PRÁCTICAS SEGURAS EN LA INFRAESTRUCTURA TECNOLÓGICA EN UNA NUBE AMAZON WEB SERVICES

LUIS DAVID HURTADO CARDONA

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

PRÁCTICAS SEGURAS EN LA INFRAESTRUCTURA TECNOLÓGICA EN UNA NUBE AMAZON WEB SERVICES

LUIS DAVID HURTADO CARDONA

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

INGENIERO EDGAR ROBERTO DULCE

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

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

AGRADECIMIENTOS

Agradecimientos para mi familia y mi amada que me brindaron su apoyo, me alentaron a continuar y buscar avanzar con este proyecto y por los ánimos y ayuda que me dieron en momentos claves. También agradezco al director de trabajo Edgar por su constante colaboración, disposición y sugerencias que ayudaron a generar un producto de calidad en esta monografía, a los tutores por su aporte para lograr alcanzar la idea apropiada para este trabajo de grado, y a la Universidad Nacional Abierta y a Distancia por brindarme esta gran oportunidad de adquirir conocimientos sobre esta especialización tan crucial en la actualidad como lo es la seguridad informática.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

CIFRADO: “método de protección de datos que consiste en alterarlos hasta hacerlos ilegibles. Los datos pasan de ser texto sin formato a ser texto cifrado por medio de un método denominado algoritmo. Quien desee acceder a los datos cifrados debe descodificarlos primero con la clave de descifrado correcta.” [1]

CONFIGURACIÓN: conjunto de datos e información que establece el comportamiento y funcionamiento de una herramienta software o equipo de hardware. Dicha información puede encontrarse predeterminada de fábrica, o personalizarse según las necesidades del usuario.

DOCUMENTACIÓN: conjunto de archivos, documentos, manuales o textos que recopilan información correspondiente a procesos, procedimientos, pasos a seguir o prácticas que facilitan la comprensión de una actividad o configuración a realizar.

FIREWALL: sistema hardware o software diseñado para analizar, permitir y bloquear el tráfico de datos entre redes y computadores, basado en políticas y reglas configuradas.

IDENTIDAD: datos, información y activos que determinan que un usuario es quien dice ser dentro de un sistema.

INFRAESTRUCTURA TECNOLÓGICA: elementos necesarios para operar y gestionar entornos de TI empresariales. La infraestructura de TI puede implementarse en un sistema de cloud computing o en las instalaciones de la empresa. Estos elementos incluyen el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos. Todos ellos se utilizan para ofrecer servicios y soluciones de TI. [2]

INSTANCIA: “entorno informático virtual”[3] que viene preconfigurado para iniciar un conjunto de recursos necesarios a la hora de lanzar un servidor o equipo de cómputo en la nube.

---

[1] DEWITT, Derek [En línea]. Cifrado de datos: ¿en qué consiste? [Publicado: 22 de abril 2021]. [Consulta: 24 de septiembre 2022]. Disponible en: https://www.avast.com/es-es/c-encryption.

[2] RED HAT [En línea]. ¿Qué es la infraestructura de TI? [Publicado: 17 de junio 2019] [Consulta: 7 de marzo 2022]. Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure#:~:text=La%20infraestructura%20de%20la%20tecnolog%C3%ADa,las%20instalaciones%20de%20la%20empresa.

[3] AWS [En línea]. ¿Qué es Amazon EC2? [Consulta: 12 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html

MIGRACIÓN: “trasladar datos o software de un sistema a otro.”[4] Según el tipo de proyecto el traslado puede ser de datos, aplicaciones, sistemas operativos o cambio de infraestructura on-premise a infraestructura de nube.

POLITICA: decisiones diseñadas para adoptar acciones que puedan proteger la confidencialidad, integridad y disponibilidad de la información en un sistema.

PRÁCTICAS: conjunto de acciones y comportamientos que se realizan de manera repetitiva aplicando conocimientos previos al desempeñar una actividad determinada.

RECURSO: cualquier hardware, software, dato o equipo que es utilizado por un sistema de información, con capacidades limitadas y finitas.

SERVICIO: conjunto de actividades y acciones que son brindadas por un proveedor para satisfacer las necesidades de su cliente. En el ámbito de informática se brindan distintos servicios, desde personal especializado en áreas determinadas hasta prestación de infraestructura para realizar operaciones.

SERVIDOR: sistema encargado de brindar servicios, datos, recursos computacionales o programas a otras máquinas conectadas mediante una red.

VPN: Red Privada Virtual, una conexión protegida por medio de cifrado utilizando redes públicas para ocultar identidad y permitir comunicación segura entre equipos y redes internas.

VULNERABILIDAD: debilidades o falencias presentes en software o hardware debido a fallos, malas configuraciones o defectos técnicos que pueden ser aprovechadas para realizar ataques y comprometer sistemas.

[4] REDHAT [En línea]. La migración de la TI. [Publicado: 4 de febrero 2021]. [Consulta: 23 de septiembre 2022]. Disponible en: https://www.redhat.com/es/topics/automation/what-is-it-migration.

RESUMEN

En la presente monografía se tiene en cuenta la importancia que requiere el aseguramiento de las infraestructuras de nube, por lo que se analizan las recomendaciones y prácticas que brinda Amazon Web Services (AWS) desde su documentación para así configurar, implementar y ejecutar sus servicios con niveles más altos de seguridad.

Durante este análisis, se categorizan las prácticas de forma que su agrupación facilite la comprensión de su utilidad según cómo afectan los servicios contratados con Amazon Web Services, se realiza una labor para destacar las prácticas que mejor se adapten a necesidades generales de aseguramiento de activos informáticos de las organizaciones, al reunirlas según cómo qué pilar de la seguridad de la información afectan más. Luego de realizar esta labor de destacar las prácticas, se procede con el planteamiento de escenarios en los cuales éstas puedan aplicarse, partiendo de necesidades generales de las organizaciones y mostrando el antes y el después de implementar las prácticas de seguridad en la infraestructura tecnológica.

Tomando como insumo estos escenarios planteados, se realiza la evaluación de seguridad de cada caso basándose en algunos pasos de la metodología Architecture Tradeoff Analysis Method, con el fin de determinar cómo se vio afectada la seguridad de la infraestructura propuesta al aplicar las prácticas de seguridad destacadas y obtener una conclusión de si es efectivo o no aplicarlas.

Para finalizar, se obtienen las conclusiones sobre las labores de examinar las prácticas, el destacarlas, el planteamiento de escenarios y su evaluación, y las recomendaciones correspondientes según la experiencia obtenida durante la realización de estas actividades.

INTRODUCCIÓN

La tecnología con el pasar de los años y su evolución, se ha convertido en el soporte de sinnúmero de industrias y negocios. Contar con equipos de cómputo, aplicaciones, sistemas que permitan atender la demanda de parte de clientes y usuarios ha sido el enfoque principal de las organizaciones, si desean sobrevivir en el contexto actual.

Las infraestructuras tecnológicas cumplen un papel protagónico en este punto, ya que éstas son las encargadas de hacer que la magia ocurra. Brindar capacidades para las organizaciones puedan ofrecer al cliente servicios que antes debían hacerse de manera personal, soluciones al alcance de la mano y expandir el alcance a comunidades de clientes más amplias y alejadas de sus locaciones físicas, requiere para lograrse de poder de procesamiento, comunicaciones y almacenamiento de información.

Para lograr que las organizaciones puedan mantener su oferta, hace unos años se requería contar con distintos equipos de cómputo con capacidades superiores de procesamiento, almacenamiento y comunicación que confirmaban una infraestructura tecnología corporativa, la cual permitiera ofrecer servicios estables que atendieran las solicitudes de grandes cantidades de clientes. Sin embargo, la adquisición, configuración, gestión y mantenimiento de estas infraestructuras era (y sigue siendo) costosa, compleja y demandaba muchos recursos, tanto económicos como humanos, ya que, sin los conocimientos apropiados, la operación de los equipos de cómputo podría convertirse en un desastre y generar perdidas mayores para la organización.

Las cosas empezaron a cambiar para los años 2012 – 2014, en los que las grandes compañías tecnológicas (Google, Amazon, Microsoft) empezaron a ofrecer de manera más global servicios denominados como computación en la nube. Este concepto significó un cambio de paradigma para las infraestructuras tecnológicas, debido a que se pasó pensar que para que los servicios soportados por tecnología se necesitaban tener grandes servidores, sistemas de almacenamiento y redes internas enormes, a tener la idea de que ahora todos estos equipos de cómputo podrían ser utilizados de manera tercerizada, rentando según las necesidades del negocio, y su administración no dependería de la organización sino del proveedor. Los beneficios ofrecidos por los proveedores eran (y siguen siendo) bastante tentadores: reducción de costos en adquisición de sistemas de cómputo de gran capacidad y alto valor, disminución enorme en los esfuerzos para gestión y mantenimiento de la infraestructura, niveles de disponibilidad más altos, todo esto por un precio más accesible.

A partir de esos años se ha visto un crecimiento en la acogida de la computación en la nube para soportar las infraestructuras tecnológicas de las organizaciones. A tal punto que para 2022 muchas pymes surgen como organizaciones “cloud native”, es decir, nativas en nube. Todos los procesos tecnológicos que soportan sus servicios y operación son ejecutados en infraestructuras tecnológicas alojadas 100% en nubes públicas. Sin embargo, a pesar de la evolución, hay un elemento que sigue constante sin importar si la infraestructura es on-premise o en la nube: los datos e información son valiosos y hay que protegerlos, y siempre están en riesgo de ataque por actores maliciosos que quieren sacar provecho de estos.

A medida que la tecnología ha ido evolucionando, las maneras en que los atacantes buscan obtener beneficios de información o daños a organizaciones también lo han hecho. Para seguir el ritmo, los métodos de protección y practicas también han tenido que seguir evolucionando. Para cuando las infraestructuras eran on-premise, se requería de personal especializado que pudiera configurar servidores y equipos e implementar herramientas de seguridad para proteger los datos y procesos organizacionales soportados por tecnologías. Las buenas prácticas y recomendaciones de seguridad pueden encontrarse en distintas fuentes, de manera extensa y explicada.

Ahora que la mayoría de las infraestructuras se encuentran en la nube o buscan hacer su traslado en esta dirección, los atacantes han enfocado su atención a este sector para lograr perjudicar las organizaciones y aprovecharse de los datos que logren recuperar. Cada proveedor brinda distintas prácticas, configuraciones, herramientas y servicios para realizar los aseguramientos, pero está información tiende a ser algo densa y los clientes no logran aplicarla correctamente.

Partiendo de esta situación, se realizará una revisión documental de la información que brinda el proveedor de servicios de computación en nube Amazon Web Services, con el objetivo de brindar una herramienta para que las organizaciones y especialistas en seguridad puedan aprovechar, comprender y dar uso a las herramientas y configuraciones disponibles, logrando así mejorar la seguridad de las infraestructuras tecnológicas en situaciones corporativas generales que se dan de manera general al ejecutar procesos de negocio soportados en tecnología.

1. DEFINICIÓN DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo mejorar la seguridad informática en implementaciones de infraestructura de Tecnologías de Información en nube Amazon Web Services mediante la adopción buenas prácticas?

La evolución de las tecnologías de información se ha ido dando de manera acelerada y constante, logrando que las prácticas y formas de trabajar y dar apoyo a las organizaciones mediante infraestructura también cambien y se adapten a las novedades y ofertas actuales. Esta evolución ha marcado un punto de quiebre para el concepto de infraestructura de TI, pasando de tener en las instalaciones de las organizaciones equipos de cómputo de buenas capacidades para dar soporte a las necesidades tecnológicas, tales como servidores dedicados para aplicaciones de gestión, sistemas de almacenamiento compartido, switches y routers para canalizar las redes, entre otros tantos componentes necesarios para un funcionamiento correcto de los sistemas de tecnologías de información; a acceder a todos estos equipos por medio de páginas web, ya que todos los recursos necesarios ahora pueden ser encontrados en la nube.

Con cada vez más compañías se encuentran trasladando sus infraestructuras físicas a estos servicios de cómputo en la nube, ya sea nube pública o privada, cómo lo expone Flexera en su reporte “Flexera 2020 State of the Cloud Report”, donde se evidencia una adopción creciente se han desplazado también los riesgos y peligros que se presentaban en dichas infraestructuras a un ambiente que puede ser más accesible para atacantes, ya que se necesita tener internet para acceder a estos recursos. Malas prácticas en las configuraciones, despliegues inseguros de instancias o componentes, conexiones mal definidas; todas estas acciones ponen en riesgo la información de las compañías, y dicho riesgo lograría evolucionar a perdidas irreparables, daños críticos a la operación, peligro para personas de las que se tengan datos, entre otros posibles casos de afectación negativa a los actores involucrados con las organizaciones.

Las posibilidades de ataque, los métodos y herramientas para realizar dichos ataques han evolucionado y se han adaptado también al desarrollo de las tecnologías de información, por lo que protegerse es necesario si se quiere tener una confianza plena en las implementaciones de infraestructuras virtuales en nube.

2 JUSTIFICACIÓN

El desarrollo de esta monografía intenta presentar buenas prácticas para que los distintos actores que deben utilizar infraestructuras en la nube logren comprender y alcanzar niveles altos de aseguramiento de sus recursos y activos informáticos soportados en el proveedor Amazon Web Services.

Se espera facilitar el acceso a configuraciones seguras, logrando destacar las mejores de estas que pueden implementarse en situaciones corporativas que sueles darse de manera general en las organizaciones.

Con esto, se podrá disminuir riesgos de mala utilización de recursos computacionales, pérdida de información crítica o suplantación de identidades, traduciendo estos beneficios en costos operativos, de tiempo y otras malas consecuencias que podrían afectar gravemente a una organización.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar las prácticas de seguridad informática que ofrece Amazon Web Services para infraestructuras de TI en nube, mediante la revisión de la documentación oficial brindada por Amazon Web Services para establecer las mejores prácticas que deben implementarse en una infraestructura de TI en nube.

3.2 OBJETIVOS ESPECÍFICOS

Examinar la documentación oficial de AWS en búsqueda de las sugerencias y recomendaciones de seguridad al utilizar componentes de nube.

Destacar las configuraciones y prácticas adecuadas para aplicar en los componentes de nube más utilizados en infraestructuras de TI organizacionales en la nube.

Proponer escenarios de aplicación de las prácticas y configuraciones identificadas para facilitar la comprensión de la implementación de estas prácticas.

Evaluar los escenarios propuestos basados en una metodología de evaluación de arquitecturas, determinando así la efectividad de las practicas identificadas.

4 MARCO REFERNCIAL

4.1 MARCO CONCEPTUAL

La seguridad informática, elemento inherente a cualquier organización que soporte sus labores con tecnologías de información, es una necesidad y desafío que debe afrontarse desde distintas perspectivas requerimientos y prácticas para cumplir un objetivo específico: proteger los sistemas de información, abarcando todos los elementos que los componen. Asegurar infraestructura, software, hardware, canales de comunicación y equipos de almacenamiento de información es la tarea principal del personal encargado de seguridad, todo esto en busca de lograr proteger los tres principios básicos de la seguridad de la información:

- Integridad: la información se mantiene en el tiempo, sin que se agreguen o quiten partes que la comprometan.

- Confidencialidad: la información solo puede ser accedida y consultada por el personal que tenga los accesos y permisos correspondientes. Un tercero, sin los privilegios necesarios, no podrá acceder.

- Disponibilidad: la información debe estar a la mano de los usuarios en el momento que lo requieran.

Dentro de esta gran necesidad, los procesos de aseguramiento han ido evolucionando y adaptándose a las nuevas tecnologías y prácticas que han surgido con el tiempo. Tal es el caso de la infraestructura tecnológica.

La infraestructura tecnológica, que en años anteriores se definía como el conjunto de elementos hardware (servidores, routers, switches, estaciones de trabajo, cableado, sistemas de almacenamiento, entre otros) y software (programas, sistemas operativos, firmware, aplicaciones, entre otros) que requiere adquirir una empresa para ofrecer servicios y soluciones de TI, de forma que puedan soportar sus operaciones; pasó a dividirse en dos opciones debido al crecimiento de nuevas tendencias tecnológicas:

- Infraestructura on - premise: es el concepto típico de infraestructura mencionado anteriormente.
- Infraestructura cloud: contrato de servicios de infraestructura consumidos a través de internet ofrecido por proveedores, quienes se encargan de gestionar y realizar mantenimiento al hardware y sistemas base, para que el cliente solo deba preocuparse de la administración de recursos consumidos, instalación de componentes software requeridos y consumo de servicios según las necesidades. Se cobra con base a los recursos utilizados.

La infraestructura Cloud ha sido cada vez más asimilada por las organizaciones a nivel mundial, al ir descubriendo los beneficios y facilidades que trae adquirir estos servicios. Según el reporte “Flexera 2022 State of the Cloud Report”, los “heavy users”, organizaciones que soportan más del 25% de su carga de trabajo en servicios de nube, creció del 53% en 2020 al 63% en el 2022, demostrando como las organizaciones cada día se atreven más a aventurarse al mundo cloud. Además de esto, se presentó un crecimiento en la adopción de la nube del proveedor Amazon, conocida como AWS. Del 2020 al 2021 pasó de 77% al 79% de empresas que adoptaron sus servicios[5].

Con un crecimiento como este, la urgencia por proteger y asegurar la información y correcto funcionamiento en este nuevo modelo de infraestructura. La seguridad de infraestructura cloud se convierte en una necesidad que debe ser abordada adecuadamente por las organizaciones para proteger su bien más preciado: la información. Desplazar los conceptos y estrategias de aseguramiento conocidos en la seguridad on - premise a la infraestructura cloud es un requerimiento en el que las organizaciones deben confiar en las herramientas, tecnologías y controles brindados por los proveedores para cumplir el objetivo.

Para lograr esa migración, se sugiere tener en cuenta los tres principios de la seguridad cloud propuestos por Velev y Zlateva:[6]

- Seguridad de identidades: mantener la integridad y confidencialidad de los datos y aplicaciones mientras los usuarios correctos acceden a estos. Aumentar las capacidades de componentes para la gestión de identidades tanto para usuarios como infraestructura, teniendo en cuenta los requerimientos de autentificación más fuerte y autorización más rigurosa.
- Seguridad de información: los métodos de aseguramiento tradicionales usados en infraestructura on premise dejan de ser viables en cloud, ya que la virtualización hace que la información necesite su propio modelo de aseguramiento teniendo en cuenta los siguientes requerimientos:
    - Aislamiento de datos usando modelos y tecnologías existentes en cloud.
    - Asegurar los datos agregando controles a nivel de bloque, archivo o campo con el fin de que la información en nube no corra riesgos y se cumplan regulaciones.

5 FLEXERA [En línea]. 2022 State of the Cloud Report. 2022.[Consulta: 10 de marzo 2022]. Disponible en: https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2022.pdf?elqTrackId=414badd9b3cd4eee979d7f8bbfa8269e&elqaid=6925&elqat=2

6 VELEV Dimiter y ZLATEVA Plamena. Cloud Infraestructure Security. Sofia, Bulgaria: iNetSec, Publicado: marzo 2010. Hal Inria [Base de datos en línea]. Recuperado de: https://hal.inria.fr/hal-01581343/document el 11 de marzo 2022.

        - Clasificación efectiva de los datos basada en el conocimiento e identificación de la información que será almacenada, el lugar donde será almacenada y método de prevención de perdida de datos que serán implementados.
        - Gestión de los derechos sobre la información definiendo políticas estrictas de manipulación de información y fijando responsabilidades entre cliente y proveedor de servicios de infraestructura.
        - Validar que se pueda ejercer gobernanza y dar cumplimiento regulatorio tanto a nivel nacional e internacional aplicando controles y utilizando herramientas brindadas por el proveedor de servicios cloud.
    - Compromisos de seguridad entre los tres modelos de despliegue cloud: se comparten los compromisos de seguridad entre el cliente el proveedor, según el modelo que contrate para infraestructura de nube:
        - Software as a Service (SaaS): el consumidor tiene menos responsabilidad sobre la seguridad, ya que solo se debe encargar de asegurar la aplicación con buenas prácticas de código seguro. En cambio, el proveedor debe garantizar que el hardware, sistema operativo, ambiente y plataforma que soporta la aplicación tenga las medidas de seguridad suficientes.
        - Platform as a Service (PaaS): el consumidor adquiere más responsabilidad en las configuraciones de la plataforma contratada, debiendo tener ajustados los parámetros según las recomendaciones del proveedor. El proveedor debe encargarse del hardware y sistema operativo, integrando menos funciones de seguridad que en el primer caso.
        - Infraestructure as a Service (IaaS): el cliente cumple papel fundamental en el aseguramiento. En este caso el encargado de asegurar el sistema operativo, aplicaciones y datos que serán gestionados es el cliente, mientras que el proveedor se encarga del hardware e infraestructura de red.

Deben ser considerados estos principios para lograr un esquema de aseguramiento adecuado en infraestructura cloud. Partiendo de esta base, se realizará el análisis de las prácticas de seguridad de nube que se presentan actualmente para el proveedor AWS, ya qué, el cumplimiento de estos tres pilares será la forma correcta de evaluar la efectividad de estas prácticas.

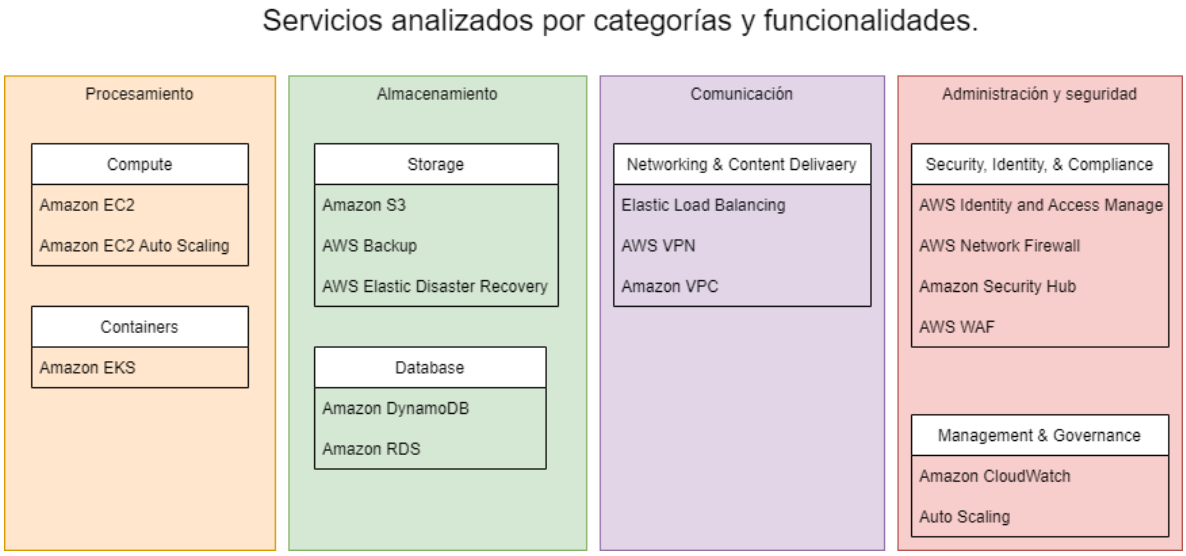
5 DESARROLLO DE LOS OBJETIVOS

5.1 EXAMINAR LA DOCUMENTACIÓN OFICIAL DE AWS EN BÚSQUEDA DE LAS SUGERENCIAS Y RECOMENDACIONES DE SEGURIDAD AL UTILIZAR COMPONENTES DE NUBE.

Siguiendo el planteamiento realizado en el objetivo, se inicia el desarrollo de la monografía examinando prácticas y configuraciones que brinda el proveedor AWS. Para esto, se ingresa en la documentación oficial, donde se encuentran las distintas categorías de su oferta al cliente.

Se propone un modelo basado en las funcionalidades, donde se agrupan las categorías de servicios que son utilizados en los entornos corporativos.

Figura 1. Modelo propuesto para análisis de servicios agrupados por funcionalidades.



Fuente: elaboración propia.

Siguiendo este modelo, se inicia la presentación de las prácticas examinadas, tomadas desde la Documentación oficial de Amazon Web Services, agrupando por la funcionalidad en la que fueron agrupadas, el servicio afectado por la practica en cuestión o el servicio utilizado para poner en marcha la práctica.

5.1.1 Procesamiento.

En esta funcionalidad fueron agrupados los recursos de procesamiento de datos e instrucciones en los que despliegan aplicaciones. Se empiezan a listar las prácticas identificadas:

- Configurar políticas de escalado automático de instancias: definir políticas y configurar instancias o grupos de instancias que, según una condición establecida, sean creados de manera automática para lograr procesar y responder en posibles casos donde aumente la demanda de transacciones a uno o varios servicios que sean ejecutados en la infraestructura.[7]

- Usar de manera predeterminada el inicio de sesión usando token temporal en los cluster Kubernetes: se sugiere usar el servicio AWS Security Token Service para la generación de tokens de acceso para las cuentas creadas usando el IAM, que son proporcionados de manera temporal mientras se tiene la conexión con el cluster de contenedores, y luego de finalizado el tiempo pierden vigencia estos tokens. [8]

- Aislar redes: utilizando la herramienta Virtual Private Cloud (VPC) se pueden crear redes virtuales dentro de un área específica, aisladas unas de otras a menos que se defina una conexión entre ellas. Dentro de las VPC se crean subredes que son usadas por instancias de otros componentes como EC2, buckets o motores de bases de datos, de manera que pueda aislarse a nivel de aplicación los componentes de infraestructura que interactúan entre sí para el funcionamiento correcto de una aplicación o servicio. Con esto se logra evitar accesos indeseados desde internet a dichos componentes.[9]

5.1.2 Almacenamiento.

En esta funcionalidad fueron agrupados los servicios destinados al almacenamiento datos y archivos, además de su interacción. Se empiezan a listar las prácticas identificadas:

- Creación de copias de seguridad: mediante la definición de planes de creación de copias de seguridad de manera automática programada cada cierto tiempo, o realización de labores manuales para generar las copias de seguridad. Estas copias se generan implementando el servicio AWS Backup. Con esto, se puede lograr un trabajo automatizado y ágil para responder de manera rápida ante ataques. [10]

---

[7] AWS. [Sitio web] ¿Qué es Amazon EC2 Auto Scaling? Consulta: 05 de mayo 2022. Disponible en: https://docs.aws.amazon.com/es_es/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html.

[8] AWS. [Sitio web] Seguridad de la infraestructura de Amazon EKS. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/eks/latest/userguide/infrastructure-security.html.

[9] AWS. [Sitio web]. Seguridad de la infraestructura en Amazon VPC. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/vpc/latest/userguide/infrastructure-security.html.

[10] AWS. [Sitio web]. AWS Backup: How it works. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/aws-backup/latest/devguide/how-it-works.html.

- Controlar acceso a buckets S3 usando enlaces de VPC: dentro de las VPC, existe un componente llamado Puntos de enlace que permite lanzar entidades S3 y comunica la VPC de manera directa con el bucket S3 para realizar cualquier acción dependiendo de los permisos que tenga el usuario al recurso S3 (carga de archivo, descarga, modificación, entre otros). Al usar el punto de enlace, solamente estará visible el bucket para la VPC que tenga definido el punto, bloqueando cualquier intento de acceso desde internet o de otra VPC que quiera acceder a este.[11]

- Bloquear acceso público a los buckets S3: los administradores de cuentas de AWS pueden definir controles de manera centralizada para todos los recursos, incluyendo bloquear el acceso público para todos los buckets S3 que se creen, sin importar el método usado para dicha creación.[12]

- Definir ACL para recursos S3: mediante la definición de ACL para cada bucket que se crea, se puede asignar permisos y recursos específicos a cada instancia creada facilitando la administración y prevención de accesos indebidos por usuarios no autorizados.[13]

- Cifrar información en tránsito o en reposo: mediante funciones brindadas por AWS como el cifrado usando una llave administrada por el proveedor o utilizar llave brindada por el cliente, se puede asegurar la información que es cargada en los buckets S3. Recomiendan también cargar la información ya cifrada desde los equipos on-premise del cliente, siempre y cuando la llave para el descifrado sea administrada de manera segura. Para el caso del cifrado en tránsito, se puede habilitar la opción de autorizar solo conexiones cifradas a través de HTTPS para el envío de información al configurar las políticas de los buckets.[14]

- Usar servicios de recuperación de desastres: dentro del portafolio de servicios, cuentan con Elastic Disaster Recovery (DRS), diseñado para minimizar tiempos fuera de operación y pérdida de datos. Se activa la función para crear réplicas de los servidores, aplicaciones basadas en nube o servicios que están corriendo en una región distinta, seleccionada por el cliente. Según las políticas, controles o disparadores definidos, se inicia el

[11] AWS. [Sitio web]. Prácticas recomendadas de control de acceso. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/access-control-best-practices.html.
[12] AWS. [Sitio web]. Bloquear el acceso público a su almacenamiento de Amazon S3. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html.
[13] AWS. [Sitio web]. Administración de acceso con ACL. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/acls.html
[14] AWS. [Sitio web]. Protección de datos mediante cifrado. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/UsingEncryption.html.

proceso de replicado de servidores en nuevas instancias o en instancias alternas ya corriendo en una nueva región.[15]

- Encriptar información en reposo de bases de datos NoSQL: tener información sensible almacenada en bases de datos siempre será una condición para estar en alerta de ataques. Para disminuir el riesgo de filtración de datos, el proveedor ofrece dentro de servicio DynamoDB para bases de datos NoSQL, la función de encriptado en reposo de la base de datos en la infraestructura de Amazon Web Services. EL servicio encripta toda la información usando llaves de encriptación, que son gestionadas por otro servicio para gestión de llaves llamado AWS Key Management Service. [16]

- Gestionar autenticación para acceder a bases de datos relacionales: se debe utilizar algún método de autenticación para conectarse a las bases de datos almacenadas en el servicio Amazon Relational Database Service (RDS). Sugieren implementar autenticación con contraseña, siempre y cuando la cantidad de usuarios que requieran conexión a la base de datos sea pequeña. En este caso la asignación de permisos y gestión de usuarios se realiza desde la base de datos. El otro método recomendado, y que más apoyo le brindan, es el de autenticación mediante el servicio IAM. Con este método, en vez de utilizar contraseñas para cada usuario, se ingresa mediante token de autenticación gestionados por IAM.[17]

- Encriptar bases de datos relacionales: similar a la encriptación de bases de datos NoSQL, en este caso se habilita la opción de encriptado al crear la base de datos y se utilizan llaves de encriptación gestionadas por AWS dentro del servicio Amazon Relational Database Service.[18]

5.1.3 Comunicación.

- En esta funcionalidad fueron agrupados los servicios usados para el intercambio, transmisión y flujo de datos, además de interacción entre servicios y comunicación con clientes externos. Se empiezan a listar las prácticas identificadas:

---

[15] AWS. [Sitio web]. Security in AWS Elastic Disaster Recovery. [Consulta: 06 de mayo 2022] Disponible en: https://docs.aws.amazon.com/es_es/drs/latest/userguide/security.html.

[16] AWS. [Sitio web]. Cifrado en reposo en DynamoDB. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/amazondynamodb/latest/developerguide/EncryptionAtRest.html.

[17] AWS. [Sitio web]. Autenticación de bases de datos con Amazon RDS. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/database-authentication.html.

[18] AWS. [Sitio web]. Cifrado de recursos de Amazon RDS. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

- Controlar el tráfico hacia los recursos mediante grupos de seguridad: dentro del componente de red conocido como VPC, se activa una clase de firewall virtual llamado grupo de seguridad. Este grupo controla el tráfico que entra y sale de una instancia de cómputo EC2, bloqueando o permitiendo el paso de paquetes con base a su protocolo, puerto usado o aplicación a la que se dirigen los paquetes.[19]

- Combinar grupos de seguridad con ACL: las listas de control de acceso (ACL por su sigla en inglés) con conjuntos de permisos asignados a un determinado recurso dentro de un sistema. Combinar los bloqueos a paquetes maliciosos que brindan los grupos de seguridad junto con la asignación de permisos de las ACL ayuda a disminuir las posibilidades de acceso a recursos de personal no autorizado.[20]

- Prácticas para AWS Client VPN: administrar las identidades, es decir, los usuarios que pueden conectarse y acceder a recursos de AWS a través de Client VPN, definir reglas de autorización para conceder o denegar conexiones o utilización de recursos específicos de la nube (creación de instancias, acceso a BD, uso de VPC, entre otros), lista de revocación de certificados del cliente para quitar los accesos a los endpoint según políticas diseñadas por el cliente (vencimiento cada cierto tiempo, remover acceso a personas que salen de la organización, entre otros) o utilizar herramientas de monitoreo para hacer seguimiento a la disponibilidad y rendimiento de los puntos de acceso de Client VPN.[21]

- Utilizar subredes públicas y privadas para despliegues de clusters de contenedores: para tener un cluster seguro, donde los contenedores estén aislados de la red pública y puedan procesar información y ejecutar funcionas sin ser visibles para externos, debe tenerse redes privadas definidas en la VPC. Para poder garantizar el acceso al cluster desde la red, se requiere que el balanceador de cargas requerido para el funcionamiento de los contenedores esté desplegado en una subred publica que se comunique con los contenedores dentro de la subred privada.[22]

---

[19] AWS. [Sitio web]. Amazon EC2 security groups for Linux instances. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html.

[20] AWS. [Sitio web]. Controlar el tráfico hacia los recursos mediante grupos de seguridad. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/vpc/latest/userguide/VPC_SecurityGroups.html.

[21] AWS. [Sitio web]. Prácticas recomendadas de seguridad para AWS Client VPN. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/vpn/latest/clientvpn-admin/security-best-practices.html.

[22] Ibid. Seguridad de la infraestructura de Amazon EKS. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/eks/latest/userguide/infrastructure-security.html.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: con el objetivo de asegurar la disponibilidad de los recursos informáticos y servicios desplegados en la nube de Amazon Web Services, se usa el balanceador de cargas, de manera que puedan distribuirse las cargas de trabajo de manera eficiente, se monitoree el estado de los recursos antes de enviar solicitudes y se pueda crear nuevas instancias de los recursos en caso que las capacidades actuales sean sobrepasadas por la demanda. [23]

5.1.4 Administración y seguridad.

- En esta funcionalidad fueron agrupados los recursos diseñados para administrar, asignar permisos, bloquear accesos, hacer monitoreo e iniciar procesos de escalado automático para mantener la disponibilidad. Se empiezan a listar las prácticas identificadas:

- Bloquear accesos usando IAM: definiendo de manera granular las políticas de acceso a recursos según los tipos de usuarios, de manera que pueda bloquearse accesos según la IP que hace la solicitud, el grupo de usuarios al que pertenece las credenciales, la API que realiza peticiones, entre otros; puede evitarse el uso no autorizado de recursos de AWS por usuarios autenticados y verificados.[24]

- Implementar políticas de mínimos privilegios: para cualquier recurso que se utilice dentro de la infraestructura contratada con AWS, se le debe asignar los mínimos privilegios posibles según el rol del usuario que deba interactuar dicho recurso. Utilizando IAM pueden definirse roles con permisos detallados para los recursos de manera que pueda administrarse fácilmente.[25]

- Revisar el estado de seguridad de la infraestructura: utilizando el servicio Security Hub, se realizan chequeos predefinidos, recolecta información y valida las configuraciones de toda la infraestructura AWS, desde la configuración de las cuentas hasta el estado de instancias y servicios en

[23] AWS. [Sitio web]. Seguridad en Elastic Load Balancing. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/userguide/security.html.
[24] AWS. [Sitio web]. Prácticas recomendadas de seguridad en IAM. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/IAM/latest/UserGuide/best-practices.html#grant-least-privilege.
[25] AWS. [Sitio web]. Prácticas recomendadas de seguridad en IAM. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

ejecución. Esta información es centralizada y correlacionada, de manera que se facilita su comprensión y administración en un solo módulo.[26]

- Configurar políticas de seguridad para usar AWS Firewall Network: utilizar políticas acordes a las necesidades del cliente para usar el servicio AWS Network Firewall para el filtrado de paquetes en tráfico dentro de las subredes públicas de la VPC. Los paquetes pueden ser filtrados basados en direcciones IP conocidas, instancias de otros servicios, crear listas de dominios sospechosos que los que se debe limitar o prohibir acceso o reconocer protocolos dentro de los paquetes para permitir el paso solo de los protocolos definidos por el usuario.[27]

- Configurar políticas de seguridad para usar AWS WAF: utilizar políticas que permitan proteger aplicaciones web de accesos no deseados o dañinos, mediante el servicio AWS Web Application Firewall. Este servicio monitoriza las solicitudes HTTP y HTTPS que ingresan a la red interna de las aplicaciones, y bloquea aquellos paquetes definidos como no deseados. [28]

- Monitorear recursos usando Amazon CloudWatch: con el objetivo hacer seguimiento al funcionamiento de los recursos, realizar acciones automáticas basadas en el estado de las instancias, e incluso ahorrar dinero, se usa el servicio Amazon CloudWatch. Al estar recopilando información de logs de las instancias, validando que se cumplan con métricas definidas por el usuario, este servicio puede notificar situaciones de alerta como caída de servicios o falta de espacio de almacenamiento, o por otra parte puede crear nuevas instancias para cumplir con las cargas de trabajo, e incluso eliminar instancias para ahorrar dinero con recursos infrautilizados.[29]

5.2 DESTACAR LAS CONFIGURACIONES Y PRÁCTICAS ADECUADAS PARA APLICAR EN LOS COMPONENTES DE NUBE MÁS UTILIZADOS EN INFRAESTRUCTURAS DE TI ORGANIZACIONALES EN LA NUBE.

Se plantea como estrategia que facilite la labor de destacar las configuraciones y prácticas de seguridad listados en el objetivo anterior, el tema de los pilares de la seguridad de la información o tríada CIA (por sus siglas en inglés): Confidencialidad, Integridad y Disponibilidad.

---

[26] AWS. [Sitio web]. ¿Qué es AWS Security Hub? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/securityhub/latest/userguide/what-is-securityhub.html

[27] AWS. [Sitio web]. Security in AWS Network Firewall. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/network-firewall/latest/developerguide/security.html.

[28] AWS. [Sitio web]. Seguridad en el uso del servicio AWS WAF. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/security.html.

[29] AWS. [Sitio web]. ¿Qué es Amazon CloudWatch? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html

La triada CIA es un modelo en la seguridad de la información que fue desarrollado con el pasar del tiempo, con el objetivo de guiar procedimientos y procesos que permitieran proteger los datos, activo más valioso de la organización[30].

Figura 2. Tríada CIA de seguridad de la información.

Fuente: https://miro.medium.com/max/640/1*8Nxb2G-ziTZ5nEswHtPhJA.webp

Estos tres elementos: Confidencialidad, Integridad y Disponibilidad han permitido el desarrollo de las tecnologías para asegurar la información basándose en cómo pueden verse afectados por ataques o controles débiles y qué hacer para solucionar estás debilidades.

Para destacar las configuraciones y buenas prácticas, se decide trabajar agrupando las buenas prácticas y configuraciones en cada uno de los pilares de la tríada. Además de esto, a cada práctica se le hace un análisis y se agregan referentes que soporten porque fue elegida en la agrupación de vulnerabilidades y como cumplen su tarea para proteger los datos relacionados con la práctica.

5.2.1 Confidencialidad.

Está relacionado con mantener los datos de las organizaciones privados. Esto significa que solo personal autorizado puede acceder a la información para procesarla o solo leerla. [31] Partiendo de esta premisa, se presentan de las prácticas

[30] SecurityScorecard. [Sitio web]. What is the CIA Triad? Definition, Importance, & Examples. [Publicado: 1 de septiembre 2021] [Consulta: 06 de diciembre 2022]. Disponible en: https://securityscorecard.com/blog/what-is-the-cia-triad.
[31] Ibid. Disponible en: https://securityscorecard.com/blog/what-is-the-cia-triad.

identificadas, todas las que apuntan a proteger la confidencialidad de la información en la infraestructura cloud:

- Controlar el tráfico hacia los recursos mediante grupos de seguridad: Bloquear intentos de acceso no deseado a los recursos adquiridos con AWS; evitando así intentos de robo de información o modificación de los sistemas en ejecución. Gracias a esta práctica se puede limitar el acceso a las instancias EC2 de manera efectiva. [32] La implementación de estos grupos, que en definitiva son firewalls, se convierte en la primera barrera de protección[33] para las instancias, debido a los bloqueos de paquetes ya mencionados que realiza.

- Combinar grupos de seguridad con ACL: Se sigue el mismo planteamiento anterior, solo que se utiliza para complementar la seguridad generada por los security groups, aplicando directamente los bloqueos a componentes específicos conectados a la VPC y limitando permisos a instancias o recursos específicos dentro de la infraestructura. Ya que bloquean el tráfico entrante o saliente, sirven para agregar una capa adicionar de seguridad a la infraestructura. [34] Brinda beneficios similares a los firewalls.

- Configurar políticas de seguridad para usar AWS Firewall Network: continuando con la línea conceptual de las dos prácticas anteriores, se logra evitar accesos a recursos disponibles mediante el bloqueo de peticiones basados en direcciones IP y protocolos. Se logra prevenir mal uso de los recursos por personal no autorizado. Aparte de esto, permite agregar una capa extra de protección a la red, que con el bloqueo de tráfico realizado por las dos prácticas anteriores limita a posibilidades aún más bajas que paquetes maliciosos logren ingresar a la VPC y afectar distintos servicios. Además, brinda versatilidad para cubrir un mayor rango de servicios prestados y utilizados de los que brinda el proveedor.[35]

- Prácticas para AWS Client VPN: con el uso de la herramienta que fue fundamental durante pandemia para soportar la operación remota, se vio el real valor que aportaba esta tecnología a la operación de las organizaciones.

---

[32] Mufti T, Pooja M y Gupta B. A review on Amazon Web services (AWS), Microsoft Azure & Google Cloud Platform (GCP). [Consulta. 16 de diciembre 2022]. Disponible en: https://eudl.eu/pdf/10.4108/eai.27-2-2020.2303255.

[33] Mora E. y Villero S. Importancia de la implementación de firewall en redes empresariales como mecanismo para la protección de información. [Publicado: 26 de julio 2019] [Consulta: 16 de diciembre 2022] http://revistas.uniguajira.edu.co/rev/index.php/cei/article/view/202/194

[34] AWS. [Sitio web]. Control traffic to subnets using Network ACLs. [Consulta. 16 de diciembre 2022]. Disponible en: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

[35] AWS. [Sitio web]. What is AWS Network Firewall? [Consulta. 16 de diciembre 2022]. Disponible en: https://docs.aws.amazon.com/es_es/network-firewall/latest/developerguide/what-is-aws-network-firewall.html.

Como mencionan Sharma y Kaur [36] en su artículo de 2020, es un método de protección de comunicaciones efectivo de bajo costo, que permite tener comunicaciones privadas a través de internet, no hay límites geográficos para su uso, y brinda un canal encriptado que protege los datos en transporte de ser accedidos o visualizados por atacantes o cibercriminales. Además, para el caso de recursos AWS se comporta igual, protegiendo de accesos no permitidos a las redes virtuales diseñadas en la infraestructura a personal sin acceso al canal protegido de comunicación.

- Bloquear accesos usando IAM: a pesar de que los accesos a los recursos se realicen desde cuentas autenticadas, no se puede asegurar que dichas cuentas no hayan sido robadas o estén comprometidas por atacantes o personal ajeno a la organización. Está configuración permite asegurar, hasta cierto punto, que los accesos son del personal interno, y que se hace desde equipos o direcciones conocidas y validadas con anterioridad, protegiendo la infraestructura de utilización indebida. Aparte de esto, limitar los accesos del personal de la organización exclusivamente a los recursos que necesita para cumplir sus labores, posibilita evitar uso indebido o manipulación de información que afecte los intereses de la organización. Este acceso definido a nivel granular de manera centralizada facilita la gestión de recursos e información[37], logrando evitar como se menciona que datos sean visualizados por personal que no corresponde.

- Implementar políticas de mínimos privilegios: está práctica es general, tanto para infraestructura de nube como para infraestructura on premise. De hecho, este principio lleva más de 45 años en la industria, propuesto por Jerome H. Saltzer y Michael D. Schroeder en 1975, en su publicación “The Protection of Information in Computer Systems”. Tal como exponen en su propuesta: “Cada programa y cada usuario del sistema debe operar utilizando el conjunto mínimo de privilegios necesarios para completar el trabajo”[38], con esto se evitan daños o malos usos de usuarios con altos privilegios, facilita la revisión de daños a los sistemas y permite identificar de manera rápida que usuario o que programa causó dichos daños.

[36] Sharma Y. y Kaur C. The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World. [Publicado: marzo 2020] [Consulta: 17 de diciembre 2022]. Disponible en https://www.researchgate.net/profile/Chamandeep-Kaur-3/publication/340336829_The_vital_role_of_VPN_in_making_secure_connection_over_internet_world/links/5e8440c24585150839b2d6eb/The-vital-role-of-VPN-in-making-secure-connection-over-internet-world.pdf.

[37] Mukherjee S. Benefits of AWS in Modern Cloud. [Consulta: 17 de diciembre 2022]. Disponible en: https://arxiv.org/ftp/arxiv/papers/1903/1903.03219.pdf.

[38] SALTZER Jerome y SCHROEDER Michael, The Protection of Information in Computer Systems, Massachusetts, Estados Unidos, 1975.

- Controlar acceso a buckets S3 usando enlaces de VPC: similar a la práctica anterior, el principal objetivo es evitar el acceso no deseado a los archivos, documentos o datos que se almacenen en las instancias de buckets S3. Evitar manipulación indebida o daños a los datos almacenados por personal no autorizado.

- Definir ACL para recursos S3: esta práctica va más enfocada a los accesos que son concedidos a los usuarios del servicio de almacenamiento. Definir quién puede modificar, leer o eliminar archivos según su cargo y tareas asignadas, y asignar los permisos correspondientes basados en esto garantiza que la información sea manipulada, en lo posible, según lo esperado por la organización. Está protección brindada por las ACL va de la mano con las políticas de mínimos privilegios y sus beneficios.

- Bloquear acceso público a los buckets S3: una configuración que debe ser prioritaria, ya qué no se quiere que toda la información quede abierta a que cualquier persona pueda revisarla, usarla o sacar provecho de esta. Habilitar esta opción es crucial en el proceso de aseguramiento de la infraestructura y protección de la información. Aprovechar las opciones que brinda el servicio, se logra evitar que personas ajenas a la organización puedan obtener datos privados, y estos bloqueos se pueden lograr de manera rápida siguiendo las guías que Amazon Web Services ponen a disposición de los clientes[39].

- Aislar redes: similar al bloque de acceso público a los buckets, debe protegerse las redes y evitar el acceso libre de cualquier persona a las mismas. Asegurar los servicios y programas que corren en la infraestructura, limitando las comunicaciones entre los recursos de manera que solo haya intercambio de datos entre instancias y componentes enviando los paquetes necesarios para su operación correcta.

- Gestionar autenticación para acceder a bases de datos relacionales: con esta práctica, se logra identificar al usuario que tendrá acceso a la base de datos, con permisos claramente definidos y asignados para que la manipulación de los datos se ajuste a las necesidades de la administración, y no se abuse de los privilegios para realizar operaciones maliciosas. Además, al tener autenticado el usuario, se limita el acceso al personal no autorizado que podría dañar los datos u obtener información sensible que podría afectar en el futuro la organización.

[39] AWS. [Sitio web]. Bloquear el acceso público a su almacenamiento de Amazon S3. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html.

- Usar de manera predeterminada el inicio de sesión usando token temporal en los cluster Kubernetes: para evitar que atacantes se apoderen de los recursos de cómputo que ofrecen los clusters de contenderos, es necesario que la conexión al recurso se dé mediante tokens de acceso brindados por la plataforma y gestionados por el administrador de la infraestructura. Con esto se identifica que el recurso que se comunica con los contenedores es una instancia autorizada, y puede intercambiar información sin riesgos.

- Utilizar subredes públicas y privadas para despliegues de clusters de contenedores: la comunicación entre instancias mediante la red debe ser gestionada, evitando que cualquier recurso pueda interactuar con otros sin necesidad. Separando en distintas subredes los balanceadores de los contenedores, se logra aislar lo suficiente la información y procesamiento de los contenedores de posibles atacantes que estén en busca de este activo.

5.2.2 Integridad.

Este pilar trata sobre que los datos deben ser confiables. Deben mantenerse en un estado correcto, sin ser manipulados, deben estar correctos y auténticos.[40] Las practicas identificadas que se encargan de proteger la integridad son:

- Cifrar información en tránsito o en reposo: con la implementación de esta configuración, se logra mantener la información a salvo, en un estado correcto sin modificaciones no deseadas. Aprovechando la libertad que brinda el proveedor para usar una llave propia que se gestione de manera propia, o sacando ventaja de la facilidad que es el brindar una llave al cliente, que será destinada exclusivamente para el cifrado de la información. Aparte de esto, obligar conexiones con HTTPS aumenta una capa más de protección a los datos, y hace que se pueda generar algo de confianza al enviar y recibir información.

- Revisar el estado de seguridad de la infraestructura: con la validación de configuraciones, monitoreo de estados y centralización de fuentes de datos de seguridad y estados, se logra evitar posibles daños a la información o instancias, al detectar a tiempo incidentes.

- Encriptar información en reposo de bases de datos NoSQL: se logra proteger los datos, activo de alto valor para una organización, mediante la encriptación usando llaves, ya sean gestionadas por el proveedor o administradas por el cliente. Tener datos que pueden ser manipulados de manera normal para la

[40] Securityscorecard [Sitio web]. What is the CIA Triad? Definition, Importance, & Examples. [Publicado: 1 de septiembre 2021] [Consulta: 06 de diciembre 2022]. Disponible en: https://securityscorecard.com/blog/what-is-the-cia-triad..

operación de la organización, pero se convierten en inútiles para atacantes que cuentan con las llaves de encriptación, reduce drásticamente riesgos en caso de que se materialicen filtraciones o robos de información.

- Encriptar bases de datos relacionales: similar a la práctica anterior, se logra proteger la información almacenada en la base de datos y contar con la habilidad de poder procesarla sin problemas. Además, los atacantes no podrán obtener valor de los datos encriptados en caso de que logren llegar hasta ellos.

5.2.3 Disponibilidad.

En este caso, se debe entender que los datos deben estar disponibles para que los usuarios autorizados puedan acceder a estos en cualquier momento que lo requieran. Para esto se requiere que los sistemas, redes y dispositivos se encuentren disponibles y corriendo apropiadamente.[41] Las practicas que fueron agrupada por proteger esta parte de la triada son:

- Creación de copias de seguridad: la prevención es crucial para recuperarse de siniestros, ya sean causados por ataques dirigidos o desastres naturales que afecten al proveedor. Por esto, tener copias de seguridad activas y actualizadas es la mejor manera de evitar pérdidas de datos y reactivar operaciones. Información crucial para la compañía, datos de los clientes necesarios para el funcionamiento adecuado de servicios, o incluso información financiera interna de la organización deben respaldarse y cuidarse con medidas estrictas.

- Usar servicios de recuperación de desastres: sacar ventaja de las funciones que brinda AWS para evitar estar fuera de operación facilita la protección de la disponibilidad de los servicios de la organización. Configurar la replicación automática de instancias y recursos para recuperar de manera pronta la operación afectada, posibilita que la operación se recupere rápidamente y los tiempos fuera de servicio sean bajos.

- Configurar políticas de seguridad para usar AWS WAF: al ser un firewall enfocado en las aplicaciones directamente, se logra evitar ataques y afectaciones a los servicios web que se alojan en la infraestructura de nube. Se evita que atacantes logren alcanzar aplicaciones con paquetes maliciosos, y logren obtener datos almacenados y gestionados por las

[41] Securityscorecard [Sitio web]. What is the CIA Triad? Definition, Importance, & Examples. [Publicado: 1 de septiembre 2021] [Consulta: 06 de diciembre 2022]. Disponible en: https://securityscorecard.com/blog/what-is-the-cia-triad.

aplicaciones desplegadas en los servicios o afectar la disponibilidad de estos servicios.[42]

- Configurar políticas de escalado automático de instancias: sumando prácticas de prevención, se debe planear que hacer con los momentos en que la operación tendrá picos o los servicios serán utilizados por una cantidad masiva de usuarios que supera la normalidad de la operación. Al aumentar recursos de manera preventiva en los momentos que se dé una subida en la operación, y solo aumentando los recursos necesarios, se logra evitar interrupciones.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: junto con la práctica anterior, deben tenerse medidas preventivas para atender los picos de uso de los recursos. Usando esta herramienta, se logra tomar medidas de manera rápida y automatizada para escalar recursos, monitorear estados validando el correcto funcionamiento, e incluso reducir recursos existentes innecesarios para evitar gastos monetarios no deseados. Con esto se logra reducir los tiempos fuera de servicio, ahorrar dinero y notificar novedades para acelerar tiempos de respuesta.

- Monitorear recursos usando Amazon CloudWatch: con un objetivo similar a la práctica anterior, pero dispuesta con un alcance más global en la infraestructura de nube que se implementa, al monitorear los recursos y definir métricas y políticas se puede crear nuevas instancias, eliminar instancias y notificar cualquier situación inesperada para reducir posibles ventanas de tiempo sin disponibilidad de los servicios o ahorrar dinero al no malgastar recursos sin uso.

5.3 PROPONER ESCENARIOS DE APLICACIÓN DE LAS PRÁCTICAS Y CONFIGURACIONES IDENTIFICADAS PARA FACILITAR LA COMPRENSIÓN DE LA IMPLEMENTACIÓN DE ÉSTAS.

Tomando como base el contexto corporativo en general, se plantean los siguientes escenarios hipotéticos de necesidades de las organizaciones, en los cuales se tendrá una versión sin asegurar para luego aplicar las prácticas destacadas en la sección 5.1 y clasificadas en la sección 5.2 y hacerlos seguros.

5.3.1 Acceso a archivos compartido.

Para este escenario, la necesidad de la organización es almacenar archivos de uso compartido en los distintos equipos de trabajo para ser accedidos desde internet.

[42] Rath A, Spasic B. Boucart N.y Thiran P. Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure. [Publicado: 3 de mayo 2019] [Consulta:16 de diciembre 2022]. Disponible en: https://www.mdpi.com/2073-431X/8/2/34

Estos archivos deben ser modificados, visualizados y descargados para uso en las labores diarias de la organización.

Para esta necesidad, se propone el uso del servicio Simple Storage Service (S3), creando buckets para cada área de la organización que lo requiere, y que estos buckets puedan ser accedidos desde internet por parte de los colaboradores. En el escenario se presentan dispositivos y servicios que estarán conectados para lograr el almacenamiento de archivos accesible desde internet:

- Teléfonos celulares corporativos: estos teléfonos le permiten la conexión a los archivos a los usuarios que estén en cualquier lugar, conectados desde internet y logrando así visualizar la información en el momento que lo requieran.

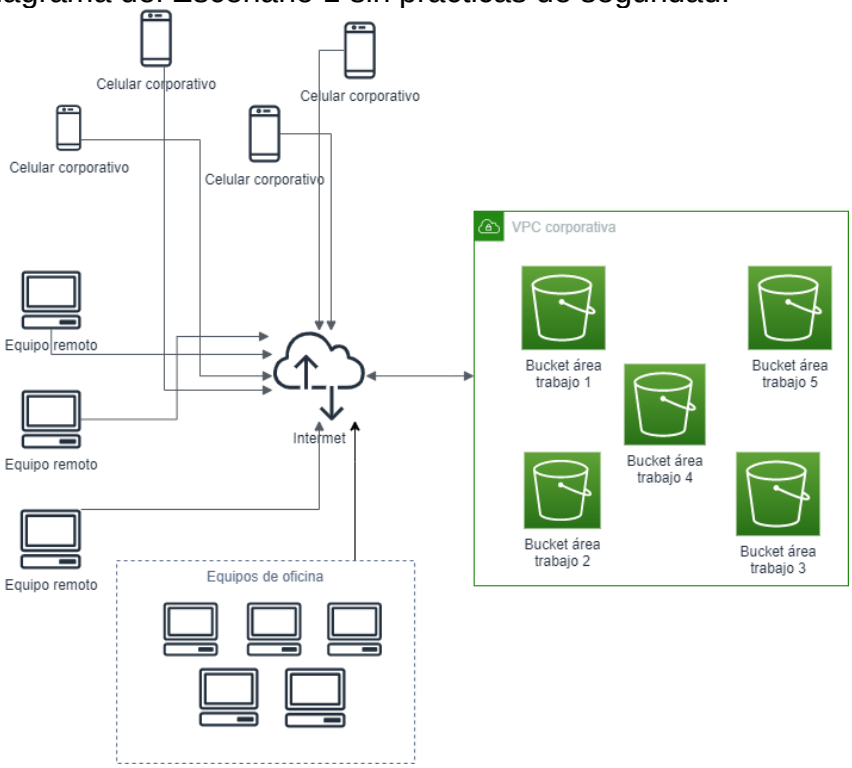
- Equipos remotos: computadores utilizados por el personal que trabaja en modo remoto, que no accede a la red de las instalaciones físicas de la organización. Para lograr visualizar y manipular la información, se conectan desde internet, cada uno en su casa o lugar donde desempeñe sus tareas.

- Equipos de oficina: computadores interesados por el personal desde las instalaciones físicas de la compañía. Se conectan a través de internet a los buckets para realizar las operaciones usando los datos almacenados.

- VPC corporativa: servicio principal de comunicación de los recursos provistos por Amazon Web Services. Por medio de este servicio los buckets son accesibles y pueden hacerse conexiones para utilizar los datos y archivos almacenados.

- Buckets: servicios de almacenamiento de objetos que brinda Amazon Web Servicios para alojar archivos que puedan ser accedidos desde internet. Con este recurso se logra el almacenamiento compartido al que los colaboradores puedan acceder y utilizar los archivos guardados.

Figura 3. Diagrama del Escenario 1 sin prácticas de seguridad.



Fuente: elaboración propia.

Analizando la propuesta inicial, se identifica un riesgo inmediato en la disposición de los buckets: pueden ser accedidos por cualquier persona desde internet que tenga el enlace del bucket. Esto puede derivar en filtración de datos, divulgación, pérdida e incluso eliminación de información de la organización que puede contener datos privados críticos. Agregado a esto, no hay privacidad para los datos. Cualquier colaborador puede investigar información de otras áreas, que en condiciones normales no debería ser accesible y podría provocar comportamientos dañinos en la operación.

Para proteger los datos, se implementan las practicas:

- Implementar políticas de mínimos privilegios: con esto se asegura la integridad de los datos almacenados, evitando modificaciones realizadas por colaboradores no autorizados.

- Bloquear acceso público a los buckets S3: se mitiga el riesgo principal que es el acceso de personas no relacionadas con la organización a información confidencial.

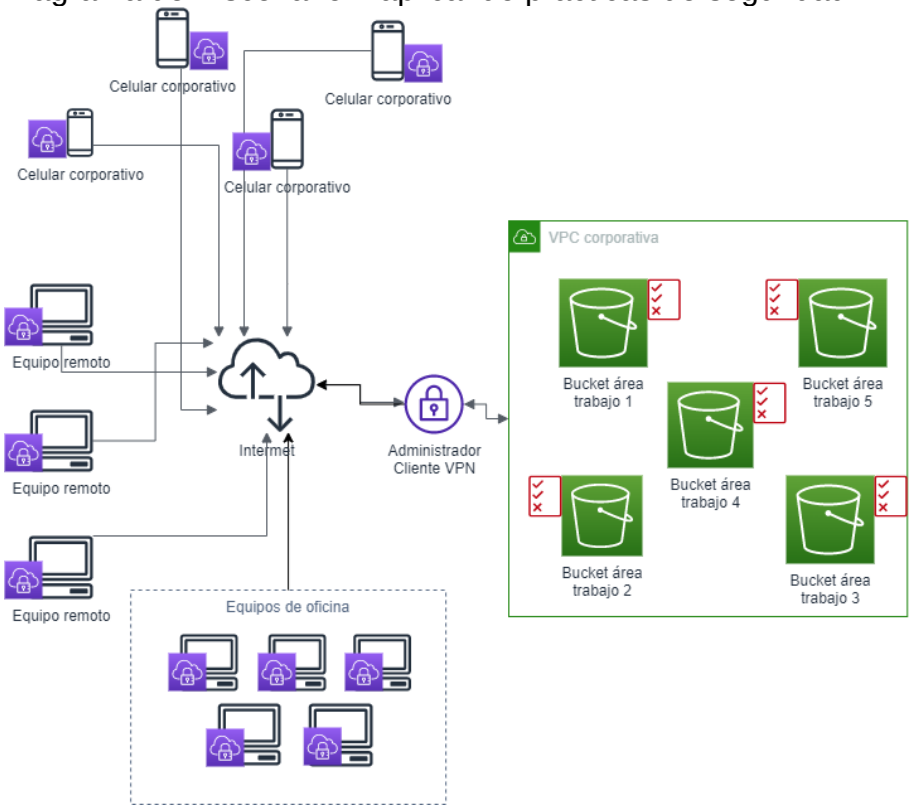
- Bloqueas accesos usando IAM: se controla los permisos de los colaboradores sobre los activos en la nube (en este caso los buckets) a los

que tienen permitido acceder. Además, con esta medida se evita el acceso a información que no es necesaria para desempeñar las tareas correspondientes.

- Definir ACL para recursos S3: con esta medida se logra controlar los permisos y privilegios que tienen los colaboradores sobre los buckets y los archivos dentro de estos. Este control está relacionado con la implementación de políticas de mínimos privilegios.

- Prácticas para AWS Client VPN: para asegurar que la persona que necesita acceder hace parte de la organización y su identidad es válida, se utiliza el servicio de VPN para validar sus credenciales y permitir conexión con los servicios de nube, para que así pueda adquirir acceso a la información almacenada y compartida.

Figura 4. Diagrama del Escenario 1 aplicando prácticas de seguridad.



Fuente: Elaboración propia.

5.3.2 Aplicación web con base de datos relacional.

En el escenario dos, la propuesta va enfocada en una necesidad de cualquier organización en la actualidad, que es utilizar un servicio web que almacene datos estructurados. Este tipo de aplicaciones las requieren por distintos motivos en sus tareas del día a día.

Se sugiere el uso de los servicios Elastic Compute Cloud (EC2) para crear la máquina que alojará el servidor web y Relational Database Service (RDS) para almacenar los datos.

Los recursos presentados en el escenario son:

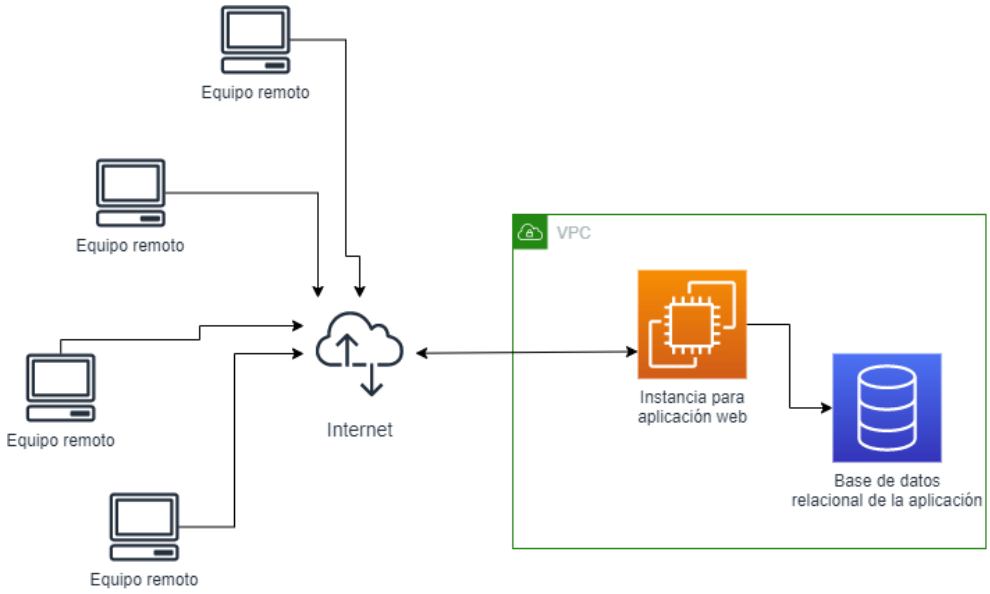
- Equipos remotos: computadores de usuario final, ya sea cliente o personal interno, que acceden a la aplicación desde internet.

- VPC: servicio principal de comunicación de los recursos provistos por Amazon Web Services. En este caso, mediante el servicio la aplicación puede recibir las peticiones de los usuarios desde internet.

- Instancia para aplicación web: servicio diseñado para ofrecer capacidades de computo a los clientes. En este escenario, la instancia permite la ejecución de la aplicación web.

- Base de datos relacional para la aplicación: servicio brindado por el proveedor de nube para almacenar y ejecutar bases de datos relacionales. En este caso, se almacena la base de datos con la información requerida por la aplicación web para funcionar y presentar a los usuarios.

Figura 5. Diagrama del Escenario 2 sin prácticas de seguridad.



Fuente: Elaboración propia.

Al analizar el escenario, se encuentran varios riesgos que deben ser atendidos: Similar al caso anterior, se encuentra accesible para cualquiera desde internet, sea

colaborador o no. No existen validaciones de identidades. No hay implementadas medidas para prevenir caídas del servicio, situación que podría afectar la operación. La base de datos podría ser atacada a través del servidor web, por ende, se corre el riesgo de filtración o pérdida de información. Por último, la red que comunica las instancias con internet no tiene contramedidas ante paquetes maliciosos.

Para mitigarlos, se usan las siguientes prácticas:

- Prácticas para AWS Client VPN: para asegurar que la persona que necesita acceder hace parte de la organización y su identidad es válida, se utiliza el servicio de VPN para validar sus credenciales y permitir conexión con los servicios de nube, específicamente para que pueda adquirir acceso a la aplicación.

- Configurar políticas de seguridad para usar AWS Firewall Network: como segunda capa preventiva, se usa el Firewall para descartar paquetes y peticiones desde direcciones no reconocidas como seguras, además de evitar paquetes maliciosos de usuarios maliciosos que hubieran podido obtener credenciales validas.

- Configurar políticas de seguridad para usar AWS WAF: control complementario de los dos anteriores, en busca de depurar lo mejor posible los paquetes y peticiones que recibe la aplicación web, minimizando en gran nivel riesgos de ataques.

- Implementar políticas de mínimos privilegios: asegurar que el acceso de los usuarios verificados sea el necesario para evitar que un mal uso de la aplicación o del acceso a las instancias provoque daños en el sistema.

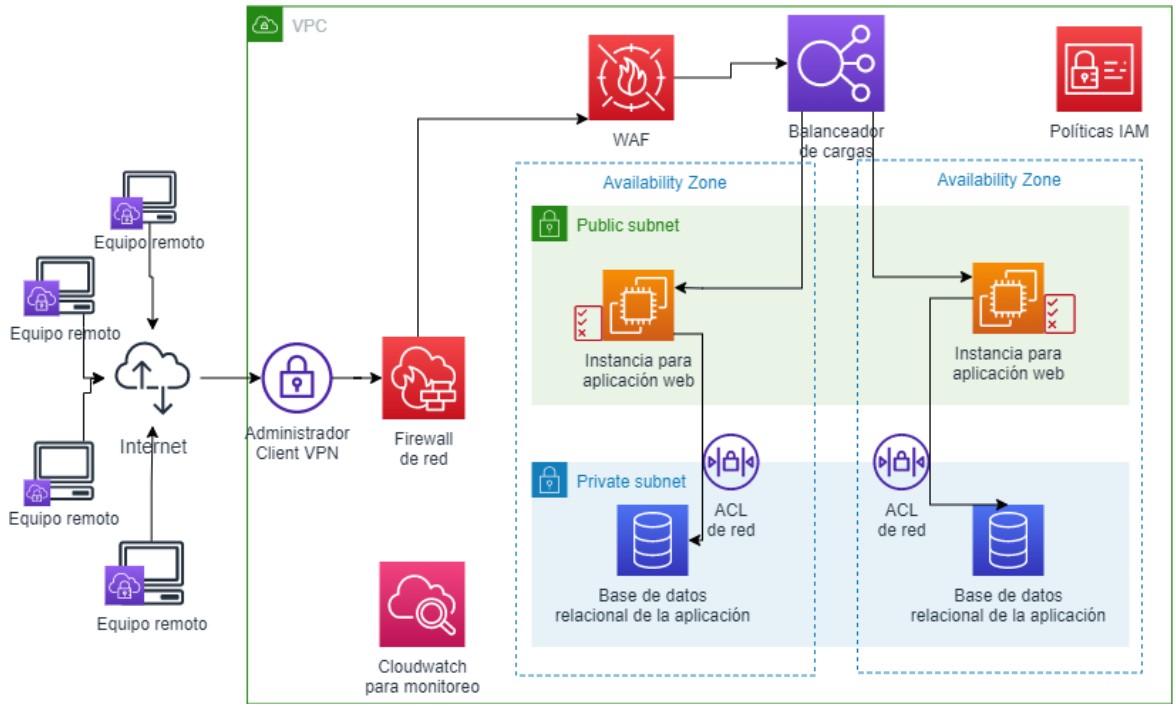
- Combinar grupos de seguridad con ACL: se complementa con la práctica anterior para asegurar el acceso mínimo necesario para que los usuarios puedan cumplir con sus tareas al usar la aplicación. Además, se definen también ACL de red para permitir la comunicación entre servidor y base de datos, esto con el objetivo de limitar posibles accesos a la información desde otros recursos disponibles en la infraestructura implementada.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: con el objetivo de mantener disponible la aplicación, se utiliza el balanceador para distribuir las cargas de manera apropiada en las instancias, evitando caídas y tiempos muertos.

- Monitorear recursos usando Amazon CloudWatch: otra práctica que sirve para apoyar las medidas ante el aseguramiento de la disponibilidad. Este

control permite notificar novedades, crear más instancias de ser necesario, y trabaja de la mano con el balanceador de carga.

Figura 6. Diagrama del Escenario 2 aplicando prácticas de seguridad.



Fuente: Elaboración propia.

5.3.3 Aplicación web con base de datos no relacional.

Para este escenario, la propuesta va enfocada que una organización requiere desplegar una aplicación con datos no estructurados y que deben ser almacenados y leídos a gran velocidad, agregando que tendrá una tasa de crecimiento rápida. Esta vez la aplicación va dirigida al público en general, no solamente a clientes internos.

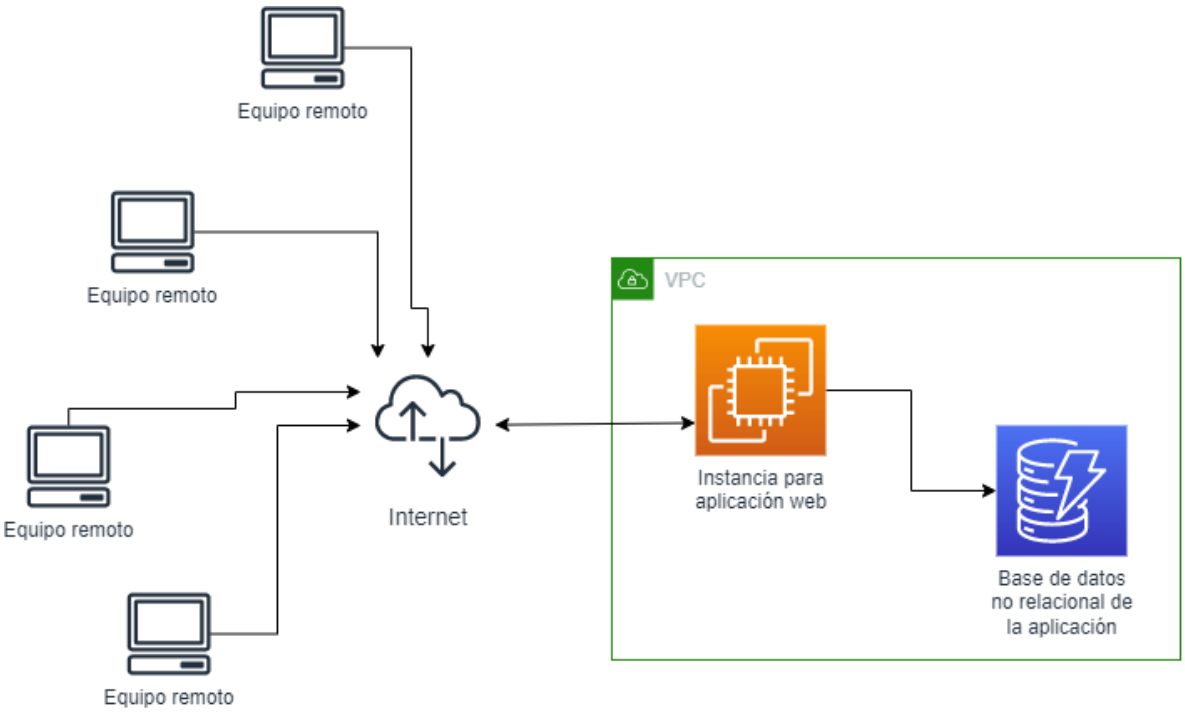
Se sugiere el uso de los servicios Elastic Compute Cloud (EC2) para crear la máquina que alojará el servidor web y DynamoDB para almacenar los datos. Los recursos utilizados en este escenario son muy similares al anterior:

- Equipos remotos: computadores de usuario final, ya sea cliente o personal interno, que acceden a la aplicación desde internet.

- VPC: servicio principal de comunicación de los recursos provistos por Amazon Web Services. En este caso, mediante el servicio la aplicación puede recibir las peticiones de los usuarios desde internet.

- Instancia para aplicación web: servicio diseñado para ofrecer capacidades de cómputo a los clientes. En este escenario, la instancia permite la ejecución de la aplicación web.
- Base de datos no relacional para la aplicación: servicio brindado por el proveedor de nube para almacenar y ejecutar bases de datos, pero en este caso no relacionales. Para el escenario, almacena la base de datos que necesita la aplicación web.

Figura 7. Diagrama del Escenario 3 sin prácticas de seguridad.



Fuente: elaboración propia.

Este escenario es bastante similar al anterior, aunque cambia el tipo de usuario a quien va dirigido. Sin embargo, se encuentran riesgos para ser revisados: aunque debe estar accesible para cualquiera desde internet, hay que prevenir ataques desde direcciones IP que se conocen como maliciosas. No hay implementadas medidas para prevenir caídas del servicio, situación que podría afectar a todos los usuarios y afectar la reputación de la organización. La base de datos podría ser atacada a través del servidor web, por ende, se corre el riesgo de filtración o pérdida de información.

Para mitigarlos, se proponen las siguientes prácticas:

- Configurar políticas de seguridad para usar AWS Firewall Network: practica primordial, más cuando el servicio está disponible a cualquier usuario. En este caso, se usa el Firewall para descartar paquetes y peticiones desde

direcciones reconocidas como no seguras, basados en herramientas como blacklist disponibles en internet. Además, se logra evitar el ingreso de paquetes maliciosos de atacantes.

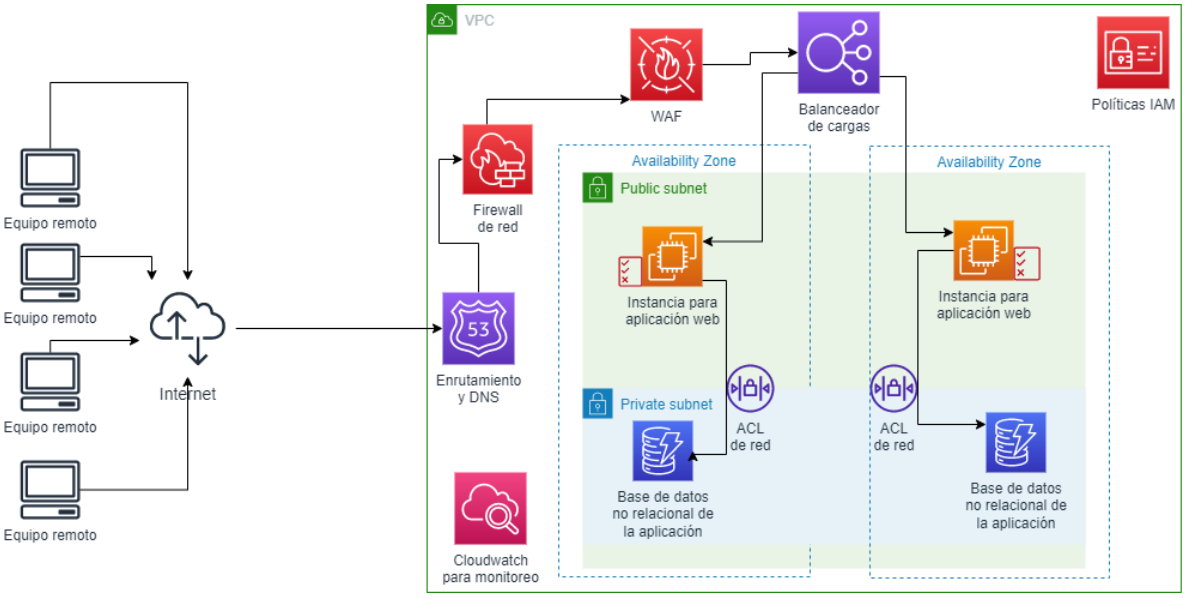
- Configurar políticas de seguridad para usar AWS WAF: control complementario del anterior, en busca de depurar lo mejor posible los paquetes y peticiones que recibe la aplicación web, minimizando en gran nivel riesgos de ataques.

- Implementar políticas de mínimos privilegios: asegurar que los privilegios de los usuarios sean los mínimos necesarios para evitar abuso que pueda afectar a la aplicación o del acceso a las instancias provoque daños en el sistema.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: para mantener disponible la aplicación, se utiliza el balanceador para distribuir las cargas de manera apropiada en las instancias, evitando caídas y tiempos muertos. Herramienta que cobra mayor importancia al estar disponible de manera abierta para usuarios en internet.

- Monitorear recursos usando Amazon CloudWatch: práctica de apoyo para asegurar la disponibilidad. Este control permite notificar novedades, crear más instancias de ser necesario, y trabaja de la mano con el balanceador de carga.

Figura 8. Diagrama del Escenario 3 aplicando prácticas de seguridad.



Fuente: elaboración propia.

5.3.4 Servicio de intranet.

Las organizaciones requieren compartir información que solamente le incumbe a personal interno, por lo que las intranets son la mejor opción para hacer llegar estos contenidos sin involucrar terceros externos.

En este escenario, se sugiere desplegar una intranet separando los servidores front-end y back-end en dos instancias de EC2, además de conectarse con una base de datos relacional y un bucket de S3 para almacenar contenido multimedia que será presentado en la intranet.

Los componentes presentados para este caso son:

- Equipos corporativos: computadores del personal interno que acceden a la aplicación desde internet, desde las instalaciones físicas de la compañía.

- VPC: servicio principal de comunicación de los recursos provistos por Amazon Web Services. En este caso, mediante el servicio la aplicación puede recibir las peticiones de los usuarios desde internet y para permitir la comunicación entre los distintos componentes utilizados para que la intranet sea accesible.

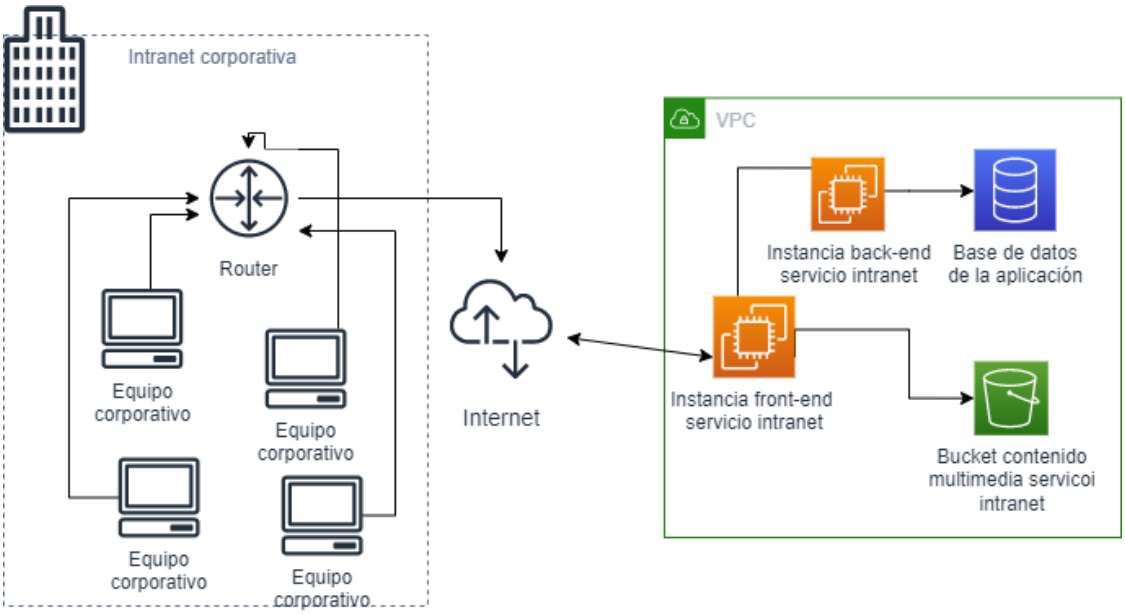
- Instancia para front-end: servicio diseñado para ofrecer capacidades de cómputo a los clientes. En este escenario, la instancia permite que el servicio front-end esté disponible para el acceso del personal de la compañía.

- Instancia para back-end: la instancia permite que el servicio back-end esté disponible, y los datos almacenados y procesados sean visibles por parte de la instancia del front-end.

- Base de datos de la aplicación: en este caso, se utiliza el servicio para ejecutar una base de datos que permita almacenar y procesar datos mostrados en la intranet

- Bucket de contenido multimedia: la instancia del front-end requiere imágenes, vídeos y audios para mostrar al personal que accede a la intranet. Este contenido multimedia lo carga desde los archivos almacenados en este bucket

Figura 9. Diagrama del Escenario 4 sin prácticas de seguridad.



Fuente: elaboración propia.

La confidencialidad del sitio es muy baja, ya que el servidor se encuentra disponible desde internet y accesible para cualquiera. No se tienen medidas para asegurar la disponibilidad de los servidores. La base de datos se encuentra en la misma red del servidor, por lo que podría recibir conexiones externas, misma situación que sucede con el bucket. Además, el bucket tiene acceso desde la red, exponiendo el contenido multimedia.

Para asegurar el escenario, se sugieren las practicas:

- Prácticas para AWS Client VPN: se asegura que solo usuarios pertenecientes a la organización puedan visualizar la información mediante el uso de la VPN. Se validan sus credenciales para que pueda tener acceso a la intranet.

- Configurar políticas de seguridad para usar AWS Firewall Network: se usa el Firewall para descartar paquetes y peticiones desde direcciones no pertenecientes a la organización. También se usa para bloquear paquetes maliciosos que puedan ser enviados por un atacante interno.

- Implementar políticas de mínimos privilegios: asegurar que el acceso de los usuarios internos verificados sea el necesario para lograr acceder a intranet y visualizar o interactuar con la información, para evitar ajustes que afecten el funcionamiento correcto del servicio.

- Combinar grupos de seguridad con ACL: se complementa con la práctica anterior para asegurar el acceso mínimo necesario a los recursos. Además, se definen también ACL de red para permitir la comunicación entre los servidores back y front, la base de datos y el bucket con el contenido multimedia necesario.

- Definir ACL para recursos S3: limitar el acceso a los archivos y acciones sobre estos, para evitar perdida de información o manipulación indebida. Además, con esto se restringe a que solo el servidor back pueda acceder al bucket.

- Bloquear acceso público a los buckets S3: crucial para que no se pueda visualizar los archivos y datos almacenados por cualquier tercero. Complementa la practica anterior al evitar accesos distintos al servidor del back-end.

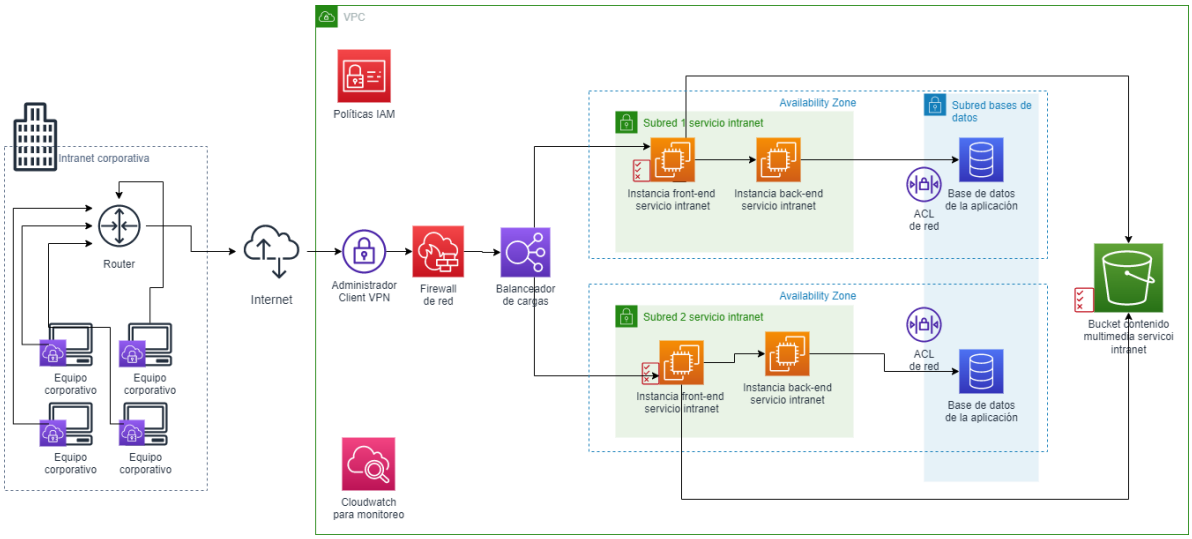
- Controlar acceso a buckets S3 usando enlaces de VPC: control diseñado para restringir el acceso a los buckets a solo las instancias o servicios designados. En este caso, permitiendo que solo el servidor front-end pueda comunicarse con el bucket.

- Aislar redes: segmentar las redes para que la comunicación entre recursos sea acorde a su funcionamiento, y no haya personal que pueda tener contacto con la información almacenada o el servicio desplegado.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: con el objetivo de mantener la intranet operativa, se utiliza el balanceador para distribuir las cargas de manera apropiada en las instancias, evitando caídas y tiempos muertos. Aunque la carga es menor a otros casos, al tenerla distribuida se evita afectar la operación de la organización por indisponibilidad.

- Monitorear recursos usando Amazon CloudWatch: Este control permite notificar novedades, crear más instancias de ser necesario, y trabaja de la mano con el balanceador de carga.

Figura 10. Diagrama del Escenario 4 aplicando prácticas de seguridad.



Fuente: elaboración propia.

5.3.5 Aplicaciones desarrolladas en contenedores.

Escenario planteado para aplicaciones diseñadas en el modelo de microservicios, que requieren ser gestionadas para su ejecución correcta.

Este escenario plantea usar el servicio Elastic Kubernetes Service para la gestión y ejecución de contenedores, además de Elastic Load Balancing como elemento necesario para el balanceo de cargas de los contenedores.

Los componentes propuestos en el caso son:

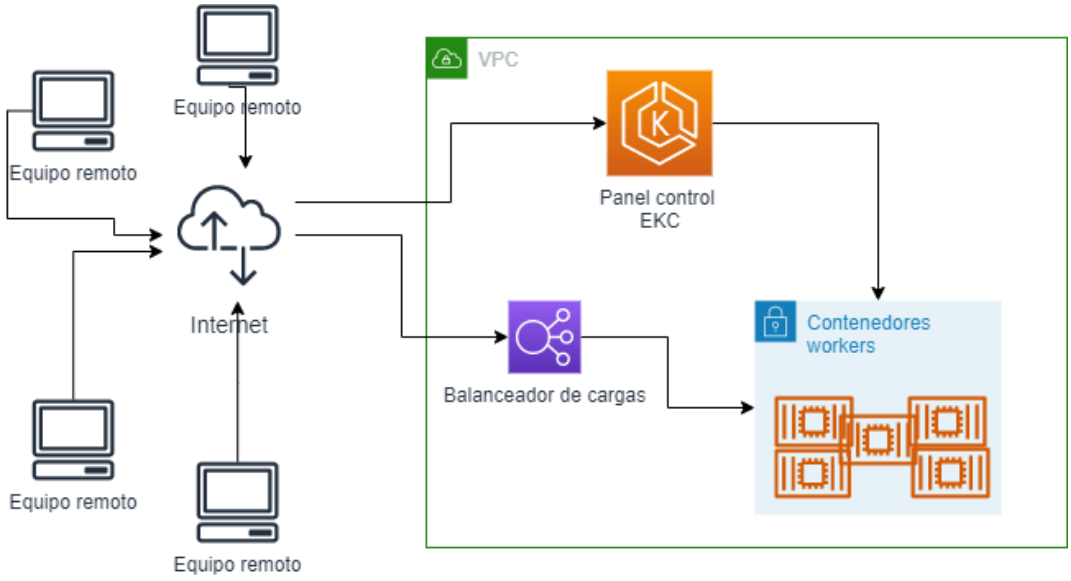
- Equipos remotos: computadores de usuario final, ya sea cliente o personal interno, que acceden a la aplicación desde internet.

- Balanceador de cargas: servicio brindado por Amazon Web Services para distribuir las peticiones y cargas de trabajas en instancias de cómputo. Para este caso en particular, la distribución la hace en los contenedores en ejecución.

- Panel de control EKC: herramienta para la administración del clúster de contenedores desplegados. Permite conocer el estado actual de cada contendor, cambiar su estado y otras tareas de gestión. Es requerido para lograr una implementación del servicio de contenedores.

- Clúster de contenedores: conjunto de contenedores desplegados para la ejecución de un servicio. En este escenario, en el clúster se despliega la aplicación que fue desarrollada para ser ejecutada en esta tecnología.

Figura 11. Diagrama del Escenario 5 sin prácticas de seguridad.



Fuente: elaboración propia.

Analizando el escenario, se encuentran distintas situaciones de riesgo: sigue el patrón de acceso sin restricciones de usuario, tanto al orquestador de contenedores como al servicio. Hay riesgo de afectar la disponibilidad de los servicios, además de poder usar la aplicación para recopilar datos y causar fugaz que pueden afectar la organización.

Teniendo en cuenta esto, se sugieren las practicas:

- Prácticas para AWS Client VPN: se asegura que solo usuarios pertenecientes a la organización puedan administrar el panel de control de los contenedores, para así realizar cualquier actividad necesaria para el correcto funcionamiento, y evitando que externos puedan manipular el servicio.

- Configurar políticas de seguridad para usar AWS Firewall Network: se usa el Firewall para descartar paquetes y peticiones desde direcciones identificadas como maliciosas. También se usa para bloquear paquetes dañinos que puedan ser enviados por un atacante.

- Implementar políticas de mínimos privilegios: asegurar que el acceso de los usuarios que deben gestionar los contenedores sea el mínimo necesario, evitando así que por mala manipulación afecten la disponibilidad del servicio o editar los datos almacenados y utilizados.

- Combinar grupos de seguridad con ACL: se complementa con la práctica anterior para evitar que los administradores afecten otros recursos que no deben manipular.

- Definir ACL para recursos S3: limitar el acceso a los archivos y acciones sobre estos, para evitar perdida de información o manipulación indebida. Además, con esto se restringe a que solo a los contendores puedan acceder al bucket.

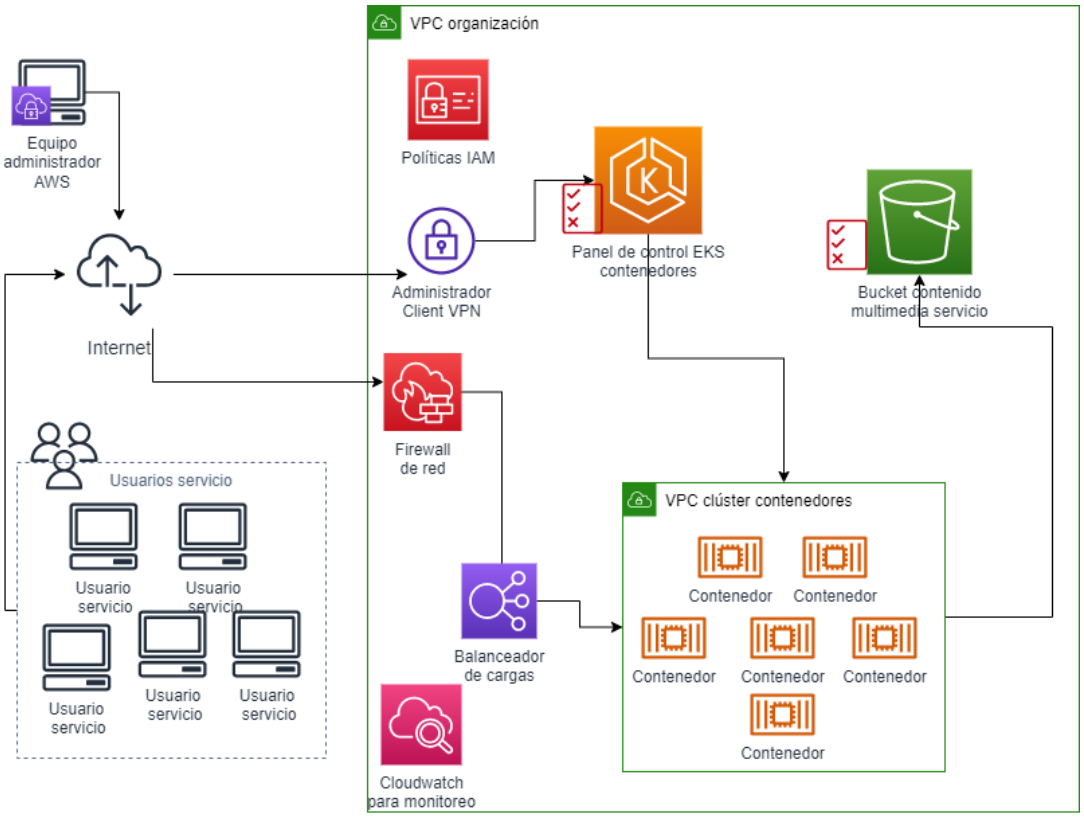
- Bloquear acceso público a los buckets S3: crucial para que no se pueda visualizar los archivos y datos almacenados por cualquier tercero.

- Controlar acceso a buckets S3 usando enlaces de VPC: control diseñado para restringir el acceso a los buckets a solo los contenedores que lo requieran.

- Utilizar Elastic Load Balancing para distribución de carga en distintos recursos: se utiliza el balanceador para distribuir las cargas de manera apropiada en los contenedores. Distribuir cargas, crear nuevos contenedores o eliminar los que no se usen son las tareas del balanceador. Esto para favorecer la disponibilidad.

- Monitorear recursos usando Amazon CloudWatch: monitorear el servicio.

Figura 12. Diagrama del Escenario 5 aplicando prácticas de seguridad.



Fuente: elaboración propia.

5.4 EVALUAR LOS ESCENARIOS PROPUESTOS BASADOS EN UNA METODOLOGÍA DE EVALUACIÓN DE ARQUITECTURAS, DETERMINANDO ASÍ LA EFECTIVIDAD DE LAS PRACTICAS IDENTIFICADAS.

Para evaluar los escenarios propuestos, se toman varios pasos como base de la metodología de evaluación de arquitecturas Architecture Tradeoff Analysis Method (ATAM), Método de Análisis de Acuerdos de Arquitectura. Este método propuesto por el Software Engineering Institute[43] tiene "el propósito de evaluar las consecuencias de las decisiones arquitectónicas en relación con determinados atributos de calidad definidos." También permite identificar riesgos potenciales dentro de las arquitecturas de software que plantean los equipos de arquitectura, pensado para realizarse al inicio de los ciclos de desarrollo de software.[44]

[43] Universidad Politécnica de Valencia. Introducción a ATAM. [Publicado: 26 de agosto 2016] [Consulta: 18 de diciembre 2022]. Disponible en: https://silo.tips/download/calidad-de-software-cso-practica-2-calidad-de-arquitecturas-software-introduccio.

[44] González Rodrigo, *et al*. Arquitectura de Software, Análisis de ATAM. [Consulta: 18 de diciembre 2022]. Disponible en: https://www.studocu.com/cl/document/universidad-metropolitana-de-ciencias-

Al ser una metodología planteada para la evaluación riesgos presentes en las decisiones de arquitecturas, se ajusta de buena manera para la evaluación de los escenarios propuestos, donde se requiere validar que tan seguros pasan a ser los escenarios luego de la implementación de las prácticas de seguridad, que vendrían siendo decisiones de arquitectura para los servicios desplegados.

Aunque los beneficios obtenidos de la implementación de ATAM pueden aprovecharse mejor por organizaciones, ya que permite filtrar mejor los requisitos de calidad definidos por los interesados de la organización en el servicio a desplegar en una infraestructura, ayuda a fomentar la comunicación entre los interesados, aunque desarrollen sus actividades en distintos contextos y áreas y permite mejorar los diseños de arquitectura de los servicios[45], para la evaluación de escenarios en esta monografía permite reducir tiempo al aprovechar que con el planteamiento de mejoras se ha realizado una fase de la metodología, presentar consecuencias antes los cambios realizados al aplicar las prácticas y analizar las mejoras en seguridad obtenidas. Con esto se logra una propuesta de evaluación que brinda herramientas adaptables a cualquier tipo de organización que utiliza servicios de nube para su infraestructura, con casos similares a los presentados en el desarrollo del objetivo anterior.

De los ocho pasos que propone la metodología, se van a utilizar cuatro, los cuales se aplican mejor al caso ya qué son independientes del contexto organizacional y van más dirigidos a la arquitectura que es analizada, pueden aplicarse de manera teórica a los casos sin necesidad de implementación funcional real y no requieren más actores externos que entreguen opiniones o necesidades extras. Los pasos son los siguientes:

- Presentar la arquitectura: para esta actividad, se presenta la arquitectura haciendo énfasis en como aborda objetivos de negocio[46]. En el desarrollo del objetivo tres se realizó este paso al momento de plantear cada escenario de manera inicial, antes de implementar las practicas. Aunque en la definición de esta acción en la metodología la parte principal es como se abordan los objetivos de negocio, se ajusta esa parte al exponer en el escenario la necesidad de la organización para implementar el servicio.

- Identificar los enfoques arquitectónicos: se presentan enfoques arquitectónicos distintos para cada arquitectura de manera que se logre el

de-la-educacion/adaptacion-de-la-planificacion/metodologia-atam-metodo-de-analisis-de-acuerdos-de-arquitectura/21857035

[45] Ibid. Disponible en: https://www.studocu.com/cl/document/universidad-metropolitana-de-ciencias-de-la-educacion/adaptacion-de-la-planificacion/metodologia-atam-metodo-de-analisis-de-acuerdos-de-arquitectura/21857035

[46] Universidad Politécnica de Valencia. Introducción a ATAM. [Publicado: 26 de agosto 2016] [Consulta: 18 de diciembre 2022]. Disponible en: https://silo.tips/download/calidad-de-software-cso-practica-2-calidad-de-arquitecturas-software-introduccio.

funcionamiento adecuado del sistema a implementar y alcanzar el cumplimiento de los objetivos de negocio.[47] Similar al paso anterior, esta actividad ya fue realizada en el desarrollo del objetivo anterior, aunque no fue realiza de manera estricta. Debido a que no se necesita abordar distintos objetivos de negocio que requieran planteamientos distintos para abarcarlos a todos a cabalidad, sino que las propuestas siguiendo las practicas solo se enfocan en los temas de seguridad, una sola propuesta basta para determinar que este paso fue realizado.

- Analizar los enfoques arquitectónicos: se realiza un análisis de los enfoques propuestos para determinar cómo afectan los factores de calidad (disponibilidad, rendimiento, integridad, entre otros). [48] Para ajustar esta actividad a la necesidad de evaluar los escenarios, son definidos como los factores de calidad los tres pilares de la seguridad informática: confidencialidad, integridad y disponibilidad, siguiendo así el planteamiento del desarrollo del objetivo dos y trabajando en la misma línea. Durante el desarrollo del objetivo cuatro se realiza este análisis a cada escenario con las prácticas de seguridad aplicadas del objetivo tres, identificando para cada caso las afectaciones en los tres pilares.

- Presentación de resultados: tal como su nombre lo indica, se presentan los resultados obtenidos de los análisis. En este caso, se presentarán las conclusiones obtenidas del análisis del paso anterior, mostrando así si cumple con el aseguramiento esperado de los factores de calidad. Esto se presenta luego del análisis de cada escenario con las prácticas implementadas.

Se procede entonces con la realización de los pasos tres y cuatro para evaluar los escenarios propuestos:

5.4.1 Evaluación de escenario Acceso a archivos compartidos.

Para el este escenario, las prácticas aplicadas presentan las siguientes consecuencias y afectan los tres pilares así:

- Confidencialidad: aumenta la confidencialidad de los archivos y datos almacenados en los buckets, esto debido al bloqueo de accesos públicos y limitación de privilegios y permisos de usuarios que no deberían visualizar o modificar información debido al rol que ocupan y el tipo de datos con el que van a interactuar. Además, los medios para conexión requeridos aseguran

[47] Ibid. Disponible en: https://silo.tips/download/calidad-de-software-cso-practica-2-calidad-de-arquitecturas-software-introduccio
[48] Ibid. Disponible en: https://silo.tips/download/calidad-de-software-cso-practica-2-calidad-de-arquitecturas-software-introduccio

que la identidad de los usuarios que interactúan con los buckets es de personal de la organización, debido a la obligación de usar credenciales autenticadas.

- Integridad: presentará un aumento ya que los datos no pueden ser modificados por personas sin autorización, además de que los cambios que se realicen serán fáciles de rastrear para determinar quién los realizó, ya que la cantidad de usuarios con acceso es reducida y controlada. La información se mantendrá en estados aceptables sin modificaciones no esperadas.

- Disponibilidad: no presenta afectación, ya que las configuraciones y practicas aplicadas para el escenario no se relacionan con la disponibilidad de los servicios.

Con base a esto, se obtiene un amento a la seguridad de la información respecto al escenario inicial, aunque no se ven afectados los tres pilares por las practicas. La disponibilidad no se ve afectada ya que el servicio de almacenamiento S3 tiene niveles de disponibilidad predefinidos, y las practicas implementadas van enfocadas a la protección de accesos por personal no deseado o modificación indebida de datos.

5.4.2 Evaluación de escenario Aplicación web con base de datos relacional.

Para el este escenario, las prácticas aplicadas presentan las siguientes consecuencias y afectan los tres pilares así:

- Confidencialidad: se restringe el acceso a la aplicación en varias capas, reforzando de manera considerable la prevención de accesos no autorizados o no deseados que puedan visualizar u obtener datos sensibles de la organización. Mediante las tres capas que componen la VPN, el firewall de red y el WAF se logran bloquear intentos de acceso en una escala mayor que solo incluyendo un servicio de inicio de sesión o dejando la aplicación sin restricciones de usuario.

- Integridad: con los controles de políticas de mínimos privilegios implementados mediante la configuración de los usuarios complementada con la definición de grupos de seguridad mediante ACL se logra limitar los accesos a los datos y servicios por parte de usuarios que podrían manipular la información y crear inconsistencias. Se pasó de una aplicación sin restricciones de acceso disponible para ser utilizada por cualquier usuario, incluyendo capacidad de modificar la arquitectura mediante configuración de los servicios implementados, a una aplicación bien definida y limitada según las necesidades y responsabilidades de los usuarios a la hora de interactuar u usarla.

- Disponibilidad: el uso de balanceador de carga junto con la herramienta de monitoreo aumenta la disponibilidad de la aplicación al brindar opciones automáticas de escalado para responder a la demanda que pueda tener el servicio, junto con un sistema de alertas que le permite al equipo encargado tomar decisiones y actuar a tiempo para evitar caídas del servicio. Son dos controles que se complementan de manera apropiada para garantizar el funcionamiento del servicio. Aparte, los firewalls utilizados logran evitar posibles ataques de denegación de servicios que podrían inhabilitar la aplicación o los servidores. Por último, la política de mínimos privilegios protege la aplicación de que la utilización no apropiada de los servicios repercuta en una disminución de sus capacidades para soportar el funcionamiento del servicio, mediante la reducción o eliminación de recursos.

Los cambios efectuados de la primera a la segunda arquitectura con los controles de seguridad logran aumentar los niveles de disponibilidad de la aplicación, reducir los riesgos de ver afectada la operación del servicio y el acceso de los usuarios y mitigar el exceso de carga de trabajo para los recursos que ejecutan el servicio. Además, protege los datos y los recursos del mal uso o manipulación de las herramientas de formas que puedan afectar negativamente la organización.

5.4.3 Evaluación de escenario Aplicación web con base de datos no relacional.

Para el este escenario, las prácticas aplicadas presentan las siguientes consecuencias y afectan los tres pilares así:

- Confidencialidad: similar al caso anterior, mediante el uso de los firewalls se minimiza el riesgo de que usuarios malintencionados puedan interactuar con la aplicación y los datos, más teniendo en cuenta que es una aplicación disponible para cualquiera con acceso a internet. Al lograr bloquear direcciones conocidas como maliciosas o sospechosas, de descarta gran cantidad de conexiones que pondrían en riesgo la información almacenada por la aplicación de sus usuarios. Junto con las políticas de mínimos privilegios para reducir la interacción del usuario a lo más mínimo, se logra una disminución considerable a las posibilidades de acceso a información crítica.

- Integridad: se limita el acceso y modificación de los datos mediante las políticas de mínimos privilegios, logrando así los usuarios no puedan modificar información con la interacción que tengan con la aplicación o manipulación indebida de datos por permisos excesivos. Además, mediante los bloqueos por firewalls se evita que paquetes dirigidos para alterar los datos existentes, enviados desde direcciones bloqueadas por ser identificadas como maliciosas.

- Disponibilidad: de manera parecida al escenario anterior, por medio del uso de los servicios de monitoreo y balanceo de cargas se logra mantener el servicio arriba el mayor tiempo posible, y con estas herramientas se logra tener una reacción rápida ante los casos donde pueda caerse el servicio por falta de recursos y exceso de demanda por parte de los usuarios. Por otra parte, los bloqueos de firewalls de direcciones sospechosas evitan posibles ataques de denegación de servicios desde los equipos identificados que usan los atacantes para afectar aplicaciones.

Con estos controles, la arquitectura de aplicación web no relacional pasó de estar con visibilidad total y riesgo de acceso latente a disminuir la capacidad de acceso desde direcciones sospechosas, se evita la divulgación total de datos y se asegura que se encuentre disponible la aplicación el mayor tiempo posible gracias a las estrategias de monitoreo y respuesta basadas en la información brindada por los servicios contratados con el proveedor Amazon Web Services.

5.4.4 Evaluación de escenario Servicio de intranet.

Para el este escenario, las prácticas aplicadas presentan las siguientes consecuencias y afectan los tres pilares así:

- Confidencialidad: dado que el escenario demanda que el acceso al servicio sea solo de los usuarios internos de una organización, los controles usados para garantizar que se cumpla esta condición son apropiados: limitar el acceso mediante el servicio de VPN para que pueda iniciar sesión solo cuentas autorizadas y el bloqueo mediante Firewall de direcciones que no se encuentren dentro de la red de la organización hace que todo lo divulgado para el mero conocimiento interno de colaboradores se mantenga así, sin que un tercer accediendo desde internet pueda interactuar con esta información. Junto con estos controles, mediante el bloqueo de accesos a los buckets y que solo se visualice los archivos multimedia que se requieran en la intranet, sin que ningún tercero pueda obtenerlos se logra mantener protegida la información que estos archivos contenga. Otro agregado para evitar la obtención de información de manera indebida es el aislamiento de redes realizado mediante la configuración de equipos y redes de nube, ya que recursos como las bases de datos, las instancias y los buckets se comunican solo por los canales definidos y controlados por el usuario, y bloquea cualquier comunicación proveniente de equipos no autorizados.

- Integridad: siguiendo la práctica común en todos los escenarios, la limitación de privilegios y acceso a los recursos facilita evitar que los datos y archivos sean alterados o modificados por personal que no debe interactuar, terceros externos o usuarios autorizados para acceder a la aplicación pero que no

deben crear contenido o modificar datos presentados. Esto se logra gracias a la combinación de grupos de seguridad con ACL para definir permisos sobre los recursos, la definición de ACL específicos para los buckets de S3 donde se alojan archivos multimedia o datos y el bloqueo de acceso público a los buckets.

- Disponibilidad: siguiendo el patrón aplicado en los dos escenarios anteriores, mediante el uso de servicios de monitoreo para estar atento al estado de los recursos usados para desplegar la intranet y uso de balanceadores de carga que permitan provisionar más capacidades o crear nuevas instancias para mejorar el procesamiento se logra evitar pérdidas de servicio o indisponibilidad que afecte la capacidad de presentar información a los colaboradores internos.

Se pasó de una arquitectura accesible por cualquiera en internet con el riesgo de mostrar información de interés interno a cualquier tercero que lograra interactuar con la aplicación, a una intranet protegida, con alta disponibilidad y con riesgos bajos de ser accedida por personal ajeno a la organización. Se logra determinar el crecimiento de la protección de los recursos de nube utilizados, además de la alta certeza de que no se darán cambios inesperados por usuarios sin permisos suficiente, que podrían afectar el funcionamiento o integridad de la información presentada.

5.4.5 Evaluación de escenario Aplicaciones desarrolladas en contenedores.

Para el este escenario, las prácticas aplicadas presentan las siguientes consecuencias y afectan los tres pilares así:

- Confidencialidad: se implementan el servicio de VPN para garantizar que el acceso a la aplicación solo sea de personas autorizadas para interactuar con esta, reduciendo interacciones innecesarias de terceros no involucrados, además de bloquear conexiones maliciosas que quieran adquirir datos almacenados y que manipula la aplicación para su funcionamiento. Junto a estos controles, se logra quitar total visibilidad de los contenidos multimedia y archivos grandes que se almacenan para el funcionamiento correcto de la aplicación al público en general que navega por internet y pueda llegar a encontrar las direcciones de los buckets. Se logra protección reforzada de varias capas tanto para datos almacenados como archivos manejados por la aplicación.

- Integridad: se evita una interacción más de la necesaria de los usuarios con los datos, mediante los controles de mínimo privilegio y configuraciones de ACL en la arquitectura asegurada. Esa limitación de interacción permite la protección contra atacantes que quieran manipular la información, o de

colaboradores que por curiosidad o intención quieran interactuar con los datos y archivos almacenados en el sistema.

- Disponibilidad: al trabajar con microservicios, la gestión de los contenedores es crucial, por lo que el control de implementar balanceador de cargas se hace clave para su funcionamiento correcto. Debido a la facilidad para desplegar y eliminar estos componentes, se logra mantener en buenos niveles de disponibilidad la aplicación. Además, el monitoreo ayuda a decidir si es necesaria la intervención manual para aumentar las capacidades de procesamiento de los recursos usados pensar estrategias para solventar de manera rápida emergencias o novedades.

Gracias a los controles implementados en la arquitectura, la protección de los datos y limitación de acceso a los contenedores brinda la tranquilidad y confianza requeridas para el funcionamiento de la aplicación. Aparte de esto, se minimizan riesgos de disponibilidad y de exposición de información al definir los permisos de los usuarios y direcciones que pueden comunicarse con el servicio. Se logra un aumento a la protección de los tres pilares, reflejando una mayor seguridad para la aplicación.

6 CONCLUSIONES

Se examinó la documentación oficial categorizando las prácticas con base a un modelo planteado que toma a las funcionalidades de seguridad brindadas por estas prácticas para asegurar los servicios, encontrando que el proveedor Amazon Web Services brinda una cantidad grande y especializada de sugerencias para realizar configuraciones, implementación de controles y políticas de seguridad de los servicios que ofrecen. Las configuraciones, componentes y herramientas son diseñadas y propuestas para cumplir con el aseguramiento de los tres pilares de la seguridad de la información en los activos de nube usados.

Se destacaron las prácticas examinadas e identificadas agrupándolas, teniendo en cuenta a qué pilar de la seguridad de la información afectaba cada práctica, logrando así reconocer y comprender mejor su funcionamiento, su importancia y sobre todo el papel crucial que cumplen dentro de las infraestructuras tecnológicas de nube. Está labor facilitó la aplicación de las prácticas en el desarrollo de objetivos posteriores, ya que se entendió qué activos estaban protegiendo, qué tipo de uso era más favorable según la necesidad del escenario y permitió entender cómo podrían interactuar con otras prácticas.

Se propusieron escenarios en dos momentos, un momento inicial donde se usaban servicios con configuraciones mínimas, detallando los servicios de AWS que fueron utilizados en la infraestructura, analizando que falencias de seguridad se presentan con el estado inicial y luego aplicando las prácticas destacadas para mitigar la seguridad. Además, al estar basados en situaciones comunes dentro de los entornos corporativos, se visualizó la utilidad e importancia de estas prácticas para asegurar apropiadamente entornos, junto con la reducción en la dificultad para planear la implementación, evitando afectar así las operaciones corporativas.

Se evaluaron las arquitecturas de los escenarios propuestos, tomando como atributos de calidad los tres pilares de la seguridad de la información, determinando que se logra la mejora de seguridad de los escenarios planteados en el tercer objetivo con la implementación de prácticas de seguridad identificadas en el desarrollo del segundo objetivo. Se pudieron identificar claramente los factores y condiciones de riesgo mitigadas con las practicas, y como al disminuir el riesgo aumenta la seguridad del servicio mediante una confidencialidad e integridad de datos mayor y una disponibilidad alta.

7 RECOMENDACIONES

Para agilizar la revisión de la documentación brindada por Amazon Web Services, se sugiere revisar acorde a los activos utilizados por la infraestructura tecnológica de la organización. Al tener detallados los componentes, servicios e instancias que son implementados para correr aplicaciones o procesos de negocio, el tiempo de búsqueda se reduce, debido a que el análisis extra requerido para abarcar de manera general entornos organizacionales desaparece, y ese esfuerzo libre puede ser enfocado en estudiar a profundidad las configuraciones y prácticas específicas de los componentes de nube usados.

Validar de manera periódica la actualización de las prácticas clasificadas, ya que en la documentación se encuentran presentes sugerencias de configuraciones e implementaciones de servicios que actualmente no se encuentran disponibles o han adquirido nuevas características que no necesitan de la aplicación de esas configuraciones obsoletas encontradas.

En caso de usar este documento como referencia para la implementación o estudio de prácticas de seguridad, se recomienda validar que aún sean vigentes e implementables en los componentes actuales, o qué los servicios mencionados aún se encuentren disponibles para su uso. Si el servicio no está disponible, buscar que otro servicio puede sustituir sus funciones y características, además de consultar sus respectivas configuraciones y métodos de aseguramiento.

Al momento de proponer nuevos escenarios para la aplicación de las prácticas, se recomienda evaluar el contexto actual de la industria, con el fin de saber que procesos se están usando en el momento, que tecnologías son las más favorables, que modelos son los más populares y utilizados para lograr así que los escenarios sean lo más alineados con la realidad posible.

De ser posible, al idear escenarios de prueba, se recomienda utilizar casos que se presenten en una organización especifica. De este modo, la profundización en las amenazas presentes, el estado de las configuraciones y los controles serán más detallados y permitirá encaminar la búsqueda de prácticas de seguridad por una ruta más clara, en los activos y servicios a proteger son fáciles de determinar y su implementación se verá plasmada en casos reales donde puedan evaluarse con métricas puntuales.

Para futuras evaluaciones se recomienda validar si se ha desarrollado una nueva metodología o marco de trabajo para evaluación de arquitecturas de aplicaciones o infraestructuras tecnológicas, qué permita medir de manera más puntual y precisa, acorde a las características que tiene la tecnología de nube y sus servicios, como se ven afectados los pilares de la seguridad de la información u otros atributos que se consideren convenientes para comprobar que la seguridad en la infraestructura ha aumentado.

A la hora de evaluar los escenarios, en caso de que se apliquen dentro de una organización, se recomiendo implementar la metodología ATAM usando todos los pasos que propone, de modo que puedan verse evaluados más atributos de calidad acordes a las necesidades y solicitudes de todos los interesados e involucrados con las infraestructuras tecnológicas de nube que requieran implementar prácticas de seguridad para mejorar sus condiciones actuales de seguridad.

BIBLIOGRAFÍA

ALEGSA [Sitio web]. Definición de Recurso (informático). [Publicación: 2 de mayo 2019] [Consulta: 24 de septiembre 2022] Disponible en: Definición de Recurso (informático)

AWS [Sitio web]. ¿Qué es Amazon EC2? AWS. [Consulta: 12 de abril 2022] Disponible en: https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html

AWS [Sitio web]. ¿Qué es Amazon EC2 Auto Scaling? [Consulta: 12 de abril 2022] Disponible en: https://docs.aws.amazon.com/es_es/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html.

AWS. [Sitio web]. Administración de acceso con ACL. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/acls.html

AWS. [Sitio web]. Amazon EC2 security groups for Linux instances. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html.

AWS. [Sitio web]. Autenticación de bases de datos con Amazon RDS. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/database-authentication.html.

AWS. [Sitio web]. AWS Backup: How it works. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/aws-backup/latest/devguide/how-it-works.html.

AWS. [Sitio web]. Bloquear el acceso público a su almacenamiento de Amazon S3. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html.

AWS. [Sitio web]. Cifrado en reposo en DynamoDB. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/amazondynamodb/latest/developerguide/EncryptionAtRest.html.

AWS. [Sitio web]. Cifrado de recursos de Amazon RDS. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/Overview.Encryption.html.

AWS [Sitio web]. Control del acceso desde puntos de enlace de la VPC con políticas de bucket. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/AmazonS3/latest/userguide/example-bucket-policies-vpc-endpoint.html

AWS [Sitio web]. Controlar el tráfico hacia los recursos mediante grupos de seguridad [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/vpc/latest/userguide/VPC_SecurityGroups.html

AWS [Sitio web]. Creación de una copia de seguridad. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/aws-backup/latest/devguide/creating-a-backup.html

AWS [Sitio web]. Informática para cualquier carga de trabajo. AWS [Consulta: 12 de abril 2022]. Disponible en: https://aws.amazon.com/es/products/compute/

AWS. [Sitio web]. Prácticas recomendadas de control de acceso. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/access-control-best-practices.html.

AWS. [Sitio web]. Prácticas recomendadas de seguridad en IAM. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

AWS [Sitio web]. Prácticas recomendadas de seguridad para AWS Client VPN. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/vpn/latest/clientvpn-admin/security-best-practices.html

AWS. [Sitio web]. Protección de datos mediante cifrado. [Consulta: 06 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/UsingEncryption.html.

AWS [Sitio web]. ¿Qué es AWS Security Hub? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/securityhub/latest/userguide/what-is-securityhub.html

AWS. [Sitio web]. ¿Qué es Amazon CloudWatch? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html

AWS [Sitio web]. ¿Qué es Amazon EC2 Auto Scaling? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html

AWS [Sitio web]. Reglas de autorización. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/vpn/latest/clientvpn-admin/cvpn-working-rules.html

AWS. [Sitio web]. Security in AWS Elastic Disaster Recovery. [Consulta: 06 de mayo 2022] Disponible en: https://docs.aws.amazon.com/es_es/drs/latest/userguide/security.html.

AWS. [Sitio web]. Security in AWS Network Firewall. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/network-firewall/latest/developerguide/security.html.

AWS [Sitio web]. Seguridad de la infraestructura de Amazon EC2. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/AWSEC2/latest/WindowsGuide/infrastructure-security.html

AWS. [Sitio web] Seguridad de la infraestructura de Amazon EKS. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/eks/latest/userguide/infrastructure-security.html.

AWS [Sitio web]. Seguridad de la infraestructura en AWS Identity and Access Management. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/es_es/IAM/latest/UserGuide/infrastructure-security.html

AWS. [Sitio web]. Seguridad de la infraestructura en Amazon VPC. [Consulta: 16 de abril 2022]. Disponible en: https://docs.aws.amazon.com/es_es/vpc/latest/userguide/infrastructure-security.html.

AWS. [Sitio web]. Seguridad en el uso del servicio AWS WAF. [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/security.html.

AWS [Sitio web]. What is Elastic Disaster Recovery? [Consulta: 05 de mayo 2022]. Disponible en: https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html

BEMBIBRE Cecilia. [Sitio web]. Definición de práctica. DefiniciónABC. [Publicado: 1 de julio 2012] [Consulta: 10 de abril 2022]. Disponible en: https://www.definicionabc.com/tecnologia/practica.php

BEMBIBRE Victoria. [Sitio web]. Definición de Configuración. DefiniciónABC. [Publicado: 1 de febrero 2009] [Consulta: 10 de abril 2022]. Disponible en: https://www.definicionabc.com/tecnologia/configuracion.php

BORILLO Ricardo [Sitio web] Qué es serverless y por qué adoptarlo en el desarrollo de tu próxima aplicación. Genbeta. [Publicado: 1 de abril 2019] [Consulta: 15 de marzo 2022] Disponible en: https://www.genbeta.com/desarrollo/que-serverless-que-adoptarlo-desarrollo-tu-proxima-aplicacion

CARISIO Emanuele [Sitio web] Vulnerabilidad informática: ¿cómo protegerse?. Mediacloud. [Consulta: 11 de abril 2022]. Disponible en: https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

CYBERSECURITY INSIDERS. [Sitio web] 2021 Cloud Security Report. [Consulta: 16 de marzo 2022] Disponible en: https://www.isc2.org/-/media/ISC2/Research/Resource-Thumbnails/Resource-Center/Research/2021-Cloud-Security-Report-FINAL.ashx?la=en&hash=365C243EC4B2196B9C4B55AF8E3C4E1EC4B0C5B6

DEWITT Derek [Sitio web]. Cifrado de datos: ¿en qué consiste? Avast. [Publicación: 22 de abril 2021] [Consulta: 24 de septiembre 2022]. Disponible en: https://www.avast.com/es-es/c-encryption

EMERGENT CHAOS [Sitio web]. The Security Principles of Saltzer and Schroeder. [Consulta: 12 de mayo 2022]. Disponible en: https://www.emergentchaos.com/the-security-principles-of-saltzer-and-schroeder

FLEXERA. 2022 State of the Cloud Report. [Sitio web]. Flexera. [Consulta: 10 de marzo 2022]. Disponible en: https://resources.flexera.com/web/pdf/Flexera-State-of-the-Cloud-Report-2022.pdf?elqTrackId=414badd9b3cd4eee979d7f8bbfa8269e&elqaid=6925&elqat=2

FOOTE Keith [Sitio web]. A Brief History of Cloud Computing. Dataversity. [Publicado: 17 de diciembre 2021] [Consulta: 23 de noviembre 2022]. Disponible en: https://www.dataversity.net/brief-history-cloud-computing/

FORTUNE BUSINESS INSIGHTS. Cloud Computing Market Size, Share & Growth [2021-2028]. Cloud Computing [Sitio web], Fortune Business Insights. [Publicado: 1 de mayo 2021] [Consulta: 5 de marzo de 2022], Disponible en: https://www.fortunebusinessinsights.com/cloud-computing-market-102697

GOBIERNO DE CANARIAS [Sitio web]. ¿Qué es la Identidad digital? [Consulta: 24 de septiembre 2022] Disponible en: https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/identidad-digital-profesorado/que-es-la-identidad-digital/#:~:text=La%20Identidad%20Digital%20es%20el,%2C%20amistades%2C%20aficiones%2C%20etc.

GRUPO ACS [Sitio web] Política de seguridad de la información. [Consulta: 24 de septiembre 2022]. Disponible en: https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

HEWLETT PACKARD ENTERPRISE [Sitio web]. Definición de infraestructura de la nube. [Consulta: 14 de marzo 2022]. Disponible en: https://www.hpe.com/lamerica/es/what-is/cloud-infrastructure.html#:~:text=Definici%C3%B3n%20de%20infraestructura%20de%20la,consumido%20a%20trav%C3%A9s%20de%20Internet.

IBM [Sitio Web]. ¿Qué es infraestructura de TI? [Consulta: 5 de marzo 2022] Disponible en: https://www.ibm.com/pe-es/topics/infrastructure

ID GRUP [Sitio web] ¿Qué es un Firewall y cómo funciona? [Consulta: 24 de septiembre 2022] Disponible en: https://idgrup.com/firewall-que-es-y-como-funciona/

INFOTECS [Sitio web]. ACL: Lista de Control de Accesos. [Publicado: 21 de enero 2019] [Consulta: 16 de abril 2022] Disponible en: https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html

ITILCOM [Sitio web]. Servicios de informática. Concepto, funciones y beneficios. Itilcom. [Publicado: 10 de junio 2020] [Consulta: 12 de abril 2022]. Disponible en: https://www.itilcom.com/blog/servicios-de-informatica-concepto-funciones-y-beneficios/

KASPERSKY [Sitio web]. ¿Qué es una VPN y cómo funciona? [Consulta: 24 de septiembre 2022] Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn

ORTIZ Angel [Sitio web]. ¿Qué es una vulnerabilidad en seguridad informática? Ejemplos. HostDimeBlog. [Publicado: 22 de julio 2020] [Consulta: 11 de abril 2022] Disponible en: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/

PAESSLER [Sitio web] IT Explained: Servidor. [Consulta: 23 de septiembre 2022]. Disponible en: https://www.paessler.com/es/it-explained/server#:~:text=Un%20servidor%20es%20un%20sistema,comparten%20recursos%20con%20m%C3%A1quinas%20cliente.

PÉREZ PORTO Julián. y GARDEY Ana. [Sitio web]. Definición de Configuración. DefiniciónABC. [Publicado:2016] [Consulta: 10 de abril 2022]. Disponible en: https://definicion.de/configuracion/

PÉREZ PORTO Julián. y GARDEY Ana. [Sitio web]. Definición de práctica. DefiniciónABC. [Publicado:2010] [Consulta: 10 de abril 2022]. Disponible en: https://definicion.de/practica/

RAE [Sitio web]. Documentación. RAE. [Consulta: 11 de abril 2022]. Disponible en: https://dle.rae.es/documentaci%C3%B3n

RED HAT. [Sitio web] ¿Qué es la infraestructura de TI? [Publicado: 17 de junio 2019] [Consulta: 7 de marzo 2022] Disponible en: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

RED HAT. [Sitio web] La migración de la TI. [Publicado: 4 de febrero 2021] [Consulta: 23 de septiembre 2022] Disponible en: https://www.redhat.com/es/topics/automation/what-is-it-migration

SECURITYSCORECARD [Sitio web]. What is the CIA Triad? Definition, Importance, & Examples. [Publicado: 1 de septiembre 2021] [Consulta: 06 de diciembre 2022]. Disponible en: https://securityscorecard.com/blog/what-is-the-cia-triad.

SISTEMAS [Sitio web]. Definición de Documentación. [Consulta: 11 de abril 2022]. Disponible en: https://sistemas.com/documentacion.php#:~:text=En%20inform%C3%A1tica%2C%20sin%20embargo%2C%20la,y%20conozca%20sus%20funciones%20principales.

TRISKELE LABS. [Sitio web] Cloud cyber attacks: The latest cloud computing security issues. [Consulta: 16 de marzo de 2022] Disponible en: https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues

TRUSTWAVE.2020 Trustwave Global Security Report [Sitio web]. Trustwave [Publicado: 1 de febrero 2020] [Consulta: 5 de marzo 2022]. Disponible en: https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

VEGAGESTION [Sitio web]. La infraestructura tecnológica: definición, tipos e importancia. [Publicado: 6 de febrero 2018] [Consulta: 14 de marzo 2022] Disponible en: https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

VELEV Dimiter y ZLATEVA Plamena. Cloud Infraestructure Security. Sofia, Bulgaria: iNetSec, Publicado: marzo 2010. Hal Inria [Base de datos en línea]. Recuperado de: https://hal.inria.fr/hal-01581343/document el 11 de marzo 2022.

WIKIPEDIA [Sitio web]. Servicio de tecnologías de la información. Wikipdia. [Consulta: 12 de abril 2022]. Disponible en: https://es.wikipedia.org/wiki/Servicio_de_tecnolog%C3%ADas_de_la_informaci%C3%B3n#:~:text=Un%20servicio%20de%20tecnolog%C3%ADas%20de,el%20riesgo%20inherente%20del%20sistema.