de plataformas y el gran número de paneles que son necesarios monitorear para detectar eventos anómalos, genera un desgaste operativo y no garantiza la seguridad de la infraestructura, uno de los principales factores que ocasionan infraestructuras vulnerables, esta relaciona directamente con la aplicación de configuraciones por defecto o simplemente malas prácticas debido a la falta de conocimiento, el atender asuntos del día a día en cuanto a la administración de la plataforma conlleva a la perdida de relevancia de algunos eventos de seguridad que son notificados.

Es necesario identificar las brechas seguridad, mediante la verificación periódicamente las configuraciones realizadas (hardening), definición del plan de detección y remediación de vulnerabilidades, así como la automatización y notificación de alarmas.

En la siguiente sección se describen los servicios de seguridad nativos que se encuentran disponibles en AWS, es necesario que los administradores de las plataformas los activen y realice los ajustes correspondientes en cuanto a la configuración con el fin de proteger cada uno de los activos que son implementados.

5.1 CARACTERIZACIÓN DE LOS SERVICIOS DE SEGURIDAD NATIVOS DE AWS

A continuación, se realiza la descripción de los servicios de seguridad ofrecidos por AWS, para que sus clientes aseguren sus plataformas de manera óptima.

Para facilitar la lectura y el estudio de los servicios de seguridad en AWS, serán organizadas por categorías.

En el siguiente cuadro se muestran los servicios de seguridad propuestos por el cloud providers y los casos de uso típicos para estos servicios.

Cuadro 1. Servicios de seguridad AWS.

Categoría	Casos de uso	Servicio AWS
Gestión de identidad y acceso	Gestión del ciclo de vida de identidades (usuarios, roles, cuentas de servicio).	AWS IAM
	Cloud Single-sign-on SSO.	AWS Single Sign-On
	Cloud Active Directory.	AWS Directory Service
	Gestión y control de múltiples cuentas en la nube.	AWS Organizations
Detección	Centralización de alertas de seguridad cloud.	AWS Security Hub
	Protección de 'cuentas' cloud utilizando técnicas de threat intelligence.	AWS GuardDuty
	Solución de tipo Vulnerability management para activos cloud.	AWS Inspector
	Registro y seguimiento de los cambios realizados sobre un activo cloud (gestión de versiones sobre la configuración).	AWS Config
	Registro y seguimiento de solicitudes API.	AWS CloudTrail
Protección de la infraestructura	Gestión central de reglas de firewall sobre múltiples soluciones cloud.	AWS Network Firewall
	Protección contra ataques de tipo DDoS.	AWS Shield
	Protección contra ataques web (capa 7).	AWS WAF (Web Application Firewall)
Protección de los datos	Gestión del ciclo de vida de las llaves de cifrado en la nube.	AWS Key Management Service (KMS)
	Gestión del ciclo de vida de certificados (públicos y privados) en la nube.	AWS Certificate Manager
	Gestión y protección de secretos (passwords, string de conexión, Access keys, etc.) en la nube.	AWS Secrets Manager

Fuente: AMAZON WEB SERVICES. [Sitio Web]. Servicios de seguridad, identidad y conformidad de AWS. [Consulta: 10 de marzo del 2022]. Disponible en: https://aws.amazon.com/products/security/?nc1=h_ls

5.1.1 AWS IAM (Identity and Access Management)

Este es un servicio que permite controlar el acceso de forma segura a los recursos que se encuentran en AWS, dentro de las funciones de este servicio está controlar a quien se está autenticando, es decir iniciando sesión y validar los usuarios autorizados, que son aquellos que cuenta con los permisos para utilizar los recursos; mediante esta forma se mantiene el control del contenido que se

encuentra en la infraestructura.[19]

De acuerdo con las recomendaciones de AWS, para proteger los recursos se debe tener en cuenta IAM (Identity and Access Management), para los siguientes servicios.

- Proteger las claves de acceso del usuario raíz de la Cuenta de AWS: La cuenta de acceso raíz, concede todos los permisos a los recursos y servicios que se encuentren en AWS, por lo cual no se recomienda utilizarla en tareas cotidianas de administración básica, se debe crear un rol definido para la administración de los recursos.
- Utilizar roles para delegar permisos: Es indispensable crear roles de acuerdo con el tipo de trabajo o función específica que va a realiza el usuario, de esta manera es posible asignar este rol a un usuario determinado desde la consola de administración de AWS.
- Conceder privilegios mínimos: Dentro de la definición de las tareas y funciones a realizar, se deben emplear políticas destinadas únicamente a permitir ejecutar las tareas definidas de acuerdo con el rol.
- Introducción sobre el uso de permisos con políticas administradas de AWS: Se recomienda empelar políticas con menor privilegio y en lo posible realizar configuraciones de políticas personalizadas, siendo la forma más segura de otorgar permisos, pero es requerido contar con la definición de roles adecuada.
- Validar sus políticas: Es recomendable verificar las políticas que se encuentren configuradas, al igual que validar la sintaxis con el fin de garantizar su funcionalidad.
- Utilizar políticas administradas por el cliente en lugar de las políticas en línea: Se pueden crear dos tipos de políticas, políticas personalizadas y políticas insertadas.
- Utilizar niveles de acceso para revisar permisos de IAM: Es necesario realizar verificaciones periódicas de los roles y funciones definidos para los usuarios, garantizando la aplicación de políticas que permitan el menor privilegio posible.
- Configurar una política de contraseña segura para los usuarios: Permite que las contraseñas que sean creadas por los usuarios contengan ciertos parámetros de seguridad, como cantidad de caracteres, combinaciones

[19] AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es IAM? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html

alfanuméricas y la inclusión de caracteres especiales.

- Habilitar MFA: Es recomendable habilitar para todos los usuarios el múltiple factor de autenticación, ya que de esta manera se protege el inicio de sesión de los usuarios y se agrega otra capa de protección para acceder a los recursos habilitados.
- No compartir las claves de acceso: Se debe asegurar que al momento de compartir las credenciales entre usuarios estas estén cifradas, al igual que se debe verificar que no se hayan dejado las contraseñas en ninguna parte del código.
- Cambiar las credenciales de forma periódica: Es muy importante realizar el cambio de contraseña de forma periódica, el tiempo para realizar este cambio es definido por cada organización, esta debe ser una política obligatoria para todos los usuarios que se encuentren configurados.
- Eliminar credenciales innecesarias: Las contraseñas que no sean necesarias deben ser eliminadas, esto es posible de realizar mediante el monitoreo que se ejecuta en la cuenta de AWS.
- Utilizar condiciones de política para mayor seguridad: Es empelado para definir permisos de acceso de acuerdo con el tipo de recurso, dentro de las condiciones que pueden ser empleadas, está el filtro por dirección IP, y el tiempo en el que puede llegar a ser usada la política, mediante la creación de eventos de tipo calendario.
- Monitoreo de la actividad de su cuenta de AWS: Permite verificar los recursos que han sido utilizadas y que acciones se han realizado desde la cuenta de un usuario.

5.1.2 AWS Security Hub

Permite visualizar el estado de seguridad de las configuraciones que se encuentra en AWS y realiza una comparación con estándares y mejores prácticas de seguridad disponibles en la industria, para esto utiliza la recopilación de datos que se encuentran en las cuentas, servicios y productos para así analizar las tendencias de seguridad, con el fin de identificar problemas[20].

AWS es responsable de garantizar la protección de la infraestructura que se encuentra ejecutando servicios y a su vez proporciona funcionalidades que pueden ser empeladas para asegurar las plataformas, por otra parte, los clientes de AWS deben ser los responsables de implementar factores y políticas que garanticen la protección y confidencialidad de los datos.

[20] AMAZON WEB SERVICES. [Sitio Web]. What is AWS Security Hub? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

Estas son algunas de las recomendaciones a tener en cuenta:

- Protección de datos en AWS Security Hub: La protección de los datos es indispensable para el desarrollo de cualquier labor, por lo cual se recomienda poner en práctica las siguientes funciones:
  - Utilizar doble factor de autenticación.
  - Utilizar SSL/TLS, para comunicarse; dentro de las versiones recomendadas se encuentra TLS 1.2 o posterior.
  - Validar el registro de actividad de los usuarios.
  - Utilizar las funciones de cifrado disponibles en AWS.
- WS IAM, para AWS Security Hub: Se debe tener en cuenta la definición de roles de acuerdo a la función, para la creación de políticas con menor privilegio.
- Políticas administradas por AWS para AWS Security Hub: Para realizar la configuración de las políticas de acuerdo al tipo de usuario, grupo o rol, se debe garantizar la ejecución de los controles definidos, empleando políticas administradas.
- Validación de conformidad para AWS Security Hub: Se realizan auditorías externas por parte de AWS, con el fin de garantizar los controles sobre la seguridad de las infraestructuras.
- Seguridad de la infraestructura en AWS Security Hub: Es empleado para asegurar los procedimientos sobre la red de AWS.

5.1.3 AWS GuardDuty

Este servicio realiza monitoreo continuo a la seguridad, analizando y procesando el origen de los datos, dentro de los que se encuentran:[21]

- Logs de flujo de VPC.
- AWS CloudTrail registros de eventos de administración.
- CloudTrail registros de eventos de datos de S3.
- Registros de auditoría de EKS.
- Registros DNS.

Para realiza el análisis de los datos se utilizan listados de direcciones IP, catalogadas como “Black List”, y la información correspondiente a dominios

[21] AMAZON WEB SERVICES. [Sitio Web]. Qué es Amazon GuardDuty. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/guardduty/latest/ug/what-is-guardduty.html

maliciosos, adicionalmente se identifican actividades con parámetros fuera de lo común que no se encuentra permitidas a través del aprendizaje automático.

Estas son algunas de las recomendaciones a tener en cuenta:

- Protección de datos en AmazonGuardDuty:
  - Utilizar doble factor de autenticación.
  - Utilizar SSL/TLS, para comunicarse; dentro de las versiones recomendadas se encuentra TLS 1.2 o posterior.
  - Validar el registro de actividad de los usuarios.
  - Utilizar las funciones de cifrado disponibles en AWS.
- AWS políticas administradas por para AmazonGuardDuty: Se debe agregar la funcionalidad al rol que incluye el listado de usuarios que tiene acceso para desplegar la función.
- Validación de la conformidad para Amazon GuardDuty: Se realizan pruebas periódicas, con el fin de validar la efectividad y así identificar las direcciones IP, y dominios catalogaos como maliciosos.
- Resiliencia en Amazon GuardDuty: La infraestructura de AWS está conformada por regiones y zonas, dentro de las zonas es posible que se realicen zonas de disponibilidad, con el fin de empelar la conmutación automática en caso de error causado por las interrupciones en el servicio.
- Seguridad de la infraestructura de Amazon GuardDuty: Para utilizar este tipo de servicio los clientes deben ser compatibles con TLS, versiones superiores a la 1.2, también deben incluir una capa de cifrado tales como Ephemeral Diffie-Hellman (DHE).

5.1.4 AWS Inspector

Este servicio permite realizar la administración de vulnerabilidades, ejecutando escaneo de forma continua y analizando instancias de AWS EC2 y contenedores (AWS Elastic Container Registry), con el fin de detectar vulnerabilidades en el software y componentes de red, para prevenir incidentes de seguridad[22].

Dentro de las principales características que se encuentran en este servicio, está la de realizar escaneo a todos los dispositivos, ajustando la automatización para definir la recurrencia con la cual se debe realizar este tipo de análisis; estas medidas permiten que el administrador realice la instalación de parches de seguridad o

[22] AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es Amazon Inspector? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/inspector/latest/user/what-is-inspector.html

corregir las vulnerabilidades identificadas.

Estas son algunas de las recomendaciones a tener en cuenta:

- Protección de datos en Amazon Inspector
  - Utilizar doble factor de autenticación.
  - Utilizar SSL/TLS, para comunicarse; dentro de las versiones recomendadas se encuentra TLS 1.2 o posterior.
  - Validar el registro de actividad de los usuarios.
  - Utilizar las funciones de cifrado disponibles en AWS.
- Resiliencia en Amazon Inspector: Permite realizar la conmutación a otra zona de disponibilidad ante cualquier incidente de seguridad.
- Seguridad de la infraestructura en Amazon Inspector: Para utilizar este tipo de servicio es necesario que los clientes tengan habilitado:
  - Utilizar SSL/TLS, para comunicarse; dentro de las versiones recomendadas se encuentra TLS 1.2 o posterior.
  - Utilizar doble factor de autenticación.
  - Incluir una capa de cifrado tales como Ephemeral Diffie-Hellman (DHE).

Respuesta frente a incidencias en Amazon Inspector, es importante que el cliente conozca la respuesta ante incidentes de seguridad de AWS, de igual manera definir políticas y planes de acción para la recuperación y remediación del incidente.

5.1.5 AWS Network Firewall

Este servicio permite realizar filtrado de tráfico a través de las políticas de seguridad configuradas, adicionalmente permite crear VPN, configurar publicaciones y utilizar sistemas de IPS para la detección y prevención de eventos de seguridad[23].

El Network Firewall es utilizado para monitorear el tráfico entrante y saliente de la red, también puede realizar las siguientes protecciones:

- Permitir el tráfico solo desde dominios y direcciones IP de confianza.
- Utilizar listas personalizadas de direcciones IP y dominios para limitar el acceso a las aplicaciones desplegadas.
- Realiza una inspección profunda de los paquetes que circulas a través de la red.
- Utiliza los IPS con el fin de detectar y bloquear posibles ataques.

[23] AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es el cortafuego de red de AWS? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/network-firewall/latest/developerguide/what-is-aws-network-firewall.html

5.1.6 AWS Shield

Este servicio es utilizado para proteger la infraestructura y publicaciones frente ataques de DDoS, este servicio se incluye de forma automática[24], los ataques de denegación de servicios distribuidos, tiene como fin congestionar la red y generar un número elevado de peticiones para que el servidor quede sin recursos y no pueda atender las demás solicitudes legitimas que le llegan. AWS Shield, detecta e identifica los patrones del ataque y aplica mitigación de forma instantánea con el fin de evitar la caída de los servicios.

5.1.7 AWS WAF (Web Application Firewall)

Este firewall protege y permite realizar monitoreo de las aplicaciones web, sobre el tráfico y solicitudes generadas por el puerto HTTPS, adicionalmente realiza las siguientes protecciones[25].

- Scripts que probablemente sean maliciosos.
- Direcciones IP o rangos de direcciones de las que procedan las solicitudes.
- País o ubicación geográfica de donde provienen las solicitudes.
- Longitud de la parte especificada de la solicitud, como la cadena de consulta.
- Ataques de SQL INJECTION.

5.2 RIESGOS DE SEGURIDAD EN LA NUBE

La utilización de servicios en la nube implica ciertos riesgos que deben ser claramente identificados y tratados, con el objetivo de reducir el impacto en la operación de las organizaciones.

En el siguiente cuadro se describen las amenazas y vulnerabilidades a las que se encuentra expuesta la información en la nube.

Cuadro 2. Principales riesgos asociados a la nube

Amenaza	Vulnerabilidad
Fuga de la información	• Error humano. • Ataques informáticos. • Vulnerabilidades en servidores.

[24] AMAZON WEB SERVICES. [Sitio Web]. AWS Shield. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/shield-chapter.html
[25] AMAZON WEB SERVICES. [Sitio Web]. AWS WAF. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/waf-chapter.html

	• Falta de controles de seguridad.
Pérdida de datos	• Catástrofes naturales. • Error humano. • Falla en los equipos de cómputo. • Fallas de electricidad.
Amenazas internas	• Empleados insatisfechos. • Administrador (rougue admin). • Partner.
DDoS	• Arquitectura de red no resiliente. • Protocolos de redes no seguros. • Aplicaciones vulnerables.
APIs vulnerables	• APIs expuestas en internet sin controles de seguridad. • Ataques tipo ‘man-in-the-middle’. • Gestión de llaves API.
Infraestructuras compartidas	• Vulnerabilidades en el hypervisor. • Vulnerabilidades en las instancias (servidores).
Políticas y control	• Falta de políticas de seguridad. • Falta de SLA.

Fuente: Elaboración Elkin Rivera

A partir de lo anterior es importante resaltar que el personal encargado de administrar las plataformas que son desplegadas en la nube de AWS, debe conocer el tipo de suscripción que fue adquirido por la organización, los servicios y funcionalidades que se encuentran disponibles en los servicios nativos, con el fin de asegurar, activar, gestionar y ajustar los servicios basados en las necesidades de la organización, debe tener la premisa que por defecto algunos de estos servicios se encuentran preconfigurados.

Adicionalmente es necesario validar periódicamente las recomendaciones de los diferentes fabricantes y portales de seguridad con el fin aplicar hardening a las infraestructuras desplegadas, se debe buscar que todos los componentes estén configurados de forma apropiada de tal manera que permita disminuir las brechas de seguridad que puedan estar presentes dentro de una infraestructura.

6 ROTECCIÓN DE LOS DATOS EN TRÁNSITO Y REPOSO

La implementación masiva de la nube por parte de las grandes empresas se ha visto en dificultades debido a la noción de gobierno y soberanía de los datos. A partir del momento, en el cual los datos son almacenados en la nube, hay pérdida intrínseca de gobierno sobre estos datos. Por ende, es imprescindible implementar controles de seguridad suplementarios, con el objetivo de garantizar que los datos no sean accesibles por personas no autorizadas y garantizar así el principio de confidencialidad de los datos.

Esta pérdida de gobierno y el “cloud act” (ley de aclaración del uso legal de datos en el extranjero cloud), genera nuevos riesgos de seguridad, los cuales no eran tenidos en cuenta en una arquitectura clásica ‘on-premises’.

Ley de aclaración del uso legal de datos en el extranjero (CLOUD): El 23 de marzo de 2018, el Congreso de los Estados Unidos sancionó la ley Clarifying Lawful Overseas Use of Data (CLOUD, Aclaración del uso legal de datos en el extranjero), con la que se actualizó el marco legal para las solicitudes de aplicación de la ley de los Estados Unidos sobre los datos almacenados por los servidores de telecomunicaciones. También se proporcionan mecanismos de seguridad adicionales para el contenido en la nube, como el reconocimiento del derecho de los proveedores a objetar las solicitudes que entren en conflicto con las leyes o los intereses nacionales de otro país[26].

La siguiente sección describe las técnicas disponibles y que deberían ser empleadas, con el objetivo de proteger los datos en tránsito y en reposo.

6.1 PROTECCIÓN DE DATOS EN TRÁNSITO

Los datos en tránsito son cualquier tipo de información que es enviada a través de una red informática, para la protección de estos datos, se deben utilizar algoritmos de cifrado, es recomendable TLSV1.2, el cual debe aplicarse para todas las conexiones establecidas en la nube.

TLS (Seguridad de la capa de transporte). Permite que la comunicación se realice de manera íntegra y confidencial, agregado capas de cifrado a la información que es trasmitida y asegurando que los dispositivos se autentiquen entre sí.

[26] AMAZON WEB SERVICES. [Sitio Web]. Ley de aclaración del uso legal de datos en el extranjero (CLOUD). [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/compliance/cloud-act/

Algunos de los mecanismos ofrecidos por AWS para implementar este cifrado son:

6.1.1 Certificados

Estos son utilizados con el fin de proteger la comunicación por red, que son datos que se encuentran en tránsito[27], el almacenamiento de las llaves de cifrado y los certificados, deben realizarse de manera segura; las llaves de cifrado deben rotar frecuentemente y aplicar políticas de control de acceso, con el objetivo de protegerlas.

Dentro de los servicios que pueden ser utilizados en AWS, para la creación de certificados se encuentran:

- AWS ACM (Amazon Certificate Manager).
- PKI (Public Key Infrastructure).

Estos servicios son gestionados por AWS, y se integran de manera simple con la mayoría de las arquitecturas en la nube.

6.1.2 Políticas de control para hacer cumplir la utilización de TLS

Por defecto AWS utiliza TLS V1.2, para asegurar el tráfico en la mayoría de los servicios gestionados[28], sin embargo, para las máquinas virtuales (VMs), contenedores y demás componentes de la arquitectura, donde el cliente es el responsable, esta opción no es aplicada, por ende, cada cliente es responsable de aplicar y cumplir con la utilización de dicho protocolo, cumpliendo así con las políticas y requerimientos legales de cada organización.

Protocolos TLS soportados en AWS: TLSv1.3, TLSv1.2, TLSv1.1, TLSv1.

6.1.3 Autenticación del tráfico de red

El uso de protocolos de red que soportan autenticación debe ser privilegiados para proteger la comunicación en la nube. El uso de VPN’s es recomendado.

---

[27] AMAZON WEB SERVICES. [Sitio Web]. AWS Certificate Manager. [Consulta: 10 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/certificate-manager/#:~:text=Los%20certificados%20de%20SSL%2FTLS,los%20certificados%20de%20SSL%2FTLS.

[28] AMAZON WEB SERVICES. [Sitio Web]. Seguridad en la nube de AWS. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/security/

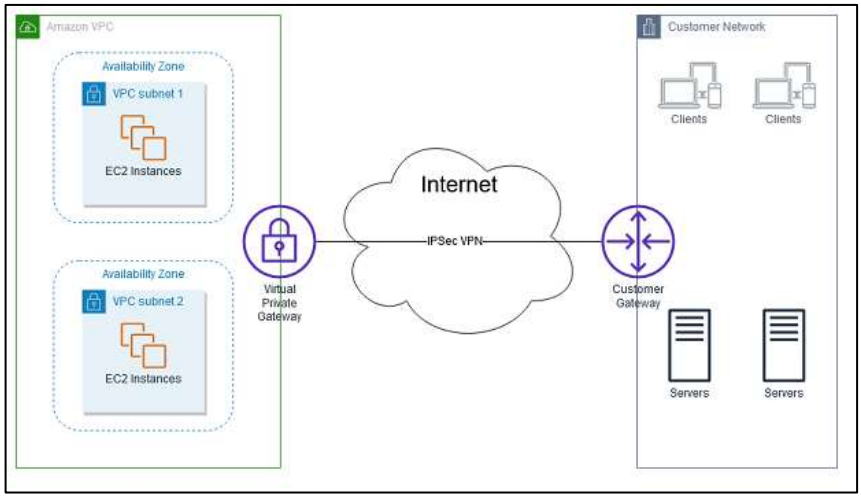
6.1.4 Utilizar enlaces privados

La mayoría de las grandes empresas conectan el Data Center local con la nube, ya que, de alguna manera u otra, algunas aplicaciones on-premises necesitan establecer comunicación con la nube, para ello existen dos opciones básicas, utilizar VPN's o enlaces privados (Direct Connect).

- Las VPN's: Establecen conexiones seguras entre las redes de los clientes y la infraestructura de AWS[29], están han generado seguridad para proteger las comunicaciones sobre enlaces no seguros (como Internet), Las VPN's, traen consigo problemas de gestión y de latencia, en el caso de contar con aplicaciones que deben tener opciones de respuesta óptimos, las VPN's quizás no son la mejor opción, es ahí donde entra en juego los enlaces privados en AWS.

A continuación, la ilustración describe el proceso requerido para la implementación de enlaces privados, utilizados para consumir servicios que se encuentran en la nube de AWS.

Ilustración 7. Esquema de conexión utilizando VPN's



Fuente: AMAZON WEB SERVICES. [Sitio Web]. AWS Managed VPN. [Consulta: 15 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-vpc-connectivity-options/images/image2.png

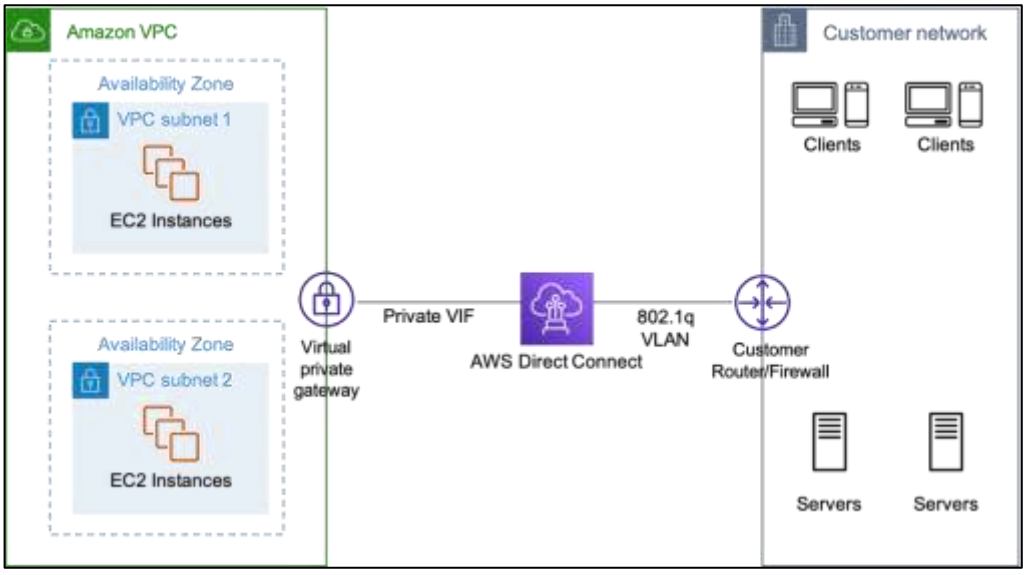
[29] AMAZON WEB SERVICES. [Sitio Web]. AWS VPN. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/vpn/

6.1.5 Enlaces privados (Direct Connect)

Es la ruta más corta hacia los recursos de AWS, es el servicio que permite establecer enlaces dedicados/privados, entre el Data Center de un cliente y la nube[30], este enlace provee un nivel de protección adicional y un desempeño de red muy superior comparado a una VPN (la desventaja es un servicio que puede ser costoso).

A continuación, la ilustración describe el proceso requerido para la implementación de Direct Connect, en la nube de AWS.

Ilustración 8. Esquema de conexión utilizando enlaces privados



Fuente: AMAZON WEB SERVICES. [Sitio Web]. AWS Direct Connect. [Consulta: 15 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-vpc-connectivity-options/images/image6.png

6.2 PROTECCIÓN DE DATOS EN REPOSO

La protección de los datos en reposo es primordial y es una de las actividades a tener en cuenta antes de comenzar una migración hacia servicios de tipo cloud público. Para poder aplicar esta protección tenemos que basarnos en diferentes técnicas u algoritmos de cifrado. A continuación, se lista las opciones disponibles en AWS para implementar esta protección:

[30] AMAZON WEB SERVICES. [Sitio Web]. AWS Direct Connect. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/directconnect/

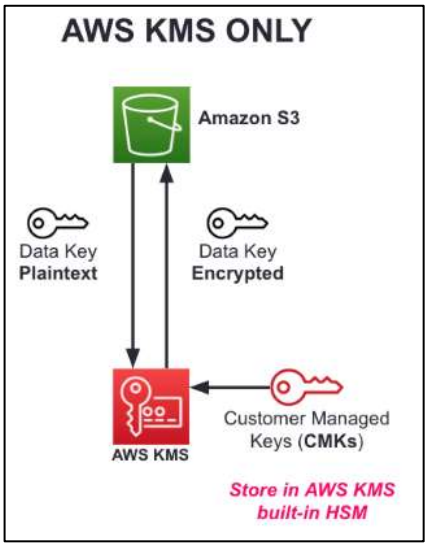
6.2.1 AWS KMS

Es un servicio gestionado por AWS, que permite administrar el ciclo de vida de las llaves de cifrado asimétrico[31], utilizadas en la nube. Las llaves son almacenadas en módulos de seguridad HSM (Hardware Security Module), estos módulos están certificados (FIPS 140-2), para temas de reglamentación y conformidad.

Este servicio permite la integración nativa con muchos de los otros componentes de una infraestructura cloud, su principal inconveniente es que es un servicio mutualizado, es decir, es compartido con otros clientes (Políticas de control y segregación de roles para limitar los accesos), y para algunas organizaciones con requerimiento de seguridad especiales (Bancos, aseguradoras, empresas del estado), esta no es una buena práctica.

La siguiente imagen ilustra el proceso de creación de llaves criptográficas con el servicio AWS KMS.

Ilustración 9. Servicio AWS KMS



Fuente: AMAZON WEB SERVICES. [Sitio Web]. AWS. [Consulta: 14 de mayo 2022]. Disponible en: https://d2908q01vomqb2.cloudfront.net/22d200f8670dbdb3e253a90eee5098477c95c23d/2021/03/09/Demystifying-KMS-keys-2021-2.png

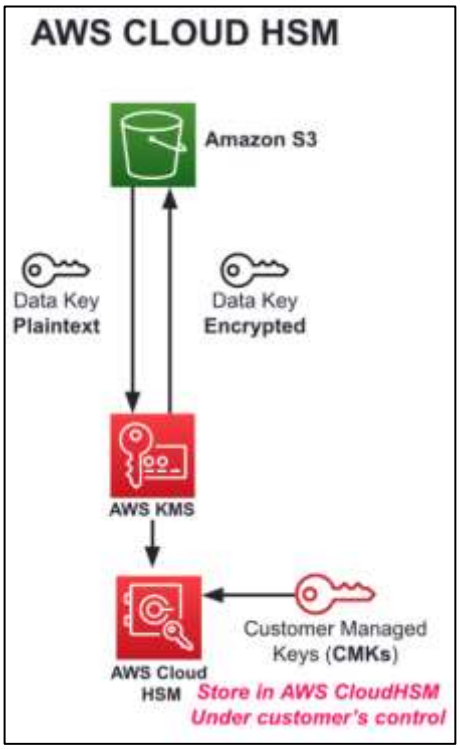
[31] AMAZON WEB SERVICES. [Sitio Web]. AWS Key Management Service (AWS KMS). [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/kms/

6.2.2 AWS Cloud HSM

Permite generar y usar con facilidad las claves de cifrado en la nube de AWS[32], si las normativas aplicadas a una organización exigen manejo y gestión de llaves de cifrado en módulos dedicados, AWS tiene a disposición el servicio Cloud HSM, cuyo funcionamiento, integración y modo de despliegue es el mismo que por AWS KMS, la única y principal diferencia, es que los módulos son dedicados a un único cliente, el inconveniente es el costo de la implementación.

La siguiente ilustración muestra el proceso de creación de llaves criptográficas con el servicio AWS Cloud HSM.

Ilustración 10. Servicio AWS Cloud HSM



Fuente: AMAZON WEB SERVICES. [Sitio Web]. AWS. [Consulta: 14 de mayo 2022]. Disponible en: https://d2908q01vomqb2.cloudfront.net/22d200f8670dbdb3e253a90eee5098477c95c23d/2021/03/09/Demystifying-KMS-keys-2021-2.png

[32] AMAZON WEB SERVICES. [Sitio Web]. AWS CloudHSM. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/cloudhsm/

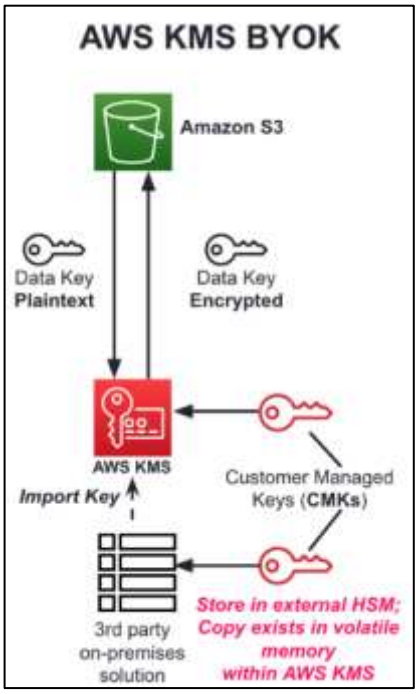
6.2.3 AWS KMS BYOK

Las claves generadas en otras aplicaciones pueden ser usadas con aplicaciones personalizadas y servicios de AWS integrados en KMS[33]. Otro caso de uso, que podríamos encontrar en la nube, es utilizar un servicio externo de cloud provider, de hecho, esta es una buena práctica de seguridad, almacenar los datos y las llaves de cifrado en diferente proveedor.
Para responder a este caso de uso, AWS permite la integración con soluciones externas y estándares del mercado.

Este último escenario es el más costoso y el más complejo en términos de implementación, en algunos casos, puede llegar a ser la opción más “segura” o la opción que mejor responde a las necesidades de un cliente.

A continuación, la ilustración del proceso de creación de las llaves de cifrado y la integración con AWS.

Ilustración 11. Servicio AWS KMS BYOK



Fuente: AMAZON WEB SERVICES. [Sitio Web]. AWS. [Consulta: 14 de mayo 2022]. Disponible en:

[33] AMAZON WEB SERVICES. [Sitio Web]. Cómo BYOK. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/blogs/security/how-to-byok-bring-your-own-key-to-aws-kms-for-less-than-15-00-a-year-using-aws-cloudhsm/

https://d2908q01vomqb2.cloudfront.net/22d200f8670dbdb3e253a90eee5098477c95c23d/2021/03/09/Demystifying-KMS-keys-2021-2.png

En el desarrollo del capítulo dos y los componentes que tenemos a disposición para proteger la información es importe aplicar capas de cifrado, de esta, manera se busca aumentar la seguridad y confidencialidad de los datos, adicionalmente se requiere validar la latencia y tiempos de respuesta de la aplicación ya que el utilizar algoritmos de cifrado robustos ocasiona que el proceso de desempaquetar el paquete genere lentitud en el proceso de comunicación cliente servidor.

En cuento a la protección de los sitios web, tenemos como recurso, implementar llaves de cifrado, que garantizar el acceso, se debe tener en cuenta que existen dos tipos de cifrado

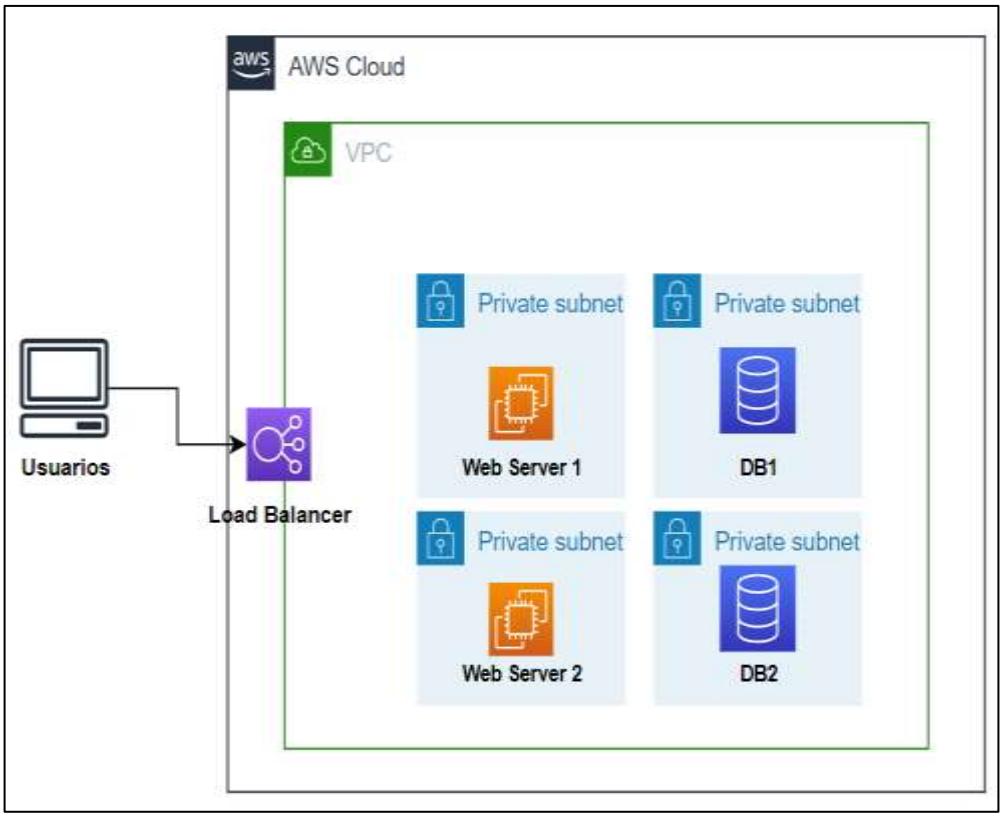
- Cifrado simétrico: que usa una misma llave para cifrar y para descifrar.
- Cifrado asimétrico: utiliza dos llaves para cifrar un mensaje, una llave pública y otra privada.

7 RECOMENDACIONES Y BUENAS PRÁCTICAS PARA DESPLEGAR UNA APLICACIÓN WEB EN UN MODELO DE IMPLEMENTACIÓN IAAS.

En el desarrollo de la prueba de concepto serán utilizadas e implementadas buenas prácticas de seguridad, teniendo como premisa que esta actividad se realiza desde cero, que es el momento inicial, cuando una organización migra sus servicios y realiza el despliegue de un servicio tipo IaaS.

En la siguiente ilustración la topología de red que va a ser empleada en la prueba de concepto:

Ilustración 12. Topología prueba de concepto



Fuente: Elaboración Elkin Rivera

Se presentan dos servidores de aplicación y de base de datos en zonas de disponibilidad diferentes, con el fin de garantizar alta disponibilidad y redundancia de la aplicación, estas están siendo balanceadas con el fin de distribuir el tráfico y no generar saturación y consumos elevados de hardware de los equipos.

7.1 GESTIÓN DE IDENTIDADES Y POLÍTICA DE ACCESO

Una de las primeras actividades que deben ser tenidas en cuenta en el momento de utilizar servicios en la nube, consiste en configurar y asegurar la cuenta “root”, de AWS, para esto se utiliza el servicio de AWS IAM (Identity and Access Management), este servicio permite administrar el ciclo de vida de los usuarios, cuentas de servicios y todos los recursos con los que se interactúan en la nube.

La mayoría de los administradores utiliza la cuenta “root”, para realizar actividades de administración y del día a día, la cual es considerado como una mala práctica, ya que esta cuenta tiene todos los privilegios y visibilidad de los servicios contratados, se deben crear cuentas de acuerdo con el tipo de perfil y rol de los usuarios.

Dentro de las opciones que tenemos para asegurar la cuenta “root”, consiste en utilizar múltiple factor de autenticación y contraseñas seguras, estas recomendaciones en lo posible deben ser aplicadas para todas las cuentas.

A continuación, en la ilustración se muestra el proceso de asegurar la cuenta “root” en AWS.

Ilustración 13. Asegurar cuenta root

Fuente: Elaboración Elkin Rivera

7.2 ESTABLECIMIENTO DE UNA POLÍTICA DE CONTRASEÑA SEGURA

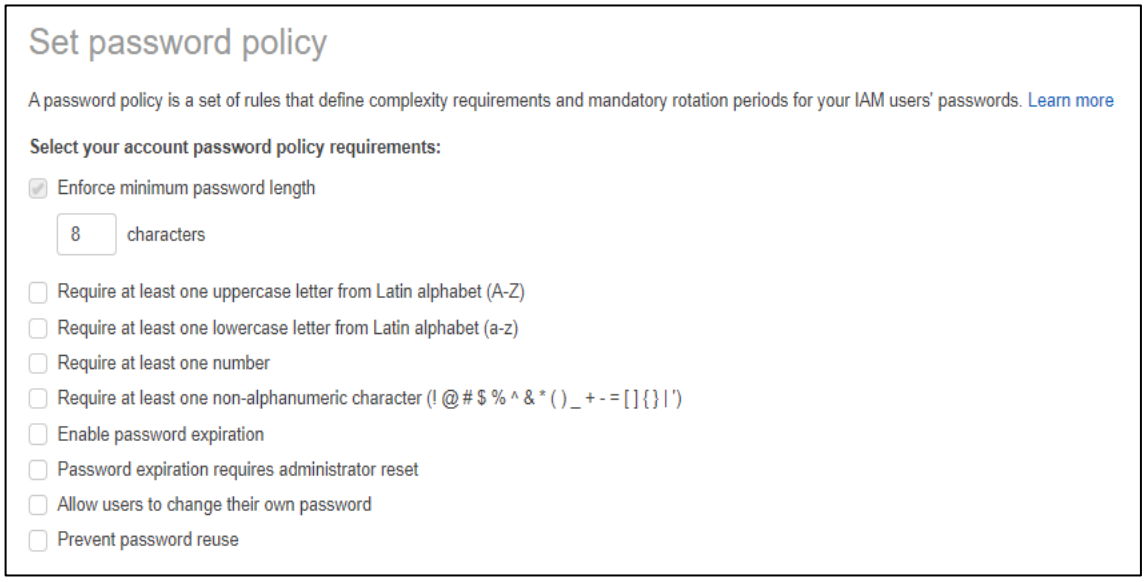
Hoy en día es muy común, tener un alto número de cuentas de acceso a diferentes plataformas y aplicaciones, el tener que memorizar diferentes usuarios y contraseñas para autenticarse, ocasiona que las contraseñas que son generadas no sean seguras, o se utilice la misma contraseña para todos los accesos, lo que nos puede llegar a generar problemas si logran descubrirla, es importante tener en cuenta las recomendaciones para generar contraseñas seguras, por ejemplo:

- Definir un tamaño mínimo para la contraseña (12 caracteres o superior).
- Usar una combinación de letras, números y caracteres especiales.

- Incluir al menos una letra en mayúscula/minúscula.
- Forzar el cambio de contraseña a ciertos intervalos (cada 90 días).
- La reutilización de contraseñas no debe estar autorizada.

En la siguiente ilustración, la configuración de parámetros para asegurar la política de contraseñas seguras de los usuarios IAM.

Ilustración 14. Definición de política de contraseñas

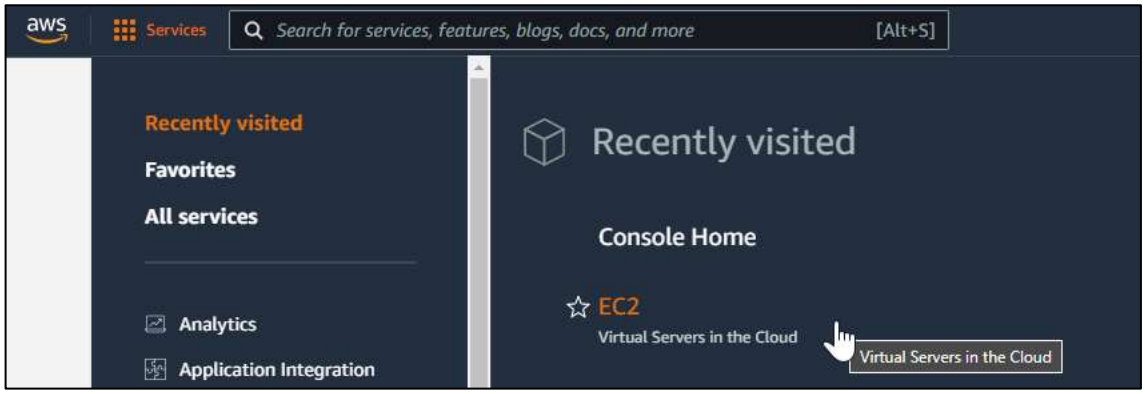


Fuente: Elaboración Elkin Rivera

7.3 CREACIÓN DE LOS SERVIDORES WEB (FRONTEND)

En la siguiente ilustración, el menú de servicios, se selecciona la opción EC2 (Elastic Compute Cloud, el servicio que permite desplegar servidores en la nube de AWS).

Ilustración 15. Despliegue de servidores



Fuente: Elaboración Elkin Rivera

El siguiente paso se debe seleccionar la zona de disponibilidad donde los servidores serán desplegados, idealmente y para poder tener alta disponibilidad los servidores serán desplegados en dos zonas de disponibilidad diferente.

Una zona de disponibilidad está conformada por una o más Data Center completamente aislados, si un problema impacta un Data Center el otro no será afectado

A continuación, la ilustración del proceso de selección de las zonas de disponibilidad.

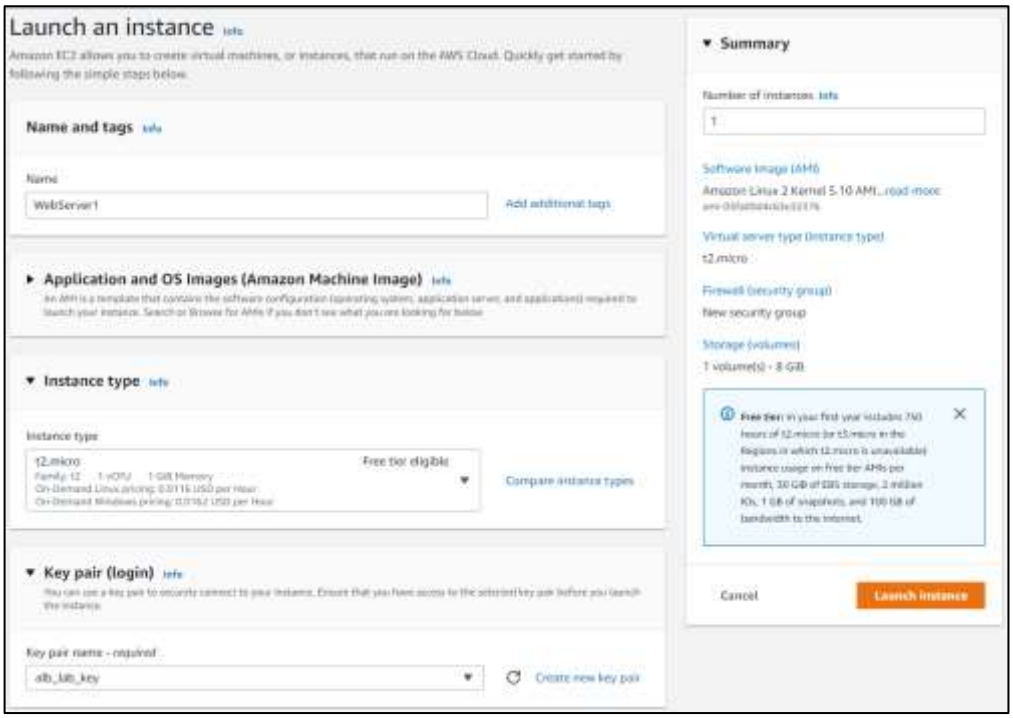
Ilustración 16. Zonas de disponibilidad

Fuente: Elaboración Elkin Rivera

Dentro de la opción “Launch instance”, se define la cantidad de servidores web que se desea, se elige el sistema operativo y las características del servidor en cuanto al hardware (memoria RAM, disco duro).

A continuación, la ilustración del proceso de elección de las características de hardware que permitirán el despliegue de los servidores.

Ilustración 17. Características de hardware servidores



Fuente: Elaboración Elkin Rivera

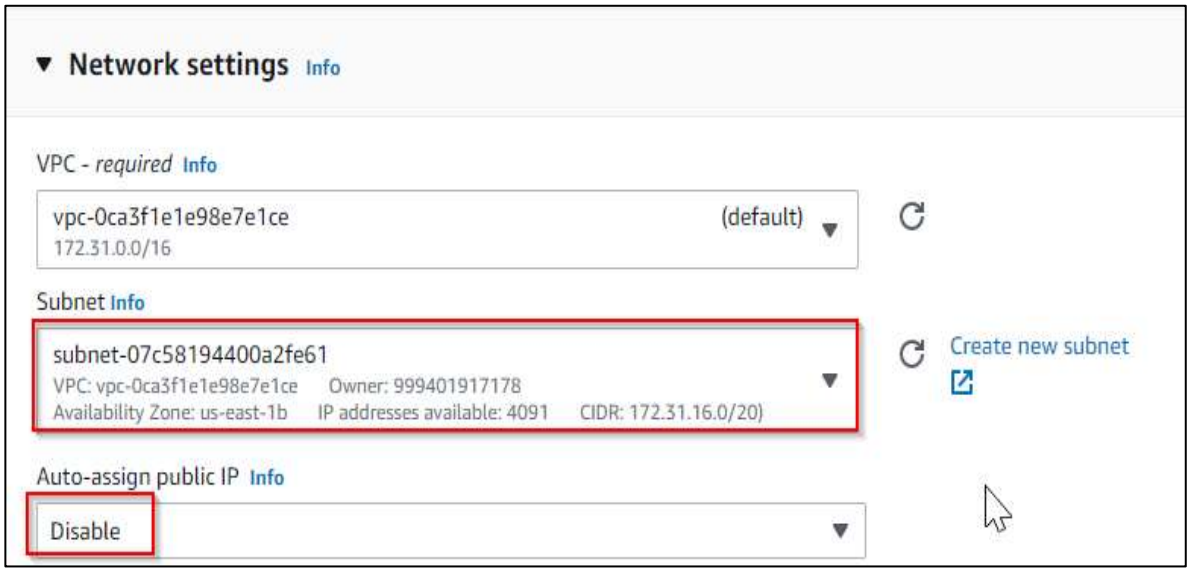
Por último, se selecciona el VPC (Es el servicio relacionado con la parte “networking”, definición de rangos de direccionamiento IP y enrutamiento).

De igual manera, dentro de este apartado se selecciona el “security group” o las reglas de Firewall que se quieran implementar.

- Las reglas del “security group” deben ser restrictivas, aplicando así el principio de “last privilege”.
- Como buena práctica de seguridad es recomendado no asociar direcciones IP públicas a los servidores WEB.
- El servidor web será accesible desde internet, sin embargo, los usuarios no podrán acceder directamente a la URL/IP del servidor, todas las conexiones deben pasar por un “load balancer”. En el “load balancer” podemos aplicar medidas de seguridad adicionales.

En la siguiente ilustración la configuración de VPN.

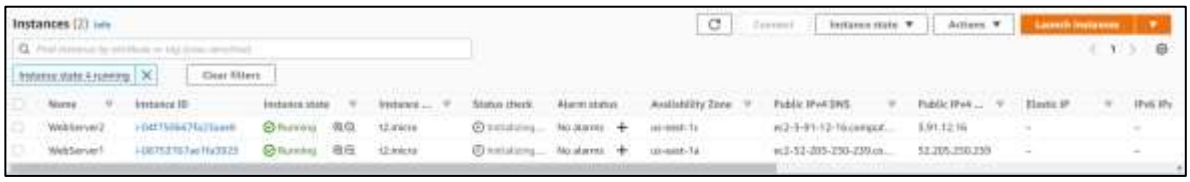
Ilustración 18. Configuración de VPN



Fuente: Elaboración Elkin Rivera

En la siguiente ilustración, se verifica que los servidores estén creados correctamente en el menú de “Instances”.

Ilustración 19. Verificación de los servidores



Fuente: Elaboración Elkin Rivera

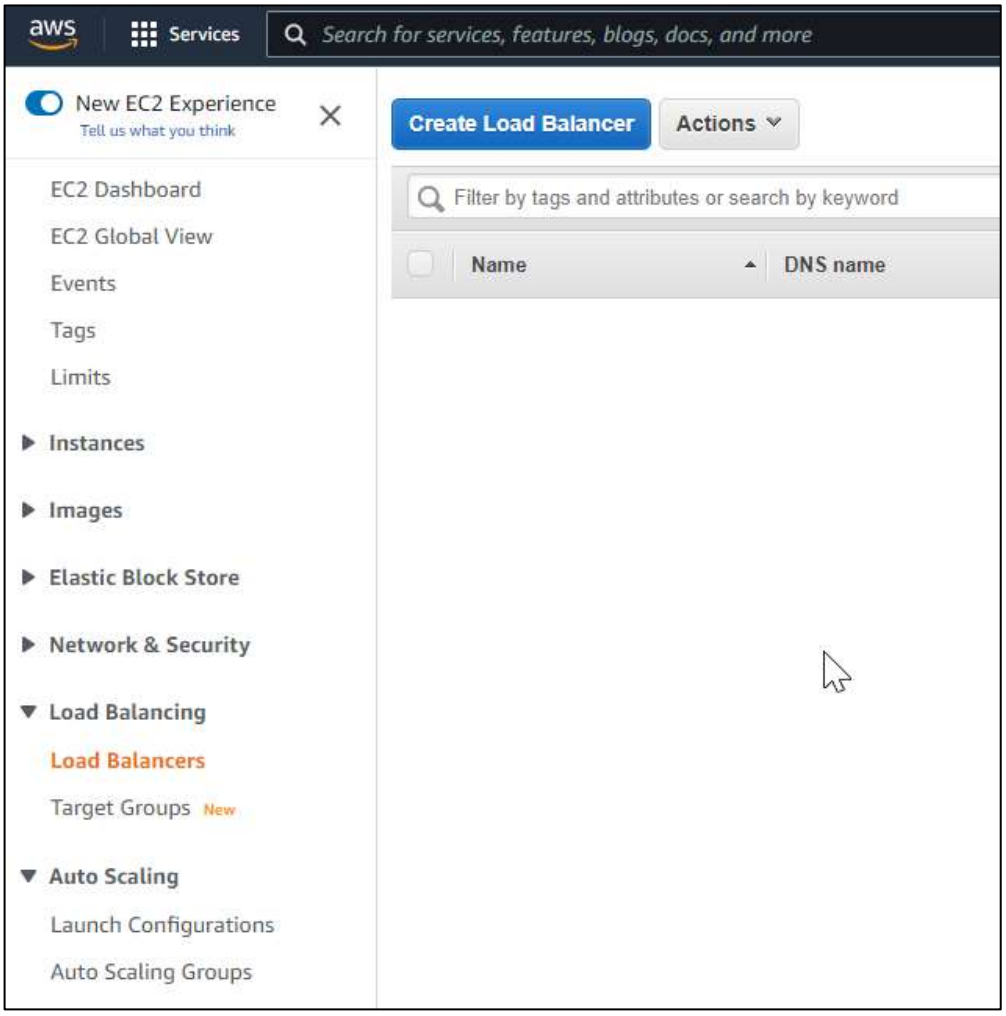
Es importante tener en cuenta que, en la nube, todos los recursos (Servidores, contenedores, bases de datos, etc) son por principio efímeros, lo que quiere decir que tienen un tiempo de vida bastante corto, por esta razón el direccionamiento IP privado no es importante, los servidores cambian de dirección IP, regularmente, y para hacer referencia a los servidores u otros componentes se utiliza el ID del objeto y no la dirección IP como se haría en una infraestructura clásica on-premises.

7.4 CREACIÓN DE UN LOAD BALANCER

Con el objetivo de asegurar alta disponibilidad de la aplicación, un balanceador de carga será ubicado delante de los servidores web, este balanceador recibirá y manejará todas las solicitudes HTTP/HTTPS dirigidas hacia la aplicación.

En la siguiente ilustración el proceso de crear el balanceador en el menú “Load Balancing”, “Load Balancer”, seleccionamos “Create Load Balancer”.

Ilustración 20. Creación del balanceador

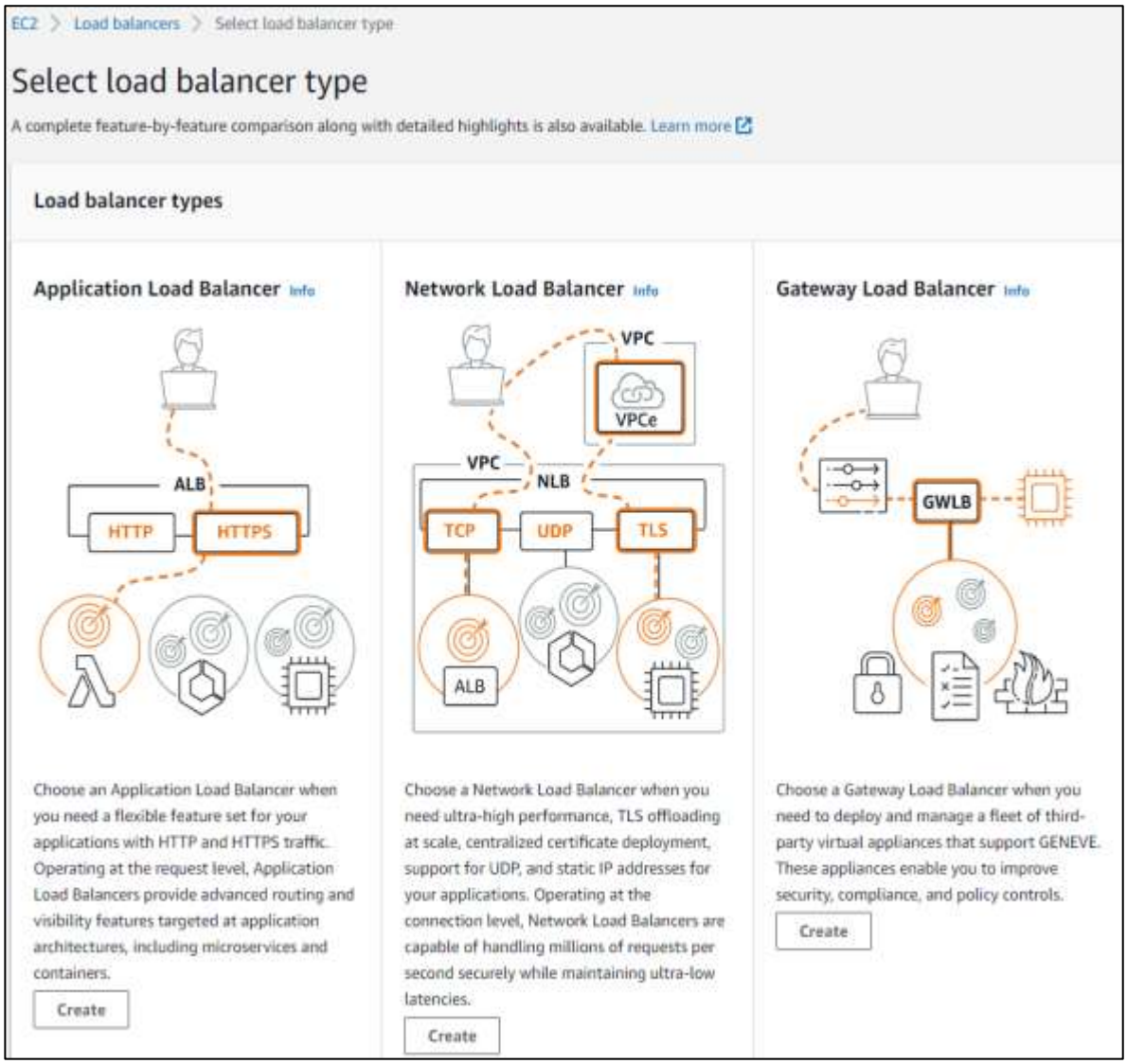


Fuente: Elaboración Elkin Rivera

En esta etapa, se debe seleccionar el balanceador que mejor responde a las necesidades de la aplicación. Para este caso, será elegido un “Network Load Balancer”.

A continuación, la ilustración del proceso de creación del balanceador de carga.

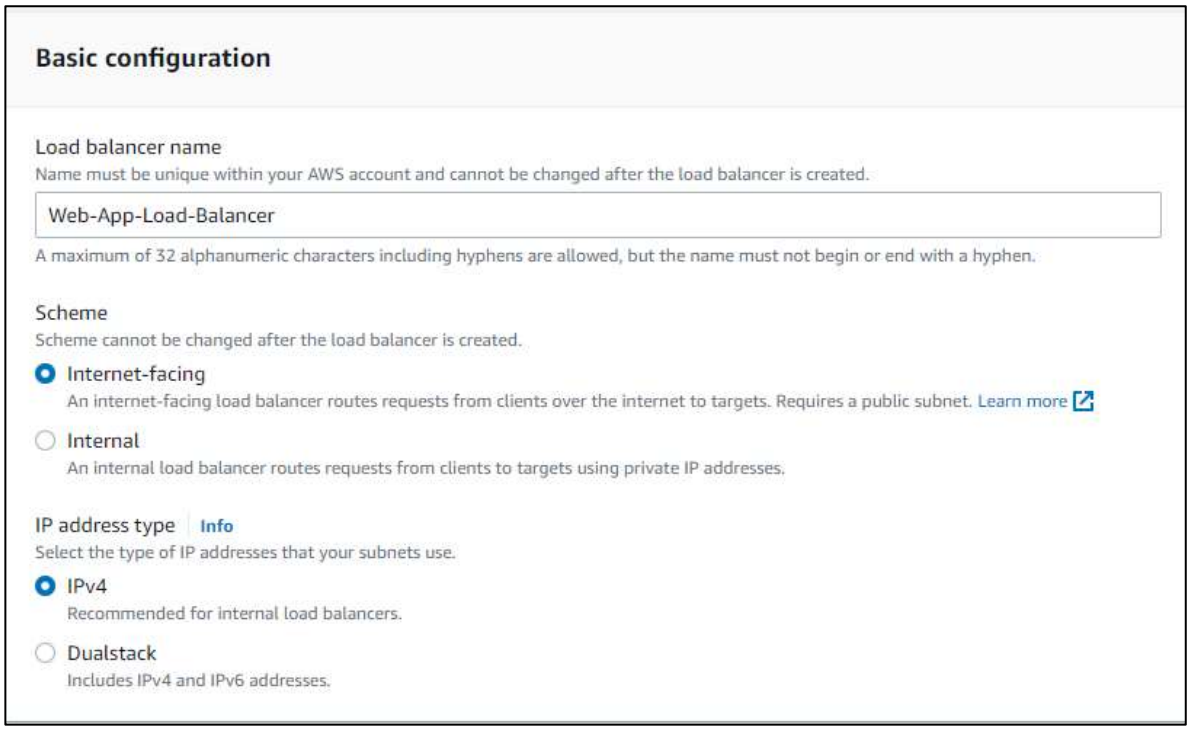
Ilustración 21. Opciones de balanceador



Fuente: Elaboración Elkin Rivera

En la siguiente ilustración se asigna un nombre al balanceador, se define si es un balanceador de cara a internet o un balanceador interno.

Ilustración 22. Tipo de balanceador



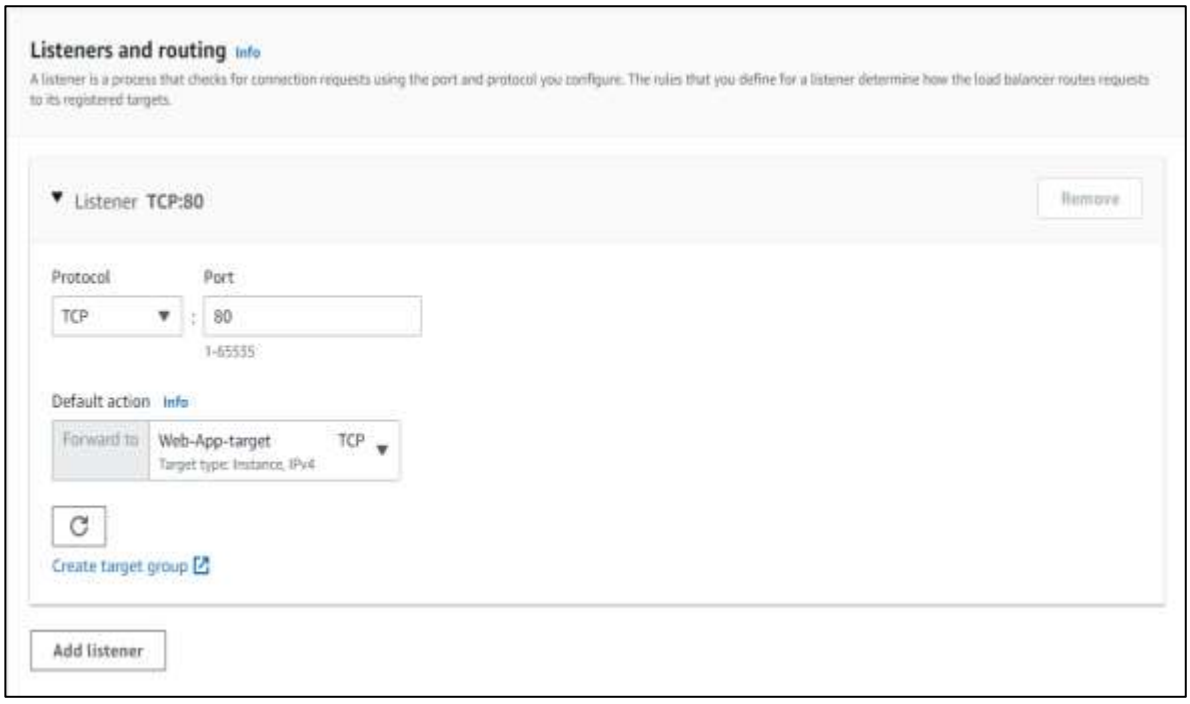
Fuente: Elaboración Elkin Rivera

Por último, se debe configurar el puerto por el cual el balanceador recibirá las solicitudes, para esta prueba de concepto se selecciona HTTP y un “target group” (Los servidores hacia los cuales el balanceador enviará las solicitudes).

Como buena práctica de seguridad los únicos puertos expuestos en internet deben ser puertos seguros HTTPS/TLS.

A continuación, la ilustración del proceso de configuración de los puertos permitidos en el balanceador de carga.

Ilustración 23. Configuración de puertos



Fuente: Elaboración Elkin Rivera

En la siguiente ilustración, se verifica que el balanceador se encuentre creado correctamente.

Ilustración 24. Creación del balanceador

Fuente: Elaboración Elkin Rivera

7.5 REGISTRO DE LOS SERVIDORES ANTE EL BALANCEADOR

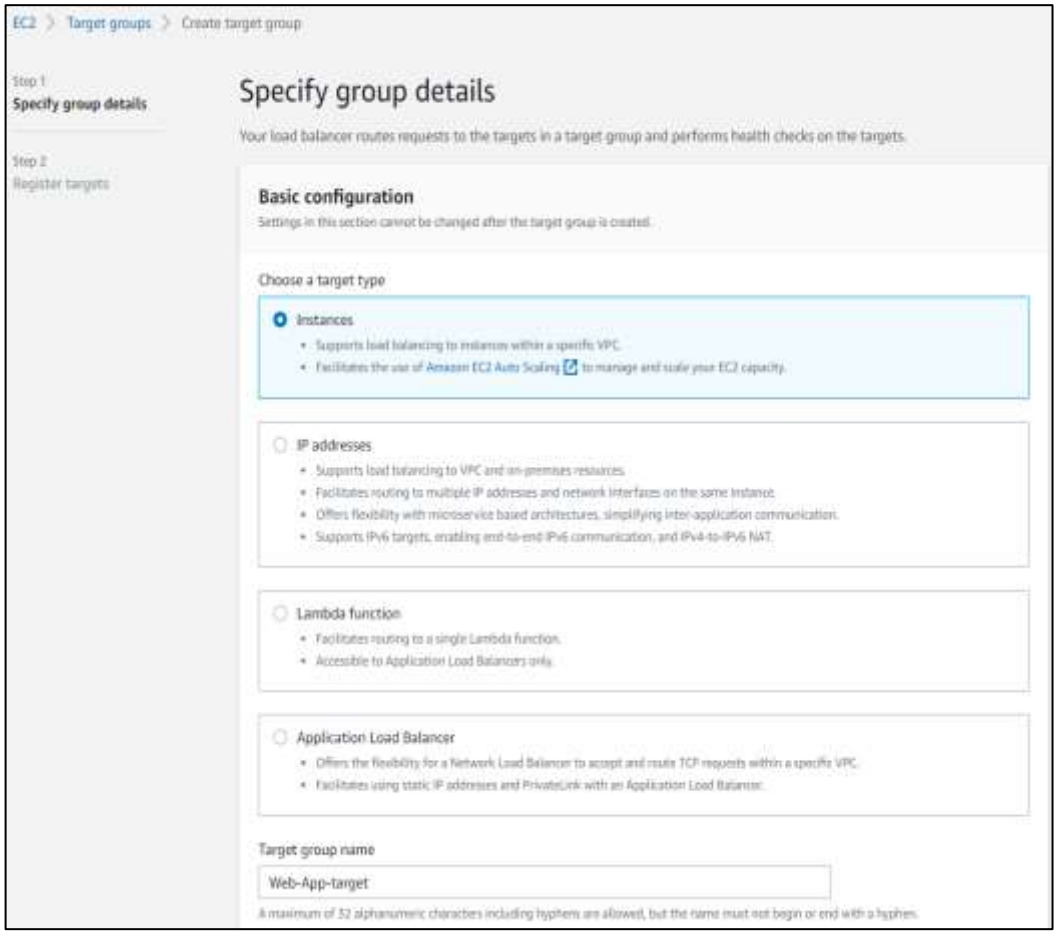
Después de que los servidores estén creados, deben registrarse en el balanceador, de esta manera se podrá redirigir las solicitudes web que se reciban.

- Se selecciona “Target Groups”, se define el tipo de “target group”, para este caso ‘Instances’ y se asigna un nombre al “target group”.

- Con el objetivo de verificar que los servidores están funcionando correctamente, se utilizan los “Health checks” (Solicitudes enviadas desde el balanceador hacia los servidores).

En la siguiente ilustración, se verifica el registro y configuración del balanceador.

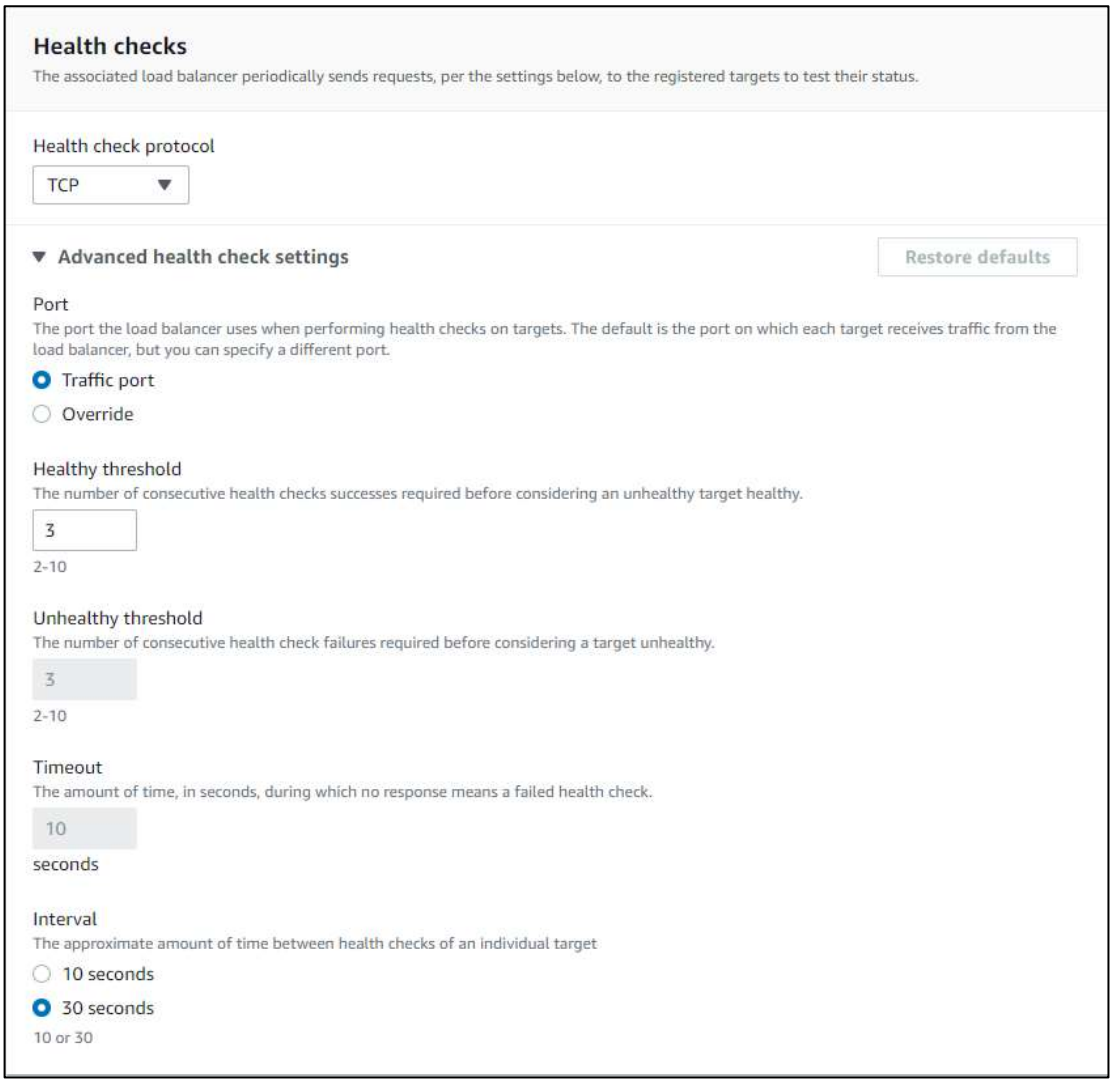
Ilustración 25. Configuración del balanceador



Fuente: Elaboración Elkin Rivera

A continuación, la ilustración del proceso de verificación del estado de salud de los servidores que fueron desplegados.

Ilustración 26. Configuración health checks



Fuente: Elaboración Elkin Rivera

Finalmente, se deben registrar los servidores y se termina la configuración del “target group”.

En la siguiente ilustración, se verifica el registró y presentación de los servidores.

Ilustración 27. Verificación de registro de los servidores

Fuente: Elaboración Elkin Rivera

A continuación, la ilustración del proceso de verificación de acceso al servidor uno, por medio del balanceador de carga.

Ilustración 28. Acceso a la aplicación servidor 1

Fuente: Elaboración Elkin Rivera

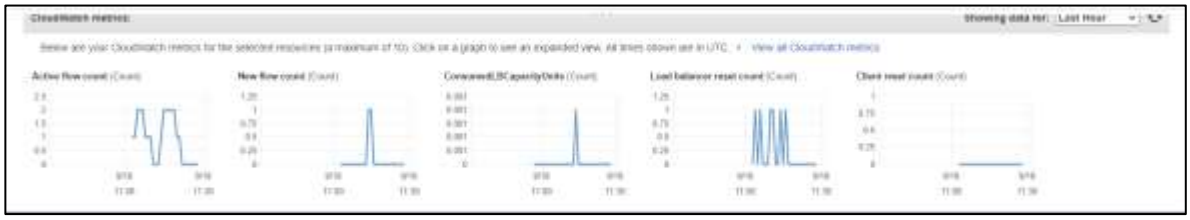
A continuación, la ilustración del proceso de verificación de acceso al servidor dos, por medio del balanceador de carga.

Ilustración 29. Acceso a la aplicación servidor 2

Fuente: Elaboración Elkin Rivera

En la siguiente ilustración, se verifica que el balanceador esté recibiendo y procesando las solicitudes.

Ilustración 30. Solicitudes procesadas por el balanceador



Fuente: Elaboración Elkin Rivera

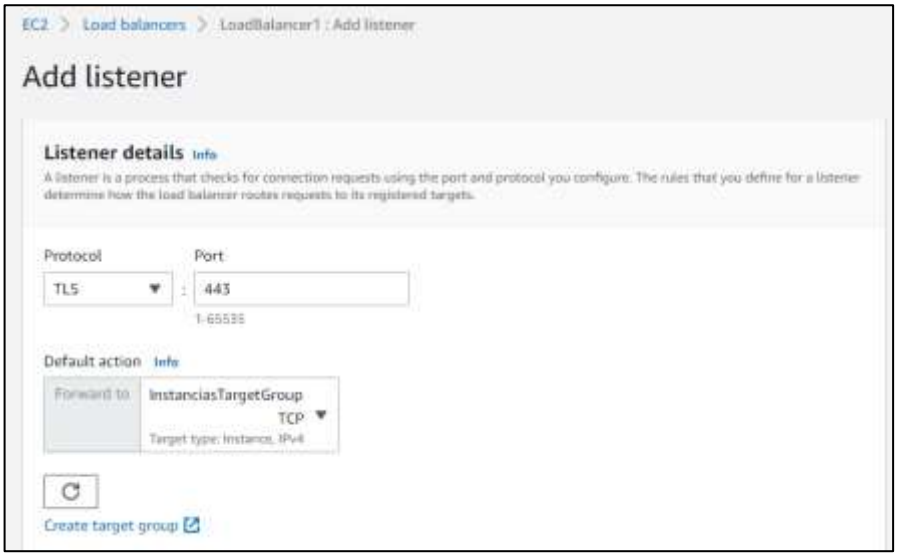
7.6 PROTECCIÓN DE DATOS EN TRÁNSITO

Con el fin de proteger los datos en tránsito, se utilizan certificados TLS, como buena práctica se recomienda como mínimo utilizar la versión TLSv1.2.

Para crear el certificado se selecciona en el menú EC2 > Load Balancer > LoadBalancer1 y se crea un nuevo “listerner”. De esta manera el balanceador recibirá y tratará todas las solicitudes HTTPS.

A continuación, la ilustración muestra el proceso de creación del certificado.

Ilustración 31. Creación de certificado



Fuente: Elaboración Elkin Rivera

7.7 PROTECCIÓN DE LOS DATOS EN REPOSO

Para proteger los datos en reposo, AWS propone diferentes métodos de cifrado de datos, el servicio típicamente utilizado es AWS KMS (Key Management Service), este servicio permite de administrar el ciclo de vida de las llaves de cifrado (Creación, revocación, supresión, etc).

A continuación, la ilustración del proceso de creación de la llave de cifrado para los volúmenes EBS, discos duros en la nube.

Ilustración 32. Cifrado de volúmenes EBS

Elaboración Elkin Rivera

Como buena práctica de seguridad es recomendado crear llaves de cifrado personalizadas y no utilizar las llaves por defecto de AWS. De igual manera, se debe limitar el acceso a esta llave únicamente a las entidades (User/Application) autorizadas. Este control se aplica mediante políticas de acceso.

En la siguiente ilustración el proceso de configuración de la política de acceso.

Ilustración 33. Política de acceso

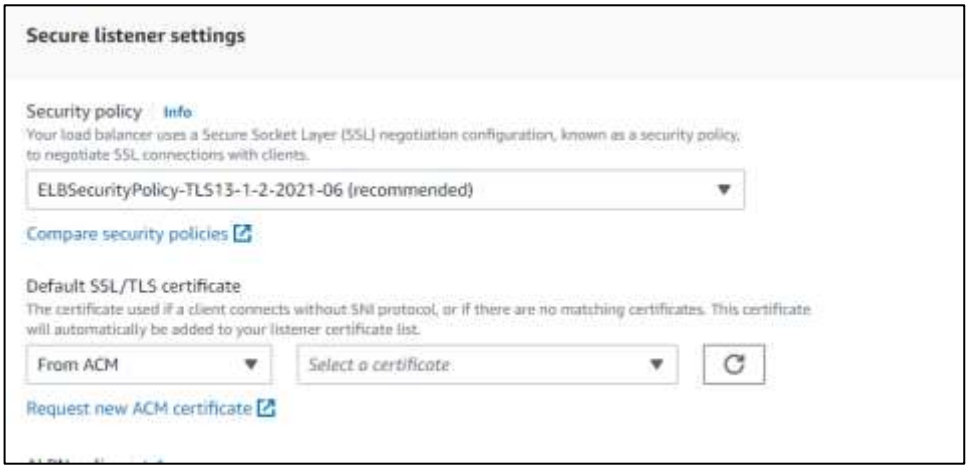
Fuente: Elaboración Elkin Rivera

7.8 CREACIÓN DE POLÍTICA DE CERTIFICADO

La política de certificados permite establecer los algoritmos de cifrado y autenticación que serán utilizados durante el intercambio de certificados TLS (TLS handshake).

A continuación, la ilustración del proceso de creación de certificados empleando algoritmos de cifrado.

Ilustración 34. Política de certificado



Fuente: Elaboración Elkin Rivera

7.9 ACTIVACIÓN DEL WAF (WEB APPLICATION FIREWALL)

Para proteger la aplicación web contra ataques en la capa de aplicación, (capa 7 del modelo OSI), AWS permite integrar el servicio AWS WAF, con un balanceador de carga. Para esto vamos al servicio WAF & Shield, seleccionamos Web ACL, luego crear Web ACL.

A continuación, en la ilustración el proceso de creación del WAF en AWS.

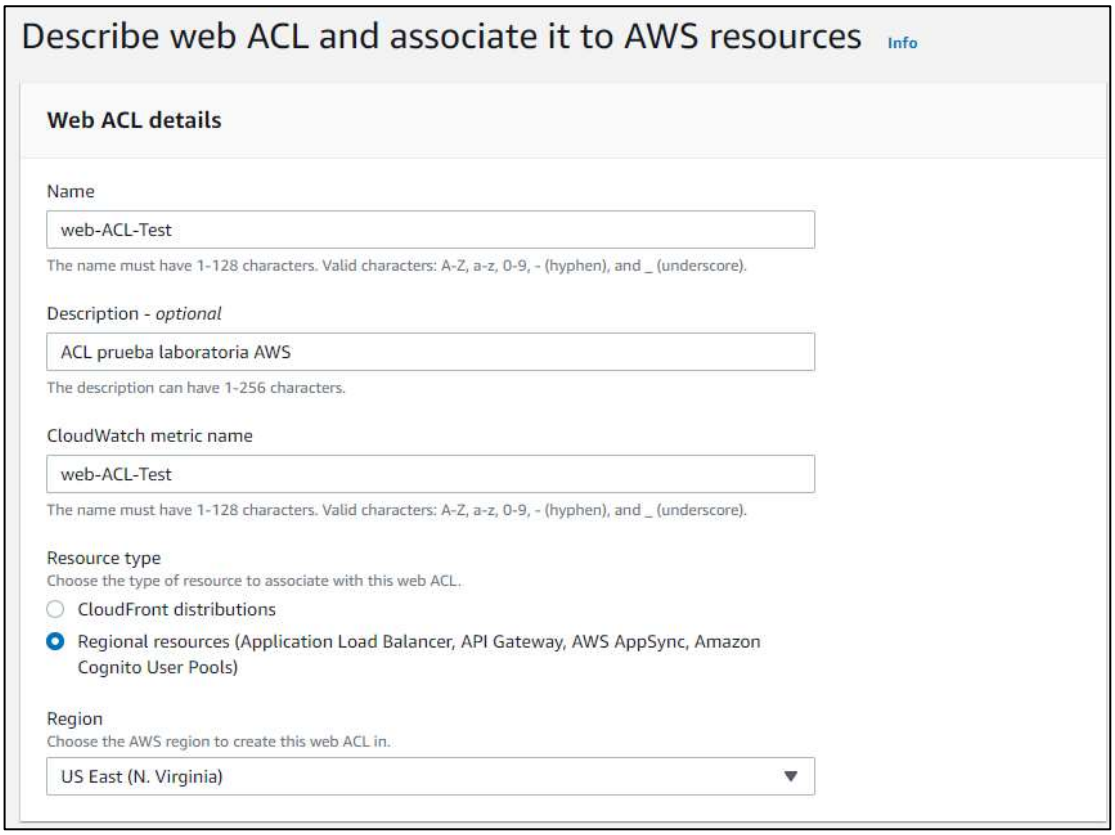
Ilustración 35. Creación de WAF

Fuente: Elaboración Elkin Rivera

El siguiente paso es configurar la lista de control de acceso, se selecciona un nombre, la región donde se quiere desplegar la regla y el recurso que se desea proteger (para este caso el balanceador).

En la siguiente ilustración el proceso de creación de las listas de control de acceso que serán implementadas.

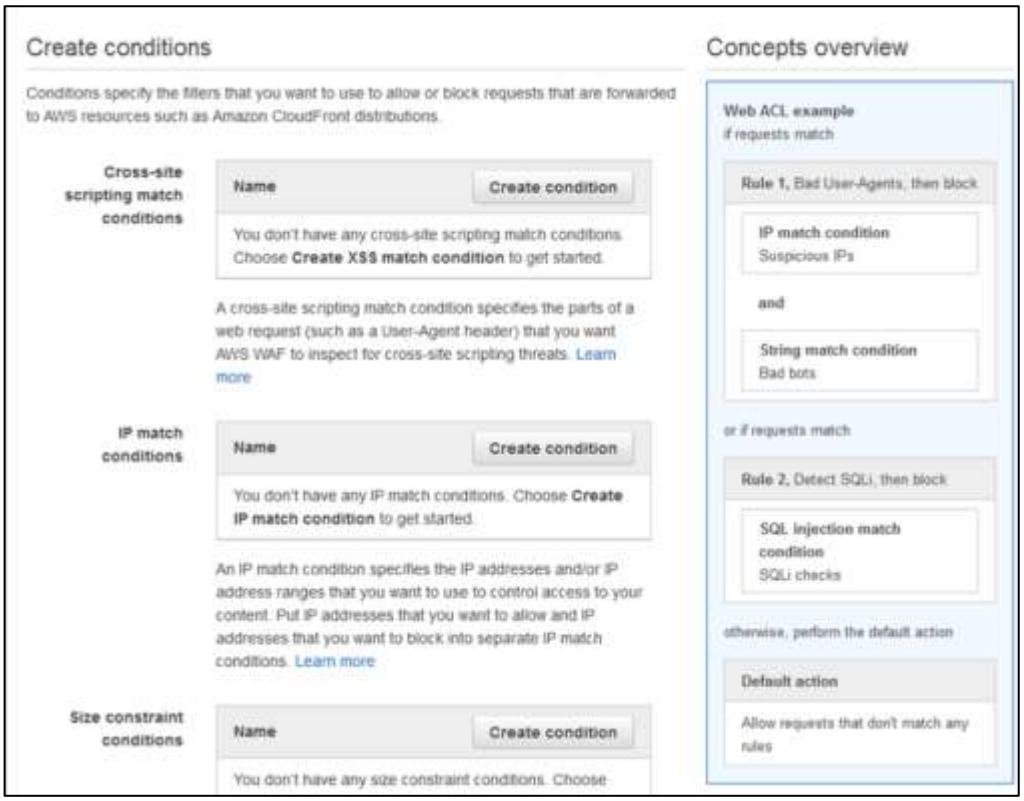
Ilustración 36. Creación de ACL



Fuente: Elaboración Elkin Rivera

A continuación, en la siguiente ilustración la configuración de las reglas aplicadas en el WAF de AWS.

Ilustración 37. Creación de reglas WAF

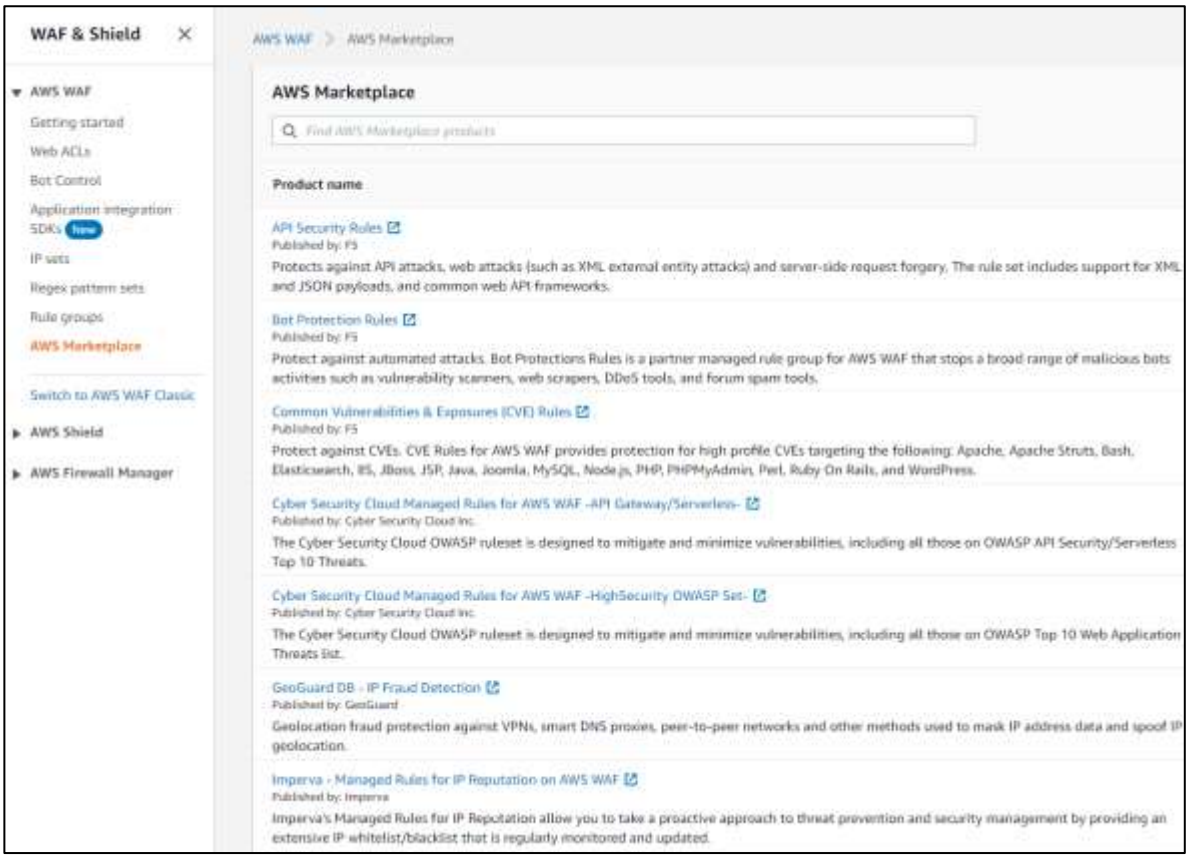


Fuente: Elaboración Elkin Rivera

Después de realizar la integración, el paso siguiente es crear las reglas para proteger la aplicación. AWS ofrece algunas reglas básicas por defecto que pueden ser utilizadas, también el usuario puede configurar sus propias reglas y por último se pueden comprar e integrar reglas de la Marketplace, donde fabricantes como Imperva, Fortinet, OWASP, ofrecen reglas mucho más avanzadas y especializadas en la protección de sitios web.

En la siguiente ilustración, las opciones de Marketplace, ofrecidas por los diferentes fabricantes de seguridad.

Ilustración 38. Opciones de Marketplace



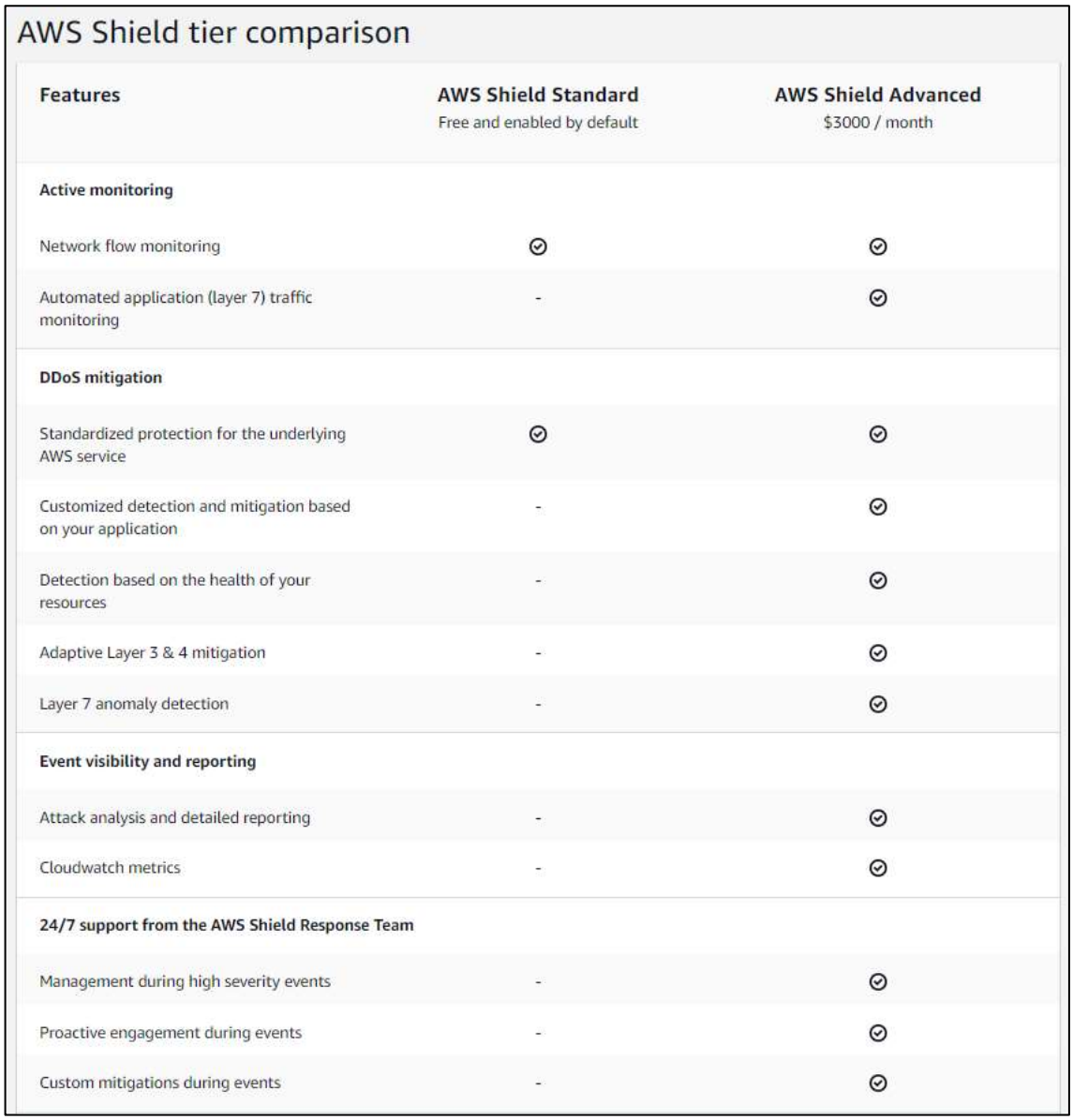
Fuente: Elaboración Elkin Rivera

7.10 Activación de AWS Shield (Anti-DDoS)

AWS Shield es una solución anti-DDoS administrada por AWS, el servicio es activado por defecto en todas las suscripciones de AWS. La versión “premium” está disponible, la cual ofrece mayor visibilidad y un soporte que incluye el acceso y contacto con el equipo de respuesta de incidentes AWS (Esta suscripción tiene un costo de 3000 dólares al mes). La integración es transparente mediante la utilización del (API) y no tiene mayor impacto sobre los servidores ya que el control se hace a nivel del backbone de AWS.

A continuación, la ilustración de los parámetros disponibles en la configuración del DDoS en AWS.

Ilustración 39. AWS Shield



AWS Shield tier comparison

Features	AWS Shield Standard Free and enabled by default	AWS Shield Advanced $3000 / month
Active monitoring		
Network flow monitoring	✓	✓
Automated application (layer 7) traffic monitoring	-	✓
DDoS mitigation		
Standardized protection for the underlying AWS service	✓	✓
Customized detection and mitigation based on your application	-	✓
Detection based on the health of your resources	-	✓
Adaptive Layer 3 & 4 mitigation	-	✓
Layer 7 anomaly detection	-	✓
Event visibility and reporting		
Attack analysis and detailed reporting	-	✓
Cloudwatch metrics	-	✓
24/7 support from the AWS Shield Response Team		
Management during high severity events	-	✓
Proactive engagement during events	-	✓
Custom mitigations during events	-	✓

Fuente: Elaboración Elkin Rivera

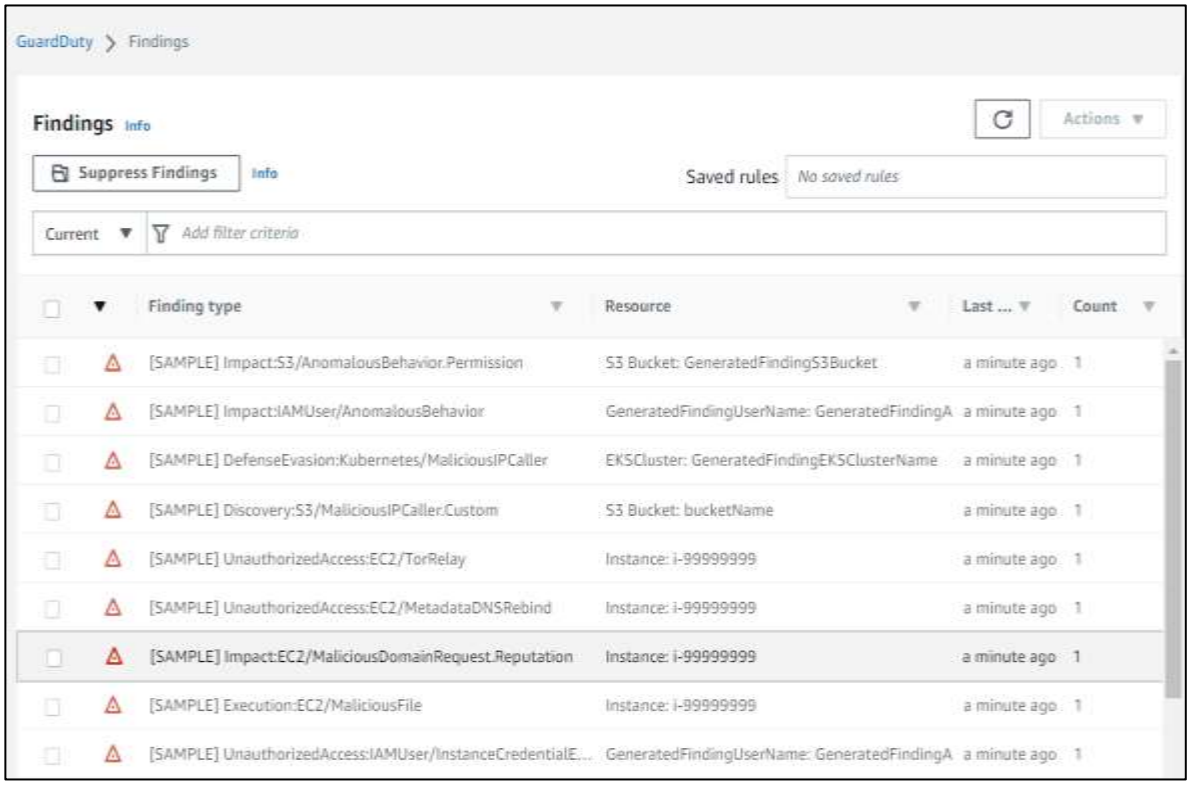
7.11 ACTIVACIÓN DE AWS GUARDDUTY

Este servicio permite monitorear las cuentas de AWS, los servidores, bases de datos, activación de los usuarios entre otros, con el objetivo de detectar posibles amenazas.

Después de activar el servicio, este analizará los diferentes logs de acceso, al igual que el comportamiento de los recursos en la nube y en función de las reglas definidas va a generar alertas de seguridad.

En la siguiente ilustración los logs generados por el acceso y consumo de los diferentes servicios disponibles en AWS.

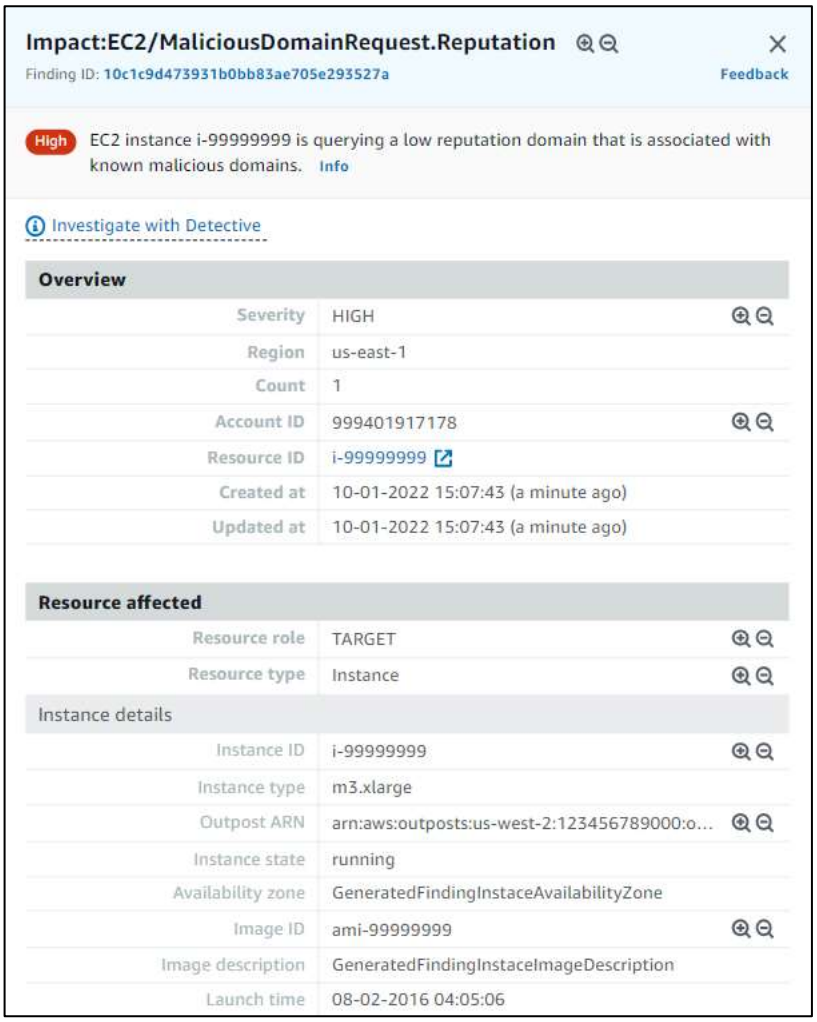
Ilustración 40. Activación GuardDuty



Fuente: Elaboración Elkin Rivera

En la siguiente ilustración, los detalles específicos de los eventos o vulnerabilidades identificadas por GuardDuty.

Ilustración 41. Detalle del log



Fuente: Elaboración Elkin Rivera

En la anterior prueba de concepto fueron utilizados cada uno de los componentes que están disponibles en AWS, y la forma en la que se deben emplear, es importante tener en cuenta que cada aplicación se ajusta a las necesidades de una organización y por ende hay parámetros que pueden ser aplicados y otros que pueden que no, por ejemplo, si tenemos un sitio de comercio que oferta productos en Colombia, la mayor parte de las transacciones se deben reflejar desde IP geolocalizadas en Colombia, pero si se observa tráfico desde países como China, posiblemente están intenta vulnerar la aplicación y podemos realizar esta restricción.

8 APLICACIÓN DEL FRAMEWORK NIST SP 800-53 V5 PARA ASEGURAR LA GESTIÓN DEL CICLO DE VIDA DE LAS IDENTIDADES PARA USUARIOS, CUENTAS DE SERVICIO Y ROLES.

El framework NIST SP 800-53, detalla los controles que deben ser aplicados con el fin de asegurar las infraestructuras y todos los elementos que interactúan dentro de un sistema, adicionalmente permite dar una guía para atender un incidente de seguridad y remediar el impacto generado por este.

En el siguiente cuadro, se encuentran las recomendaciones de seguridad basadas en el framework de NIST SP 800-53 V5, se describe el servicio que permite implementar el control en AWS y la manera en la que puede ser auditado este control, con el fin de gestionar el ciclo de vida de los usuarios y cuentas en AWS.

Cuadro 3. Recomendaciones de seguridad

ID del Control	Descripción (NIST)	Como implementar (Servicio AWS)	Como Controlar (AWS)	Descripción del control
AC-2 (1)	Soporte para la administración de cuentas del sistema mediante [Asignación: mecanismos automatizados definidos por la organización].	AWS IAM + AWS Config	iam-user-mfa -enabled	Este control garantiza que la autenticación multi-factor (MFA), pueda ser activada para todos los usuarios IAM, de esta manera es posible reducir los incidentes de cuentas comprometidas y evitar que los usuarios no autorizados accedan a los datos confidenciales.
AC-2 (1)	Soporte para la administración de cuentas del sistema mediante [Asignación: mecanismos automatizados definidos por la organización].	AWS IAM + AWS Config	iam-password -policy	Una política de contraseñas IAM es aplicada en la organización, forzando, a utilizar credenciales que otorgan privilegios de acuerdo al perfil de la cuenta del usuario.

AC-2 (1)	Soporte para la administración de cuentas del sistema mediante [Asignación: mecanismos automatizados definidos por la organización].	AWS IAM + AWS Config	access-keys-rotated	Las credenciales se auditan para los dispositivos, usuarios y procesos autorizados, con el fin de garantizar que las claves de acceso de IAM, cambien según la política de la organización.
AC-2	Definir y documentar los tipos de cuentas permitidas y específicamente prohibidas para su uso dentro del sistema; b. Asignar administradores de cuentas; c. Requerir [Asignación: requisitos y criterios previos definidos por la organización]	AWS IAM + AWS Config	iam-policy-no-statements-with-full-access	Permitir que los usuarios tengan más privilegios de los necesarios para completar una tarea, pueden llegar a vulnerar el principio de privilegio mínimo y separación de funciones.
AC-2 (4)	Audite automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas.	AWS CloudTrail	cloudtrail-enabled	AWS CloudTrail, permite aplicar el principio de no repudio, al registrar las acciones de la consola de administración de AWS, y las llamadas API. Puede identificar los usuarios y las cuentas de AWS, que llamaron a un servicio de AWS, la dirección IP de origen en la que se generaron las llamadas y los tiempos de duración de estas.
AC-2 (4)	Audite automáticamente las acciones de creación, modificación, activación, desactivación y eliminación de cuentas.	AWS Cloud Trail + AWS Lambda	cloud-trail-cloud-watch-logs-enabled	Permite detectar actividades inusuales y seguimiento de las cuentas que realizaron esta actividad. En ciertos casos, es posible automatizar el proceso de respuesta cuando un incidente o actividad no autorizada es detectada.

AC-2(12)	Supervisar las cuentas del sistema para [Asignación: uso atípico definido por la organización]; y b) Comunicar el uso atípico de cuentas del sistema a [Asignación: personal o funciones definidas por la organización].	AWS GuardDuty	guardduty-enabled-centralized	Monitorea y detecta posibles eventos de seguridad, permite habilitar módulos de auto aprendizaje para identificar actividades inusuales, también incluye control de acceso mediante listas con direcciones IP con dudosa reputación.
AC-3 (7)	Aplique una política de control de acceso basada en roles sobre sujetos y objetos definidos y controle el acceso en función de [Asignación: roles definidos por la organización y usuarios autorizados para asumir dichos roles].	AWS IAM + AWS Config	iam-root-access-key-Check	El usuario “root”, cuenta con acceso a nivel de “Admin” a toda la infraestructura AWS, se debe evitar utilizar esta cuenta, para realizar actividades de administración, para ello, los usuarios IAM, deben ser creados y solo deben asignarse los privilegios necesarios para realizar las actividades requeridas, cumpliendo así el principio de “least privilege”.
AC-3(15)	Aplicar [Asignación: política de control de acceso obligatorio definida por la organización] sobre el conjunto de temas y objetos cubiertos especificados en la política; y (b) Hacer cumplir [Asignación: política de control de acceso discrecional definida por la organización] sobre el conjunto de temas y objetos cubiertos especificados en la política.	AWS IAM + AWS Config	access-keys-rotated	El cambio de las claves de acceso de manera regular es una práctica recomendada de seguridad. Acortar el período en que una clave de acceso está activa, reduce el impacto en el negocio si las claves se ven comprometidas. Esta regla requiere un valor de rotación de clave de acceso.

AC-4 (21)	La información separada fluye lógica o físicamente utilizando [Asignación: mecanismos y/o técnicas definidas por la organización] para lograr [Asignación: separaciones requeridas definidas por la organización por tipos de información].	AWS Config + AWS Lambda	restricted-ssh	Los puertos comunes de administración no deben estar publicados, en caso de ser requerido es necesario limitar el acceso a direcciones IP de confianza.
AC-4 (21)	La información separada fluye lógica o físicamente utilizando [Asignación: mecanismos y/o técnicas definidas por la organización] para lograr [Asignación: separaciones requeridas definidas por la organización por tipos de información].	AWS Config + AWS Lambda	restricted-common-ports	Gestiona el acceso a los recursos en la nube de AWS, garantizando que los puertos comunes estén restringidos. No restringir el acceso a los puertos a fuentes confiables puede provocar ataques contra la disponibilidad, integridad y la confidencialidad de los sistemas.

Fuente: Elaboración Elkin Rivera.

Es importante realizar la definición de roles y responsabilidades de tal formar que únicamente se garanticen los accesos necesarios para el desarrollo de actividades del día a día, se debe buscar disminuir los accesos incensarios y eliminar las cuentas de usuarios que no se encuentren dentro de la organización, se debe tener en cuenta que sin importar las múltiples medidas de seguridad que sean empleadas, se requiere del aporte de todos los usuarios dentro de la organización, ya que estos son el punto más débil y constituye una brecha de seguridad.

9 CONCLUSIONES

Se realizó la descripción de los servicios de seguridad nativos con los que cuenta AWS, para proteger las plataformas que son desplegadas dentro de la nube, es importante tener en cuenta que la mayoría de estos mecanismos de protección se encuentran con configuraciones por defecto, por lo que se requiere ajustar y definir de acuerdo a las necesidades del negocio, adicionalmente se recomienda validar aquellos servicios que incurren en un costo adicional, el proveedor de nube tiene a disposición del cliente los mecanismos para la protección de la infraestructura pero el cliente es el que decide y es el responsable de la implementación y administración de estos, para garantizar la seguridad de la plataforma.

Existen diferentes mecanismos orientados a la protección de los datos que se encuentran en tránsito como en reposo, sin importar cuál de los estos sea utilizado, la definición del proceso y los procedimientos, debe ser una de las primeras actividades a desarrollar por parte del grupo de TI, buscando garantizar el cumplimiento de los pilares de la seguridad de la información en cuanto a la confidencialidad e integridad de los datos se refiere, el proteger uno de los activos más importantes para una organización genera desafíos que van de la mano con la reputación y continuidad del negocio.

Se realizó una prueba de concepto aplicando buenas prácticas de seguridad en los mecanismos de protección disponibles en AWS, adicionalmente es recomendable realizar un análisis de vulnerabilidades periódico y definir una guía de hardening que permita asegurar nuestra infraestructura, el tratamiento que le demos a las vulnerabilidades identificadas estará enfocado en cerrar brechas de seguridad y disminuir posibles incidentes de seguridad, esta guía debe ser actualizada de forma permanente ajustándose a las nuevas amenazas y buscado aplicar las mejores prácticas de seguridad.

Aplicar las recomendaciones de seguridad de los diferentes framework y fabricantes que se encuentran disponibles en el mercado, permitirá que desarrollaremos procesos orientados a fortalecer y mejorara las prácticas de seguridad que llevamos a cabo dentro de una organización, se debe tener la premisa de que los datos y la información que se encuentra circulando en la red es esencial para dar continuidad al negocio, por ende, es nuestra responsabilidad garantizar la seguridad de la misma.

10 RECOMENDACIONES

Cuando se contratan servicios en nube pública, se debe verificar los módulos y aplicaciones que encuentran incluidos, con el fin de determinar cómo pueden ser empleados, pero teniendo en cuenta que hay servicios que son compartidos y se debe garantizar conexiones óptimas hacia la infraestructura, adicionalmente se debe asegurar la protección de los datos y funcionalidad de las aplicaciones desplegadas.

En la mayoría de los países se han decretado leyes para la protección de los datos, es muy importante emplear los mecanismos que ofrece AWS para la protección de los datos en tránsito como en reposo, con el fin de garantizar su integridad y evitar el uso indebido de los mismos, por tal razón es indispensable asegurar la información, para crear lazos de confianza entre clientes y empresa.

Se debe verificar constantemente los logs y ajustar los eventos que desencadenen alertas de seguridad, ajustar los perfiles y verificar las tendencias del tráfico que procesa la infraestructura, es decir si tenemos una aplicación que ofrece servicios es Colombia no debe tener mayor tráfico generado desde el continente asiático, esto permitirá optimizar los recursos de red y hardware de los equipos.

BIBLIOGRAFÍA

AMAZON WEB SERVICES. [Sitio Web]. AWS Shield. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/shield-chapter.html

AMAZON WEB SERVICES. [Sitio Web]. AWS WAF. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/waf-chapter.html

AMAZON WEB SERVICES. [Sitio Web]. Modelos de informática en la nube. [Consulta: 16 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing/

AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en: https://aws.amazon.com/es/compliance/shared-responsibility-model/

AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en:https://d1.awsstatic.com/security-center/Shared_Responsibility_Model_V2.59d1eccec334b366627e9295b304202faf7b899b.jpg

AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es el cortafuego de red de AWS? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/network-firewall/latest/developerguide/what-is-aws-network-firewall.html

AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es Amazon Inspector? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/inspector/latest/user/what-is-inspector.html

AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es Amazon GuardDuty? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/guardduty/latest/ug/what-is-guardduty.html

AMAZON WEB SERVICES. [Sitio Web]. ¿Qué es IAM? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html

AMAZON WEB SERVICES. [Sitio Web]. Relación de componentes básicos y cómo interactúan. [Consulta: 15 de marzo del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/images/region-with-azs.png

AMAZON WEB SERVICES. [Sitio Web]. Servicios de seguridad, identidad y conformidad de AWS. [Consulta: 10 de marzo del 2022]. Disponible en: https://aws.amazon.com/products/security/?nc1=h_ls

AMAZON WEB SERVICES. [Sitio Web]. Tipos de informática en la nube. [Consulta: 14 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing

AMAZON WEB SERVICES. [Sitio Web]. What is AWS Security Hub? [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

AMAZON WEB SERVICES. [Sitio Web]. Ley de aclaración del uso legal de datos en el extranjero (CLOUD). [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/compliance/cloud-act

AMAZON WEB SERVICES. [Sitio Web]. AWS Managed VPN. [Consulta: 15 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-vpc-connectivity-options/images/image2.png

AMAZON WEB SERVICES. [Sitio Web]. AWS Direct Connect. [Consulta: 15 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-vpc-connectivity-options/images/image6.png

AMAZON WEB SERVICES. [Sitio Web]. AWS. [Consulta: 14 de mayo 2022]. Disponible en: https://d2908q01vomqb2.cloudfront.net/22d200f8670dbdb3e253a90eee5098477c95c23d/2021/03/09/Demystifying-KMS-keys-2021-2.png

AMAZON WEB SERVICES. [Sitio Web]. AWS Certificate Manager. [Consulta: 10 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/certificate-manager/#:~:text=Los%20certificados%20de%20SSL%2FTLS,los%20certificados%20de%20SSL%2FTLS.

AMAZON WEB SERVICES. [Sitio Web]. Seguridad en la nube de AWS. [Consulta: 15 de mayo del 2022]. Disponible en: https://aws.amazon.com/es/security/

EUROPEAN UNION AGENCY FOR CYBERSECURITY. [Sitio Web]. Cloud Computing Risk Assessment – Spanish. [Consulta: 14 de abril del 2022]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish.

MICROSOFT. [Sitio Web]. What is a cloud service provider? [Consulta: 15 de abril del 2022]. Disponible en: https://azure.microsoft.com/en-us/overview/what-is-a-cloud-provider/

NIST. [Sitio Web]. Framework Documents. [Consulta: 10 de marzo del 2022]. Disponible en https://www.nist.gov/cyberframework/framework

NIST. [Sitio Web]. The Five Functions. [Consulta: 10 de marzo del 2022]. Disponible en: https://www.nist.gov/sites/default/files/styles/220_x_220_limit/public/images/2018/04/12/ipdrr_circle.png?itok=qV5agiH5

REDHAT. [Sitio Web]. Tipos de cloud computing. [Consulta: 15 de abril del 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud#:~:text=Hay%20cuatro%20tipos%20principales%20de,software%20como%20servicio%20(SaaS)

SECRETARIA SENADO. [Sitio Web]. LEY 1273 DE 2009. [Consulta: 16 de abril del 2022]. Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECRETARIA SENADO. [Sitio Web]. LEY ESTATUTARIA 1266 DE 2008. [Consulta: 16 de abril del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

SECRETARIA SENADO. [Sitio Web]. LEY ESTATUTARIA 1581 DE 2012. [Consulta: 16 de abril del 2022]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

S. Gupta, A. Gupta y G. Shankar, "Cloud Computing: Services, Deployment Models and Security Challenges", 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 414-418, doi: 10.1109/ICOSEC51865.2021.9591794.

ANEXO

Resumen analítico especializado - RAE

Fecha de Realización:	21/12/2022
Programa:	Especialización seguridad informática
Línea de Investigación:	Computación en la nube
Título:	BUENAS PRÁCTICAS DE SEGURIDAD PARA APLICACIONES WEB DESPLEGADAS EN UN MODELO DE INFRAESTRUCTURA TIPO IAAS EN LA NUBE DE AWS
Autor(es):	Elkin Mauricio Rivera Mejía
Palabras Claves:	COMPUTACIÓN EN LA NUBE: Despliegue de recursos informáticos y consultados a través de redes públicas como el internet, los servicios varían dependiendo del proveedor. CLOUD PÚBLICO: Servicios ofrecidos por una empresa la cual alquila su infraestructura y son alcanzados a través de una red pública. FIREWALL: Este equipo realiza la inspección del tráfico entrante como saliente de una red y de acuerdo con sus políticas lo permite o restringe. WAF: Este dispositivo se encarga de realizar la protección de las aplicaciones web incluidas el top 10 de owasp.
Descripción:	La computación en la nube cada día tomas más relevancia para todas las organizaciones que buscan realizar despliegues de infraestructuras y servicios de forma escalable y sobre todo buscando que sea de manera rápida y efectiva, en algunas ocasiones por la flexibilidad y rapidez con la que son desplegados los servicios, no se siguen buenas prácticas de seguridad y se tiende a dejar la seguridad bajo la responsabilidad del proveedor de nube, esto ocasiona que los servicios sean vulnerables y pueden ser impactados por los ciberdelincuentes, causando perdida de datos, mala reputación de la organización y perdida de recursos económicos empleados para desplegar la infraestructura. Por lo anterior existen algunas premisas y conocimientos previos que se deben tener con

	el fin de proteger los datos y garantizar la seguridad de la infraestructura desplegada.
Fuentes bibliográficas destacadas: AMAZON WEB SERVICES. [Sitio Web]. AWS Shield. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/shield-chapter.html AMAZON WEB SERVICES. [Sitio Web]. AWS WAF. [Consulta: 16 de abril del 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/waf-chapter.html AMAZON WEB SERVICES. [Sitio Web]. Modelos de informática en la nube. [Consulta: 16 de abril del 2022]. Disponible en: https://aws.amazon.com/es/types-of-cloud-computing/ AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en: https://aws.amazon.com/es/compliance/shared-responsibility-model/ AMAZON WEB SERVICES. [Sitio Web]. Modelo de seguridad compartida. [Consulta: 16 de marzo 2022]. Disponible en: https://d1.awsstatic.com/security-center/Shared_Responsibility_Model_V2.59d1eccec334b366627e9295b304202faf7b899b.jpg	
Contenido del documento:	Este documento fue desarrollo por capítulos dentro de lo que se encuentra: Capítulo 1: Caracterización de los servicios de seguridad nativos con los que cuenta AWS para la protección de infraestructuras desplegadas en un modelo de implementación IaaS. Capítulo 2: Caracterización de los mecanismos disponibles para garantizar la seguridad de los datos que se encuentra en tránsito como en reposo. Capítulo 3: Pruebas de concepto donde están aplicadas buenas prácticas de seguridad para realizar el desplegué de infraestructuras tipo IaaS. Capítulo 4: De acuerdo con el framework de NIST, se describe el servicio utilizado en AWS para garantizar la protección del ciclo de vida de los usuarios.
Conceptos adquiridos:	Los proveedores de nube cuentan con los mecanismos necesarios para garantizar la seguridad de las infraestructuras desplegadas, pero los administradores de las plataformas son los encargados de afinar y aplicar cada una de estas herramientas.

Conclusiones:	Se realizó la descripción de los servicios de seguridad nativos con los que cuenta AWS, para proteger las plataformas que son desplegadas dentro de la nube, es importante tener en cuenta que la mayoría de estos mecanismos de protección se encuentran con configuraciones por defecto, por lo que se requiere ajustar y definir de acuerdo a las necesidades del negocio, adicionalmente se recomienda validar aquellos servicios que incurren en un costo adicional, el proveedor de nube tiene a disposición del cliente los mecanismos para la protección de la infraestructura pero el cliente es el que decide y es el responsable de la implementación y administración de estos, para garantizar la seguridad de la plataforma. Existen diferentes mecanismos orientados a la protección de los datos que se encuentran en tránsito como en reposo, sin importar cuál de los estos sea utilizado, la definición del proceso y los procedimientos, debe ser una de las primeras actividades a desarrollar por parte del grupo de TI, buscando garantizar el cumplimiento de los pilares de la seguridad de la información en cuanto a la confidencialidad e integridad de los datos se refiere, el proteger uno de los activos más importantes para una organización genera desafíos que van de la mano con la reputación y continuidad del negocio.