TRABAJO DE GRADO
Opción Seminario-Diplomado.

Introducción e implementación de servicios en la nube con AWS

Corporación Universitaria Remington.
Nombre de la facultad: Facultad de ingenierías
Nombre del programa académico:
Ingeniería de sistemas, Especialización en seguridad de la información

Alejandra Moreno Cordoba, Javier Estik Celis Torres, Michael Steven Bohorquez Uruena.
Nombre del Tutor del trabajo de grado: Juan Pablo Berrio López.
Opción de Trabajo de grado Seminario-Diplomado.
2024.

Dedicatoria

Este trabajo de grado está dedicado a nuestras familias quienes, con su amor, paciencia y esfuerzo nos han permitido llegar a cumplir hoy un sueño más, y quienes nos enseñaron que el mejor conocimiento que se puede tener es el que se aprende por sí mismo.

Agradecimientos

Agradecemos muy especialmente a nuestras familias, quien siempre nos apoyaron en este largo camino y a amigos y compañeros de trabajo y estudio quienes nos dieron una mano cuando la necesitábamos

Tabla de Contenidos

Resumen

Como equipo nosotros hemos desarrollado e implementado este trabajo con un enfoque en el utilizar la nube como opción. Inicialmente se habla de la migración a la nube de la empresa TechSolutions S.A, que dentro del contexto del documento esta organización considera migrar su infraestructura a la nube, con el fin de mejorar su escalabilidad, flexibilidad, además reducir costos operativos. De lo anterior, la nube ofrece un modelo de pago por uso, eliminando los gastos fijos en hardware y optimización de recursos, permitiendo ajustes automáticos según la demanda. Esto mejora la eficiencia operativa y la capacidad de respuesta ante posibles cambios del mercado, y fortalece la seguridad, mediante políticas de acceso y cifrado de datos avanzados, y la gestión centralizada - automática de las actualizaciones y mantenimientos suministrados por el proveedor, minimizando riesgos asegurando alta disponibilidad. Algo importante en este trabajo en este trabajo, es que, se requiere capacitación en nuevas tecnologías al equipo de IT, y a pesar de ello, la nube ofrece beneficios significativos con mayor flexibilidad para escalar globalmente, manteniendo operaciones ininterrumpidas. A partir de lo anterior, podemos decir que, migrar a la nube facilita adaptarse ligeramente, a un entorno o ambiente empresarial dinámico, mejorando, la eficiencia operativa y reduciendo la dependencia a la infraestructura física que se es costosa.

Por otro lado, en este documento podemos precisar, en dos servicios que nos ofrece AWS de Amazon (EC2 y S3) donde , se busca elegir cuál de los dos es mejor para implementar una aplicación web, aquí nosotros indicamos que la elección depende de las necesidades de la aplicación, es decir, EC2 es un servicio ideal, para aplicaciones complejas que requieren de procesamiento dinámico y bases de datos interactivas, logrando así, flexibilidad y control, sin embrago, a un costo mayor con mantenimiento más robusto, en cambio, S3 es más adecuado o enfocado para aplicaciones estáticas, como lo son , sitios informáticos, este es de menor costo y alta estabilidad, por ultimo no menos importante se puede encontrar en este documento, procesos en AWS como es: Creación de instancias, contenedores, balanceadores, auto scaling y se explica cada proceso realizado.

Palabras clave

AWS, Nube, Infraestructura, Seguridad, Contenedores, Instancias.

Marco conceptual y contextual

En este capítulo, se expone el marco conceptual y contextual, para este seminario de grado.

1. Marco conceptual

Computación en la nube 1.1.

Según (of Veterans Affairs & Iam, 2018) la computación en la nube es un modelo que permite el acceso ubicuo, cómodo y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con mínimo esfuerzo de gestión o interacción con el proveedor de servicios.

Infraestructura como servicio (Iaas)1.2.

Según (Pablo Federico Muñoz Calderón & Martin Geovanny Zhindón-Mora, n.d.) la infraestructura como servicio funciona según el llamado principio de corresponsabilidad, según el cual el proveedor y su cliente se ocupan de tareas diferentes, necesarias para poder hacer uso o aprovisionar los recursos de la nube de la forma más adecuada.

Elastic compute cloud (EC2) 1.3.

Según (Saini & Behl, 2020) Amazon EC2 elimina la necesidad de invertir en hardware para que se puedan desarrollar e implementar aplicaciones de forma rápida.

Simple storage service (S3) 1.4.

Según (AWS, 2024d) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento lideres en la industria.

Amazon S3 proporciona funciones de administración para que pueda optimizar, organizar y configurar el acceso a sus datos para cumplir con sus requisitos comerciales, organizacionales y de cumplimiento específicos.

Virtual private Cloud (VPC) 1.5.

Según (AWS, 2024e)VPC puede ejecutar recursos de AWS en una red virtual aislada lógicamente que haya definido. Esta red virtual se parece mucho a una red tradicional que operaria en su propio centro de datos, con los beneficios de usar una infraestructura escalable en AWS.

Características de una VPC:

Nubes privadas virtuales (VPC):

Una VPC es una red virtual que se parece mucho a una red tradicional que utilizarías en tu propio centro de datos. Después de crear una VPC, puedes agregar subredes.

Subredes:

Una subred es un rango de direcciones IP en su VPC. Una subred debe residir en una única zona de disponibilidad. Después de agregar subredes, puede implementar recursos de AWS en su VPC.

Direccionamiento IP:

Puede asignar direcciones IP , tanto IPv4 como IPv6, a sus VPC y subredes. También puede traer sus direcciones IPv4 públicas y direcciones GUA IPv6 a AWS y asignarlas a recursos en su VPC, como instancias EC2, puertas de enlace NAT y balanceadores de carga de red.

Enrutamiento:

Utilice tablas de rutas para determinar dónde se dirige el tráfico de red desde su subred o puerta de enlace.

Puertas de enlace y puntos finales:

Una puerta de enlace conecta su VPC a otra red. Por ejemplo, utilice una puerta de enlace de Internet para conectar su VPC a Internet. Utilice un punto de conexión de VPC para conectarse a los servicios de AWS de forma privada, sin utilizar una puerta de enlace de Internet o un dispositivo NAT.

Amazon Relational Database Service 1.6.

Según (AWS, 2024c) RDS es un servicio web que facilita la configuración, el funcionamiento y la ampliación de una base de datos relacional en la nube de AWS. Proporciona una capacidad redimensionable y rentable para una base de datos relacional estándar de la industria y administra tareas comunes de administración de bases de datos.

Elastic Beanstalk 1.7.

Según (AWS, 2024a) El balanceador de carga distribuye el tráfico entre las instancias del entorno. Cuando habilita el balanceador de carga, AWS Elastic Beanstalk crea un balanceador de carga Elastic Load Balancing dedicado en su entorno. Elastic Beanstalk gestiona completamente este balanceador de carga, cuidando la configuración de seguridad y finalizando el balanceador de carga cuando finalice su entorno.

Elastic Load Balancing tiene los siguientes tipos de balanceador de carga:

Balanceador de carga clásico**:** El balanceador de carga de la generación anterior. Dirige el tráfico HTTP, HTTPS o TCP a los distintos puertos de las instancias del entorno.

Balanceador de carga de aplicaciones: un balanceador de carga de capa de aplicación. Dirige el tráfico HTTP o HTTPS a los distintos puertos de las instancias del entorno en función de la ruta de la solicitud.

Balanceador de carga de red: un balanceador de carga de capa de red. Dirige el tráfico TCP a los distintos puertos de las instancias del entorno. Admite comprobaciones de estado tanto activas como pasivas.

Plataforma como servicio (PaaS) 1.8.

Según(Humberto Vera-Rivera & Gaona, 2017) las plataformas como servicio (PaaS), corresponden a todos aquellos componentes orientados al desarrollo y despliegue de aplicaciones sobre la Nube, en la cual los usuarios no instalan ninguna herramienta localmente para realizar sus desarrollos. Está enfocada a los desarrolladores de software y de aplicaciones web o móvil en la nube. PaaS está construida sobre la capa de infraestructura como servicio (IaaS), ofrece sistemas operativos para su uso, ya configurados e instalados, frameworks de aplicaciones y API (Application Programming Interface) para el desarrollo de software. Con PaaS se pretende minimizar la complejidad del despliegue de aplicaciones sobre máquinas virtuales

Imágenes de Maquina (AMI) 1.9.

Según (AWS, 2024b) es una imagen que ofrece AWS y que brinda la información necesaria para iniciar una instancia.

2. Marco contextual

2.1 (Radack, 2012) “el autor expone el siguiente problema con la computación en la nube que puede no ser una solución para todas las organizaciones, ni es apropiada para todas las aplicaciones. Muchas de las cuestiones abiertas con respecto al despliegue de la computación en nube son similares a las preocupaciones que se aplican a otros servicios alojados en TI. Los sistemas informáticos y de software complejos pueden contener fallos, fallar o comprometer la seguridad. Por ello, las técnicas para detectar fallos, comprender sus consecuencias, aislar sus efectos y remediarlos son fundamentales para la adopción a gran escala de las nubes.

La computación en nube tiene potencial para fomentar mercados más eficientes mediante el alquiler rápido de recursos informáticos. Los consumidores pueden renunciar a los gastos de capital a cambio de unas tarifas de servicio variables. Los proveedores de computación en nube pueden aprovechar los gastos de capital para atender a muchos clientes. Estas cuestiones económicas se mezclan con las complejidades de las configuraciones de redes y sistemas, así como con los riesgos de exponer datos y activos de software a un tercero. Los medios técnicos utilizados para proporcionar la calidad de servicio prometida por los proveedores de computación en nube no suelen revelarse al consumidor, lo que plantea interrogantes sobre cómo pueden los consumidores verificar que se ha proporcionado la calidad de servicio prometida. Además, los mercados eficientes dependen de la capacidad de los consumidores para comparar las ofertas de servicios. Esto es difícil porque los acuerdos de servicio pueden no adherirse a métricas, terminología y vocabularios estándar”.

2.2 (Badger et al., 2012) “presenta que la computación en nube no es una solución para todos los consumidores de servicios informáticos, ni es apropiada para todas las aplicaciones. Como tecnología emergente, la computación en nube contiene una serie de problemas, no todos exclusivos de la nube, que preocupan a todos los servicios alojados en TI.

Servicios informáticos. Algunas de estas cuestiones son temas tradicionales de la informática distribuida que han permanecido abiertos durante décadas, pero que ahora han adquirido mayor relevancia debido a la aparición de la computación en nube. Otras cuestiones parecen ser exclusivas de la computación en nube. Los sistemas informáticos complejos son propensos a los fallos y a comprometer la seguridad. Además, el software que debe adaptarse a requisitos complejos, como la concurrencia, la configuración dinámica y los cálculos a gran escala, puede presentar mayores densidades de defectos que el típico software comercial. Teniendo esto en cuenta, es importante entender que los sistemas en nube, como todos los sistemas informáticos complejos, contendrán defectos, experimentarán fallos y verán comprometida su seguridad. Esto no descalifica a los sistemas en nube para realizar un trabajo importante, pero sí significa que las técnicas para detectar fallos, comprender sus consecuencias, aislar sus efectos y remediarlos son fundamentales para la adopción a gran escala de las nubes".

2.3 (Rodríguez, 2019) "relata que la computación en la nube tiene múltiples ventajas, como las de carácter tecnológico, ambiental y social. Por lo que respecta a las empresas que recurren a los servicios susceptibles de ser incardinados en la computación en la nube se pueden, entre otras, mencionar las siguientes prerrogativas: de tipo económico-financiero —ahorro de costos de capital, control de costos y beneficios de tipo marginal—, foco en el negocio, continuidad de negocio y capacidad de recuperación frente a eventuales desastres, incremento de los recursos disponibles, modernización de los procesos de negocio, celeridad, escalabilidad y flexibilidad, seguridad, diversificación de los sistemas de TIC, evaluación de viabilidad y rentabilidad de posibles nuevos servicios, movilidad y plena disponibilidad. En este último sentido, no se necesita espacio físico alguno para poder almacenar servidores y bases de datos, ya que, como es conocido, están, como su propio nombre lo indica, en la nube. Sin perjuicio de las ventajas comentadas, cabe también señalar otras muchas como el incremento de la productividad de las empresas, la sensible mejora de los servicios públicos, así como de la calidad de vida y, finalmente, la evolución más avanzada hacia ciertos modelos de TIC".

2.4 (Agencia, n.d.) “menciona diferentes tipos de riesgos al utilizar infraestructura nube:

- El cliente necesariamente sede el control cede el control de una serie de cuestiones que pueden influir en la seguridad al proveedor en nube. Por ejemplo, los TdU pueden prohibir el escaneado de puertos, la evaluación de vulnerabilidades y las pruebas de penetración. Además, pueden surgir conflictos entre los procedimientos de refuerzo del cliente y el entorno en nube. Por otra parte, puede ocurrir que los Acuerdos de nivel de servicio no incluyan la prestación de dichos servicios por parte del proveedor en nube, dejando así una laguna en las defensas de seguridad.
- El uso de una infraestructura pública de nube implica que no pueden alcanzarse determinados niveles de cumplimiento, y por ello los servicios de alojamiento en nube no pueden utilizarse para los servicios que los necesitan.
- Los recursos compartidos implican la posibilidad de que las actividades maliciosas de un prestador puedan afectar al renombre de otro.
- la presión de la competencia, una estrategia de negocios inapropiada, la falta de apoyo financiero, etc., pueden provocar el cierre de algunos proveedores o, como mínimo, obligarles a reestructurar su oferta de cartera de servicios. Dicho de otro modo, es posible que a corto o medio plazo finalicen algunos servicios de computación en nube.
- Las actividades maliciosas de un iniciado pueden repercutir sobre: la confidencialidad, la integridad y la disponibilidad de todos los tipos de datos, IP, todos los tipos de servicios, y por tanto, indirectamente sobre el renombre de la organización, la confianza del cliente y las experiencias de los empleados”.

2.5 De acuerdo con Zaszczynski.E “El mantenimiento preventivo de servidores en la nube es esencial para garantizar su disponibilidad y rendimiento”. En este sentido se plantea la ejecución de un buen mantenimiento en los servidores de la nube, dicho esto, el trabajo desarrollado plantea y promueve una serie de buenas prácticas que conllevan a implementar diferentes acciones preventivas que garanticen un correcto funcionamiento.

2.6. Al hablar de EC2 y S3 estamos de acuerdo lo que dice, Pavan.Gumaste “Son dos herramientas fundamentales de AWS que ayudan a aumentar la eficiencia operativa de forma exponencial”. En eso orden de ideas, se resalta las cualidades de trabajar con estas dos herramientas que, al necesitar trabajar con EC2 contaremos con capacidad de computación flexible y escalable, mientras que, S3 ofrece almacenamiento de datos resistente y disponible.

Desarrollo e implementación del aprendizaje

3. Evaluación de riesgos y seguridad

Atributos de calidad detectados para la solución propuesta 3.1.

Rendimiento: La infraestructura IT de la empresa debe ser robusta y flexible para mantener los desarrollos y soluciones de los diferentes clientes

Fiabilidad: La infraestructura debe ser fiable y estar disponible para los usuarios cuando estos lo necesiten.

Seguridad: la infraestructura debe ser segura para proteger la información alojada en el misma.

Eficiencia: La infraestructura debe ser optima y sostenible para operar con el mínimo costo

Integridad: La infraestructura debe estar en la capacidad de proteger los datos desarrollos y soluciones de accesos o modificaciones no autorizados**.**

En la sección figuras y tablas se encuentran la ampliación de la solución del primero punto

4. Escalabilidad y Flexibilidad:

A continuación, verificaremos como se deben ajustar los requisitos y consideraciones a las necesidades de TechSolutions S.A. en relación con su crecimiento y flexibilidad estratégicamente.

Costo 4.1.

La migración de data center a la nube permite ahorrar y optimizar costos, ya que hay una reducción en infraestructura, producto de que ya no se invertirá en equipamientos mencionados como: Hardware, instalación, acondicionamiento del espacio, seguridad, entre otros, además costos en la operación-administrativa, pero, la nube permitirá invertir en costos operativos solo, eliminando el modelo de costos fijos y remplazándolo por costos de uso.

De lo anteriormente necesario resulta necesario decir que, una mala gestión operativa en la nube puede impactar económicamente ya que, puede conducir a la empresa a amortizar recursos superfluos o innecesarios.

Escalabilidad 4.2.

En temas de escalabilidad, la empresa tendrá la oportunidad de ajustar manualmente los recursos, con el fin de responder de manera ágil y eficiente a las variaciones en la demanda, es decir, TechSolutions S.A, puede mejorar la disponibilidad de uso, disminuyendo el riesgo de tiempo de inactividad, ejemplo: Puede hacer uso de 3 servidores por 5 horas dirías, de ello, solo pagará el tiempo utilizado, esto de acuerdo con su necesidad.

Además, mejora la eficiencia operativa, impulsando la innovación, puesto que, TechSolutions S.A, podrá lanzar nuevas aplicaciones –servicios respondiendo a las oportunidades de mercado de forma veloz. También escalar a nivel global a medida que su demanda aumente.

Si se presentan siniestros, por diferentes razones, el servicio estará seguro porque, se implementarán estrategias de recuperación como repartir cargas de trabajo y datos cuando se evidencie interrupciones de funcionamiento.

Seguridad y cumplimiento 4.3.

Para evaluar este factor y lograr un impacto positivo en el crecimiento y la flexibilidad de la empresa, es necesario desarrollar diversos procesos basados a políticas de seguridad.

Para asegurar la cuenta raíz y facilitar la administración diaria, se puede crear un grupo administrativo y este asigne derechos a este equipo en vez de que caiga la responsabilidad sobre una sola persona, y grupos extras para acceso detallado, a modo de lectura repartido para usuarios, con unos parámetros de acceso que limiten su interacción y mitigan riesgos.

También es importante buscar actualizaciones de seguridad , esto mantendrá un apetito y cultura de seguridad, de ello, se puede ejecutar autenticaciones de dos factores(2FA), con el fin de lograr seguridad en nuevas implementaciones, por otra parte , es importante que se restrinja el acceso a la infraestructura por medio de firewalls, para ello, abrir puertos solo cuando sea necesario, igualmente, limitar el acceso a cargas de trabajo a regiones especificas o direcciones IP, con el objetivo de reducir amenazas externas y puedan generar un impacto negativo.

En relación con las credenciales o contraseñas, se puede remplazar por infraestructura de clave publica, (PKI) para logran una seguridad más robusta. Lo anterior evita ataques y robo de información entre ello las claves. Algo importantes es que se puede hacer uso de Yubikey para una gestion segura de claves.

Asimismo, se debe implementar un sistema de evaluación de cumplimiento con el fin de garantizar que todas estas medidas de seguridad estén rigiendo correctamente, para ello, es relevante realizar auditorías periódicas y regulares, también, revisiones de seguridad que permitan identificar que la infraestructura cumpla con las políticas regulatorias de seguridad previamente ya establecidas. En consecuencia, de lo anterior podremos identificar y corregir posibles vulneraciones, anticipando a eventos con consecuencias severas.

Mantenimiento y operaciones 4.4.

TechSolutions S.A tendrá grandes ventajas, dado que, el mantenimiento en la infraestructura es proporcionadas por el prestador del servicio de la nube, de ello es importante precisar que la dinámica del mantenimiento que se realiza para garantizar el óptimo cumplimiento es preventiva, este debe ser de alta importancia con el fin de asegurar su disponibilidad – rendimiento.

Para cumplir el objetivo existen unas técnicas que a continuación validaremos en detalle,

Monitoreo continuo.

Existen herramientas que permiten validar el funcionamiento de los servidores en tiempo real, esto permitirá identificar alertas o eventos con anomalías, además, el monitoreo de la CPU, memoria, disco, y la latencia de la red para identificar y solucionar problemas que puedan afectar a los usuarios finales.

Actualizaciones - parches regulares:

Dentro del mantenimiento preventivo, es importante también automatizar las actualizaciones, de acuerdo con las políticas se debe realizar una previa configuración para su instalación automática de parches y actualizaciones de software, lo anterior optimiza el rendimiento y reducen en gran medida posibles vulnerabilidades, Por otra parte se requiere realizar pruebas en entornos de desarrollo o realizarlas antes de generar o aplicar las actualizaciones correspondientes y esto evita que no se interrumpan servicios críticos.

Optimización de recursos:

En el mantenimiento y la operación de la nube, es relevante evaluar el uso de recursos para asegurar que todos los servidores tengan las dimensiones adecuadas, para no presentar el uso insuficiente de recursos. Al aplicar políticas de auto scaling que esto permite ajustar de forma automática los recursos según la demanda.

Respaldos y recuperación:

Es importante contar con estrategias de backup desde una opción hasta 3 opciones que permitan mantener los datos en diferentes medios de almacenamiento, y adicional contar con una, fuera del sitio que podría ser en la nube o en un espacio físico pero que se encuentre por separado, con el fin de garantizar la recuperación de los datos en caso de siniestros o fallas.

Seguridad Proactiva

En este proceso se debe tener en cuenta dos aristas relevantes, las cuales son:

Cifrado de datos: Se debe asegurar que todos los datos, que se encuentren transitando o en reposo, estén cifrados para proteger a los datos sensibles contra accesos no autorizados.

Control de acceso: Es necesario implementar políticas de control que con un acceso estricto utilizando herramientas de la nube, otorgando y definiendo roles y permisos adecuados para disminuir y minimizar los riesgos de seguridad.

Documentación y procedimientos:

En todo proceso tecnológico es importante y estratégico, mantener una documentación detallada de todo lo correspondiente, con la infraestructura procedimientos mantenimiento y configuraciones de los servidores, así también, el procedimiento de backup y las políticas de seguridad y protocolos de recuperación de manera actualizada. Además, se deben contar con los procedimientos estandarizados que permitan realizar tareas de mantenimiento, reducir el margen de error humano y asegurar la consistencia en los procesos.

Desempeño y conectividad 4.5

Es relevante para TechSolutions S.A , conocer el desempeño y los temas de conectividad que ofrece trabajar bajo los servicios de la nube, en este sentido los proveedores de internet que se seleccionen deben cumplir a cabalidad con el rendimiento de las operaciones y así impactar ampliamente en la conectividad y garantizar la continuidad de las operaciones de cada uno de los clientes, por otra parte, si se habla de variaciones debemos tener en cuenta que en la nube podemos encontrar un rendimiento de red troncal aceptable.

Dado lo anterior, podemos decir, que, aunque se trabaje con proveedores de calidad y estables, siempre se debe mantener un margen de error que proviene de problemas con el rendimiento en el tráfico y la disponibilidad en riesgo de la perdida de paquetes.

Es importante precisar, que el rendimiento de latencia en la mayoría de las regiones está por debajo de umbral que es de 2 milisegundos de lo indicado, en algunos casos el rendimiento de nube a nube compite mientras en ocasiones se gestiona sin pasar por internet aplicándose directamente

5. Impacto en el Personal y Operaciones

Personal IT:

Datacenter Local:

Formación: El personal de IT necesitará adquirir las habilidades necesitadas para manejar y mantener el hardware y software del datacenter. Esto incluye los conocimientos sobre redes, servidores y seguridad física.

Responsabilidades:

Las responsabilidades aumentan, ya que deberían encargarse de la instalación, revisión, actualización y solución de problemas de la infraestructura. Este trabajo puede implicar realizar tareas fuera del horario laboral habitual para mantener el datacenter en funcionamiento y seguro.

La nube:

Formación: Se requerirá que el personal de IT se capacite en la administración y seguridad de servicios en la nube, como los ofrecidos por AWS, Azure o Google Cloud. Responsabilidades: Las responsabilidades se centran más en la revisión y optimización de los recursos en la nube, bajando la carga de mantenimiento físico. Esto ayuda al equipo IT a enfocarse en mejorar las aplicaciones y servicios.

Operaciones Diarias y Productividad:

Datacenter Local:

Impacto: Las operaciones pueden verse afectadas por problemas de hardware y mantenimiento. La necesidad de un equipo interno para solucionar estos problemas puede causar problemas temporales en las actividades diarias.

Productividad: Aunque la empresa tiene mayor control sobre el rendimiento y la personalización de la infraestructura, la necesidad de solucionar problemas técnicos puede disminuir la productividad. La capacidad para responder de manera rápida sin problemas al tener en cuenta es importante para minimizar el tiempo de inactividad.

La nube:

Impacto: El depender de la conectividad a internet y del proveedor de servicios puede ser un riesgo. Sin embargo, los proveedores para la nube suelen garantizar siempre altos niveles de disponibilidad y funcionamiento, lo que baja la probabilidad de interrupciones.

Productividad: La alta disponibilidad y funcionalidad para la nube permiten a los desarrolladores y los empleados tener los recursos cuando los vallan a necesitar, mejorando la eficiencia y ayudando a la colaboración. Sin decir, la latencia y los problemas de conectividad pueden afectar mucho el rendimiento de ciertas aplicaciones.

Costo 5.1.

Datacenter Local:

Los costos iniciales incluyen la obtención de hardware, instalación, acondicionamiento para el espacio y medidas de seguridad. Aunque estos costos son algo grandes, de manera establecido, los costos operativos son más controlados y predecibles a largo plazo. esta empresa tiene control total sobre las inversiones y los posibles gastos operativos tenidos en cuenta.

La nube:

Los costos iniciales son bajos gracias al modelo de pago por uso, que deja pagar solo por los recursos usados. Sin embargo, a medida que aumentan las necesidades de recursos y almacenamiento, los costos pueden incrementarse significativamente. Es bueno revisar y optimizar el uso de recursos para manejar los gastos.

Escalabilidad 5.2.

Datacenter Local:

El hardware y las capacidades físicas disponibles limitan la escalabilidad. La empresa debe invertir más en infraestructura para mejorar, lo que implica más costos y tiempo de implementación. Esta expansión puede ser complicada y requiere una planificación cuidadosa para garantizar que las operaciones continúen.

La nube:

La escalabilidad extremadamente flexible de la nube permite agregar o reducir recursos según las necesidades sin necesidad de invertir una cantidad adicional de dinero. Esto puede ser especialmente útil para empresas en crecimiento o con necesidades fluctuantes porque facilita la adaptación rápida a los cambios en la demanda.

Seguridad y cumplimiento 5.3.

Datacenter Local:

La empresa tiene el control total sobre la seguridad física y lógica de su infraestructura. Puede cumplir con normas y regulaciones internas y externas implementando políticas y procedimientos específicos. La gestión de accesos, las auditorías de seguridad y la protección contra amenazas físicas y cibernéticas son ejemplos de esto.

La nube:

La seguridad y el cumplimiento dependen en gran medida de las políticas y medidas del proveedor de nube.

Mantenimiento y Operaciones 5.4.

Datacenter Local:

Se necesitaría un equipo interno dedicado al mantenimiento y soporte al datacenter. Lo cual esto incluye la actualización de hardware y software, la monitorización de sistemas y la resolución de problemas. El mantenimiento regular es necesario para asegurar el rendimiento y la disponibilidad continua de los servicios.

La nube**:**

El mantenimiento de la infraestructura del datacenter es gestionado por el proveedor de servicios en la nube. Esto libera al personal IT de tareas rutinarias de mantenimiento, lo cual permitiéndoles enfocarse en actividades estratégicas y de valor agregado, como la optimización de aplicaciones y servicios.

Desempeño y Conectividad 5.5.

Datacenter Local:

El desempeño es muy controlable y optimizable ya que se podría satisfacer las necesidades específicas de la empresa. La proximidad física de los servidores puede resultar en tiempos de respuesta rápidos y baja latencia. lo que, cualquier problema en el hardware o la red local afectar directamente el rendimiento lo que podría bajar mucho la productividad.

La nube:

El desempeño depende de la conectividad a internet y de la calidad del servicio del proveedor de nube. La velocidad puede ser algo muy importante, ya que especialmente para aplicaciones que necesitan tiempos de respuesta bastante rápidos. Es algo importante asegurar una conexión de internet robusta y fiable para minimizar problemas de rendimiento. Los proveedores de nube suelen ofrecer herramientas para monitorear y optimizar el desempeño de los servicios alojados.

6. Recomendación Final

La recomendación final es migrar la infraestructura a la nube por los siguientes aspectos:

- Los servicios de la nube ofrecen seguridad y privacidad utilizando los principios de responsabilidad, confidencialidad, disponibilidad y preservación de la información.
- La nube se identifica por autoservicio bajo demanda, amplio acceso a la red y agrupación de recursos y escalabilidad.
- El crecimiento de TechSolutions S.A. con la nube será posible gracias a la capacidad de crear recursos específicos en la nube, permitiendo mejorar y reducir costos.
- La seguridad adecuada en la infraestructura nube de TechSolutions S.A dependerá de los diferentes sistemas de detección de intrusos para rastrear amenazas manera inteligente a través de la red.
- Los proveedores y clientes de la nube juegan un papel en la implementación, ya que ambas partes deben trabajar en equipo para abordar las necesidades de seguridad.
- Al inclinarse sobre la nube en cuestión de costos hay una reducción en costo, dado que, se elimina la necesidad de la infraestructura física y costosa, solo se invertirá en temas operativos.
- Permite ajustar automáticamente los recursos, dependiendo de la demanda, logrando así una eficiencia operativa con el fin de reducir los tiempos de inactividad, puesto que esto, facilita la adaptación a cambios en el mercado que se puedan presentar.
- Al optar por la nube, se podrá contar con un mantenimiento simplificado, es decir, beneficia de mantenimiento preventivo, además, de actualizaciones automáticas, gestionadas por los proveedores de servicio de la nube

- Dentro del marco de desempeño y conectividad, contara con una infraestructura tecnológica de alto nivel, dado que, contara con un rendimiento y conectividad confiable, genuina para operaciones eficientes y a nivel global.
- Estas ventajas de migrar a la nube para la empresa TechSolution S.A ayudará adaptarse a un ambiente empresarial dinámico, porque podrá aprovechar las oportunidades de crecimiento de forma efectiva y ágil.
- Otra recomendación muy importante para irse por la nube es, lograr la continuidad operativa, gracias a, poder contar con una infraestructura tecnológica resistente y sólida.

7. Implementar una instancia EC2 con dos contenedores, estos contenedores deben tener un balanceador de carga.

En la sección Apéndice se pueden observar las imágenes de la 1 a la 28 del proceso de implementación de una instancia EC2.

Video explicativo: Video_Entrega2.mkv

8. Implemente un sitio estático s3, el mismo que uso en los contenedores.

En la sección Apéndice se pueden observar las imágenes de la 1 a la 13 del proceso de implementación de un S3.

9. Explique lo siguiente, ¿Cuál de las dos alternativas elegiría para implementar o mantener este sitio web en internet? Explique las ventajas y desventajas de cada opción.

La elección entre EC2 y S3, dependerá en gran medida de las necesidades establecidas y específicas de la aplicación web que se requiera, de ello, se debe considerar factores de complejidad – tipo de contenido tendrá la página a desarrollar, y además la disponibilidad de la infraestructura.

Lo mencionado previamente, se puede detallar que cuando se trabaja con EC2 su dinámica es orientada para aplicaciones o sitios web más complejos, por ende, requieren de procesamiento dinámico, además, uso de base de datos interactivas o aplicaciones que requieren de mantenimiento frecuentes en la configuración del servidor.

Para S3 su estandarización es apta para aplicaciones estáticos o aplicaciones que inicialmente sirven de contenido estático, como lo son imágenes, archivos multimedia, asimismo, hojas de estilo y scripts.

A continuación, compararemos los servicios AWS (EC2 y S3) destacando sus ventajas y desventajas al utilizar cada uno:

Tabla 1. EC2

<table>
<tr><td colspan="2">EC2: En el momento que se esté considerando el uso de una aplicación web que sea compleja, tal vez con una base de datos, procesamiento en tiempo real o necesidades específicas para un servidor, entonces EC2 podría ser la mejor opción. De ello, Cuando hablamos de EC2(Elastic- Cumpute -Cloud) Es un servicio fundamental que permite a las empresas poder ejecutar sus aplicaciones en la nube de manera efectiva, permitiendo a los desabolladores integrar múltiples máquinas de modo virtual. Además, en EC2 podemos, automatizar la escalabilidad y simplificar la gestión de almacenamiento de forma simplificada, lo cual permite la implementación de servidores en la nube. De lo anterior, resulta necesario decir que, este servicio reduce costos, en temas de adquisición de hardware para las empresas, mejorando la eficiencia operativa optimizando los proceso desarrollo empresarial.
Cabe resaltar que, la forma de cobro depende del tamaño y el tiempo de uso de la instancia, el sistema operativo y la región, también, se factura dependiendo del consumo de los diferentes recursos.</td></tr>
<tr><td>Ventajas</td><td>Desventajas</td></tr>
<tr><td>• Tiene mayor flexibilidad y control dado que, permite a los usuarios realizar configuraciones, además, personalizar las instancias del servicio.
• Puede ejecutarse cualquier tipo de aplicación web, ya que puede extender aplicaciones en distintos entornos y configuraciones.
• Puede ser escalable según las necesidades que haya, producto de que soporta diversos sistemas</td><td>• Puede necesitar más mantenimiento.
• Es mayor su complejidad al configurarlo
• Es más costoso
• Requiere gestionar el sistema operativo, y el monitoreo necesario a la infraestructura
• Puede que terceros accedan a toda la información
• En el momento de contar con una amplia información reduce el</td></tr>
</table>

operativos y lenguajes de programación. • Servicio de tamaño modificable, según de las necesidades requeridas por el usuario. • Reducción en los tiempos de iniciación de instancias, gracias a factores como: Optimización de infraestructura / virtualización / Instancias pre-iniciadas e innovaciones tecnológicas. • Ofrece un servicio en la nube que proporciona capacidad de computación segura, redimensionable. • No se requiere invertir en hardware por anticipado. • Facilita el desarrollo y la implementación de aplicaciones de forma ágil y rápida. • De forma sencilla se tiene la oportunidad de iniciar pausar y finalizar las instancias. • Gracias a Auto Scaling (Que es una función de EC2) es posible ajustar de forma automática la cantidad de instancias.	control, sobre los permisos de quienes tenga acceso a la data. • La complejidad del sistema puede llegar a incrementar la dificulta de implementación – costos- presencia de errores- mantenimiento- curva de aprendizaje. • En el momento que exista gran cantidad de datos de información, puede que aumente los niveles de riesgos de seguridad. • La dependencia de servicios en línea puede, generar interrupción en la conectividad, disponibilidad limitada y latencia incrementada • Puede existir aumento de vulnerabilidades, accesos no permitidos y que se incumpla la normatividad.

Tabla 2. S3

<table>
<tr><td colspan="2">S3: Si el sitio web es mas de ser informativo y las páginas son tipo estáticas, S3 sería el más adecuado, ya que es fácil de usar y más mucho más económico por sus características. De lo anterior podemos decir que S3, es un servicio avanzado que almacena objetos ofreciendo alta escalabilidad, cuenta con una seguridad robusta y una velocidad eficaz. Diferentes empresas lo utilizan, ya sean pequeñas grandes, para almacenar y proteges datos en diversas aplicaciones, como los son: Sitios web, Aplicaciones Web, copias de seguridad, también IoT y análisis de big data. Es importante precisar que S3 permite personalizar y controlar el acceso a los datos, con funciones de gestion flexible, con la finalidad de cumplir con las necesidades de las empresas y los objetivos- estándares regulatorios.</td></tr>
<tr><td>Ventajas</td><td>Desventajas</td></tr>
<tr><td>• Es más fácil de configurar y además usarlo gracias de que cuenta con una interfaz intuitiva – documentación detallada y capacidad de automatización.
• Es considerablemente escalable y confiable, gracias a la capacidad de manejo automático de gran cantidad de datos, garantizando alto nivel de disponibilidad.
• Funciona mejor para los sitios web más estáticos, debido a su capacidad de almacenar, permitiendo servir y escalar archivos estáticos, de manera eficiente.
• Una solución de bajo costo para almacenamiento.</td><td>• Su diseño y sus características asignadas lo hacen más apto para sitios estáticos.
• Tiene menor flexibilidad para aplicaciones más complejas, producto a su naturaleza almacenamiento, que se enfoca en archivos estáticos.
• Se tiene menos control en la configuración a diferencia de EC2.
• Si el sitio web tiene mucho tráfico los costos de transferencia puede acumularse.</td></tr>
</table>

• Versiones de los objetos almacenados contando con una capa de control adicional. • Alta durabilidad para los datos almacenados, gracias a su replicación – colocación geográfica y verificación de integridad. • Su diseño se basa en con una disponibilidad de 99.99%. • Es capaz de contar con objetos cifrados, con el fin de proteger su contenido, esto ayuda que, los datos estén protegidos y estén siempre seguros. • Tiene la capacidad de integrarse con la gran una gran variedad de servicios de AWS. • Logra usar alojamiento de sitios web estáticos en S3, con el propósito de que los portales web, que no cuenten con contenido dinámico estén accesibles en internet.	

10. Deberá implementar una arquitectura de aws con balanceador de carga de aplicación para al menos dos instancias y que estas a su vez, tengan al interior balanceador de carga de contenedores (puede ser el mismo que se solicitó en la entrega 2).

- Se creó un Load Balancer en la consola de AWS, luego configurando sus grupos de seguridad
- Se desplegaron las dos instancias EC2 en Linux y se aseguraron de estar en la misma VPC y las subredes
- Se instalaron Docker en cada instancia para gestionar contenedores.
- Dentro de cada instancia EC2, se configuraron contenedores para el balanceo de carga interno.
- Luego de eso se verificó que quedara funcionando de manera correcta.
- Además, se creó un Auto Scaling para gestionar el escalado automático de las instancias.

Nota: En el punto 7 de la sección del apéndice se encuentran las imágenes del proceso de las instancias con balanceador de carga de contenedores

En la sección Apéndice se pueden observar las imágenes de la 1 a la 19 del proceso de implementación de balanceador de carga de aplicación y auto scaling.

Video explicativo: Entrega3.mkv

Figuras y tablas

De las tablas 1 a la 10 se expone la solución del punto 1 de evaluación de riesgos y seguridad.

Tabla 1. Riesgo y seguridad On-Premise a nivel de costo (Elaboración propia).

Riesgo y seguridad On-Premise a nivel de costo	**Mitigado Por**	**Tácticas de mitigación**
Inversiones iniciales en hardware y software.	Eficiencia.	• Contar con financiación e inversiones. • Tener claro el presupuesto inicial y proyecciones futuras. Contar con varias ofertas para la adquisición de dispositivos y licencias. • Realización del montaje de la infraestructura gradualmente
Costos en energía eléctrica y contar con generadores opcionales.	Eficiencia.	• Servidores de bajo consumo energético. • Sistemas de refrigeración. • Adquirir productos energéticos que cuenten con la etiqueta de eficiencia energética. • Utilización de energías renovables.
Mantenimiento y actualización de hardware y software.	Fiabilidad.	• Realización de contratos externos para el mantenimiento y soporte, asegurando así la operación diaria.
Mantener Seguridad física y	Seguridad.	• Instalación de centros CCTV de bajo costo Capacitaciones de seguridad al personal.

lógica en las instalaciones de la empresa.		• Controles de acceso en los aplicativos de la empresa Aplicativos gratuitos para la encriptación de la información. • Antivirus gratuitos, uso de cercas eléctricas para acordonar la estructura del data-center. • Segmentación de la red, personal especializado en cada Área.
Realización de inversiones de hardware y software si la empresa proyecta crecimiento.	Rendimiento.	• Compras de hardware segunda mano en buen estado. • Uso de software libre. • Herramientas de monitoreo gratuitas. • Automatización de procesos de despliegue de la infraestructura. • Compra de equipos modulares.

Tabla 2. Riesgo y seguridad On-Cloud a nivel de costo (Elaboración propia).

Riesgo y seguridad On-Cloud a nivel de costo	**Mitigado Por**	**Tácticas de mitigación**
Aumento de costo dependiendo la demanda de los recursos.	Rendimiento.	• Instancias reservadas. • Autoscaling automático. • Utilización de instancias spot. • Herramientas de monitoreo.
Cambios en las políticas de precios	Eficiencia.	• Revisión del contrato con el proveedor de nube.

del proveedor de la nube.		• Utilizar diferentes proveedores de la nube. • Capacitaciones internas sobre el cambio de políticas. Costos para el mejoramiento de la utilización de los recursos.
Utilización de servicios adicionales.	Eficiencia.	• Evaluar si es necesario la adopción de nuevos servicios. • Renegociar con el proveedor la adquisición de productos. • Realización de pruebas piloto.
Malas prácticas de configuración en los servicios utilizados.	Seguridad.	• Realización de auditorías internas y externas. • Prácticas de seguridad robustas. • Capacitación y evaluación constante al personal. Automatización de los servicios con mayor demanda.
Grandes volúmenes de almacenamiento de datos y transferencia.	Eficiencia.	• Utilización de servicios escalables ofrecidos actualmente por diferentes plataformas de nube. • Adoptar políticas de tiempo de almacenado de la información. • Utilización de técnicas de compresión de la información. • Uso de herramienta para el monitoreo del almacenado de los datos.

Tabla 3. Riesgo y seguridad On-Premise a nivel de escalabilidad (Elaboración propia).

Riesgo y seguridad On-Premise a nivel de escalabilidad	**Mitigado Por**	**Tácticas de mitigación**
Si la demanda de recursos aumenta es difícil satisfacer las necesidades.	Rendimiento.	• Tener proyecciones a corto, mediano y largo plazo para mitigar la demanda.
Inversión en la infraestructura.	Fiabilidad.	• Utilización de arquitecturas modulares.
Nuevas implementaciones pueden demorarse más de lo planeado.	Rendimiento.	• Herramientas de monitoreo para proveer necesidades de software o hardware futuras.

Tabla 4. Riesgo y seguridad On-Cloud a nivel de escalabilidad (Elaboración Propia).

Riesgo y seguridad On-Cloud a nivel de escalabilidad	**Mitigado Por**	**Tácticas de mitigación**
Malas prácticas de seguridad pueden poner la infraestructura en riesgo.	Seguridad.	• Controles de acceso robustos con los últimos estándares de seguridad. • Realización de pruebas de pentesting. • Mantener al personal actualizado de los últimos estándares de seguridad.
Un mal diseño de escalabilidad puede afectar la disponibilidad de los recursos.	Fiabilidad.	• Levantamiento de los requisitos no funcionales de línea base, carga y estrés. • Arquitectura escalable. • Gestión de recursos. • Monitoreo y alertas.
Tiempos de inactividad.	Fiabilidad.	• Planes de contingencia. • Arquitectura de alta disponibilidad. Redundancia de componentes. • Monitoreo y alertas.

Tabla 5. Riesgo y seguridad On-Premise a nivel de seguridad y cumplimiento (Elaboración Propia).

Riesgo y seguridad On-Premise a nivel de Seguridad y cumplimiento	**Mitigado Por**	**Tácticas de mitigación**
Fenómenos naturales.	Fiabilidad.	• Ubicación geográfica. • Diseño de infraestructura. • Planes de recuperación ante desastres.
Acceso de personal no autorizado.	Seguridad.	• Controles de acceso. • Alertas de personal sospechoso. Monitoreo. • Políticas de acceso a las instalaciones y manipulación de equipos.
Ataques informáticos.	Seguridad.	• Monitoreo para la detención de amenazas. • Cifrado de datos. • Actualización de software y hardware. • Realización de backups periódicos.

		• Equipo capacitado para solución de incidentes.
Incumplimiento de normativas.	Seguridad.	• Realización de auditorías. • Escaneo de vulnerabilidades. • Contar con personal idóneo para el cumplimiento de las normas. • Protección de la información sensible.
Errores humanos.	Fiabilidad.	• Capacitar al personal. • Realización de simulacros. • Contar con procesos claros.
Daños en la infraestructura.	Fiabilidad.	• Revisiones periódicas para identificar riesgos. • Simulacros de evacuación, normas y políticas para la manipulación de equipos. • Planes de contingencia si hay cortes de energía o daños en equipos.

Tabla 6. Riesgo y seguridad On-Cloud a nivel de seguridad y cumplimiento (Elaboración Propia).

Riesgo y seguridad On-Cloud a nivel de Seguridad y cumplimiento	**Mitigado Por**	**Tácticas de mitigación**
Perdida de información debido a ataques externos.	Integridad.	• Cifrado de datos. • Backups.
Inseguridad en las aplicaciones desplegadas en los diferentes ambientes.	Seguridad.	• Normas y estándares definidas. Revisiones periódicas.
Configuraciones incorrectas.	Seguridad.	• Monitoreo y alertas.
Secuestro de la información debido a ataques informáticos.	Seguridad.	• Equipo capacitado en ciberseguridad. • Parches de seguridad y actualizaciones.
Interrupción del servicio por parte del proveedor.	Fiabilidad.	• Escoger proveedores confiables. • Contar con SLA y arquitectura tolerante a fallos.

Tabla 7. Riesgo y seguridad On-Premise a nivel personal y operaciones (Elaboración Propia).

Riesgo y seguridad On-Premise a nivel de Personal y operaciones	**Mitigado Por**	**Tácticas de mitigación**
Indisponibilidad del servicio durante el mantenimiento.	Fiabilidad.	• Realizar mantenimientos programados y en lo posibles en horas de la noche.
Errores humanos durante el mantenimiento.	Fiabilidad.	• Capacitación periódica al personal. Simulacros antes emergencias. • Segregación de funciones.
Conflictos laborales que involucren actividades fraudulentas.	Integridad.	• Mantener un buen ambiente labora. • Alertas ante situaciones sospechosas.
Cambio de personal.	Seguridad.	• Capacitar al nuevo personal. • Eliminación de accesos. • Definición de responsabilidades.

Tabla 8. Riesgo y seguridad On-Cloud a nivel personal y operaciones (Elaboración Propia).

Riesgo y seguridad On-Cloud a nivel de Personal y operaciones	**Mitigado Por**	**Tácticas de mitigación**
Interrupciones del servicio durante el manteamiento programado.	Fiabilidad.	• Contar con ventanas de mantenimiento. • Avisar con anticipación los mantenimientos.
Configuraciones incorrectas por parte del personal.	Seguridad.	• Capacitar al personal. • Plan de contingencia por si se presentan fallos.

Tabla 9. Riesgo y seguridad On-Premise a nivel de desempeño y conectividad (Elaboración Propia).

Riesgo y seguridad On-Premise a nivel de desempeño y conectividad	**Mitigado Por**	**Tácticas de mitigación**
Problemas de rendimiento.	Rendimiento.	• Monitoreo. • Optimización del hardware. Realización de pruebas de performance.
Interrupciones en la conectividad.	Fiabilidad.	• Utilización de VPN. • Firewalls.
Latencia Alta.	Rendimiento.	• Distribución de cargas. • Priorización del tráfico de red.

Tabla 10. Riesgo y seguridad On-Cloud a nivel de desempeño y conectividad (Elaboración Propia).

Riesgo y seguridad On-Cloud a nivel de desempeño y conectividad	**Mitigado Por**	**Tácticas de mitigación**
Ubicaciones geográficas configuradas.	Seguridad.	• Seleccionar regiones que cumplan las normativas.
Gran tráfico de red.	Rendimiento.	• Sistemas de monitoreo. Segmentación de la red
Dependencia permanente a internet.	Fiabilidad.	• Contar con uno o varios proveedores de internet.

Conclusiones

Para este trabajo tenemos las siguientes conclusiones:

- Migrar a la nube reduce costos de infraestructura física, deshaciéndose de la necesidad de invertir en hardware, instalaciones y gestión de almacenamiento.
- La dinámica de pago por uso de la nube permite invertir solo en costos operativos, convirtiendo costos fijos en variables.
- Una mala gestión en la nube conlleva a elevar costos que resultan innecesarios.
- La nube permite ajustar los recursos de forma más ágil, dependiendo de las demandad, lo anterior mejora la disponibilidad reduciendo el riesgo de inactividad.
- TechSolutions S.A. pude aprovechar la estabilidad con el fin de lanzar nuevas aplicaciones y expandirse a nivel gloval.
- La implementación de estrategias de recuperación garantiza la continuidad del servicio en caso de interrupciones.
- Se deben establecer políticas de seguridad robustas, incluyendo la administración de accesos y actualizaciones periódicas y regulares.
- La implementación de autenticación de dos factores (2FA) y el uso de firewalls – control de acceso a nivel de IP y regiones son fundamentales.
- La infraestructura debe evaluarse regularmente, mediante auditorias y revisiones de seguridad para cumplir los estándares de políticas de seguridad.
- El mantenimiento preventivo –el monitoreo continuo, son fundamentales para garantizar el rendimiento óptimo de la infraestructura de la nube.
- Estrategias de backup y recuperación deben ser implementadas para asegurar la disponibilidad de datos en caso de eventos de sinestros.
- La elección de proveedores de internet confiables es importante para mantener un alto nivel de rendimiento y baja latencia.

- El rendimiento de la nube puede verse afectado, parla calidad de la conectividad a internet, de ello, es relevante asegurar una conexión robusta.
- El personal de IT necesita capacitarse en administración y seguridad de los diferentes servicios de la nube.
- Las operaciones pueden ser más eficientes y colaborativas con la alta disponibilidad de la nube, pese que la conectividad a internet siga siendo un fator crítico.
- La nube reduce el impacto de problemas de hardware, sin embargo, depende de la estabilidad del proveedor de servicios.
- La elección entre Amazon EC2 y S3 dependerá principalmente de las necesidades, específicas de la aplicación web en desarrollo, considerando algunos factores como la compresibilidad de la aplicación, el tipo de contenido y la disponibilidad de infraestructura.
- EC2 es ideal para aplicaciones web complejas, que necesiten procesamientos dinámicos, bases de datos interactivas y configuraciones de servidores personalizados.
- EC2 ofrece una capacidad de computación segura y redimensionable, sin necesidad de invertir en hardware por anticipado.
- EC2, permite el uso de diferentes sistemas operativos y lenguajes de programación, ofreciendo así, mayor flexibilidad y control.
- EC2 facilita la integración de múltiples máquinas virtuales, optimizando el proceso de desarrollo y eficiencia operativa.
- Puede ser más costoso u requiere un mayor mantenimiento.
- La configuración y el monitoreo del sistema operativo puede ser complejos, aumentando la curva de aprendizaje, además, los costos de implementación.
- Riesgo de seguridad producto a la posible accesibilidad por terceros y la dependencia de servicios en línea que pueden proporcionar interrupciones en la conexión.

- S3, es apto o adecuado para sitios web informáticos y aplicaciones que sirven contenido estático, como los son imágenes, archivos multimedia y scripts.
- Es más sencillo de configurar y usar con una interfaz intuitiva y documentación detallada.
- Ofrece alta estabilidad –durabilidad –seguridad, con una disponibilidad de 99.99% y capacidad de integración a otros servicios de AWS.
- Proporciona una solución de almacenamiento de bajo costo, con versiones de objetos y cifrado de datos para protección adicional.
- Ideal para alojar sitios web estáticos, garantizando accesibilidad – estabilidad eficiente de archivos.
- Menor flexibilidad para aplicaciones complejas, producto a su naturaleza, enfocada en el almacenamiento de archivos estáticos.
- Menos control en la configuración en comparación con EC2.
- Los costos de transferencia pueden acumularse en sitios web con mucho tráfico.
- Implementar en AWS un balanceador de carga de aplicación garantiza que el tráfico se distribuya equitativamente entre al menos dos instancias, ya que mejora la disponibilidad y la eficiencia a los diferentes fallos del sistema.
- Agregar los balanceadores de carga de contenedores dentro de cada instancia permite un mejor manejo de los recursos y una mejor distribución de la carga entre los contenedores.
- El auto escalado en AWS de manera que ajusta automáticamente la cantidad de instancias EC2 según la demanda, garantizando que las aplicaciones funcionen sin problemas y reduciendo costos, todo sin necesidad de intervención manual.

Referencias

Agencia, L. (n.d.). ACERCA DE ENISA.

AWS. (2024a). awseb-dg.pdf#using-features.managing.elb.

AWS. (2024b). ec2-ug.pdf#AMIs.

AWS. (2024c). rds-ug.

AWS. (2024d). s3-userguide.

AWS. (2024e). vpc-ug.

Bharti, Drsantosh & Goudar, R. (2012). Cloud Computing–Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication. 10.7763/IJFCC.2012.V1.95.

Badger, M. L., Grance, T., Patt-Corner, R., & Voas, J. (2012). Cloud computing synopsis and recommendations. https://doi.org/10.6028/NIST.SP.800-146

García Méndez, E. B. (s.f.). Proyecto de estadía profesional Apoyo en la migración de data center y nube Recuperado de: pública http://repositorio.uppuebla.edu.mx:8080/xmlui/bitstream/handle/123456789/269/esauBaruchGarciaMendezEP.pdf?sequence=1

Hernandez Quintero, N. L., & Smith Florez, A. (s.f.). Computación en la Nube. Dialnet-ComputacionEnLaNube-5109245.pdf.

Humberto Vera-Rivera, F., & Gaona, M. (2017). Platform as a service-PaaS for the management of technologies in the development and deployment of web applications. https://www.researchgate.net/publication/328542328

of Veterans Affairs, D., & Iam, C. (2018). Security Scoop The VA Enterprise Cloud Solutions.

J. Timmermans, B. C. Stahl, V. Ikonen and E. Bozdag, "The Ethics of Cloud Computing: A Conceptual Review," 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 2010, pp. 614-620, URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5708509&isnumber=5708426

keywords: {distributed systems;distributed computing;cloud computing;cyber-physical systems},
URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7436686&isnumber=7436668

Khalil, I.M.; Khreishah, A.; Azeem, M. Cloud Computing Security: A Survey. Computers 2014, 3, 1-35. https://doi.org/10.3390/computers3010001

Medina.A(2022) Principales claves del Informe sobre el Rendimiento de la nube 2022; de: https://www.thousandeyes.com/es-es/blog/top-takeaways-2022-cloud-performance-report

Montes.F(2012) Realidades del Cloud Computing; Recuperado de: http://revistasbolivianas.umsa.bo/scielo.php?pid=S199740442012000200038&script=sci_arttext&tlng=es

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. Sensors (Basel, Switzerland), 22(3), 927. https://doi.org/10.3390/s22030927

Pablo Federico Muñoz Calderón, & Martin Geovanny Zhindón-Mora. (n.d.). Dialnet-ComputacionEnLaNube-8638170.

Pacio, G. (2014). Data centers hoy. Alfaomega: Recuperado de: https://books.google.es/books?hl=es&lr=&id=43xNDAAAQBAJ&oi=fnd&pg=PT17&dq=como+afectaria+a+una+empresa+pasarse+a+la+nube+tanto+como+a+un+datacenter&ots=yIDW_NuTkG&sig=ie9u6guz7ECikFpK8AlWVffMkeo#v=onepage&q&f=false

Pavan.A(SF) Amazon EC2 vs Amazon S3: guía comparativa; Recuperado de: https://www.whizlabs.com/blog/amazon-ec2-vs-amazon-s3-comparison-guide/

Pavan.A(SF) ¿Qué es Amazon EC2 (Elastic Compute Cloud)?; Recuperado de: https://www.whizlabs.com/blog/amazon-elastic-compute-cloud-guide/

Radack, S. (2012). ITL BULLETIN FOR JUNE 2012 CLOUD COMPUTING: A REVIEW OF FEATURES, BENEFITS, AND RISKS, AND RECOMMENDATIONS FOR SECURE, EFFICIENT IMPLEMENTATIONS.

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. Sensors (Basel, Switzerland), 22(3), 927. https://doi.org/10.3390/s22030927

Saini, R., & Behl, R. (2020). An Introduction to AWS—EC2 (Elastic Compute Cloud). Proceedings of the International Conference on Research in Management & Technovation 2020, 24, 99–102. https://doi.org/10.15439/2020km4

Salih, S., Hamdan, M., Abdelmaboud, A., Abdelaziz, A., Abdelsalam, S., Althobaiti, M. M., Cheikhrouhou, O., Hamam, H., & Alotaibi, F. (2021). Prioritising Organisational Factors Impacting Cloud ERP Adoption and the Critical Issues Related to Security, Usability, and Vendors: A Systematic Literature Review. Sensors (Basel, Switzerland), 21(24), 8391. https://doi.org/10.3390/s21248391

S. U. Khan, "The Curious Case of Distributed Systems and Continuous Computing," in IT Professional, vol. 18, no. 2, pp. 4-7, Mar.-Apr. 2016, doi: 10.1109/MITP.2016.24.

Abstract: As distributed systems progress, they seem to continually revisit older concepts. This article examines the various types and evolution of distributed systems, and predicts where they might be headed.

Zaszcynski.E(2024) Mantenimiento Preventivo de Servidores en la Nube: https://es.linkedin.com/pulse/mantenimiento-preventivo-de-servidores-en-la-nube-zaszczynski-pzfkf

Apendice

Imágenes del 1 a la 28 implementación punto 7

Imagen 1. Creación VPC

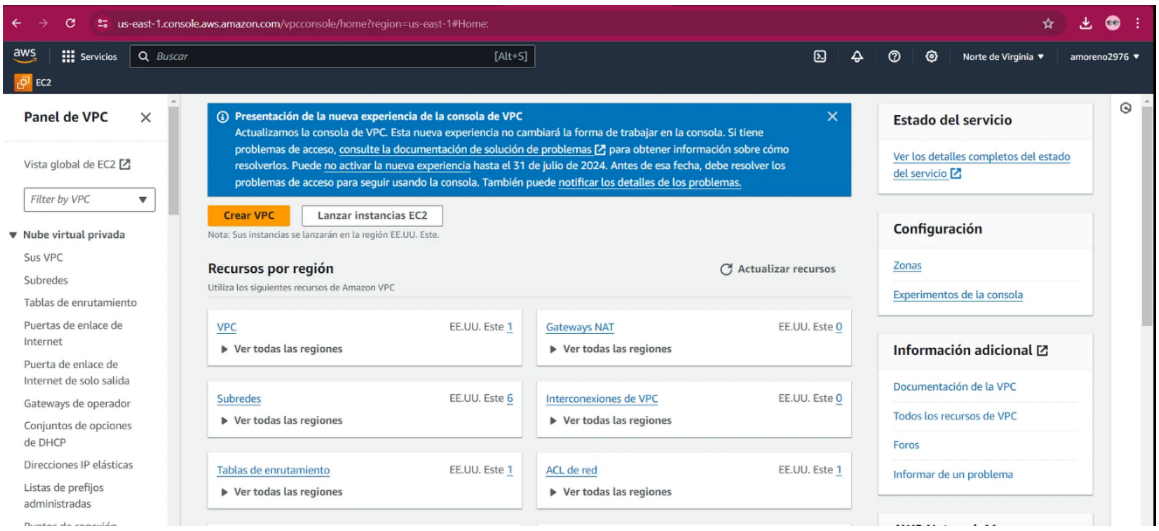


Imagen 2. Configuración de la VPC

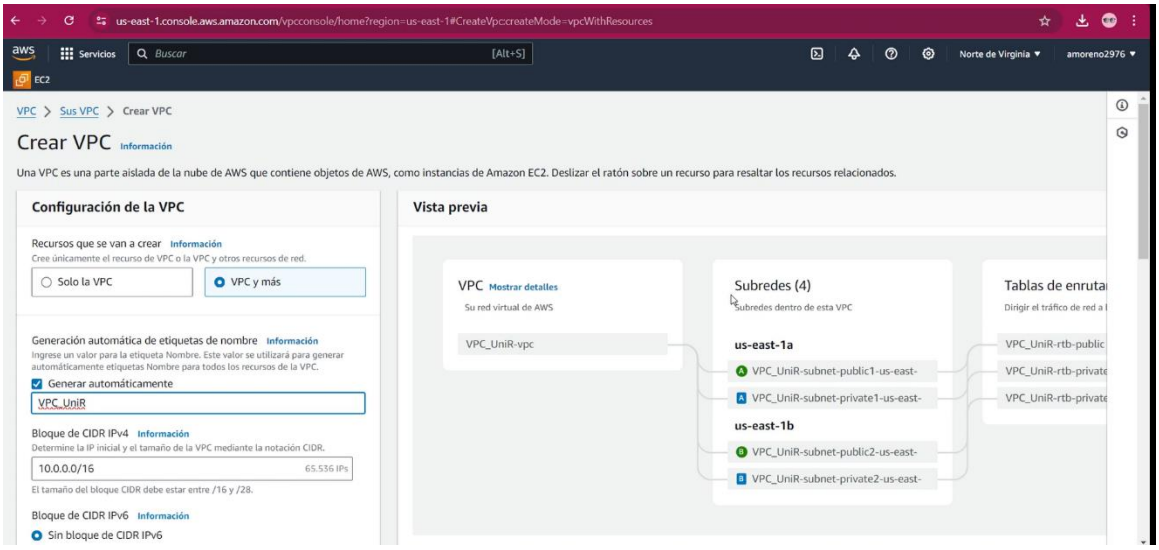


Imagen 3. Número de zonas de disponibilidad de la VPC

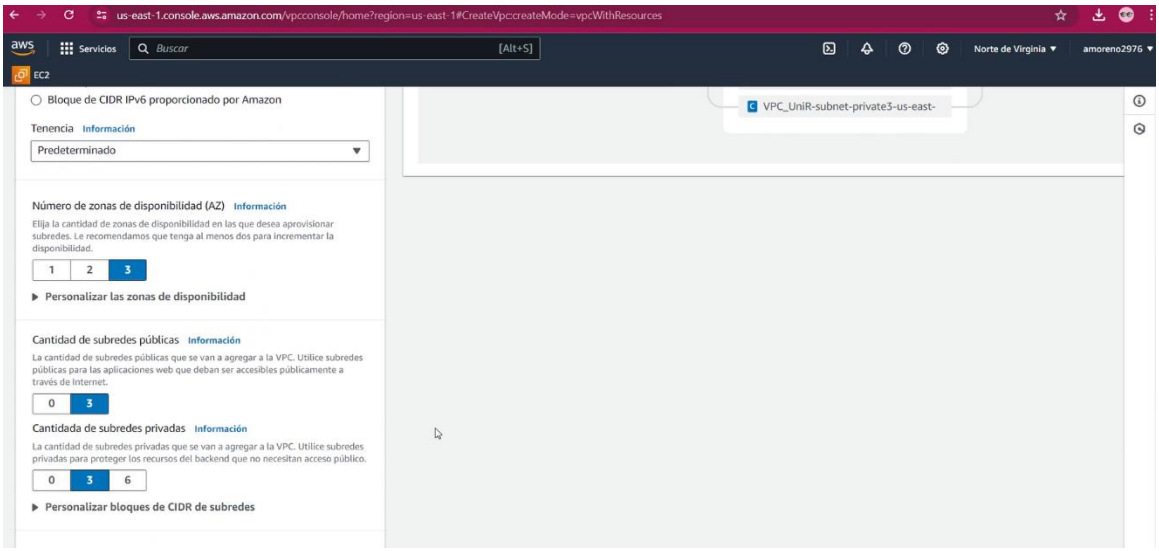


Imagen 4. Confirmación de creación de la VPC

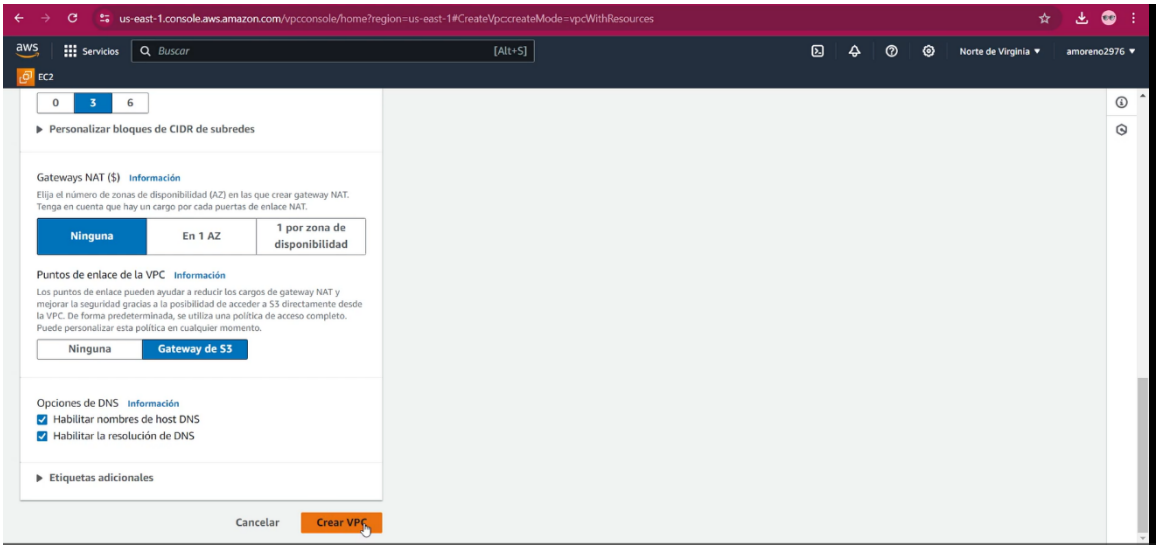


Imagen 5. Flujo de creación de la VPC

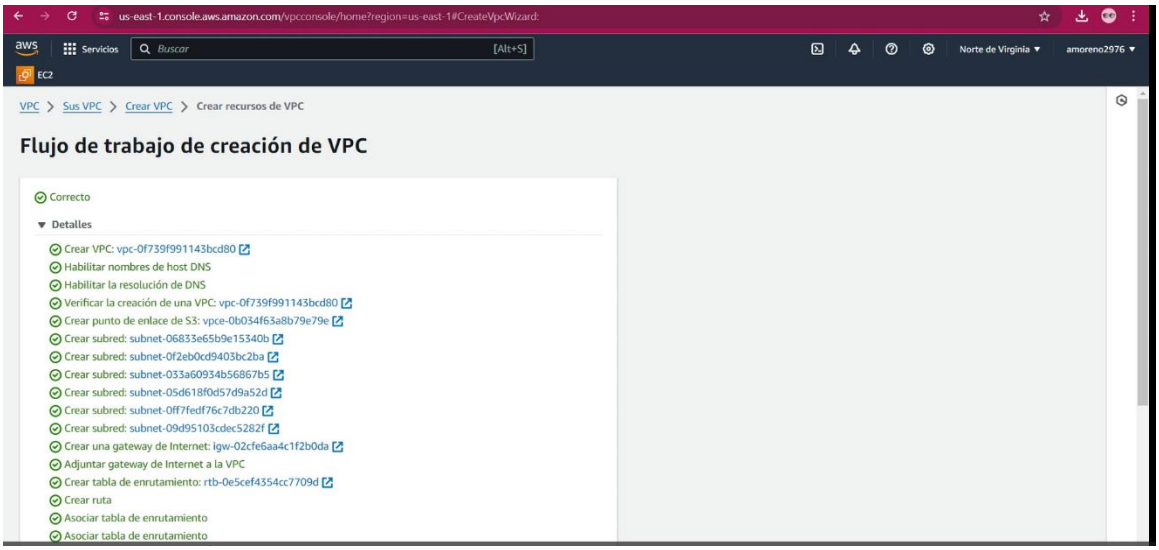


Imagen 6. Listado de VPC creadas

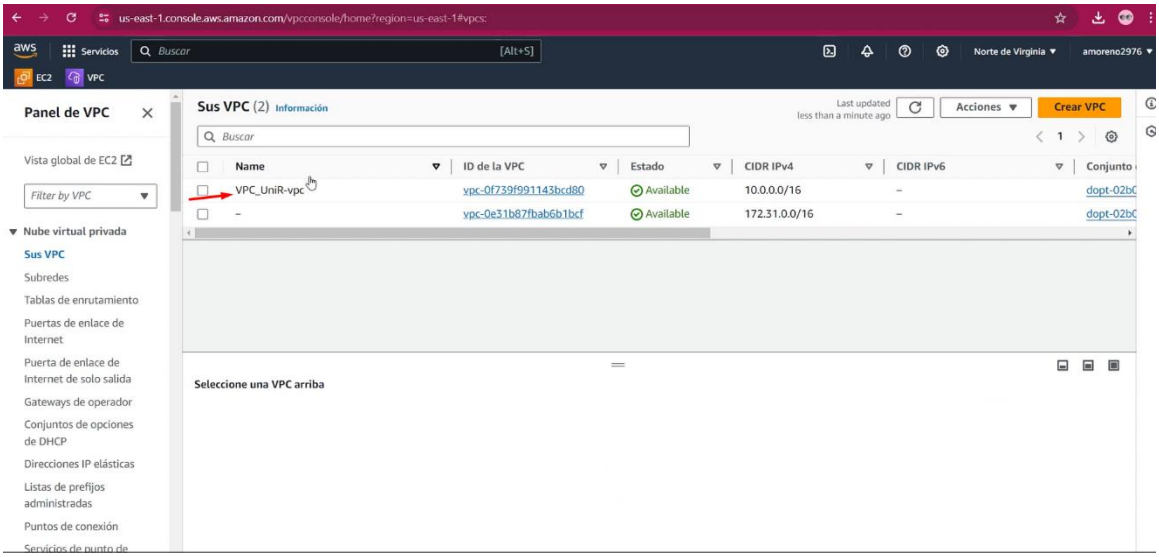


Imagen 7. Listado de subredes

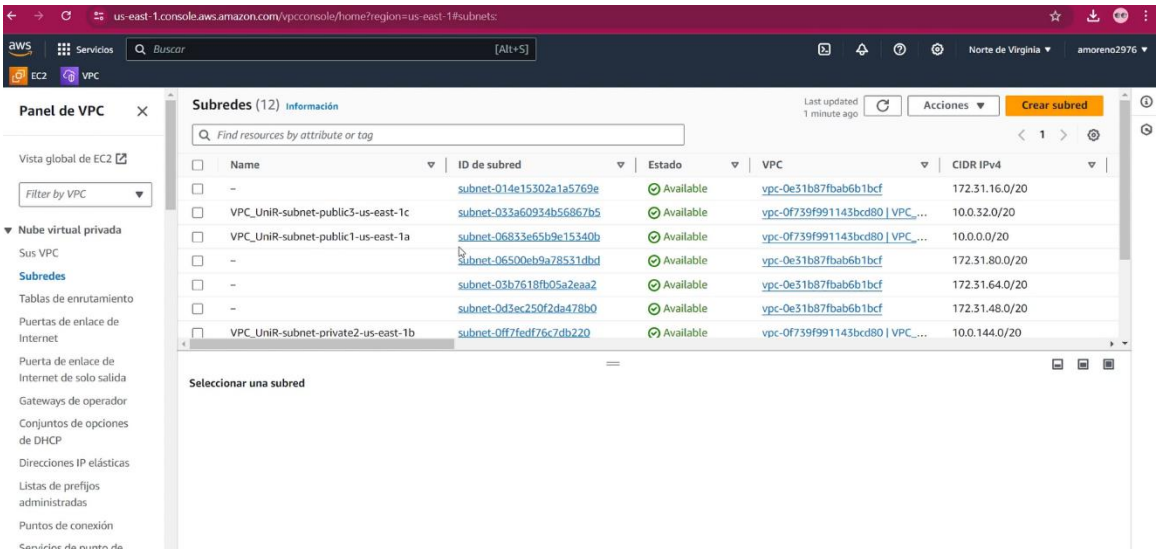


Imagen 8. Lanzamiento de la instancia

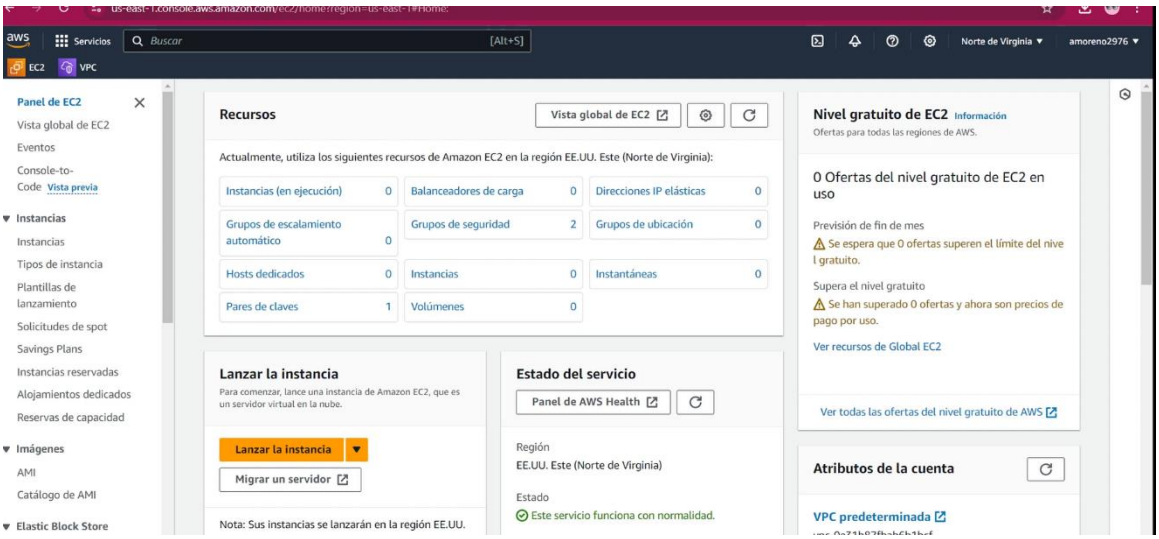


Imagen 9. Nombramiento de la instancia

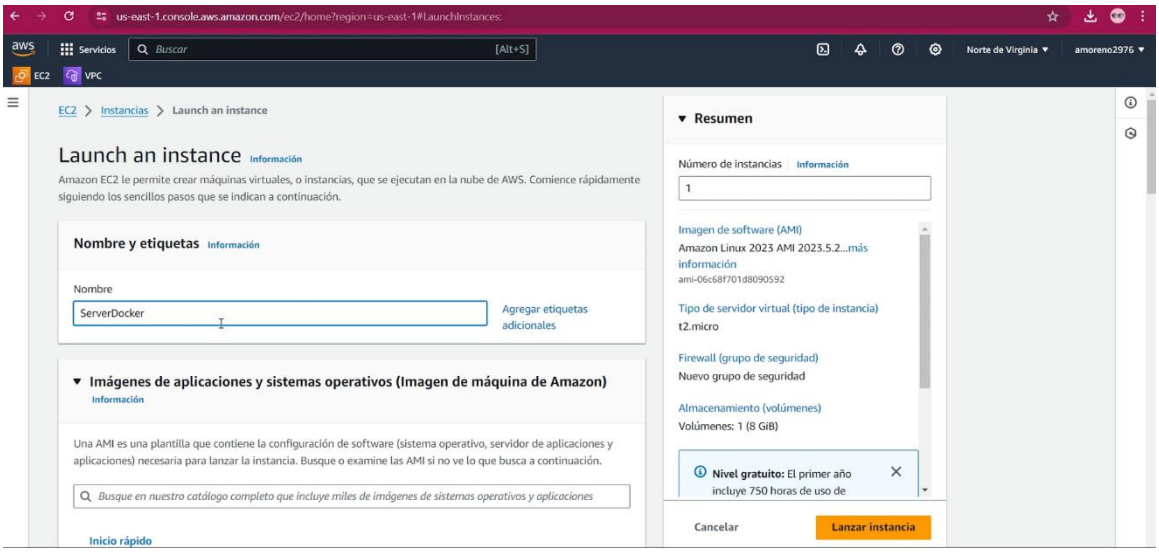


Imagen 10. Configuraciones de la instancia

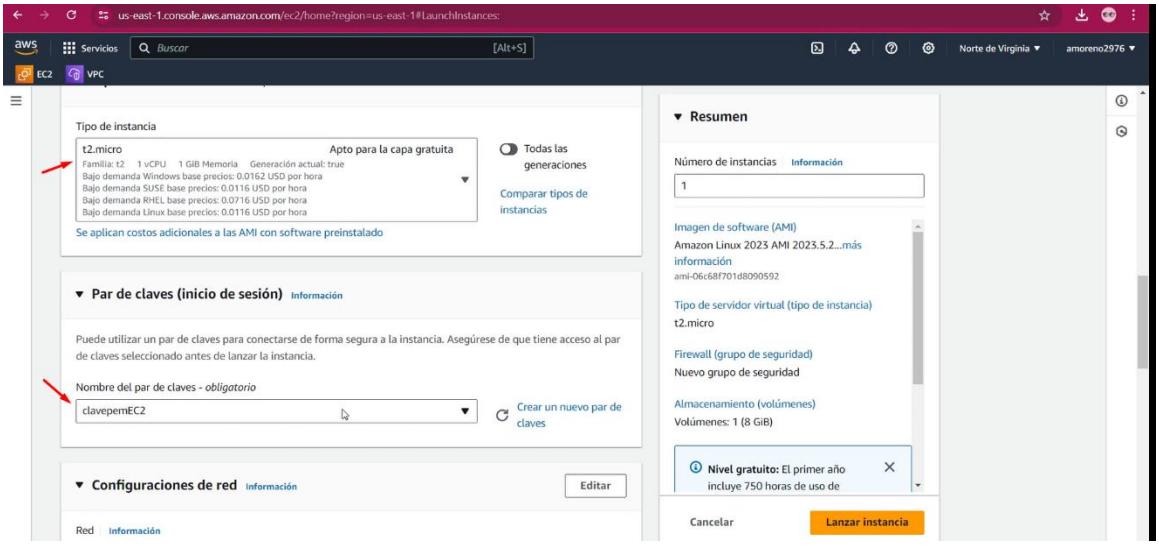


Imagen 10.1 Configuraciones de la instancia

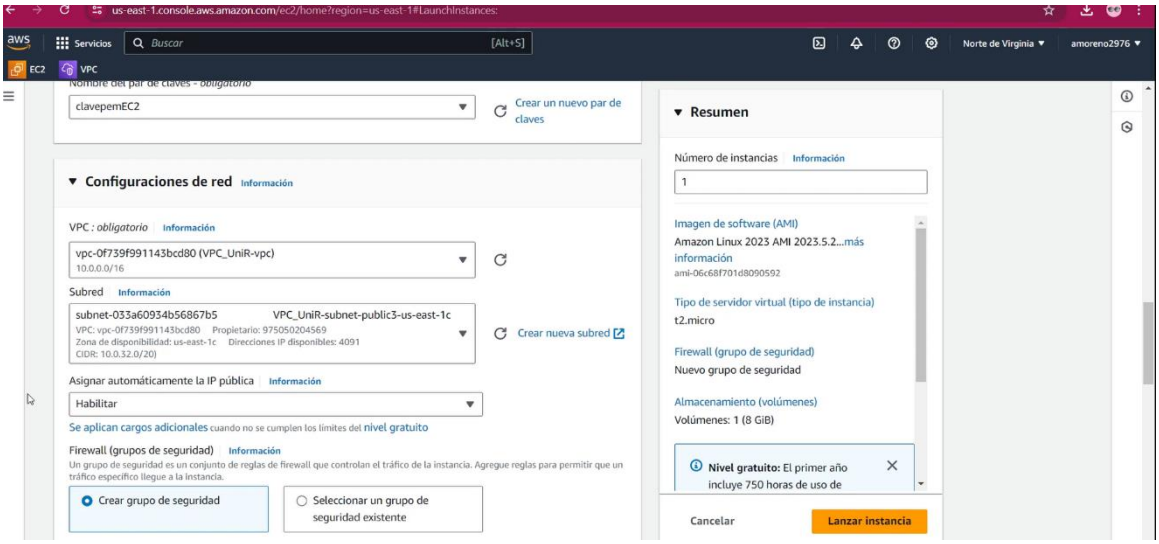


Imagen 10.2 Configuraciones de la instancia

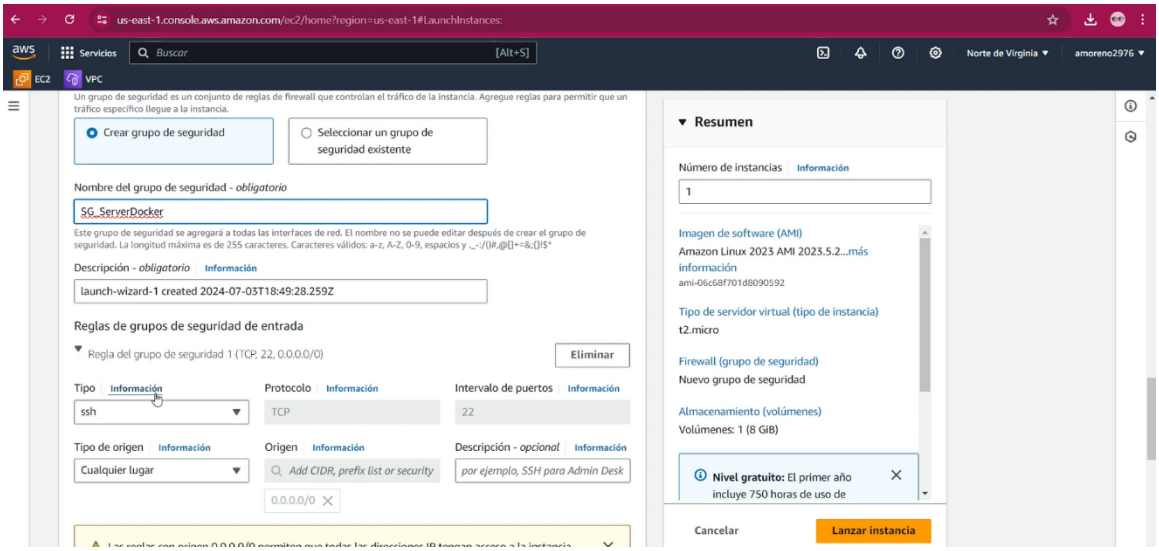


Imagen 10.3 Lanzamiento de la instancia

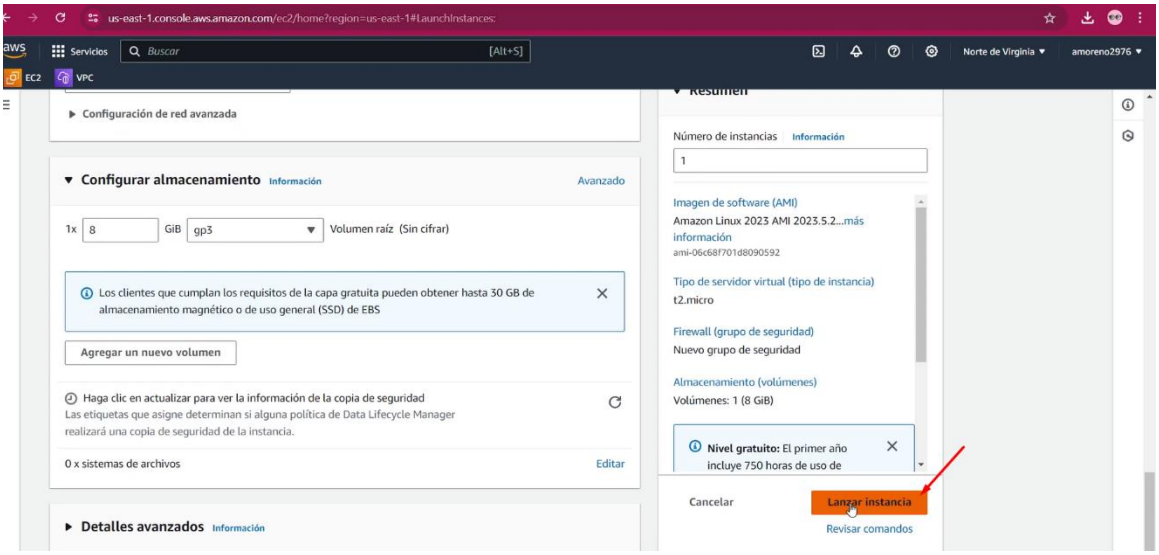


Imagen 11. Parámetros para conectarse a la instancia

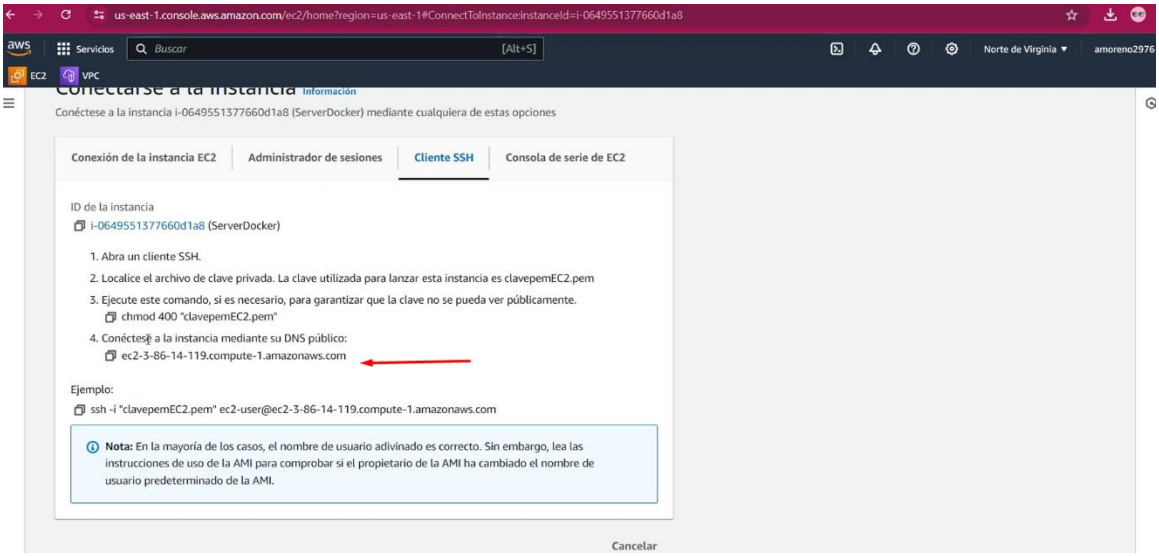


Imagen 12. Configuración conexión SHH

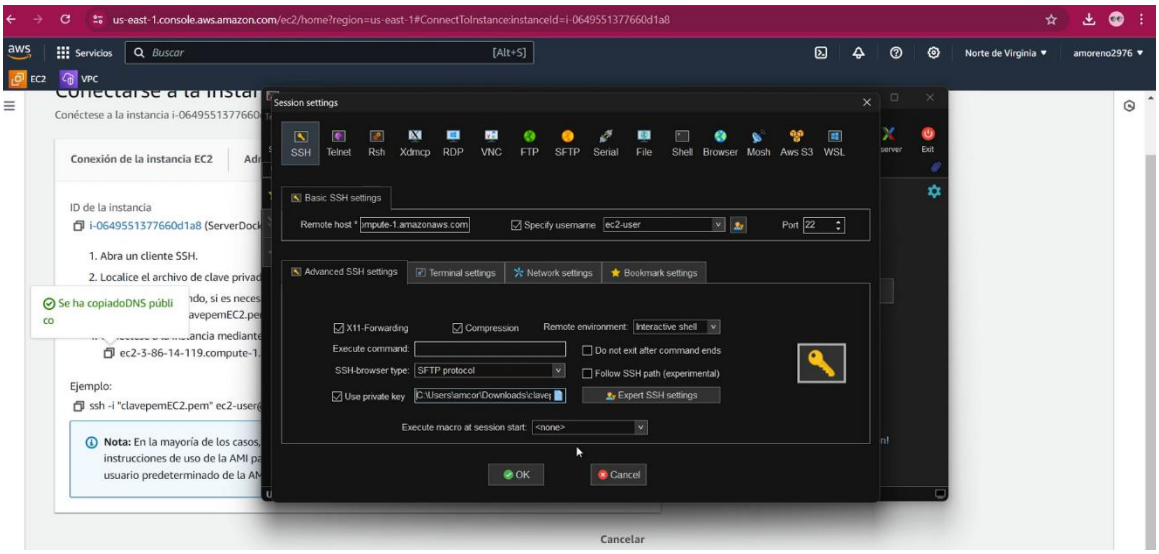


Imagen 13. Instalación del Docker en la maquina

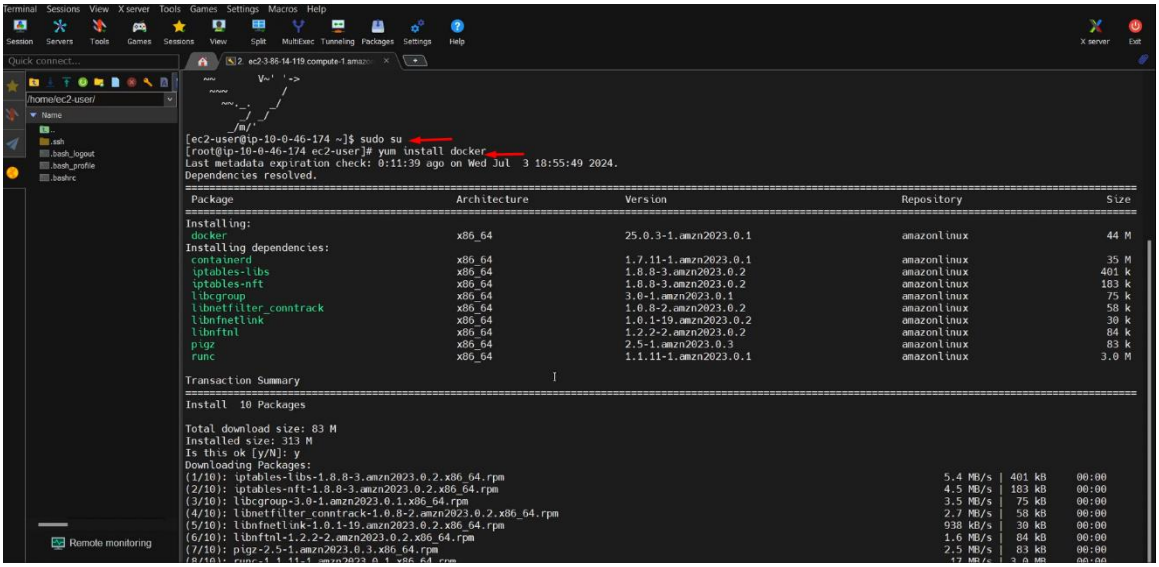


Imagen 14. Instalación de httpd

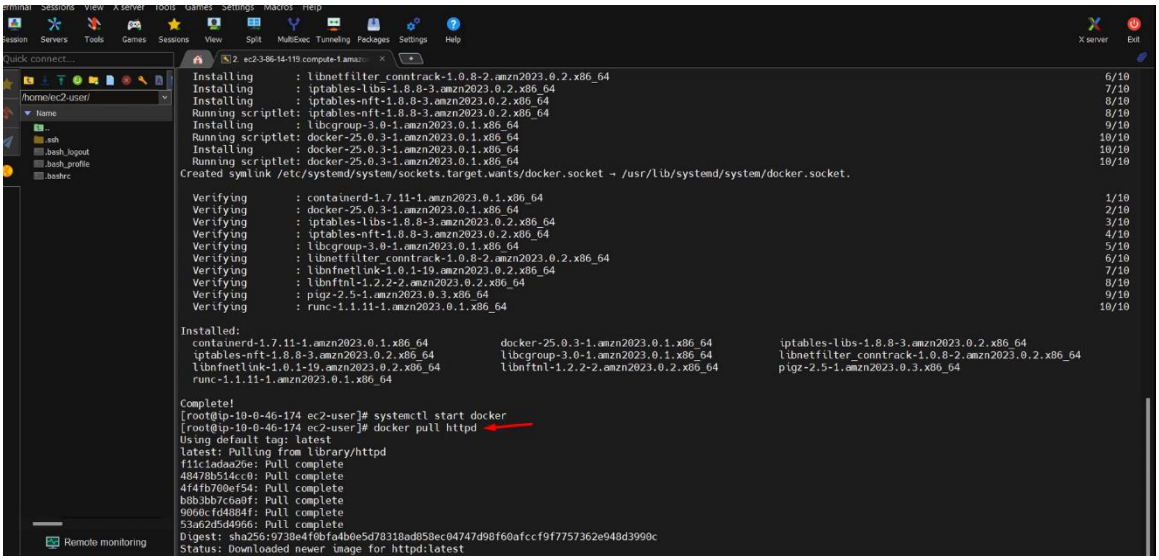


Imagen 15. Configuración del primer contenedor

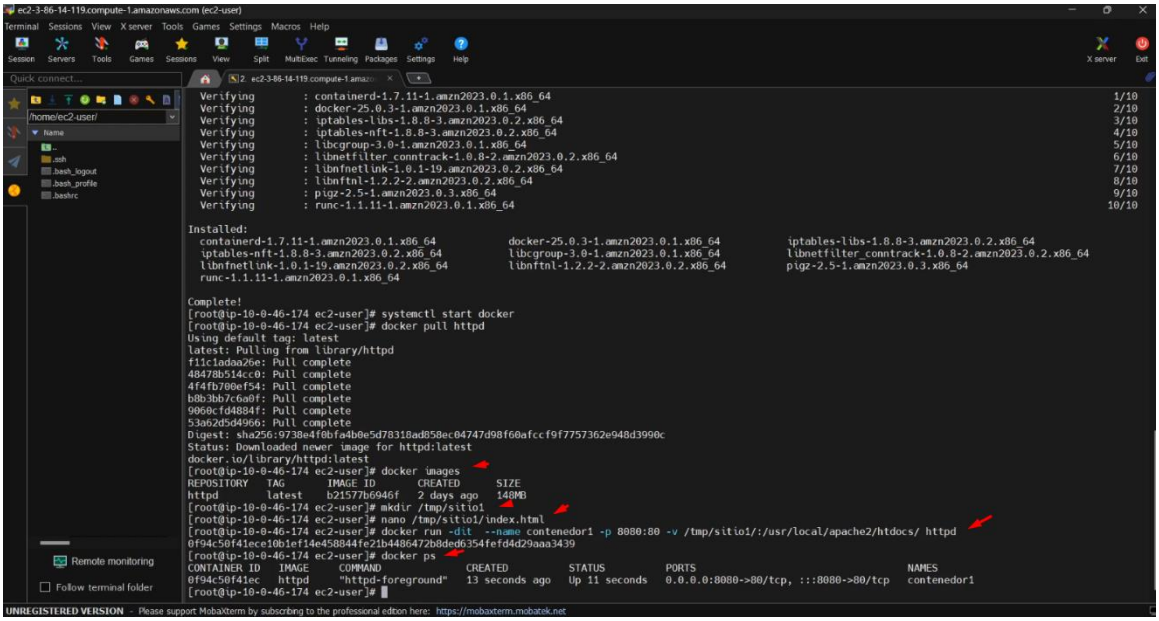


Imagen 16. Configuración de las reglas de grupo de seguridad para el contenedor uno

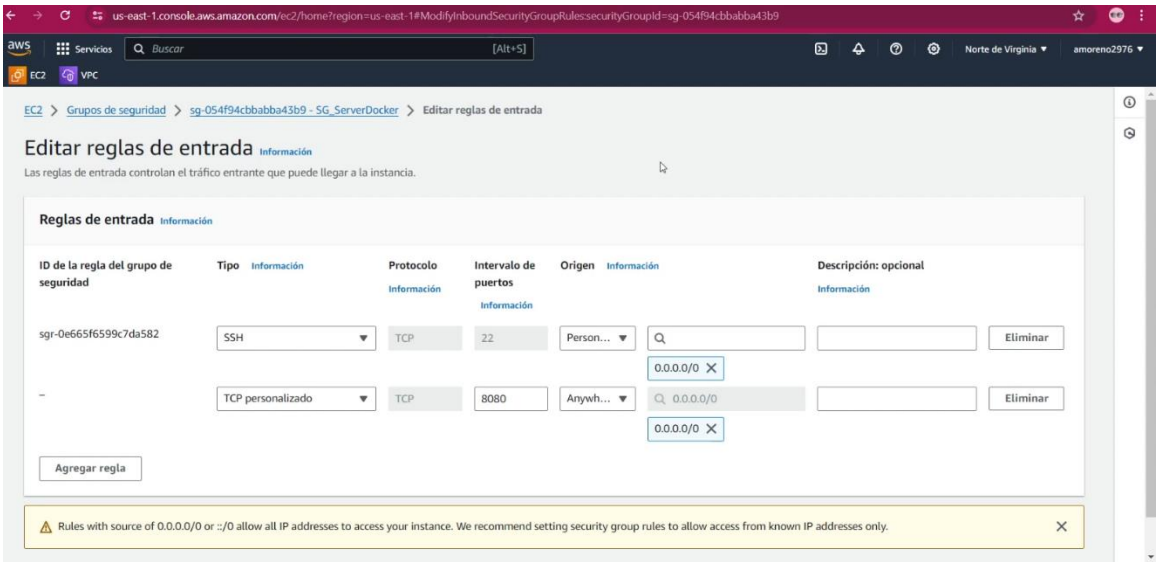


Imagen 17. Visualización de la información del contenedor uno

Imagen 18. Descarga de la plantilla HTML5

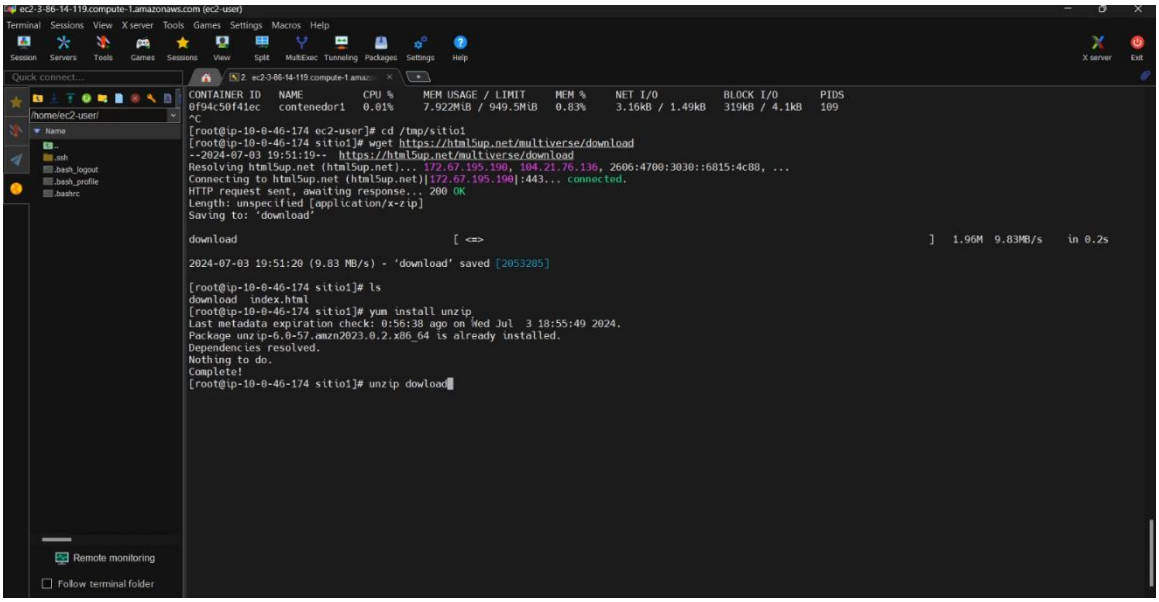


Imagen 19. Visualización de la plantilla HTML5 en la IP publica

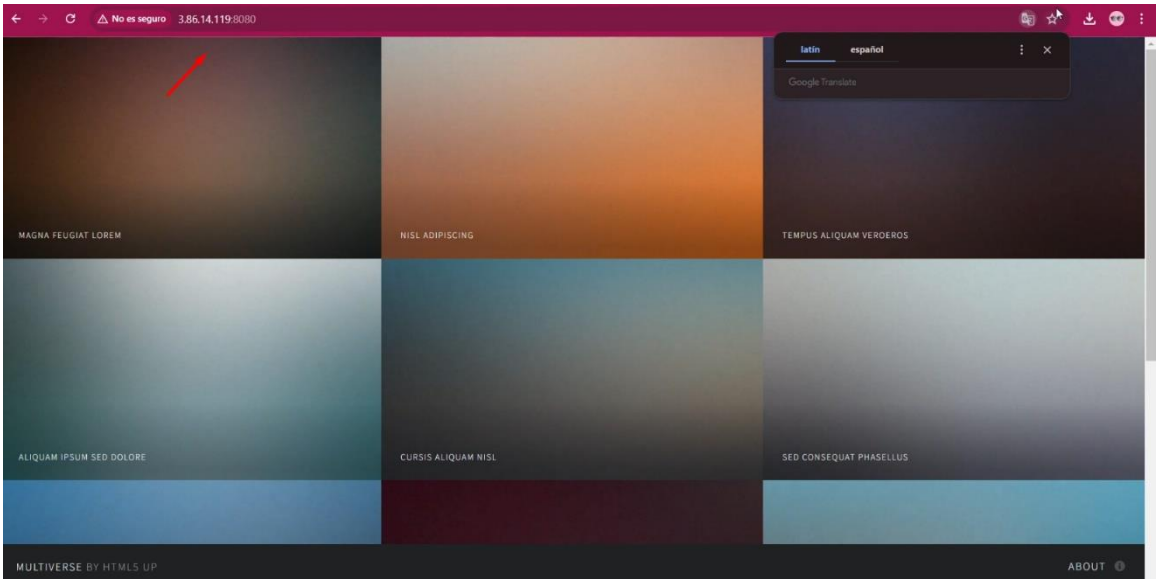


Imagen 20. Configuración del segundo contenedor

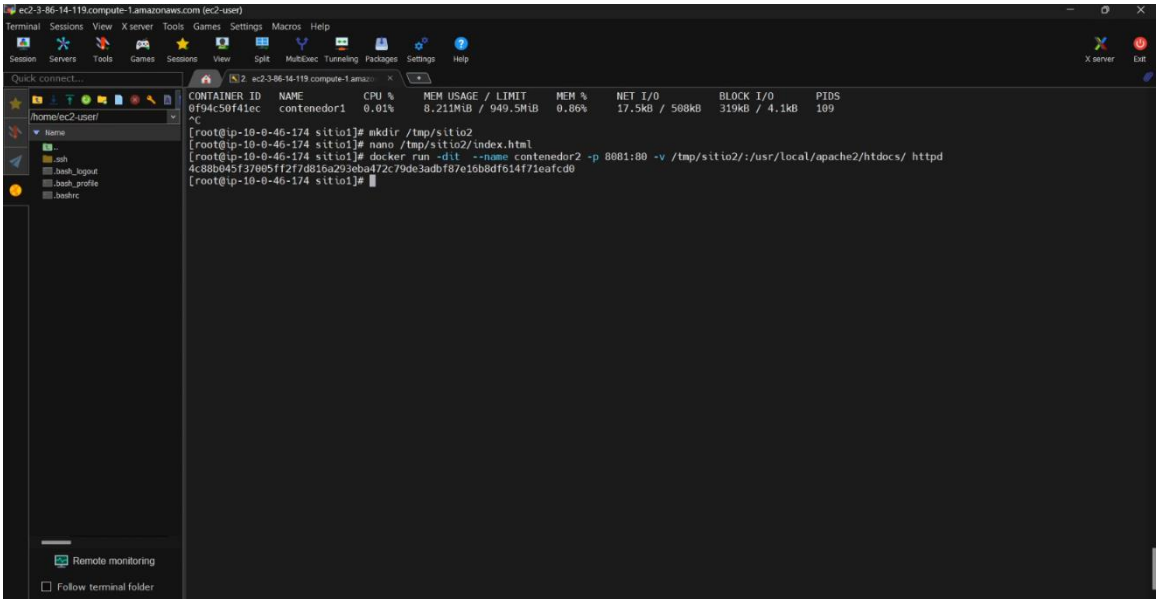


Imagen 21. Configuración de las reglas de grupo de seguridad para el contenedor dos

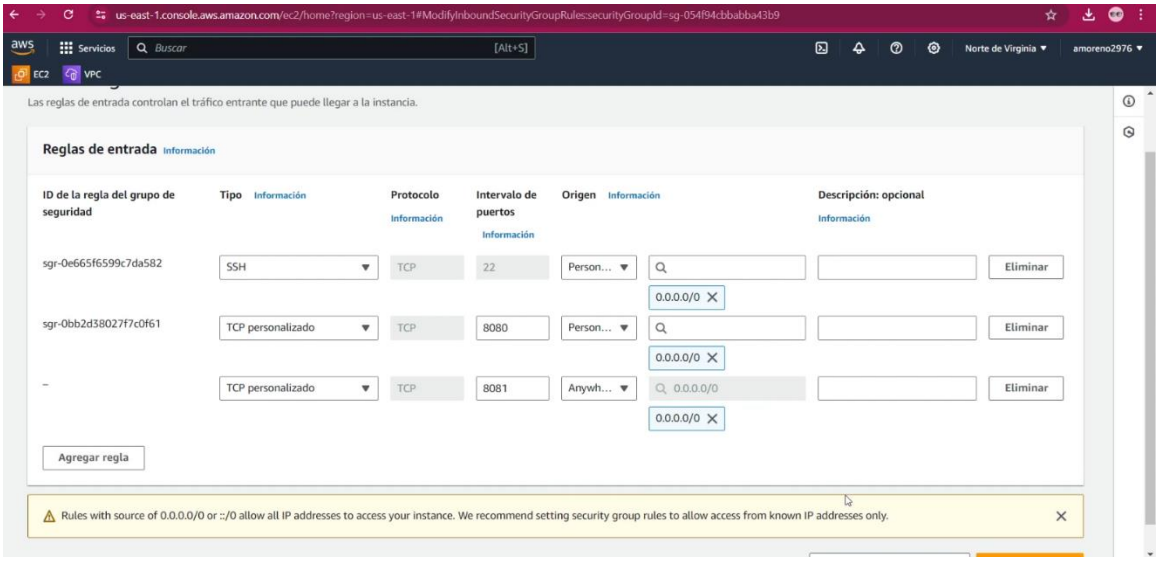


Imagen 22. Visualización de la información del contenedor dos

Imagen 23. Instalación y configuración de nginx

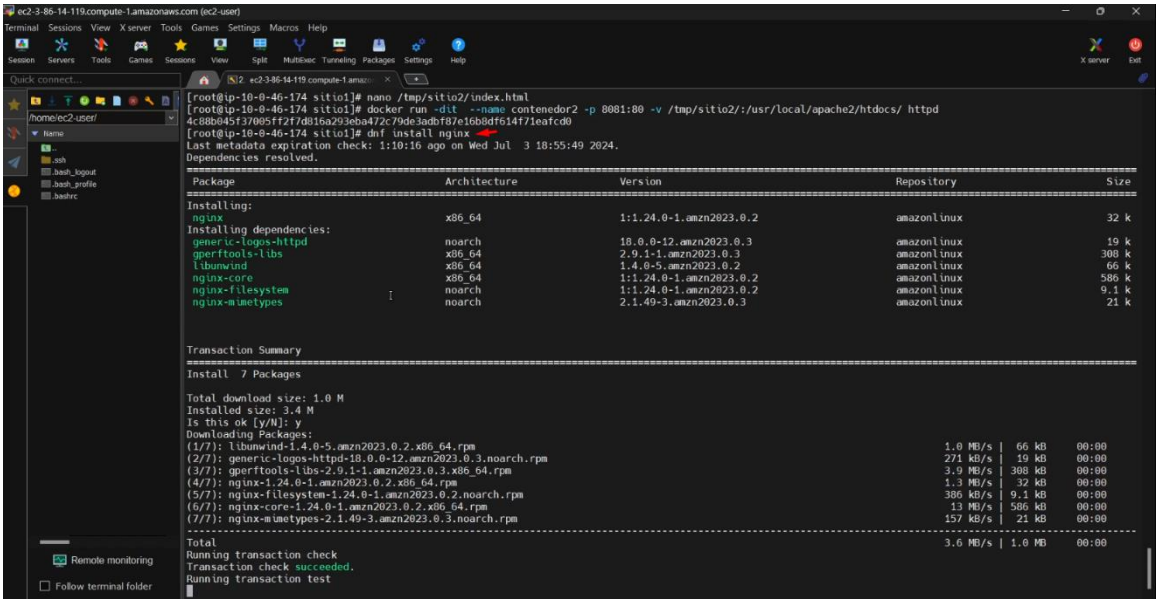


Imagen 24. Configuración de las reglas de grupo de seguridad para el puerto 80

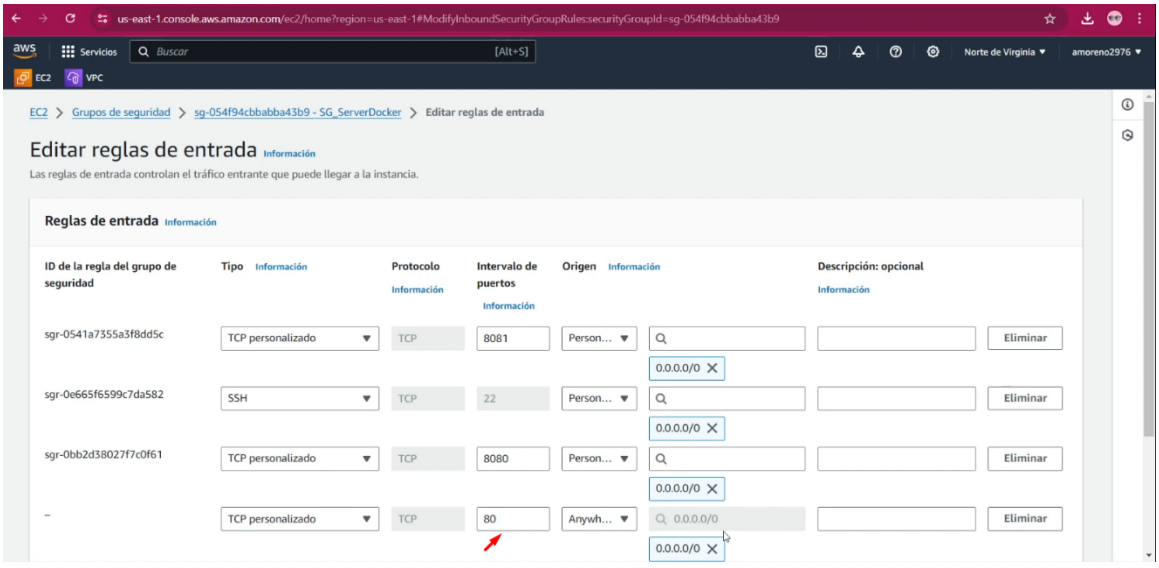


Imagen 25. Visualización de la página principal de nginx

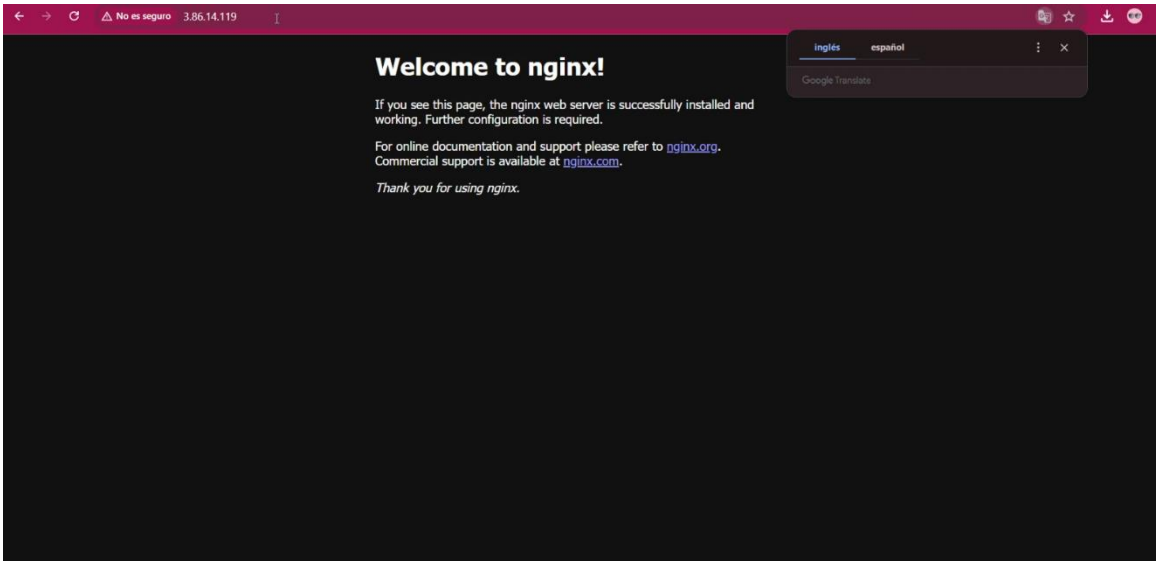


Imagen 26. Ejecución de nginx y configuración del archivo nginx.conf

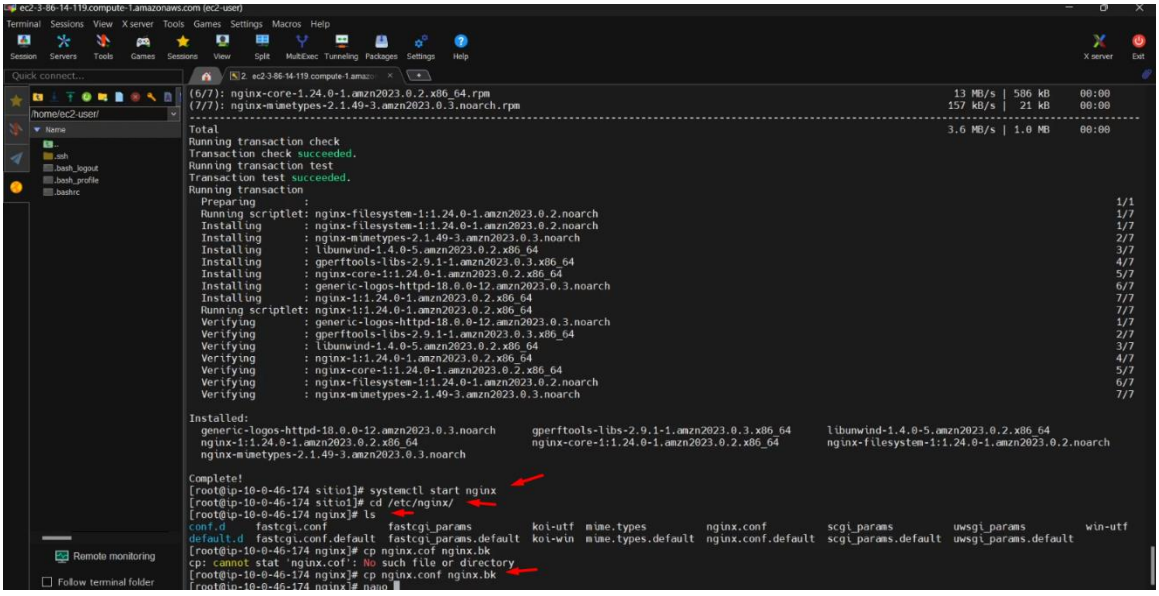


Imagen 27. Configuración del archivo nginx.conf

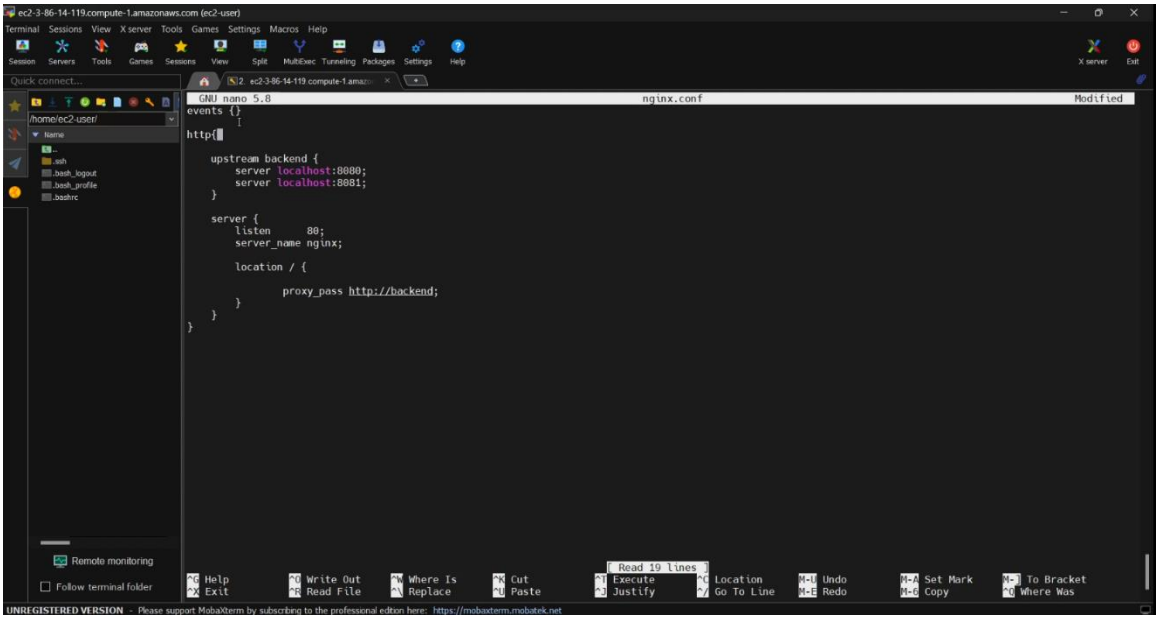
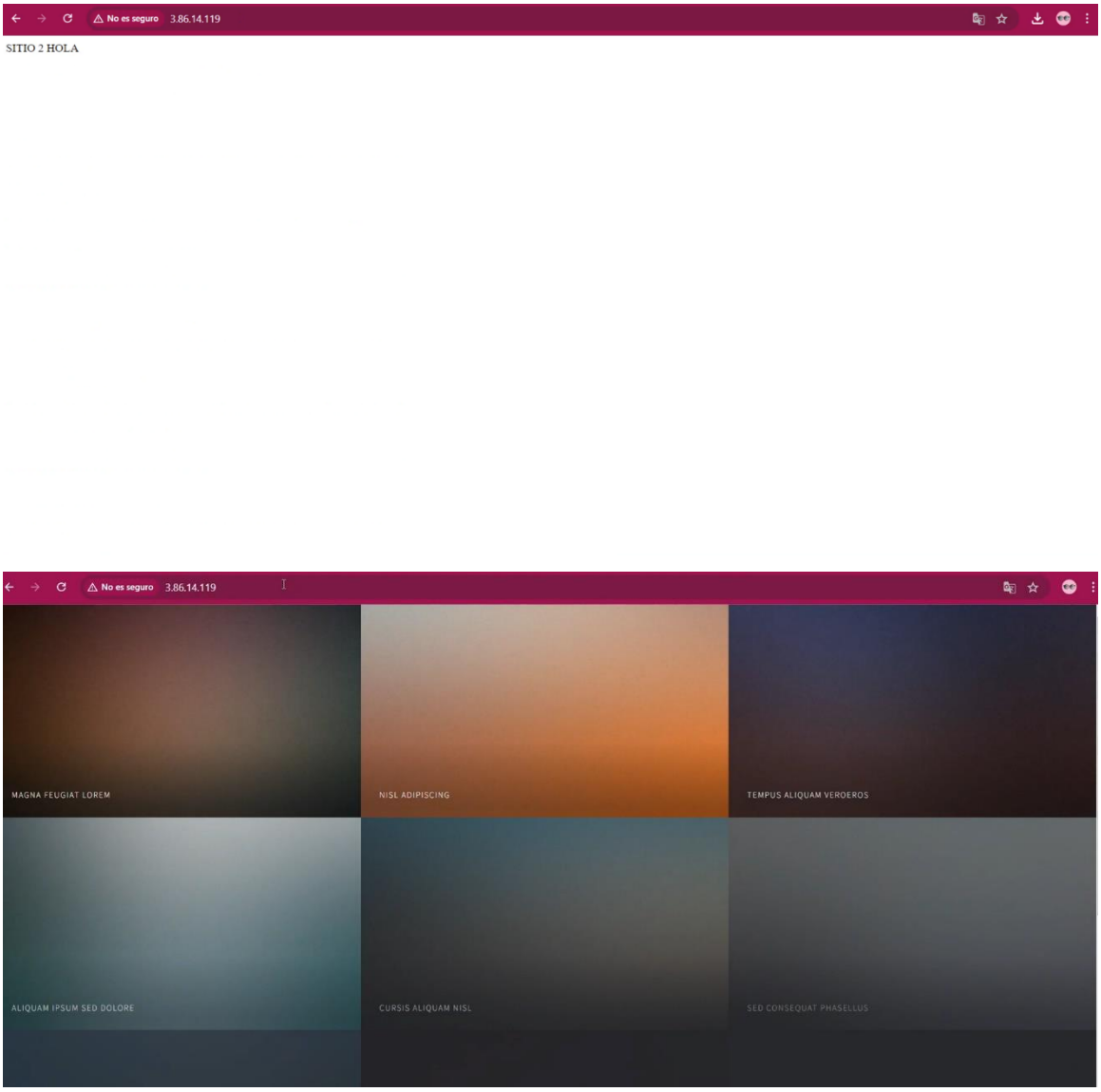


Imagen 28. Visualización del direccionamiento del balanceador de carga



Imágenes del 1 al 13 implementación punto 8

Imagen 1. Creación de un Bucket (S3).

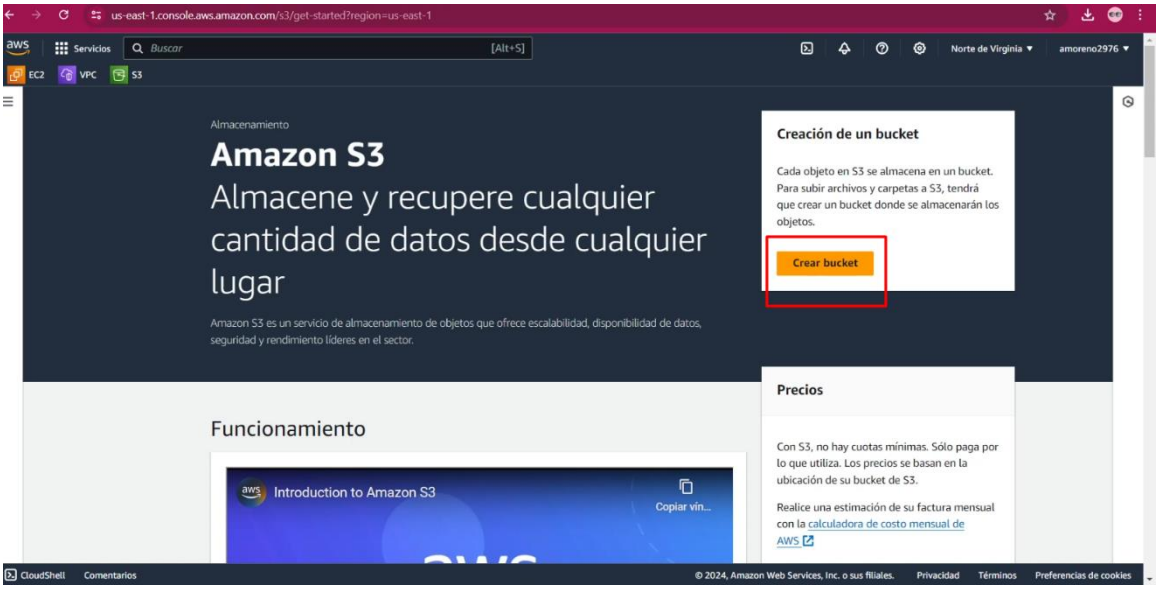


Imagen 2. Configuración del Bucket (S3).

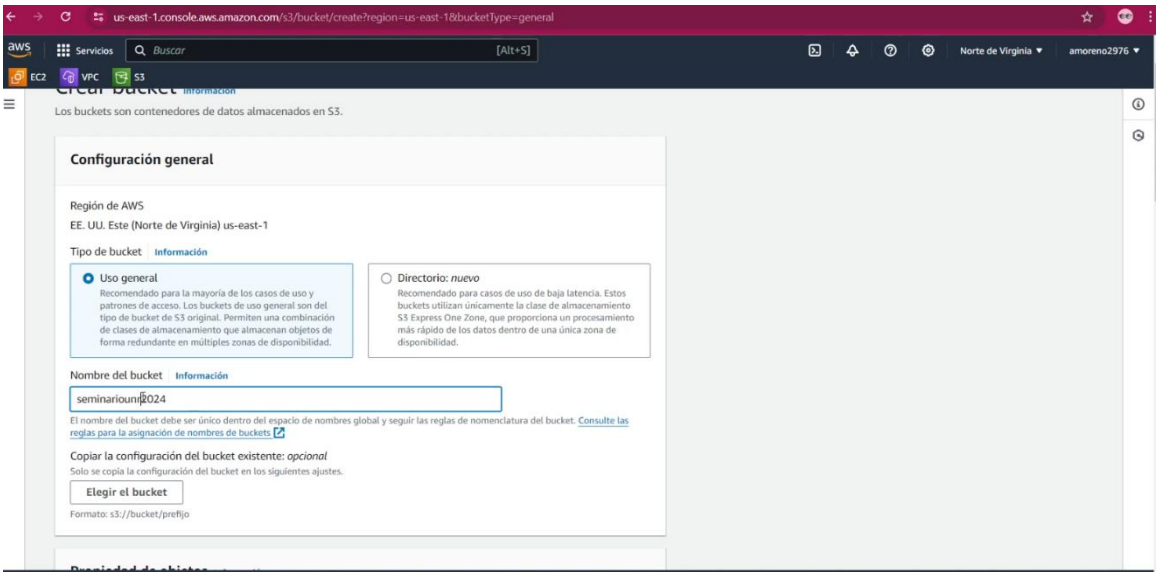


Imagen 2.1. Confirmación de la creación Bucket (S3).

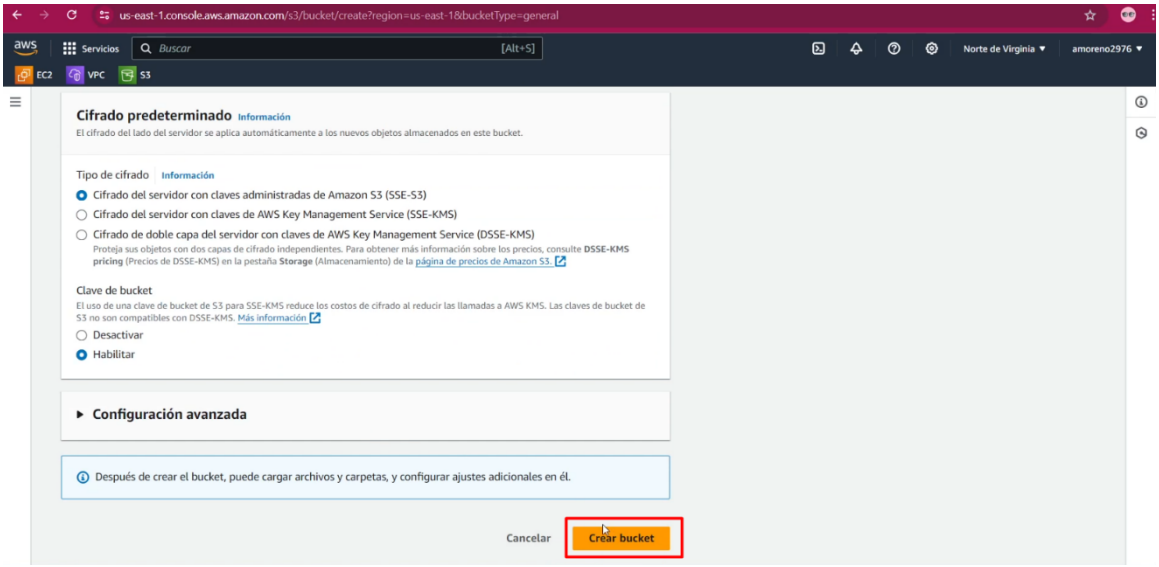


Imagen 3. Habilitación del control de versiones del Bucket (S3).

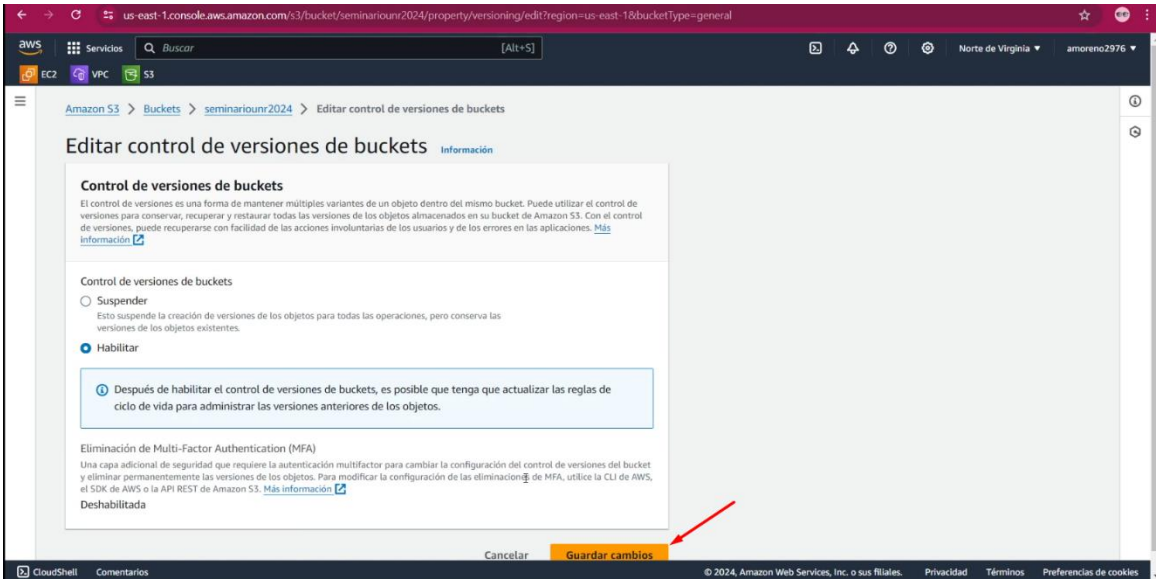


Imagen 4. Carga de archivo.

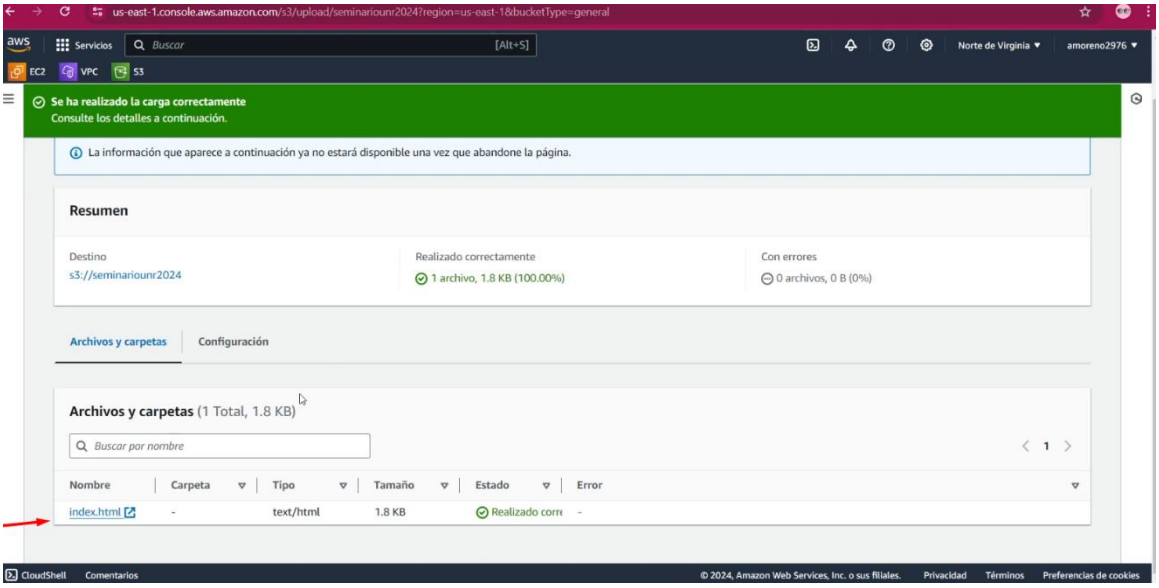


Imagen 5. Control de versiones de la Carga de archivos.

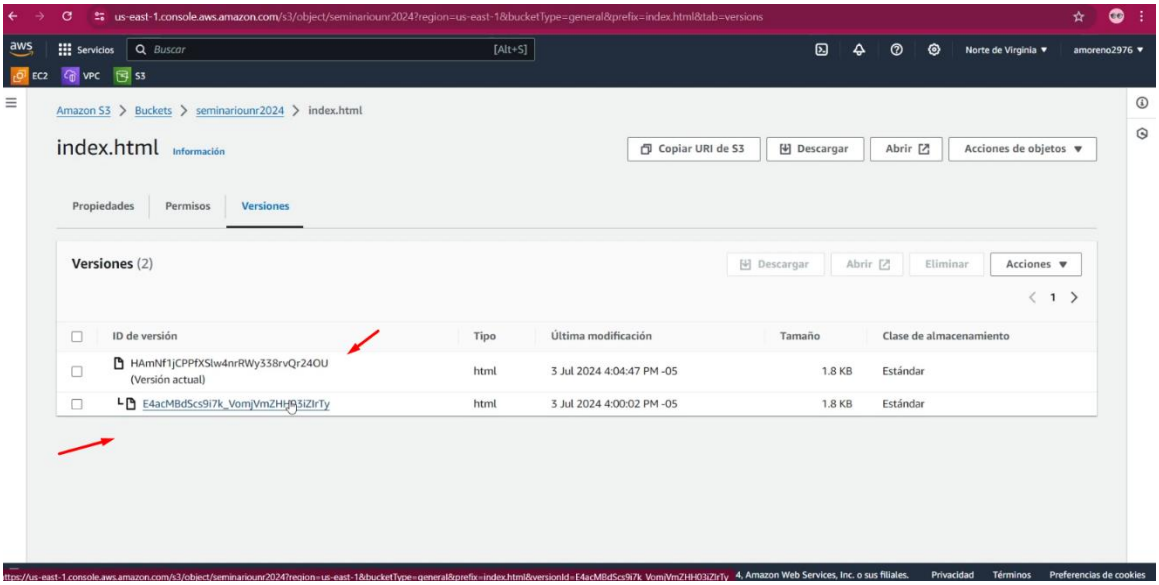


Imagen 6. Deshabilitar el bloqueo de acceso público.

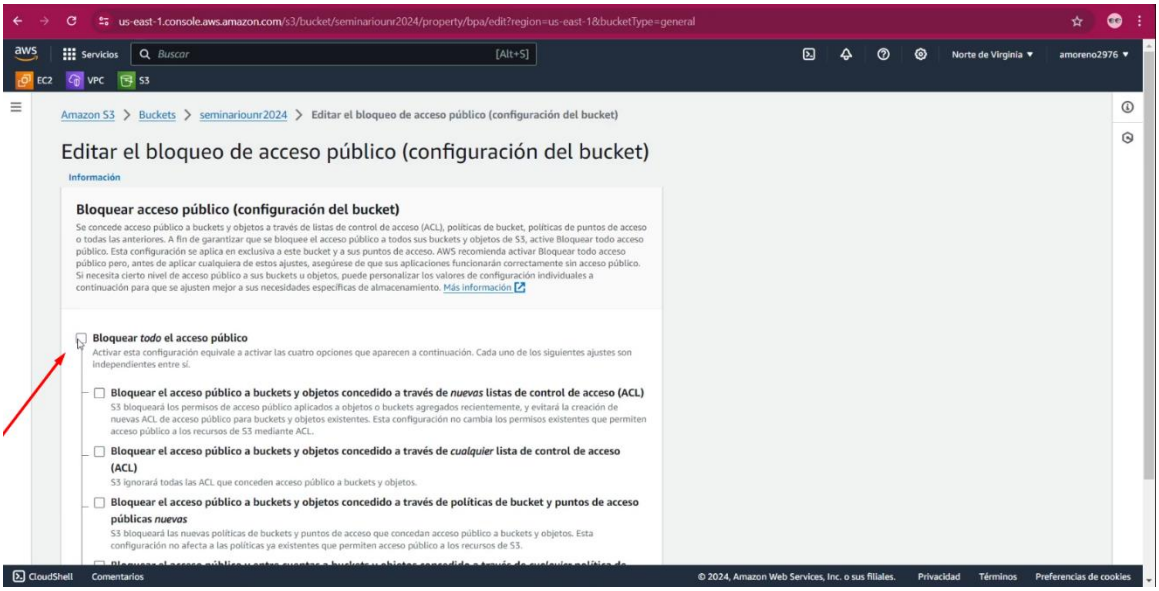


Imagen 7. Edición de la lista de control de Acceso.

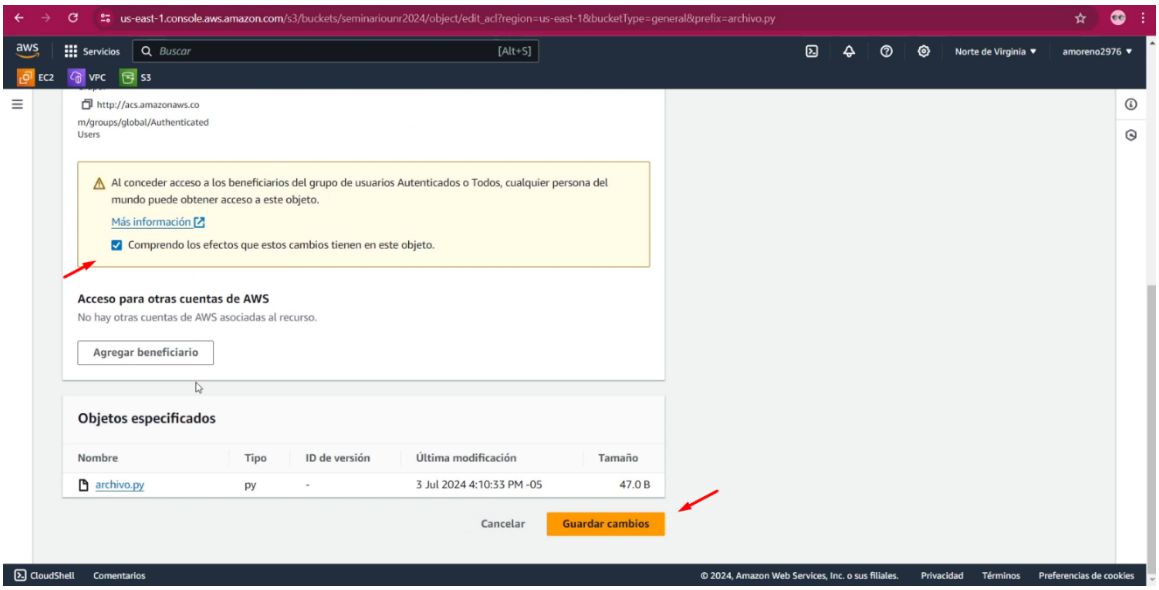


Imagen 8. Visualización de la información del archivo cargado.

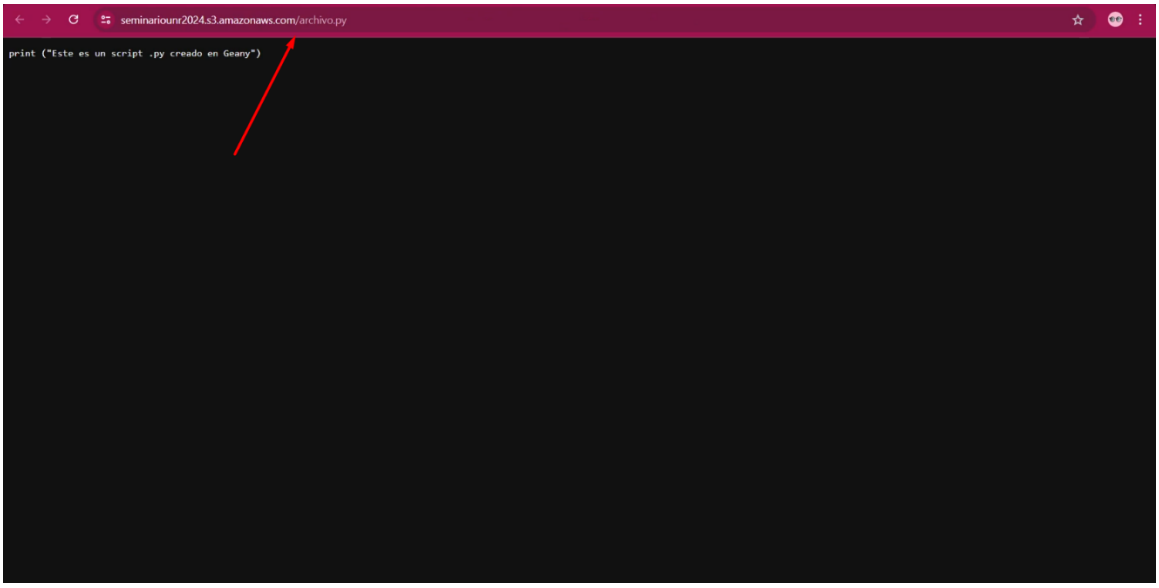


Imagen 9. Configuración del sitio a web estático.

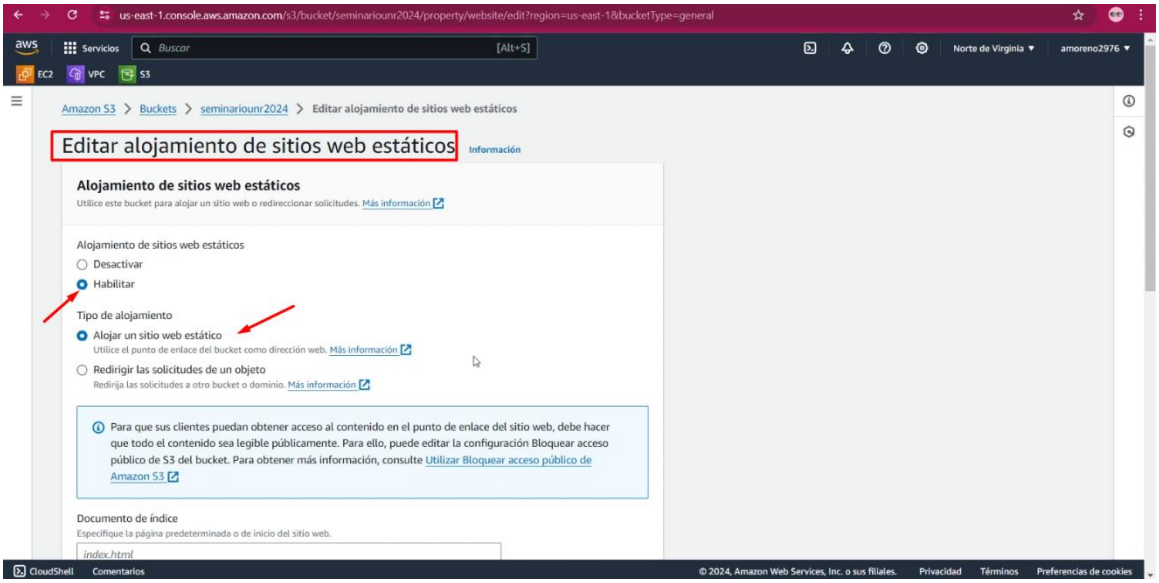


Imagen 9.1. Especificación del nombre de la página a buscar.

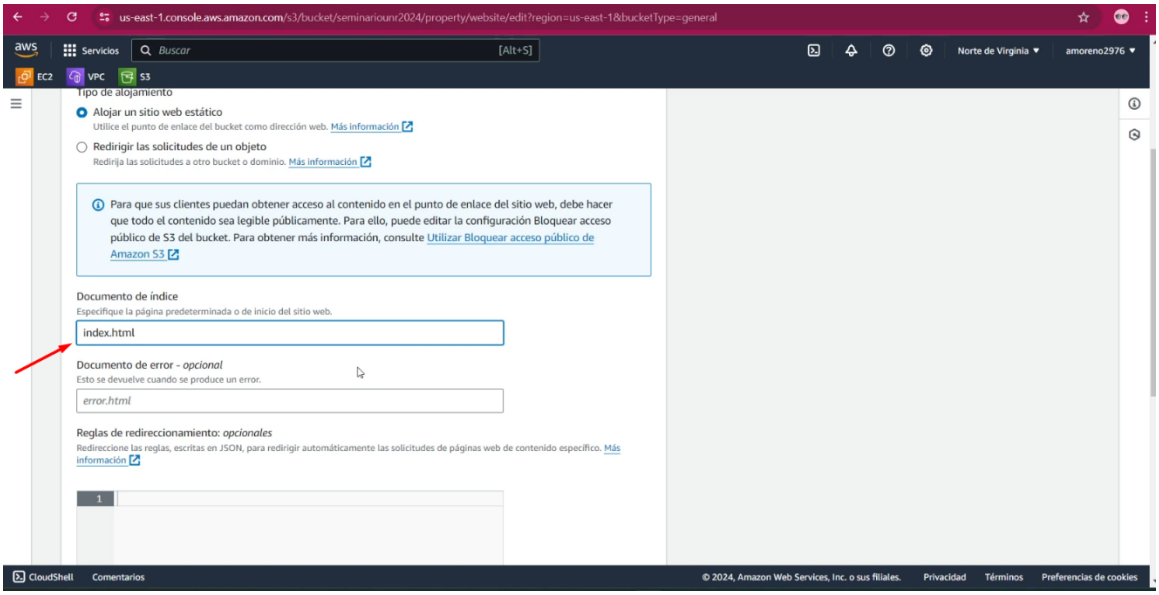


Imagen 10. Carga de los archivos del template html5.

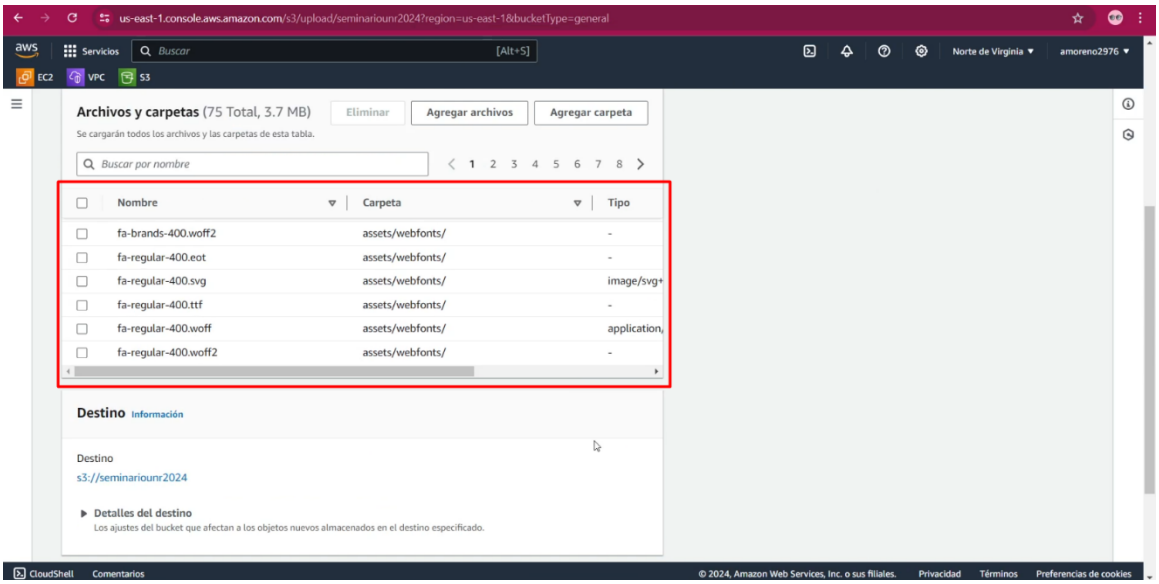


Imagen 11. Lista de los archivos cargados en el bucket

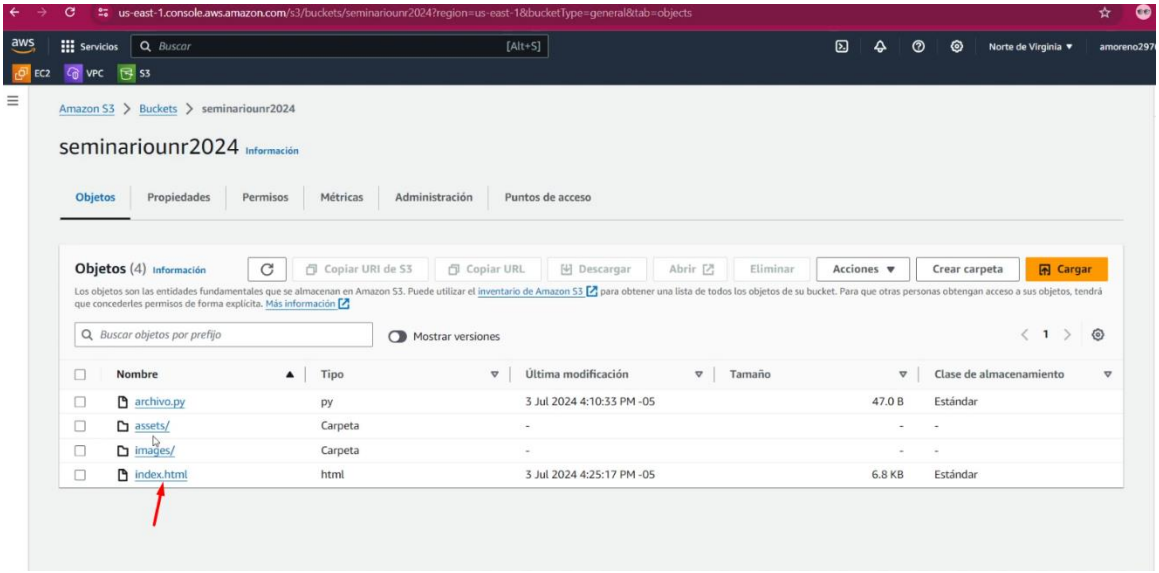


Imagen 12. Se edita la lista de control de acceso para el archivo index.html.

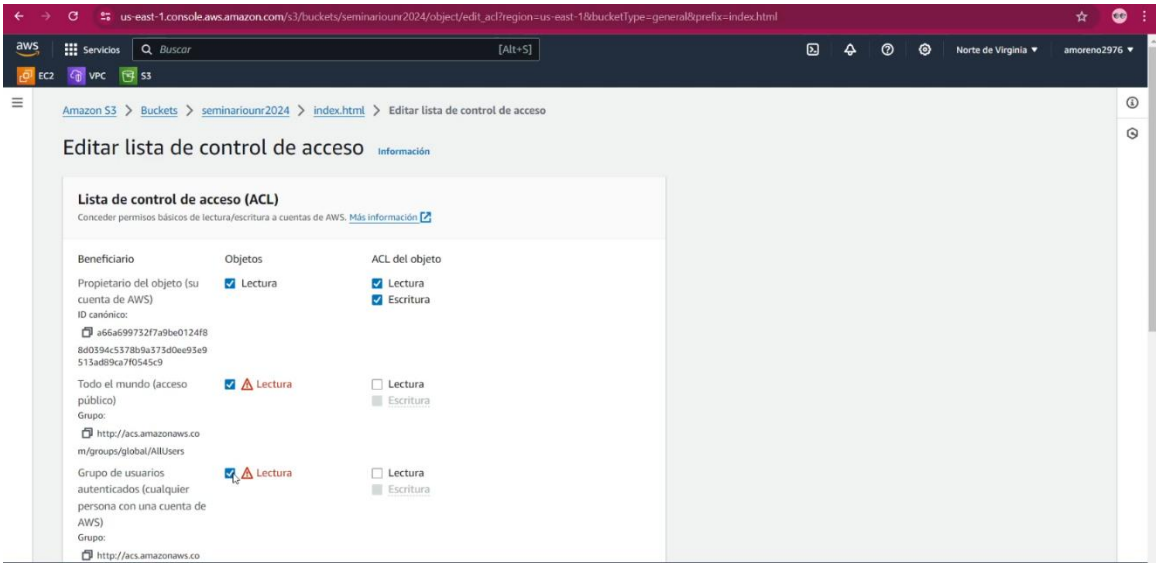
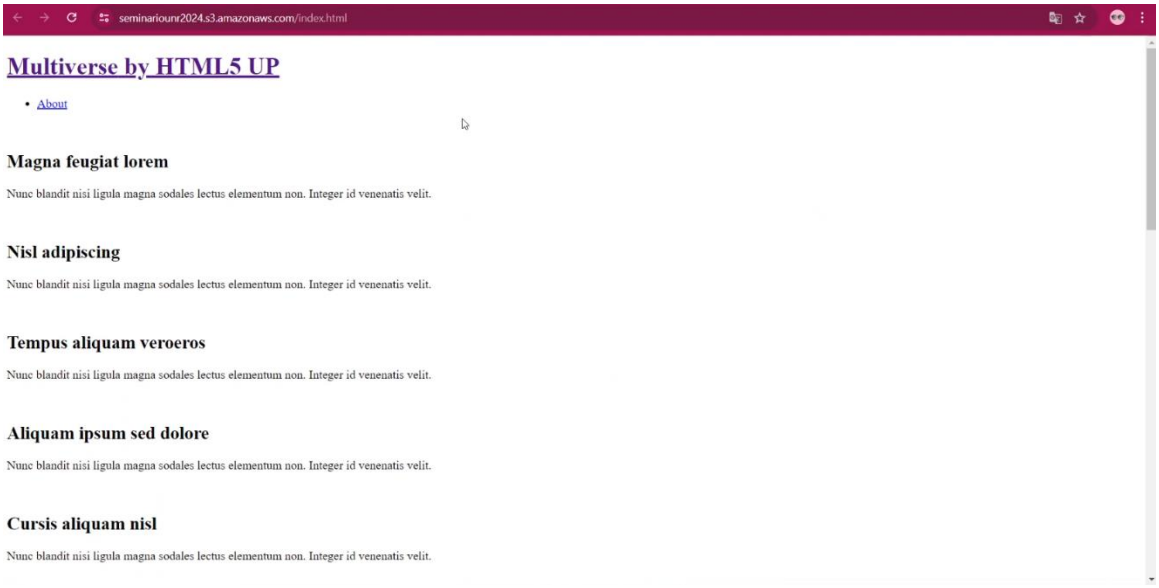


Imagen 13. Visualización de la información contenida en el index.html.



Imágenes del 1 a la 19 implementación punto 10

Imagen 1. Instancias EC2 en ejecución.

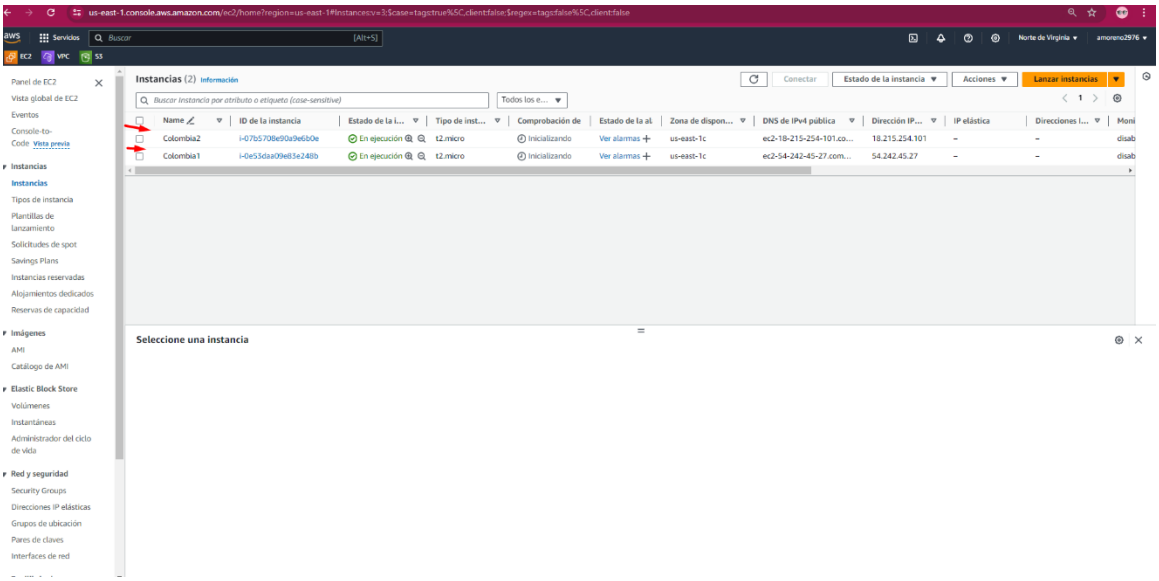


Imagen 2. Visualización de la información del balanceador de carga.

Imagen 3. Creación de una plantilla a partir de la EC2.

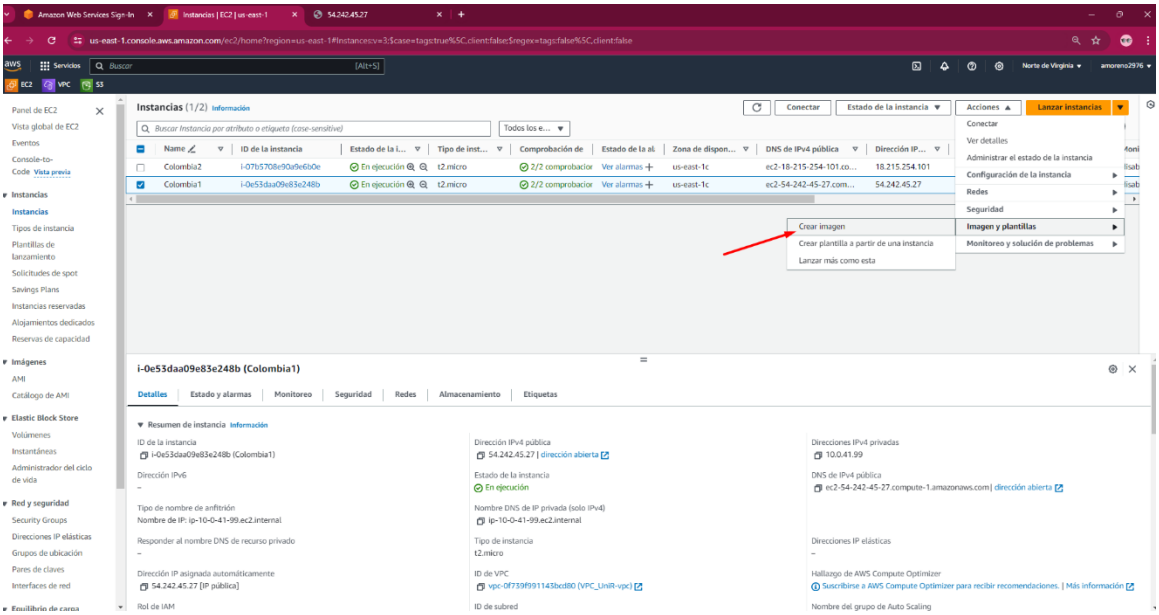


Imagen 4. Creación de la AMI a partir de la plantilla.

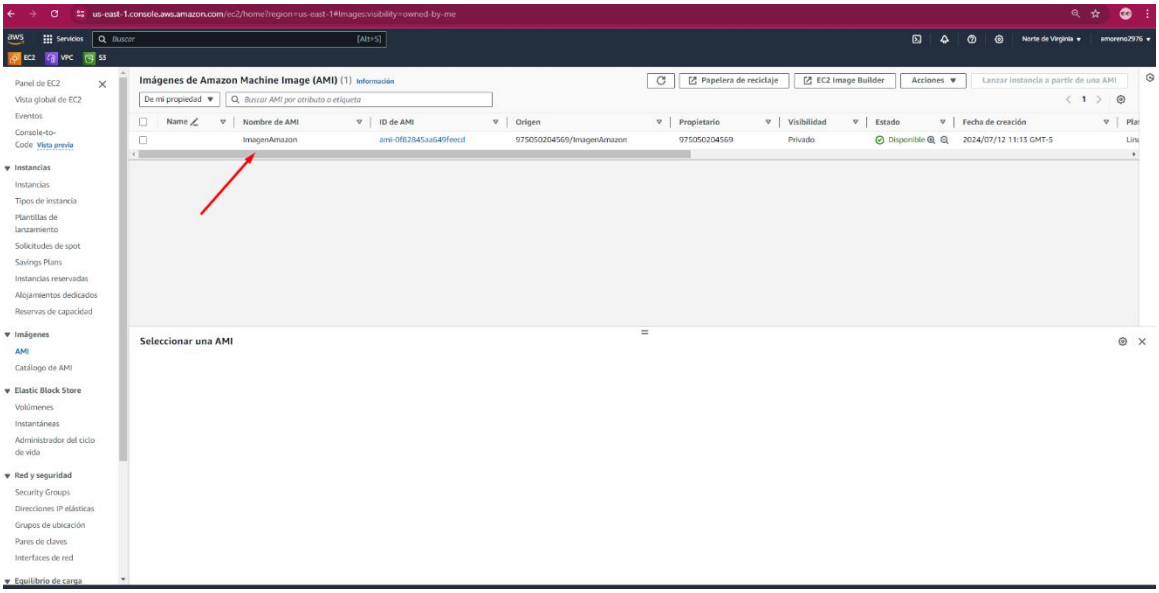


Imagen 5. Volúmenes para el almacenamiento.

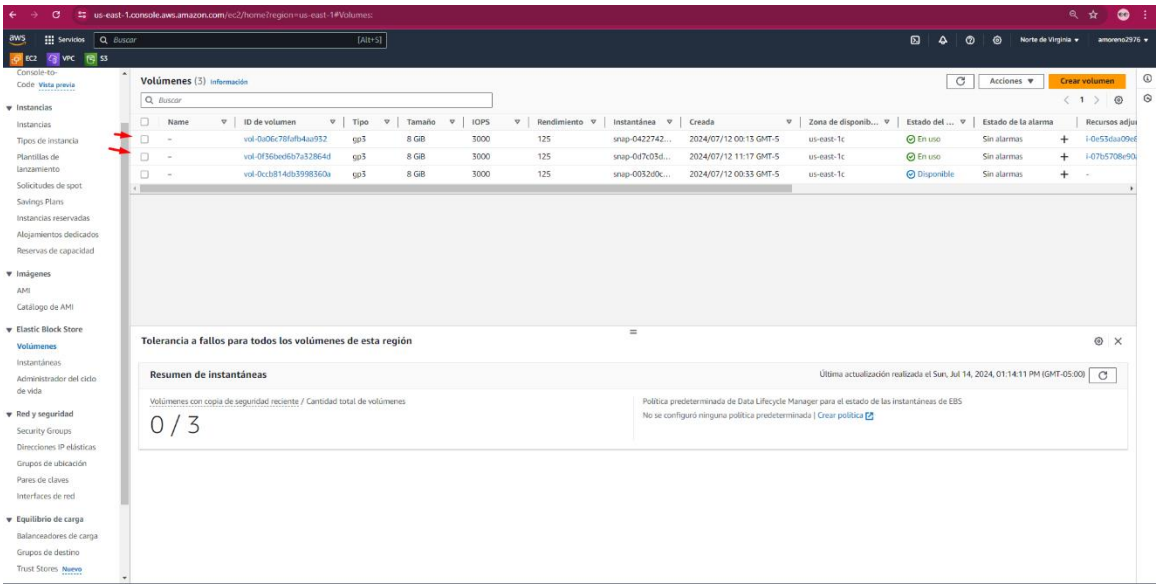


Imagen 6. Balanceador de carga creado.

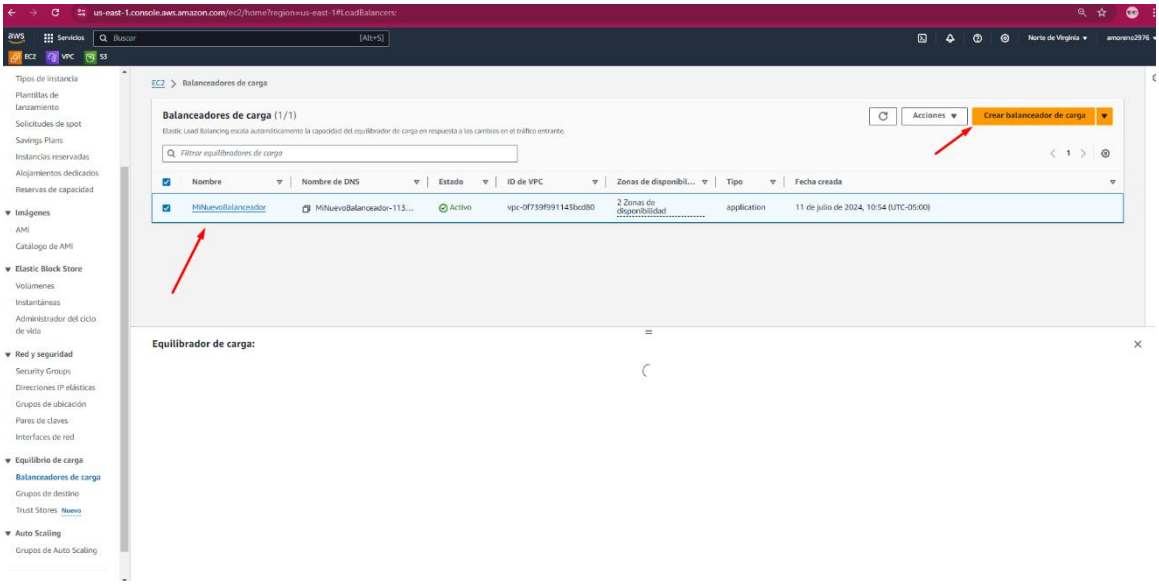


Imagen 7. Detalles del Balanceador de carga.

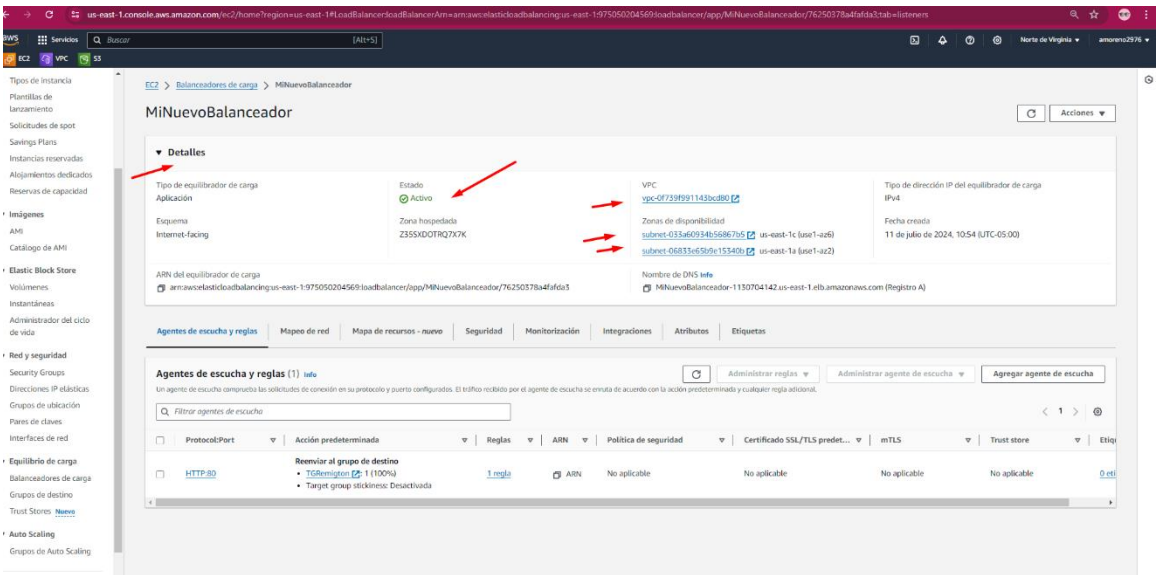


Imagen 8. Mapeo de red del balanceador de carga.

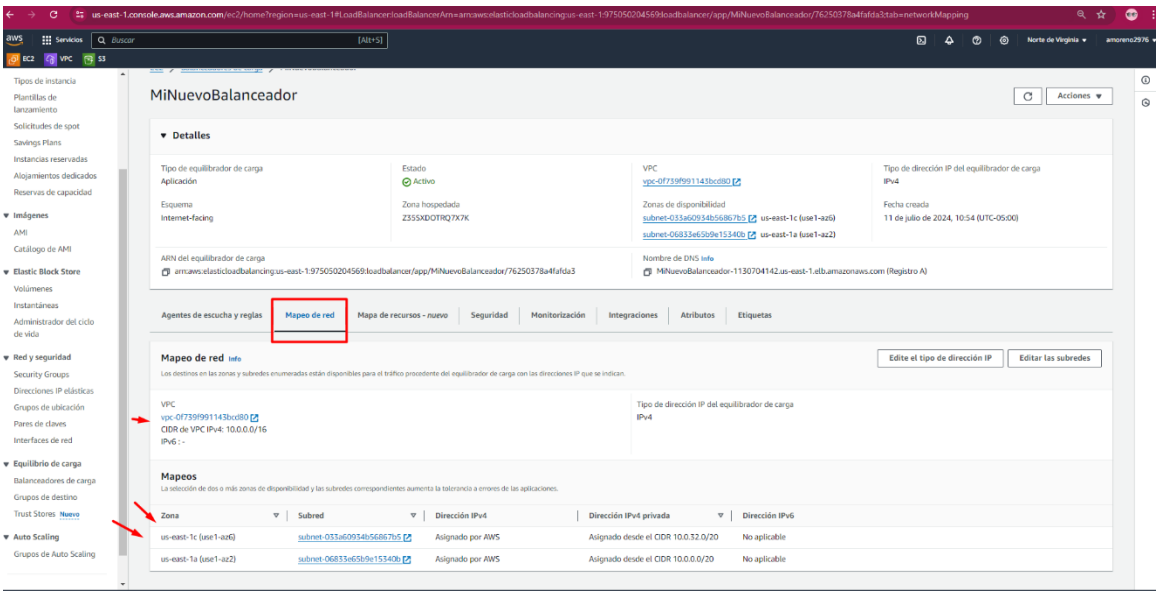


Imagen 9. Mapa de recursos del balanceador de carga.

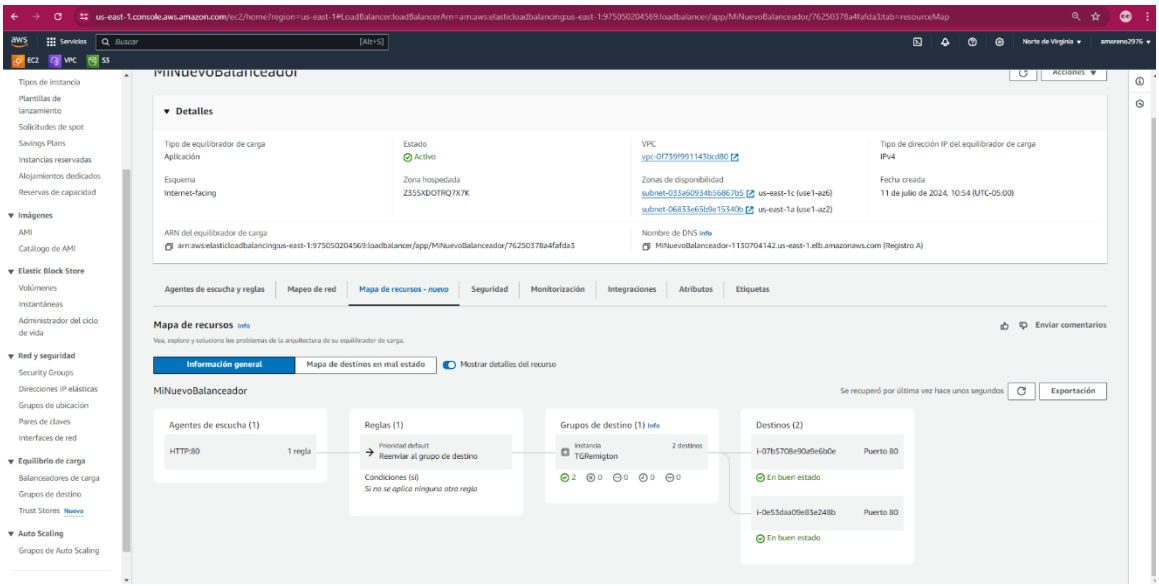


Imagen 10. Grupos de seguridad asignados al balanceador de carga.

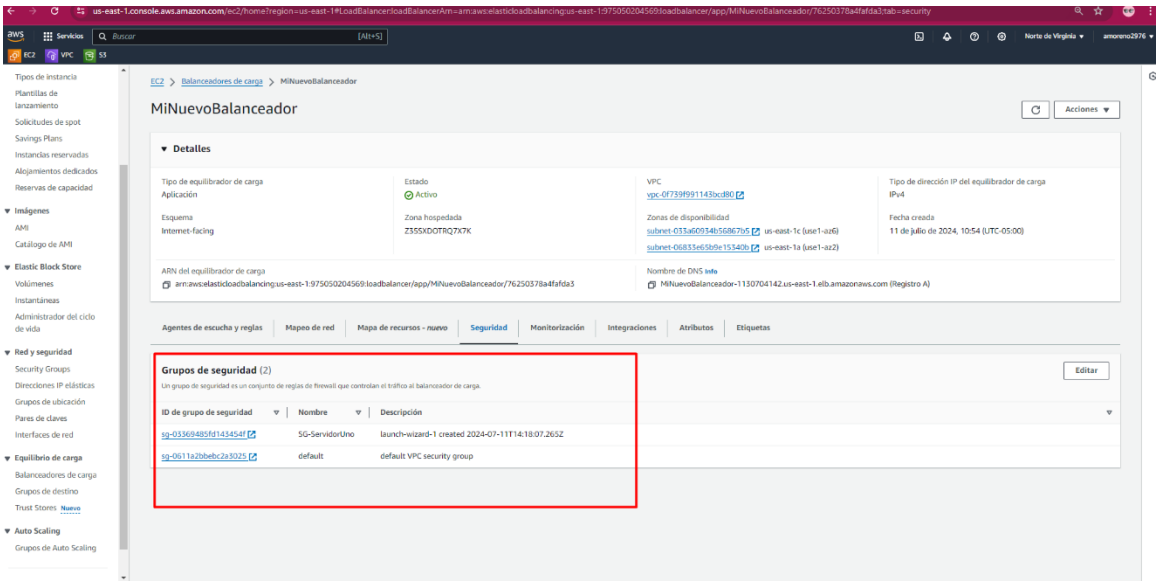


Imagen 11. Atributos del balanceador de carga.

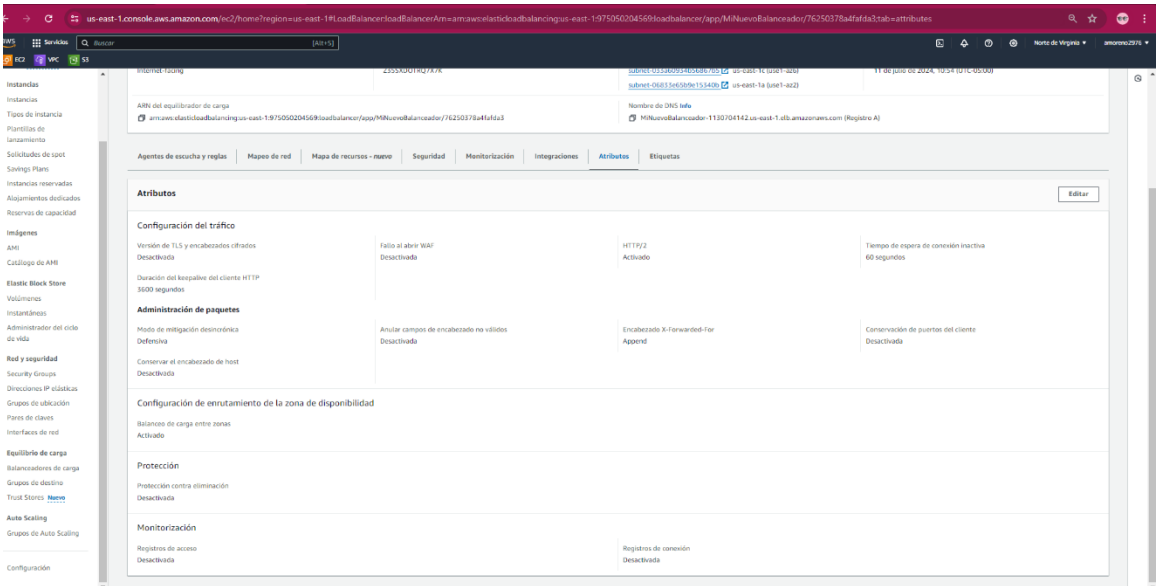


Imagen 12. TargetGroup asignado al balanceador de carga

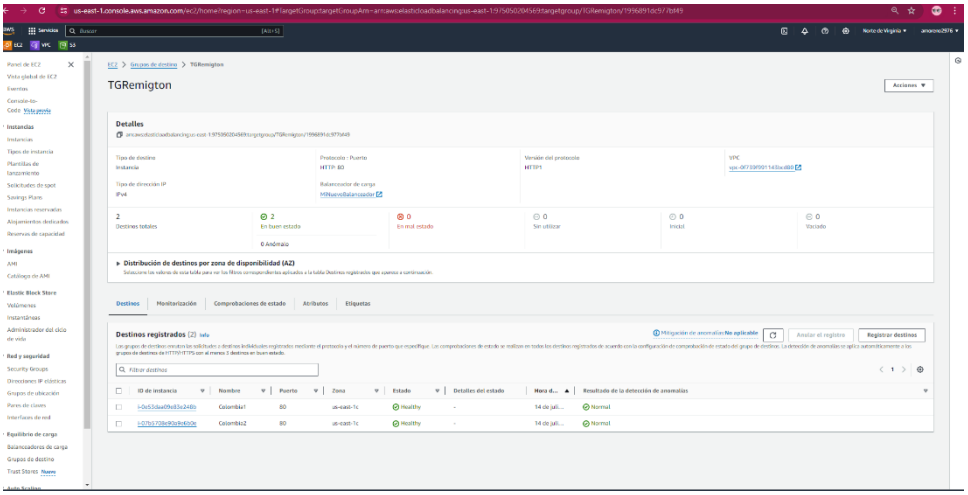


Imagen 13. Comprobaciones de estado del TargetGroup.

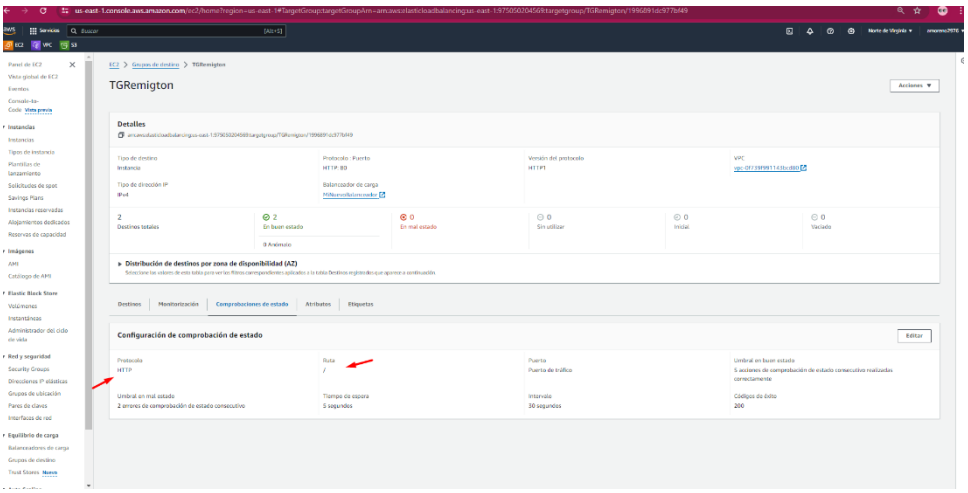


Imagen 14. Auto Scaling creado.

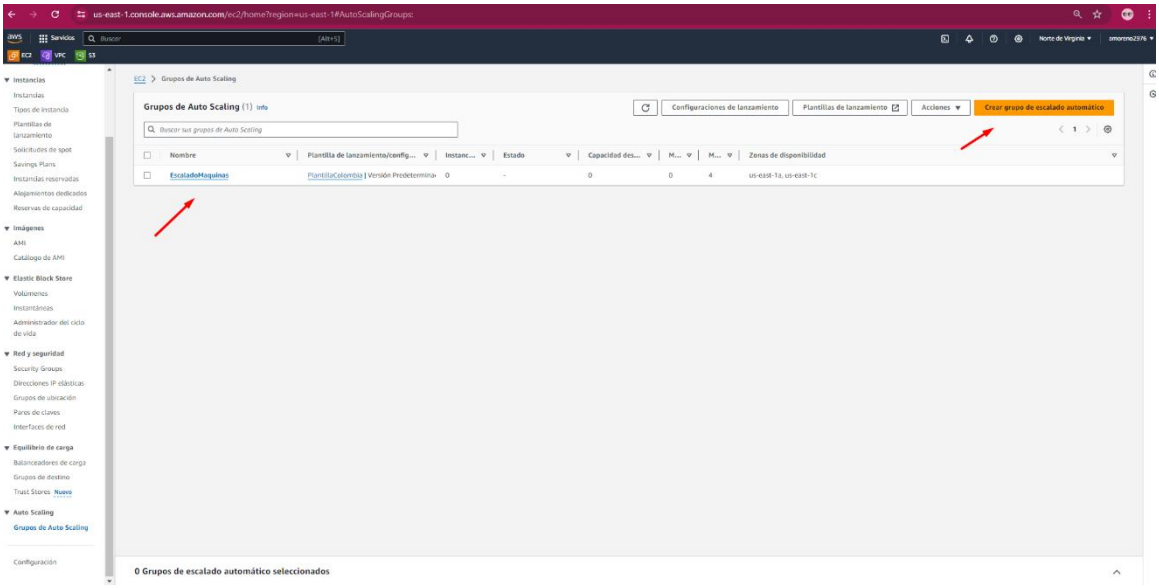
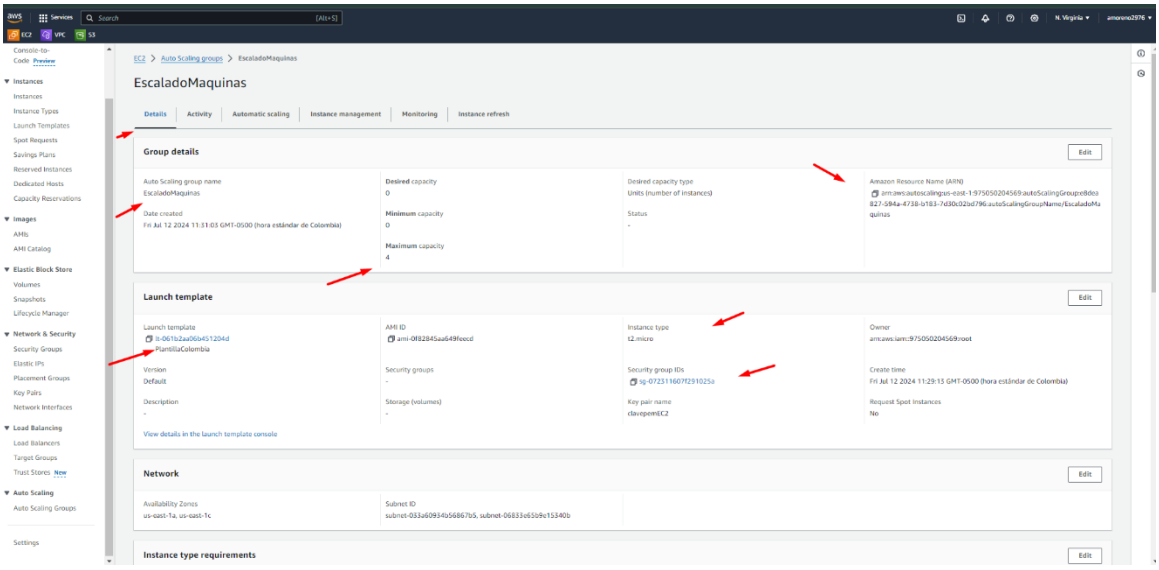


Imagen 15. Detalles del Auto Scaling.



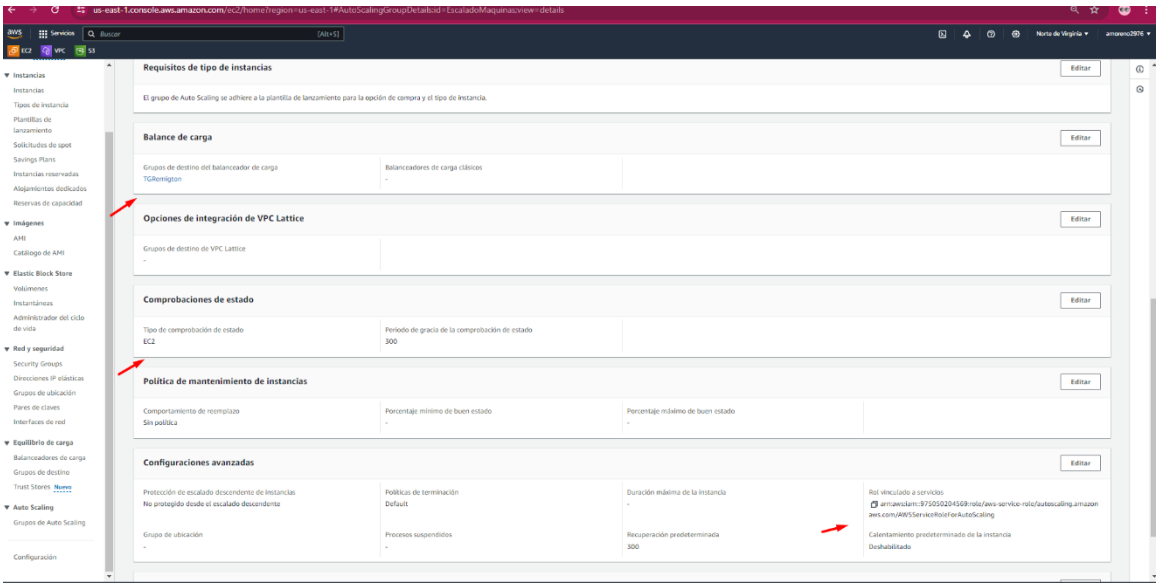


Imagen 16. Actividades del Auto Scaling.

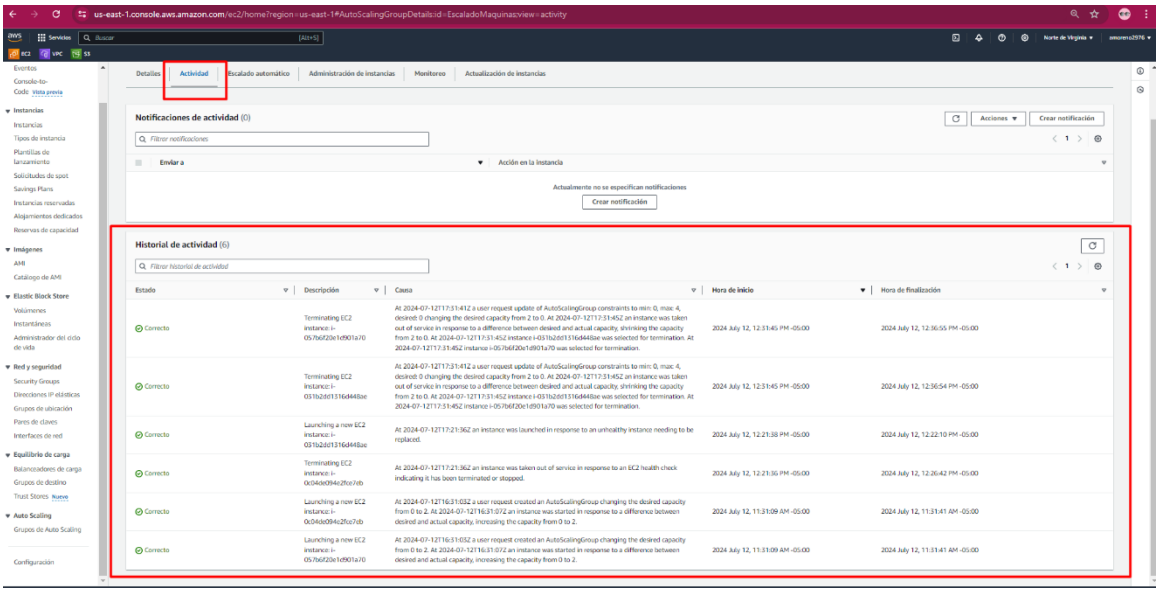


Imagen 17. Capacidad configurada para el Auto Scaling.

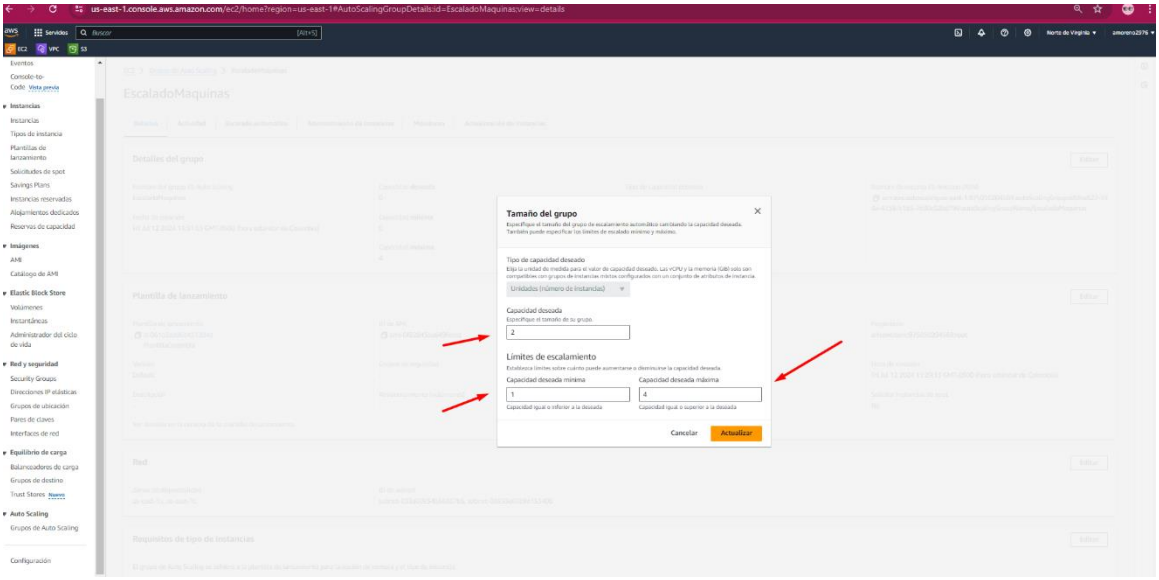
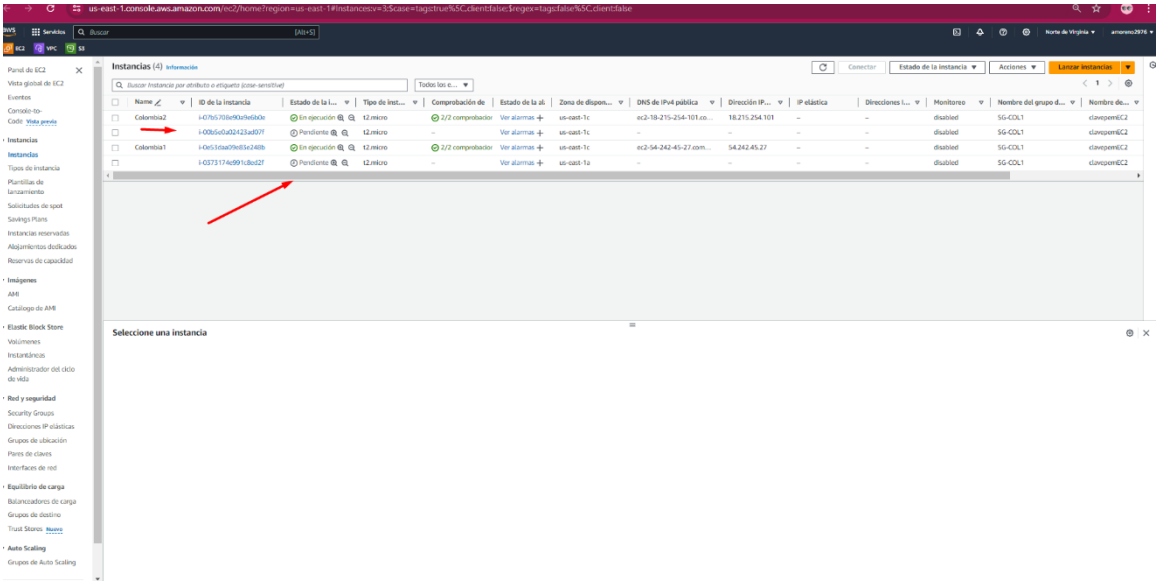


Imagen 18. Maquinas creadas a partir del Auto Scaling.



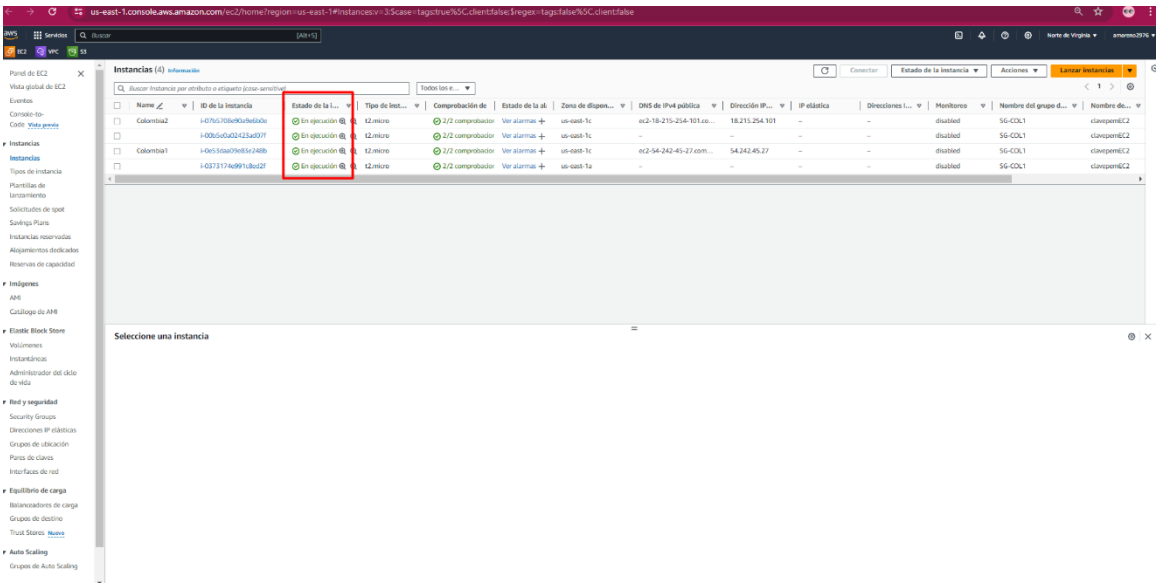


Imagen 19. Comprobaciones.