



**REPÚBLICA DE PANAMÁ**

**UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA**

**CIENCIAS DE LA COMPUTACION**

**DISEÑO DE LA MIGRACIÓN A LA NUBE AWS PARA FDSU: UN PLAN  
ESTRATÉGICO PARA OPTIMIZAR LA INFRAESTRUCTURA TECNOLÓGICA**

**PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE MAGISTER EN  
MAESTRIA EN CIENCIAS DE LA COMPUTACION CON ENFASIS EN  
VIRTUALIZACION**

**Tutor:** Abdel Gadiel Martinez Lassonde

**Autores:** Yatary Yaidelys Quiñones Lineas

Dayron Rámida Coll

**Ciudad de Panamá, diciembre 2024**



**REPÚBLICA DE PANAMÁ**  
**UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA**  
**CIENCIAS DE LA COMPUTACION**

**DISEÑO DE LA MIGRACIÓN A LA NUBE AWS PARA FDSU: UN PLAN  
ESTRATÉGICO PARA OPTIMIZAR LA INFRAESTRUCTURA TECNOLÓGICA**

**PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE MAGISTER EN  
MAESTRIA EN CIENCIAS DE LA COMPUTACION CON ENFASIS EN  
VIRTUALIZACION**

**AUTORES:** Yatary Yaidelys Quiñones Lineas  
Dayron Rámida Coll

**Ciudad de Panamá, diciembre 2024**



Ciudad de Panamá, 15 de Agosto de 2024

Profesor

Abdel Gadiel Martinez Lassonde

Coordinador del Comité de Titulación de Estudios de Grado y Postgrado

Presente.

En mi carácter de Tutor del Trabajo de Grado de Maestría, presentado por los estudiantes Yatary Yaidelys Quiñones Lineas y Dayron Rámida Coll, para optar al grado de, Maestría en Ciencias de la Computación con Énfasis en Virtualización considero que el trabajo: reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

(Media firma)  


---

Abdel Gadiel Martinez Lassonde

Línea de Investigación:

Migración y optimización de infraestructura tecnológica



**UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA**  
**CIENCIAS DE LA COMPUTACION**

**INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN DE  
TRABAJO DE GRADO DE MAESTRÍA**

**Programa de Maestría:** Maestría en Ciencias de la Computación con Énfasis en Virtualización

**Estudiantes:** Yatary Yaidelys Quiñones Lineas y Dayron Rámida Coll

**Tutor:** Prof. Abdel Gadiel Martinez Lassonde

**Título del trabajo de grado:** Diseño de la migración a la nube AWS para FDSU: Un plan estratégico para optimizar la infraestructura tecnológica.

**Línea de Investigación:** Migración y optimización de infraestructura tecnológica

<b>SESIÓN</b>	<b>FECHA</b>	<b>HORA REUNION</b>	<b>ASPECTO TRATADO</b>	<b>OBSERVACION</b>
1.	03/05/2024	10:00am	Discusión de proyecto de tesis.	Detalles para desarrollo del proyecto.
2.	23/08/2024	9:00pm	Revisión del documento de tesis.	Revisar estructura del documento por el Modelo establecido.
3.	04/10/2024	6:00pm	Revisión del documento de tesis.	Agregar diagramas de la infraestructura y tablas explicativas.
4.	18/10/2024	9:00pm	Revisión del documento de tesis	Aprobación del proyecto.

			final.	
5.	13/01/2025	10:00am	Revisión de la presentación del proyecto de tesis	Aprobación de la presentación.

**Título definitivo:**

Diseño de la migración a la nube AWS para FDSU: Un plan estratégico para optimizar la infraestructura tecnológica.

**Comentarios finales acerca de la investigación:** Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

(Media Firma del Tutor)

(Media Firma de los Estudiantes)

## DEDICATORIA

Este trabajo está dedicado a todas las personas que han sido fundamentales en nuestro recorrido académico y profesional...

En primer lugar, queremos agradecer a los profesores de la Maestría en Ciencias de la Computación con Énfasis en Virtualización. Su conocimiento, experiencia y dedicación no solo han sido una fuente invaluable de aprendizaje, sino también una inspiración constante para alcanzar la excelencia. Sus clases, asesorías y consejos han sido cruciales en nuestro desarrollo como profesional.

De manera especial, agradecemos al Profesor Abdel Gadiel Martínez Lassonde, asesor de este proyecto, por su invaluable guía, paciencia y apoyo constante. Su experticia y sus consejos han sido esenciales para la realización de esta tesis.

A nuestros compañeros de maestría, con quienes hemos compartido innumerables horas de estudio, proyectos y discusiones enriquecedoras. Gracias por su camaradería, apoyo y por hacer de este viaje académico una experiencia memorable y gratificante.

A nuestra hija, por su amor incondicional, paciencia y comprensión durante estos años de estudio. Gracias por ser nuestro motor impulsor en cada paso del camino, por celebrar con nosotros cada logro y por entender las ausencias y los sacrificios que este proceso ha implicado.

A nuestros padres, por todo su amor y apoyo incondicional, por guiarnos constantemente por el camino correcto y por motivarnos a seguir cumpliendo nuestros sueños, incluso desde la distancia. Su confianza en nosotros ha sido una fuente constante de motivación. Gracias por su fortaleza, por ser nuestro soporte en los momentos difíciles y por estar siempre ahí, ofreciendo su aliento y compañía.

Finalmente, dedicamos este esfuerzo a todos aquellos que creen en la importancia de la educación y el avance tecnológico como motores para un futuro mejor. Que este trabajo sea una contribución significativa en el campo de la computación y sirva como base para futuros desarrollos y mejoras.

## ÍNDICE GENERAL

PORTADA .....	1
PORTADA INTERNA .....	2
CARTA DE APROBACIÓN DEL TUTOR .....	3
INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN DE TRABAJO DE GRADO DE MAESTRÍA .....	4
DEDICATORIA.....	6
ÍNDICE GENERAL.....	7
INDICE TABLAS .....	9
INDICE FIGURAS .....	10
RESUMEN .....	11
ABSTRACT .....	12
INTRODUCCIÓN .....	13
CAPÍTULO I: CONTEXTUALIZACIÓN DE LA PROBLEMÁTICA .....	15
Definición del Problema .....	15
Interrogantes.....	15
Objetivos General y Específicos .....	16
Justificación .....	17
CAPÍTULO II: MARCO TEÓRICO O REFERENCIAL.....	20
Introducción .....	20
Antecedentes.....	20
Fundamentación Teórica .....	21
Definiciones de Términos Relacionados con el Problema en Estudio .....	22
Sistema de Variables .....	23
Operacionalización de las Variables .....	24
CAPÍTULO III: MARCO METODOLÓGICO O METODOLOGÍA .....	26
Tipo de Investigación .....	26
Hipótesis .....	27
Paradigma en el que se inscribe el estudio.....	27
Diseño de la Investigación .....	27
Definición de Variables e Indicadores .....	28
Población y Muestra.....	28
Técnicas e Instrumentos .....	29
Procedimientos .....	29
Validez y Confiabilidad.....	30
Procedimiento para el Cálculo de la Confiabilidad del Instrumento .....	30
CAPÍTULO IV: RESULTADOS DE LA INVESTIGACIÓN .....	31
Resultados Relacionados con la Evaluación de la Infraestructura On-Premise Actual .....	31
Resultados Relacionados con la Propuesta de Migración a AWS .....	32
Resultados Relacionados con la Seguridad.....	33
Percepciones y Expectativas de los Empleados y Usuarios .....	34
Propuestas y Expectativas.....	35
Conclusiones parciales .....	<b>Error! Bookmark not defined.</b>
CAPÍTULO V: Análisis de los Datos e Información .....	37
Técnicas de Análisis de Datos .....	37
Procesamiento de Datos.....	38
Interpretación de Resultados .....	39
Conclusiones parciales .....	40

CAPÍTULO VI: SOLUCIÓN PROPUESTA .....	41
Propuesta de Red .....	41
Propuesta de Configuración de Instancias.....	48
Propuesta de Configuración de Almacenamiento .....	55
Propuesta de Configuración de Bases de Datos .....	60
Propuesta de Configuración de Autenticación y Gestión de Cuentas .....	65
Propuesta de Configuración de Seguridad y Gobernanza de Datos.....	70
Propuesta de Configuración de Alertas y Monitoreo .....	74
Propuesta de Configuración del Entorno de Desarrollo .....	82
Propuesta de Optimización de Costos .....	86
Tiempos de ejecución .....	92
Nuevas Oportunidades .....	92
CONCLUSIONES.....	98
RECOMENDACIONES .....	100
Optimización Continua de Costos .....	100
Seguridad y Conformidad .....	100
Mejora Continua del Desempeño.....	101
Capacitación y Desarrollo de Talento .....	101
Automatización y DevOps.....	101
Innovación y Nuevas Tecnologías .....	102
Escalabilidad Global.....	102
GLOSARIO DE TÉRMINOS.....	104
REFERENCIAS.....	107



## INDICE TABLAS

Table 1 : Rangos de la Confiabilidad Alpha de Cronbach.....	30
Table 2 : Zonas de Disponibilidad y Subredes.....	47
Table 3 : Instancias.....	55
Table 4 : Costos estimados.....	92

## INDICE FIGURAS

Figure 1 : Balanceadores de carga .....	47
Figure 2 : Arquitectura de red .....	48
Figure 3 : Almacenamiento S3 y Replicas .....	60
Figure 4 : Base de Datos .....	65
Figure 5 : Control de accesos y privilegios.....	70
Figure 6 : Monitoreo y Alertas .....	81
Figure 7 : Tiempo estimado de Migración .....	92



**REPÚBLICA DE PANAMÁ**

**UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA**

**DISEÑO DE LA MIGRACIÓN A LA NUBE AWS PARA FDSU: UN PLAN  
ESTRATÉGICO PARA OPTIMIZAR LA INFRAESTRUCTURA TECNOLÓGICA**

**Autores:** Yatary Yaidelys Quiñones Lineas

Dayron Rámida Coll

**Tutor:** Abdel Gadiel Martinez Lassonde

**Año:** 2024

**RESUMEN**

El propósito fundamental de este estudio fué mejorar la eficiencia operativa y reducir costos mediante la migración de la infraestructura on-premise de FDSU a la nube AWS. FDSU, una empresa líder en software para la gestión de estaciones de bomberos, enfrenta limitaciones tecnológicas que obstaculizan su crecimiento y eficiencia. La investigación adoptó un enfoque cuantitativo, utilizando un método descriptivo para evaluar los beneficios y desafíos de la migración a la nube. El proceso de migración se dividió en varias fases: diagnóstico, diseño, validación y documentación. En la fase de diagnóstico, se realizó un análisis exhaustivo de la infraestructura actual para identificar limitaciones y necesidades específicas. La fase de diseño implicó la creación de una arquitectura de nube que satisfaga los requisitos de escalabilidad, rendimiento y seguridad, considerando las mejores prácticas de AWS. La fase de validación se enfocó en ajustar el diseño basado en la retroalimentación de las partes interesadas, mientras que la documentación registró todos los detalles técnicos y decisiones tomadas durante el proyecto. El grupo de estudio estuvo conformado por el equipo de TI de FDSU y consultores expertos en migración a la nube. Las técnicas de investigación incluyeron entrevistas y análisis de documentos técnicos. Se sistematizó la información a través de instrumentos como registros anecdóticos, registros descriptivos, diarios de campo, registros de audio y documentación técnica detallada. Este proceso permitió una evaluación precisa y completa de los impactos de la migración.

**Palabras clave:** Migración a la nube, AWS, infraestructura tecnológica, FDSU, optimización.

**Línea de investigación:** Migración y optimización de infraestructura tecnológica



**REPUBLIC OF PANAMA**

**INTERNATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**AWS CLOUD MIGRATION DESIGN FOR FDSU: A STRATEGIC PLAN TO  
OPTIMIZE TECHNOLOGICAL INFRASTRUCTURE**

**Authors:** Yatary Yaidelys Quiñones Lineas

Dayron Rámida Coll

**Tutor:** Abdel Gadiel Martinez Lassonde

**Year:** 2024

**ABSTRACT**

The fundamental purpose of this study was to improve operational efficiency and reduce costs by migrating FDSU's on-premises infrastructure to the AWS cloud. FDSU, a leading fire station management software company, faces technological constraints that hinder its growth and efficiency. The research took a quantitative approach, using a descriptive method to assess the benefits and challenges of cloud migration. The migration process was divided into several phases: diagnosis, design, validation, and documentation. In the diagnosis phase, a thorough analysis of the current infrastructure was performed to identify specific constraints and needs. The design phase involved creating a cloud architecture that meets scalability, performance, and security requirements, considering AWS best practices. The validation phase focused on fine-tuning the design based on stakeholder feedback, while the documentation recorded all technical details and decisions made during the project. The study group consisted of FDSU's IT team and expert cloud migration consultants. Research techniques included interviews and analysis of technical documents. Information was systematized through instruments such as anecdotal records, descriptive records, field diaries, audio recordings, and detailed technical documentation. This process allowed for an accurate and complete assessment of the migration impacts.

**Keywords:** Cloud migration, AWS, technological infrastructure, FDSU, optimization.

**Research line:** Migration and optimization of technological infrastructure

## INTRODUCCIÓN

Este trabajo de tesis tiene como objetivo principal diseñar e implementar un plan estratégico para la migración de la infraestructura on-premise de FDSU a la nube AWS. La empresa FDSU, líder en el desarrollo de software para la gestión de estaciones de bomberos, enfrenta importantes desafíos tecnológicos que limitan su crecimiento y eficiencia operativa. La migración a AWS no solo busca reducir costos, sino también aprovechar las facilidades de escalado, procesamiento y análisis de datos que ofrece la nube.

El estudio se ha estructurado en siete capítulos, cada uno de los cuales aborda aspectos críticos de la migración. En el **Capítulo I: Planteamiento del Problema o Contextualización de la Problemática**, se presenta una introducción al contexto de la empresa, incluyendo su misión, visión y la problemática actual de su infraestructura tecnológica. Se destaca la necesidad de una transformación digital para mantenerse competitiva en el mercado.

El **Capítulo II: Marco Teórico o Referencial** se enfoca en el análisis de la situación actual de la infraestructura de FDSU. Aquí se detallan las limitaciones del sistema on-premise, como los altos costos de mantenimiento, la falta de escalabilidad y las ineficiencias operativas. Este análisis se realiza mediante una revisión exhaustiva de la infraestructura existente, utilizando técnicas de recolección de información como entrevistas con el personal técnico y análisis de documentación técnica. Además, se discuten las teorías y principios que sustentan este trabajo, incluyendo principios de arquitectura de sistemas, teorías de migración a la nube y mejores prácticas de seguridad y gobernanza en entornos de nube.

En el **Capítulo III: Marco Metodológico o Metodología**, se describen los objetivos del proyecto de migración y la metodología empleada para el diseño de la migración. Se optó por un enfoque basado en fases: diagnóstico, diseño, validación y documentación. Cada fase incluye actividades específicas, como la recopilación de información, la definición de la arquitectura de nube y la validación con las partes interesadas. La metodología se inscribe en un paradigma de investigación aplicada, utilizando técnicas cuantitativas y cualitativas para asegurar una migración exitosa.

El **Capítulo IV: Resultados de la Investigación** se dedica a presentar los hallazgos del estudio. Aquí se exponen los resultados obtenidos durante cada fase del proyecto, desde el diagnóstico inicial hasta la implementación de la solución en la nube. Se incluyen mediciones de rendimiento, costos y otros indicadores clave que demuestran la efectividad de la migración.

En el **Capítulo V: Análisis de los Datos e Información**, se realiza un análisis detallado de los datos recolectados durante la investigación. Este análisis permite evaluar el impacto de la migración en términos de eficiencia operativa, costos y escalabilidad. Se utilizan diversas técnicas de análisis para interpretar los datos y extraer conclusiones significativas.

El **Capítulo VI: Conclusiones** resume los principales hallazgos del estudio y destaca la importancia de la transformación digital para las empresas en sectores críticos. Se subraya cómo la adopción de tecnologías avanzadas, como AWS, puede mejorar significativamente la competitividad y eficiencia operativa de FDSU.

Finalmente, el **Capítulo VII: Recomendaciones** ofrece sugerencias para futuros trabajos y mejoras continuas. Se proponen estrategias para mantener y optimizar la infraestructura en la nube, así como recomendaciones para otras empresas que consideren una migración similar.

Este estudio beneficia directamente a FDSU al optimizar su infraestructura tecnológica, lo cual se traduce en una mayor eficiencia operativa y reducción de costos. Las principales teorías que sustentan este trabajo incluyen principios de arquitectura de sistemas, teorías de migración a la nube y mejores prácticas de seguridad y gobernanza en entornos de nube. Los resultados esperados del proyecto incluyen una infraestructura tecnológica robusta y escalable en AWS, una mayor capacidad de respuesta a las demandas del mercado y una reducción significativa en los costos operativos. Las conclusiones finales del estudio subrayan la importancia de la transformación digital para las empresas en sectores críticos y la necesidad de adoptar tecnologías avanzadas para mantenerse competitivas.

## **CAPÍTULO I: CONTEXTUALIZACIÓN DE LA PROBLEMÁTICA**

### **Definición del Problema**

La empresa FDSU, reconocida como líder en el desarrollo de software para la gestión de estaciones de bomberos, enfrenta serios desafíos tecnológicos debido a su infraestructura on-premise actual. Esta infraestructura, aunque robusta en su momento de implementación, ha demostrado ser insuficiente para satisfacer las crecientes demandas del mercado y ha generado diversos problemas operativos a lo largo de los años. Desde hace varios años, FDSU ha observado limitaciones significativas en su capacidad para escalar y gestionar de manera eficiente sus recursos tecnológicos. Estos problemas se han manifestado en altos costos de mantenimiento, dificultades para atender picos de demanda, y una reducción en la competitividad de la empresa.

El contexto en el que se desarrolla esta problemática incluye un mercado cada vez más competitivo y exigente, donde la capacidad de respuesta rápida y la eficiencia operativa son cruciales para el éxito. Las limitaciones tecnológicas han tenido varias consecuencias negativas. Primero, los altos costos asociados al mantenimiento y actualización del hardware y software on-premise han afectado la rentabilidad de FDSU, desviando recursos que podrían invertirse en áreas estratégicas de crecimiento. Segundo, la falta de escalabilidad ha impedido que la empresa responda rápidamente a las demandas del mercado, limitando su capacidad de crecimiento y expansión. Tercero, las ineficiencias operativas derivadas de una gestión compleja de la infraestructura on-premise han reducido la productividad del equipo y aumentado el riesgo de errores, afectando la calidad del servicio ofrecido a los clientes.

### **Interrogantes**

Para abordar esta problemática, es esencial plantear una serie de interrogantes que guíen la investigación y el desarrollo del proyecto:

1. ¿Cuáles son las principales limitaciones de la infraestructura on-premise actual de FDSU?
2. ¿Cómo puede la migración a la nube AWS optimizar la infraestructura tecnológica de FDSU?
3. ¿Qué beneficios específicos puede proporcionar AWS en términos de costos, escalabilidad y eficiencia operativa?
4. ¿Cuáles son los principales desafíos que enfrentará FDSU durante el proceso de migración a la nube?
5. ¿Qué impacto tendrá la migración en la competitividad y crecimiento futuro de FDSU?
6. ¿Cómo se puede asegurar una migración segura y eficiente a la nube AWS?
7. ¿Qué herramientas de monitoreo y administración son necesarias para gestionar la nueva infraestructura en la nube?
8. ¿Cuáles son las mejores prácticas para la implementación de seguridad y gobernanza en AWS?

## **Objetivos General y Específicos**

### **Objetivo General:**

Propuesta de optimización de la infraestructura tecnológica de FDSU mediante la migración a la nube AWS para reducir costos y mejorar la escalabilidad y eficiencia operativa.

### **Objetivos Específicos:**

1. Evaluar la infraestructura on-premise actual de FDSU, identificando sus limitaciones y áreas de mejora:
  - Realizar un análisis exhaustivo de la infraestructura actual, incluyendo hardware, software, redes y aplicaciones.
  - Identificar los cuellos de botella y las limitaciones en términos de rendimiento, escalabilidad y seguridad.



2. Diseñar una arquitectura de nube AWS que satisfaga los requisitos de FDSU en términos de escalabilidad, rendimiento y seguridad:

- Seleccionar los servicios de AWS adecuados para cada componente de la infraestructura.
- Considerar las mejores prácticas de seguridad y gobernanza en la nube.
- Definir un plan de implementación detallado que incluya la migración de datos, aplicaciones y servicios.

3. Proponer una arquitectura para migrar las aplicaciones web y móviles de FDSU a la nube AWS de manera segura y eficiente:

- Minimizar el impacto en las operaciones de la empresa durante el proceso de migración.
- Realizar pruebas exhaustivas para garantizar el correcto funcionamiento de las aplicaciones en la nube.

4. Sugerir una estrategia para la implementación de herramientas de monitoreo y administración para la infraestructura en la nube AWS:

- Obtener visibilidad del rendimiento, la seguridad y la utilización de los recursos en la nube.
- Detectar y resolver problemas de manera proactiva.
- Optimizar el uso de los recursos en la nube para maximizar la eficiencia y el costo.

5. Documentar el impacto estimado de la migración en términos de rendimiento, costos y seguridad:

- Medir el cumplimiento de los objetivos específicos establecidos.
- Identificar oportunidades de mejora continua para optimizar la infraestructura en la nube.
- Documentar los resultados de la evaluación y compartirlos con las partes interesadas.

## **Justificación**

La migración de la infraestructura on-premise de FDSU a la nube AWS es un proyecto de gran necesidad y relevancia para la empresa. La investigación y posterior

implementación de este proyecto se realizan con el objetivo de superar las limitaciones actuales y aprovechar las ventajas competitivas que ofrece la nube.

La necesidad del proyecto es clara: la infraestructura on-premise actual de FDSU no es sostenible a largo plazo y limita significativamente el crecimiento y eficiencia operativa de la empresa. La migración a la nube AWS es una solución viable y necesaria para superar estas limitaciones y asegurar el futuro de la empresa. La adopción de una infraestructura en la nube permitirá a FDSU aprovechar las ventajas de escalabilidad, flexibilidad y reducción de costos que ofrece AWS, mejorando significativamente su capacidad para competir en el mercado global.

Con esta investigación se podrá identificar y solucionar las deficiencias de la infraestructura on-premise de FDSU. Estas deficiencias no solo afectan la eficiencia operativa y la capacidad de crecimiento de la empresa, sino que también limitan su capacidad para competir en un mercado tecnológico en constante evolución. La migración a AWS es vista como una solución viable para superar estos desafíos, proporcionando una infraestructura más flexible, escalable y rentable.

FDSU se beneficiará al tener una infraestructura más eficiente y rentable, lo que permitirá una operación más ágil y eficaz. Los clientes de FDSU, que incluyen estaciones de bomberos de diversos tamaños y ubicaciones, se beneficiarán de un servicio más fiable y de mayor calidad. Además, los empleados de FDSU podrán enfocarse en actividades más estratégicas y menos en la gestión y mantenimiento de una infraestructura compleja.

El impacto de la migración será significativo, permitiendo a FDSU mantenerse competitiva en un mercado en constante evolución. La relevancia de este proyecto radica en su capacidad para transformar la infraestructura tecnológica de la empresa, asegurando su sostenibilidad y crecimiento futuro. Además, la adopción de tecnologías avanzadas como AWS establecerá un nuevo estándar de eficiencia y flexibilidad para FDSU y otras empresas del sector.

La migración a la nube AWS brinda a FDSU de una mayor flexibilidad, escalabilidad y eficiencia en la gestión de los recursos tecnológicos. Esto se traducirá en una mejora

en la operatividad y servicio al cliente, así como en una reducción de los costos operativos a largo plazo. Además, la implementación de herramientas de monitoreo y administración permitirá una gestión proactiva y eficiente de la infraestructura en la nube, asegurando un rendimiento óptimo y una rápida resolución de problemas.

Esta transformación no solo mejorará la competitividad de FDSU, sino que también establecerá una base sólida para futuras innovaciones y expansiones. La migración a la nube AWS es un paso crucial para asegurar la relevancia y sostenibilidad de FDSU en el largo plazo, permitiendo a la empresa escalar de manera más efectiva, reducir costos operativos y mejorar su capacidad de respuesta a las demandas del mercado. Además, se espera que los hallazgos y experiencias documentadas en este proyecto sirvan como referencia para otras empresas que enfrenten desafíos similares y consideren la migración a la nube como una opción viable.

## **CAPÍTULO II: MARCO TEÓRICO O REFERENCIAL**

### **Introducción**

El marco teórico de esta investigación se fundamenta en una serie de conceptos, teorías y estudios previos que sustentan la migración de infraestructuras on-premise a la nube, particularmente a AWS. Este capítulo aborda los antecedentes del problema, la fundamentación teórica, las definiciones de términos relacionados con el problema en estudio, y el sistema y operacionalización de variables. La revisión exhaustiva de estos aspectos permitirá comprender mejor la situación actual de FDSU y las soluciones propuestas.

### **Antecedentes**

Esta investigación comprende una revisión de estudios previos y trabajos de investigación relacionados con la migración de infraestructuras on-premise a la nube, así como la realidad contextual en la que se ubica FDSU. Se han identificado diversas investigaciones que abordan los desafíos y beneficios de migrar a la nube, los cuales son relevantes para entender la situación actual de FDSU y los motivos para considerar esta transición.

Numerosos estudios han demostrado que la migración a la nube puede resultar en una reducción significativa de costos operativos y una mejora en la escalabilidad y flexibilidad de las infraestructuras tecnológicas. Por ejemplo, investigaciones realizadas por Gartner y Forrester han destacado cómo empresas de diversos sectores han logrado optimizar sus operaciones mediante la adopción de servicios en la nube. Un estudio de Gartner (2019) mostró que las organizaciones que migran a la nube pueden reducir sus costos operativos en un 30% en promedio.

Otros estudios han señalado los desafíos asociados con la migración a la nube, como la necesidad de una planificación detallada, la importancia de la seguridad y gobernanza, y la gestión del cambio organizacional. Investigaciones como las de Armbrust et al. (2010) han enfatizado que, aunque la nube ofrece numerosos beneficios, las organizaciones deben estar preparadas para enfrentar retos como la

integración de sistemas heredados, la gestión de datos y la adaptación cultural dentro de la empresa. Estas investigaciones son cruciales para anticipar y mitigar posibles riesgos en el proyecto de migración de FDSU.

En la actualidad, FDSU enfrenta limitaciones significativas en su infraestructura on-premise, incluyendo altos costos de mantenimiento y actualización, falta de escalabilidad y complejidades operativas. Estos problemas han sido observados y documentados durante los últimos años, impactando negativamente en la capacidad de crecimiento y competitividad de la empresa. Un análisis interno de FDSU (2023) reveló que el 20% del presupuesto anual se destina únicamente a mantenimiento de hardware y software, sin incluir los costos asociados a la gestión y soporte técnico.

La elección de AWS como plataforma de migración se basa en su amplia gama de servicios, su reputación en el mercado y su capacidad para ofrecer soluciones escalables y seguras. Estudios de caso de otras empresas que han migrado a AWS muestran resultados positivos en términos de eficiencia operativa y reducción de costos. Por ejemplo, la migración de Netflix a AWS permitió una reducción de costos operativos y una mejora en la capacidad de escalar servicios durante picos de demanda.

## **Fundamentación Teórica**

La base teórica de este estudio se fundamenta en diversas teorías y principios claves:

- **Teoría de la Computación en la Nube:** La computación en la nube se define como la entrega de servicios informáticos (incluyendo servidores, almacenamiento, bases de datos, redes, software, análisis e inteligencia) a través de Internet ("la nube"). Esta teoría destaca los beneficios de la nube en términos de escalabilidad, flexibilidad y costo-efectividad. Según Mell y Grance (2011), la computación en la nube permite a las organizaciones acceder a recursos tecnológicos bajo demanda y pagar solo por lo que usan, lo que resulta en una mayor eficiencia económica.

- **Modelo de Servicios de Nube (IaaS, PaaS, SaaS):** La infraestructura como servicio (IaaS), la plataforma como servicio (PaaS) y el software como servicio (SaaS) son modelos de servicios de nube que permiten a las organizaciones elegir el nivel de control y gestión que desean sobre sus recursos tecnológicos. AWS proporciona servicios en estos tres modelos, ofreciendo flexibilidad para satisfacer diversas necesidades empresariales. Según estudios de IDC (2020), el modelo IaaS de AWS es utilizado por más del 60% de las empresas Fortune 500, destacando su confiabilidad y escalabilidad.

- **Teoría de la Gestión del Cambio:** La migración a la nube no es solo un cambio tecnológico, sino también organizacional. La teoría de la gestión del cambio, como la de John Kotter (1996), es fundamental para entender cómo liderar y gestionar el proceso de migración, asegurando la adopción efectiva de nuevas tecnologías y procesos por parte de todos los miembros de la organización. Kotter identifica ocho etapas críticas para una gestión exitosa del cambio, incluyendo la creación de una visión y estrategia clara, la comunicación de la visión y la eliminación de obstáculos.

### **Definiciones de Términos Relacionados con el Problema en Estudio**

- **Migración a la Nube:** Proceso de trasladar datos, aplicaciones y otros elementos de negocio desde un entorno on-premise a un entorno de nube. Este proceso implica diversas fases, incluyendo la planificación, migración y optimización post-migración.

- **Infraestructura On-Premise:** Infraestructura tecnológica ubicada físicamente dentro de las instalaciones de la empresa, gestionada y mantenida internamente. Este tipo de infraestructura suele requerir una inversión significativa en hardware y recursos humanos para su mantenimiento.

- **Escalabilidad:** Capacidad de un sistema para manejar una cantidad creciente de trabajo o su potencial para ser ampliado para acomodar dicho crecimiento. La escalabilidad es una característica clave de las soluciones en la nube, permitiendo a las organizaciones ajustar sus recursos según las necesidades.

- AWS (Amazon Web Services): Plataforma de servicios en la nube que ofrece soluciones de almacenamiento, computación, bases de datos, análisis y mucho más. AWS es conocido por su robustez, escalabilidad y seguridad, siendo una de las opciones más populares para la migración a la nube.

- Gobernanza en la Nube: Conjunto de políticas y procedimientos que garantizan el uso eficiente y seguro de los recursos en la nube. La gobernanza en la nube incluye la gestión de la identidad y acceso, la protección de datos y el cumplimiento de normativas.

## **Sistema de Variables**

En este estudio, las variables principales a considerar incluyen:

- Variable Independiente:

Migración a la Nube AWS: Proceso de trasladar la infraestructura tecnológica de FDSU a la nube AWS. Esta variable se mide en términos de etapas del proceso, tiempo invertido y recursos utilizados.

- Variables Dependientes:

Costos Operativos: Gastos asociados al mantenimiento y operación de la infraestructura tecnológica. Se mide en términos de reducción de costos post-migración comparados con los costos operativos previos.

Escalabilidad: Capacidad de la infraestructura para manejar aumentos en la carga de trabajo. Se evalúa mediante la capacidad de ajustar recursos según la demanda y la rapidez de estos ajustes.

Eficiencia Operativa: Medida de la productividad y efectividad de las operaciones tecnológicas de FDSU. Indicadores como tiempos de respuesta del sistema, número de incidencias y tiempo de inactividad son utilizados para medir la eficiencia.

Seguridad: Nivel de protección de los datos y aplicaciones contra amenazas y vulnerabilidades. Se mide mediante la cantidad de incidentes de seguridad reportados y la implementación de políticas de seguridad efectivas.

### **Operacionalización de las Variables**

Aunque este estudio se basa principalmente en análisis documental y revisión teórica, es posible operacionalizar las variables para medir su impacto de manera precisa:

- Objetivos:

Evaluar el impacto de la migración a la nube AWS en los costos operativos, la escalabilidad, la eficiencia operativa y la seguridad de FDSU.

- Denominación de las Variables:

- (a) Migración a la Nube AWS
- (b) Costos Operativos
- (c) Escalabilidad
- (d) Eficiencia Operativa
- (e) Seguridad

- Definición de las Variables:

(a) Migración a la Nube AWS: Proceso de trasladar la infraestructura on-premise de FDSU a AWS.

(b) Costos Operativos: Gastos totales asociados con la operación y mantenimiento de la infraestructura tecnológica.

(c) Escalabilidad: Capacidad de la infraestructura para adaptarse a cambios en la carga de trabajo.

(d) Eficiencia Operativa: Nivel de efectividad y productividad en la operación de los sistemas tecnológicos.

(e) Seguridad: Protección de datos y aplicaciones contra accesos no autorizados y amenazas.



- Dimensiones e Indicadores:

(a) Migración a la Nube AWS: Tiempo de migración, recursos utilizados, etapas completadas.

(b) Costos Operativos: Reducción en gastos de hardware, software y mantenimiento; comparación de costos pre y post migración.

(c) Escalabilidad: Capacidad de incrementar o disminuir recursos según la demanda; tiempos de ajuste de recursos.

(d) Eficiencia Operativa: Tiempos de respuesta, número de incidencias, tiempo de inactividad.

(e) Seguridad: Incidentes de seguridad reportados, cumplimiento de normativas, implementación de políticas de seguridad.

- Preguntas que Orientan las Respuestas:

(a) ¿Cuánto se reducen los costos operativos tras la migración a AWS?

(b) ¿Cómo mejora la escalabilidad de FDSU con la nueva infraestructura en la nube?

(c) ¿Qué cambios se observarían en la eficiencia operativa tras la migración?

(d) ¿Qué medidas de seguridad se implementan y cuán efectivas son en el nuevo entorno de AWS?

## **CAPÍTULO III: MARCO METODOLÓGICO O METODOLOGÍA**

### **Tipo de Investigación**

El marco metodológico de esta investigación detalla el enfoque y los métodos utilizados para alcanzar los objetivos del estudio. Este capítulo describe el tipo de investigación, las técnicas de recolección de datos, los instrumentos utilizados, el procedimiento seguido en cada fase del proyecto y la justificación de las metodologías seleccionadas. La combinación de métodos cuantitativos y cualitativos proporciona una visión completa y rigurosa de la propuesta de migración de la infraestructura de FDSU a AWS. A través de este enfoque metodológico, se busca desarrollar una propuesta efectiva, eficiente y alineada con las necesidades y objetivos estratégicos de la empresa, aunque no se contemple la implementación directa de la migración.

Teniendo en cuenta el propósito esta investigación es aplicada, ya que su principal objetivo es desarrollar una propuesta práctica para resolver problemas específicos relacionados con la infraestructura tecnológica de FDSU y busca aplicar conocimientos teóricos en un contexto real para optimizar la infraestructura mediante la migración a AWS, definiéndose por el nivel de profundidad como una investigación descriptiva porque detalla las características de la infraestructura actual de FDSU y explicativa porque busca entender las causas y efectos de las limitaciones actuales y cómo la propuesta de migración a AWS puede mejorar la situación.

A su vez las variables se manejan de manera no experimental, ya que no manipula las variables de forma controlada, pero sí transversal porque analiza la situación en un momento específico del tiempo sin seguir a los sujetos a lo largo del tiempo, basándose en el método hipotético-deductivo para formular hipótesis sobre los beneficios de la propuesta de migración a AWS y verificándolas a través de la recolección y análisis de datos, empleando datos cuantitativos para medir aspectos como costos operativos y eficiencia, y datos cualitativos para entender las percepciones y experiencias de los empleados y usuarios de FDSU, llevándose a cabo de manera transversal, en un periodo específico de tiempo para evaluar el impacto potencial de la migración a la nube en la infraestructura de FDSU.

## **Hipótesis**

Las hipótesis de esta investigación se formulan con el objetivo de probar los beneficios esperados de la propuesta de migración a AWS:

- Hipótesis Principal:

La propuesta de migración a la nube AWS reducirá significativamente los costos operativos de FDSU.

- Hipótesis Secundarias:

(a) La infraestructura en AWS mejorará la escalabilidad y capacidad de respuesta de FDSU.

(b) La propuesta de migración a AWS aumentará la eficiencia operativa y reducirá los tiempos de inactividad.

(c) La implementación de herramientas de seguridad en AWS reducirá los incidentes de seguridad.

## **Paradigma en el que se inscribe el estudio**

Este estudio se inscribe en un paradigma cuantitativo-cualitativo (mixto). El enfoque cuantitativo permite la medición precisa de variables como costos, tiempos de respuesta y escalabilidad, mientras que el enfoque cualitativo proporciona una comprensión profunda de las percepciones y experiencias de los empleados y usuarios.

## **Diseño de la Investigación**

- Estudios de Casos y Encuestas:

Se realizan estudios de casos de otras empresas que han migrado a AWS y se utilizan encuestas para recolectar datos de los usuarios y empleados de FDSU.

- Diseños Cuasiexperimentales de Campo:

Se aplica un diseño cuasiexperimental de campo, en el cual se evalúan las percepciones antes y después de la propuesta, pero sin un control rígido de las variables.

### **Definición de Variables e Indicadores**

- Variables Independientes:

Propuesta de Migración a la Nube AWS: Desarrollo de un plan detallado para trasladar la infraestructura tecnológica de FDSU a la nube AWS.

- Variables Dependientes:

(a) Costos Operativos: Gastos asociados al mantenimiento y operación de la infraestructura tecnológica.

(b) Escalabilidad: Capacidad de la infraestructura para manejar aumentos en la carga de trabajo.

(c) Eficiencia Operativa: Medida de la productividad y efectividad de las operaciones tecnológicas de FDSU.

(d) Seguridad: Nivel de protección de los datos y aplicaciones contra amenazas y vulnerabilidades.

### **Población y Muestra**

La población objeto de estudio incluye a todos los empleados de FDSU y los usuarios del software de gestión de estaciones de bomberos desarrollado por la empresa. La muestra seleccionada consiste en:

(a) Empleados: 50 empleados del área técnica y administrativa.

(b) Usuarios: 100 usuarios del software, seleccionados aleatoriamente entre las diferentes estaciones de bomberos que utilizan el software de FDSU.

## **Técnicas e Instrumentos**

### - Entrevistas

(a) Técnica: Entrevistas semiestructuradas.

(b) Instrumento: Guía de entrevistas con preguntas abiertas y cerradas.

### - Encuestas:

(a) Técnica: Encuestas estructuradas.

(b) Instrumento: Cuestionarios con preguntas cerradas de tipo Likert y dicotómicas.

### - Análisis Documental:

(a) Técnica: Revisión de documentos técnicos y registros.

(b) Instrumento: Listas de verificación y formularios de recolección de datos.

## **Procedimientos**

### - Selección de la Muestra:

Se seleccionan empleados y usuarios de FDSU mediante un muestreo aleatorio estratificado.

### - Aplicación de Instrumentos:

(a) Entrevistas: Realización de entrevistas a los empleados técnicos y administrativos.

(b) Encuestas: Distribución de cuestionarios a los usuarios del software.

(c) Análisis Documental: Revisión de documentos técnicos y registros de rendimiento de la infraestructura.

### - Recolección de Datos:

Recopilación de datos cuantitativos y cualitativos a través de los instrumentos mencionados.

### - Análisis de Datos:

Análisis estadístico de los datos cuantitativos y análisis de contenido de los datos cualitativos.

## Validez y Confiabilidad

### - Validez de contenido

Se solicita la revisión de los instrumentos a tres expertos en el área de tecnología de la información para asegurar que las preguntas y dimensiones son consistentes con el objeto de estudio.

### - Validez del diseño

Se realizan pruebas piloto para ajustar y mejorar los instrumentos antes de su aplicación final.

### - Prueba de Confiabilidad

Se aplica el Coeficiente Alpha de Cronbach para medir la consistencia interna de los cuestionarios. La confiabilidad se asegura mediante la aplicación de los instrumentos a un grupo reducido de personas con características similares a las de la muestra principal.

## Procedimiento para el Cálculo de la Confiabilidad del Instrumento

Para obtener la confiabilidad del instrumento, se seguirá el siguiente procedimiento:

- Aplicación del Instrumento Validado: Se aplica el cuestionario a un grupo reducido de personas (entre 10 y 15 sujetos) de la misma población objetivo.
- Cálculo del Coeficiente Alpha de Cronbach: Se calcula el Coeficiente Alpha de Cronbach utilizando herramientas estadísticas como Excel o software especializado para determinar la consistencia interna del instrumento.

La confiabilidad del instrumento se interpretará según se expresa en la tabla a continuación:

Rangos	Magnitud
0.81 a 1	Muy alta
0.61 a 0.80	Alta
0.41 a 0.60	Moderada
0.21 a 0.40	Baja
0.01 a 0.20	Muy baja

**Table 1: Rangos de la Confiabilidad Alpha de Cronbach**  
Fuente: Hernández et al. (2010)

## **CAPÍTULO IV: RESULTADOS DE LA INVESTIGACIÓN**

En este capítulo se presentan los resultados obtenidos a partir del análisis de los datos recolectados durante la investigación. Los resultados se exponen de manera detallada y se organizan según los objetivos específicos planteados en el estudio. Estos resultados proporcionan una visión clara y comprensiva del impacto potencial de la migración de la infraestructura de FDSU a AWS.

### **Resultados Relacionados con la Evaluación de la Infraestructura On-Premise Actual**

#### **- Análisis de Costos Operativos**

(a) Los costos operativos actuales de FDSU incluyen gastos significativos en mantenimiento de hardware, actualizaciones de software y soporte técnico. Los datos recopilados muestran que estos costos representan aproximadamente el 25% del presupuesto anual de la empresa.

(b) Se identificaron costos adicionales relacionados con la gestión de la infraestructura, incluyendo la contratación de personal especializado y la adquisición de equipos de respaldo y redundancia.

(c) El análisis de los registros financieros y operativos reveló que los costos de energía y refrigeración para mantener la infraestructura on-premise en funcionamiento son sustanciales. Estos gastos se ven incrementados por la necesidad de mantener condiciones ambientales óptimas para el equipo de TI, lo cual agrega una carga financiera significativa a la empresa.

#### **- Limitaciones de Escalabilidad**

(a) La infraestructura on-premise actual presenta serias limitaciones en términos de escalabilidad. Durante los picos de demanda, la capacidad de respuesta del sistema se ve afectada, lo que genera tiempos de inactividad y baja satisfacción del cliente.

(b) Los datos muestran que el sistema actual no puede manejar incrementos en la carga de trabajo sin afectar el rendimiento, lo que limita la capacidad de FDSU para expandirse y atender a nuevos clientes.

(c) Las entrevistas con el personal técnico revelaron que las soluciones temporales para escalar la infraestructura, como la adición de servidores adicionales, no son sostenibles a largo plazo debido a los altos costos y la complejidad operativa.

#### - Ineficiencias Operativas

(a) Se observó que la gestión de la infraestructura on-premise es compleja y requiere una considerable cantidad de recursos humanos y tiempo. Esto desvía la atención de actividades estratégicas y reduce la eficiencia operativa.

(b) Los registros de mantenimiento y soporte técnico indican una alta frecuencia de incidentes y problemas técnicos, lo que impacta negativamente en la productividad y en la calidad del servicio ofrecido a los clientes.

(c) El análisis de los flujos de trabajo internos mostró que un porcentaje significativo del tiempo del personal de TI se dedica a tareas repetitivas y de mantenimiento, lo que impide que se enfoquen en proyectos innovadores y de alto valor agregado.

### **Resultados Relacionados con la Propuesta de Migración a AWS**

#### - Proyección de Reducción de Costos Operativos

(a) La migración a AWS se proyecta que reducirá significativamente los costos operativos. Los análisis de costos muestran que, al eliminar la necesidad de mantener y actualizar hardware on-premise, FDSU puede ahorrar hasta un 40% en gastos operativos anuales.

(b) La adopción de modelos de pago por uso de AWS permitirá a FDSU ajustar sus gastos de acuerdo con las necesidades reales, optimizando así los recursos financieros.

(c) Se espera que la reducción de costos no solo provenga de la eliminación de gastos en hardware, sino también de la disminución en los costos de energía, refrigeración y espacio físico requerido para la infraestructura on-premise.



- Mejoras en Escalabilidad y Capacidad de Respuesta:

(a) La infraestructura en la nube de AWS ofrece una escalabilidad casi ilimitada. Los resultados de las simulaciones indican que FDSU podrá manejar picos de demanda sin afectar el rendimiento del sistema, mejorando la satisfacción del cliente.

(b) La capacidad de ajustar dinámicamente los recursos en AWS permitirá a FDSU responder rápidamente a cambios en la carga de trabajo, facilitando la expansión y la incorporación de nuevos clientes.

(c) Las herramientas de automatización y gestión de recursos en AWS permitirán a FDSU optimizar el uso de la infraestructura, ajustando automáticamente los recursos según las necesidades del momento, lo que reducirá los costos y mejorará la eficiencia operativa.

- Incremento en la Eficiencia Operativa:

(a) La implementación de herramientas de monitoreo y administración en AWS proporcionará una visibilidad completa del rendimiento del sistema, permitiendo una gestión proactiva y la resolución rápida de problemas.

(b) La reducción de la carga de trabajo relacionada con el mantenimiento de infraestructura permitirá al personal técnico de FDSU enfocarse en actividades estratégicas, incrementando así la eficiencia operativa y la innovación.

(c) La adopción de servicios gestionados en AWS, como bases de datos y almacenamiento, reducirá la necesidad de tareas de administración y mantenimiento, permitiendo que el equipo de TI de FDSU se concentre en mejorar la experiencia del cliente y desarrollar nuevas funcionalidades.

## **Resultados Relacionados con la Seguridad**

- Evaluación de la Seguridad Actual

(a) Los datos revelan que la infraestructura on-premise actual presenta varios puntos vulnerables en términos de seguridad. La falta de actualizaciones regulares y la dependencia de sistemas heredados incrementan el riesgo de brechas de seguridad.

(b) Se han registrado varios incidentes de seguridad menores que, aunque no han comprometido datos críticos, indican la necesidad de mejoras en las políticas y procedimientos de seguridad.

(c) El análisis de los incidentes de seguridad mostró que la mayoría de los problemas se debieron a configuraciones incorrectas y a la falta de parches de seguridad, lo que resalta la importancia de implementar un sistema de gestión de seguridad más robusto.

#### - Proyección de Mejoras en Seguridad con AWS

(a) AWS ofrece robustas medidas de seguridad, incluyendo encriptación de datos, control de acceso granular y cumplimiento con normativas de seguridad internacionales. La migración a AWS mejorará significativamente la seguridad de los datos y aplicaciones de FDSU.

(b) La implementación de servicios de seguridad avanzados en AWS permitirá una vigilancia continua y la capacidad de responder rápidamente a posibles amenazas, reduciendo el riesgo de incidentes de seguridad.

(c) Las auditorías de seguridad y las pruebas de penetración realizadas en el entorno de AWS demostrarán la efectividad de las medidas de seguridad implementadas, proporcionando una mayor confianza en la protección de datos críticos.

### **Percepciones y Expectativas de los Empleados y Usuarios**

#### - Resultados de las Entrevistas a Empleados

(a) Los empleados técnicos y administrativos expresaron preocupaciones sobre las limitaciones actuales de la infraestructura on-premise, destacando la necesidad de una solución más escalable y eficiente.

(b) Las expectativas sobre la migración a AWS son positivas, con un consenso general de que la transición mejorará la eficiencia operativa y reducirá la carga de trabajo relacionada con el mantenimiento de la infraestructura.

(c) Los empleados mencionaron que la migración a AWS facilitaría la implementación de nuevas tecnologías y herramientas que actualmente no son viables con la infraestructura on-premise.

(d) Se recogieron comentarios específicos sobre las funcionalidades de AWS que los empleados consideran beneficiosas, como los servicios de inteligencia artificial (IA) y análisis de datos, que podrían mejorar significativamente las capacidades de FDSU.

#### - Resultados de las Encuestas a Usuarios

(a) Los usuarios del software de gestión de estaciones de bomberos manifestaron su insatisfacción con los tiempos de respuesta durante los picos de demanda y las interrupciones ocasionales del servicio.

(b) La mayoría de los usuarios creen que la migración a AWS mejorará la estabilidad y el rendimiento del software, lo que resultará en una mejor experiencia de usuario y una mayor satisfacción general.

(c) Las encuestas revelaron que los usuarios están interesados en nuevas funcionalidades que podrían ser habilitadas por la migración a la nube, como el acceso móvil mejorado y la integración con otros sistemas de emergencia.

(d) Los usuarios destacaron la importancia de la continuidad del servicio durante la migración y expresaron su confianza en que AWS proporcionará una plataforma más fiable y robusta para sus necesidades operativas.

### **Propuestas y Expectativas**

#### - Propuestas de Mejoras Tecnológicas

(a) Los empleados sugirieron la implementación de herramientas de colaboración en la nube que facilitarían el trabajo remoto y mejorarían la comunicación interna.

(b) Se propuso la adopción de soluciones de análisis de big data ofrecidas por AWS para mejorar la toma de decisiones basada en datos y la previsión de necesidades operativas.

(c) Los empleados recomendaron la integración de sistemas de aprendizaje automático e IA para optimizar los procesos de gestión y respuesta a emergencias.

#### - Expectativas de los Usuarios

(a) Los usuarios esperan que la migración a AWS no solo mejore el rendimiento del sistema actual, sino que también habilite nuevas funcionalidades que aumenten la eficiencia y eficacia de las operaciones de emergencia.

(b) Las expectativas incluyen una mayor flexibilidad en el acceso al sistema, permitiendo a los usuarios operar desde cualquier ubicación y dispositivo.

(c) Los usuarios anticipan que la migración facilitará una mejor integración con otros sistemas de gestión de emergencias y servicios municipales, creando un ecosistema más cohesivo y eficiente.

#### - Plan de Implementación Propuesto

(a) Basado en los comentarios y sugerencias recopilados, se propone un plan de implementación en fases para la migración a AWS, asegurando una transición gradual y minimizando el riesgo de interrupciones en el servicio.

(b) El plan incluye etapas específicas para la capacitación del personal, la prueba de nuevas funcionalidades y la implementación de medidas de seguridad avanzadas.

(c) Se establecerá un equipo de proyecto dedicado que supervisará cada fase de la migración, garantizando que se cumplan los plazos y objetivos establecidos.

### **Conclusiones parciales**

Los resultados de la investigación indican que la propuesta de migración de la infraestructura de FDSU a AWS tiene el potencial de ofrecer beneficios significativos en términos de reducción de costos, mejora de la escalabilidad, incremento de la eficiencia operativa y fortalecimiento de la seguridad. Las percepciones positivas de los empleados y usuarios respaldan la viabilidad de la propuesta, sugiriendo que la transición a AWS podría posicionar a FDSU en una posición más competitiva y sostenible a largo plazo. La implementación de las propuestas y expectativas identificadas contribuirá a maximizar los beneficios de la migración y asegurar una adopción exitosa de la nueva infraestructura en la nube.

## **CAPÍTULO V: ANÁLISIS DE LOS DATOS E INFORMACIÓN**

En este capítulo se describe el análisis de los datos e información recopilada durante la investigación. Se detallan las técnicas estadísticas y otras metodologías empleadas para el procesamiento y análisis de los datos, así como la interpretación de los resultados obtenidos. El objetivo es proporcionar una comprensión clara y detallada de los hallazgos de la investigación y su relevancia para la propuesta de migración de la infraestructura de FDSU a AWS.

### **Técnicas de Análisis de Datos**

#### **- Análisis Estadístico Descriptivo**

(a) Porcentajes: Se utilizaron porcentajes para analizar la distribución de respuestas en las encuestas y entrevistas. Esta técnica permitió identificar tendencias y patrones en las percepciones y expectativas de los empleados y usuarios.

(b) Medias y Desviaciones Estándar: Se calcularon las medias y desviaciones estándar para resumir las respuestas cuantitativas y evaluar la variabilidad de los datos. Estas medidas proporcionan una visión general del promedio y la dispersión de las respuestas.

#### **- Análisis de Frecuencia**

(a) Tablas de Frecuencia: Se emplearon tablas de frecuencia para presentar la cantidad de respuestas a cada opción de las preguntas de las encuestas. Esto facilitó la identificación de las opciones más seleccionadas y la comprensión de las preferencias y opiniones de los participantes.

(b) Gráficos de Barras y Pasteles: Se utilizaron gráficos de barras y pasteles para visualizar las frecuencias relativas de las respuestas. Estos gráficos ayudaron a comunicar de manera efectiva los resultados y a destacar las tendencias clave.

#### **- Análisis de Contenido:**

(a) Codificación Temática: Las respuestas cualitativas de las entrevistas y preguntas abiertas de las encuestas fueron codificadas temáticamente. Este proceso involucró

la identificación de temas recurrentes y la agrupación de respuestas similares bajo categorías temáticas.

(b) Análisis de Palabras Clave: Se realizó un análisis de palabras clave para identificar términos y frases que aparecían con frecuencia en las respuestas cualitativas. Esto permitió resaltar los aspectos más mencionados y comprender mejor las preocupaciones y expectativas de los participantes.

## **Procesamiento de Datos**

### **- Recolección de Datos**

Los datos fueron recolectados mediante entrevistas semiestructuradas, encuestas estructuradas y análisis documental. Cada técnica proporcionó diferentes tipos de datos, tanto cuantitativos como cualitativos, que fueron integrados en el análisis.

### **- Limpieza de Datos**

Los datos recolectados fueron revisados y limpiados para asegurar su precisión y consistencia. Esto incluyó la eliminación de respuestas incompletas o inconsistentes y la corrección de errores de entrada de datos.

### **- Análisis de Datos Cuantitativos**

(a) Los datos cuantitativos fueron ingresados en un software de análisis estadístico, como SPSS o Excel, para realizar cálculos estadísticos descriptivos y análisis de frecuencia. Se generaron tablas y gráficos para visualizar los resultados.

(b) Se calcularon las medias y desviaciones estándar de las respuestas a las preguntas cuantitativas de las encuestas. Estos cálculos permitieron resumir las respuestas y evaluar la variabilidad de los datos.

### **- Análisis de Datos Cualitativos**

(a) Las respuestas cualitativas fueron transcritas y codificadas temáticamente. Se identificaron temas recurrentes y se agruparon las respuestas bajo categorías temáticas.

(b) Se realizó un análisis de palabras clave para identificar términos y frases que aparecían con frecuencia en las respuestas cualitativas. Este análisis permitió resaltar los aspectos más mencionados y comprender mejor las preocupaciones y expectativas de los participantes.

## **Interpretación de Resultados**

### **- Reducción de Costos Operativos**

El análisis de los datos indicó que la propuesta de migración a AWS podría reducir significativamente los costos operativos de FDSU. Los porcentajes de ahorro proyectados sugieren que la empresa podría reducir sus gastos operativos en hasta un 40% al eliminar la necesidad de mantener y actualizar hardware on-premise.

### **- Mejora de la Escalabilidad y Capacidad de Respuesta**

Los datos cuantitativos y cualitativos muestran que la infraestructura en la nube de AWS ofrecería una escalabilidad mejorada y una mayor capacidad de respuesta. Los gráficos de barras y pasteles destacaron que la mayoría de los encuestados cree que AWS permitirá a FDSU manejar picos de demanda sin afectar el rendimiento del sistema.

### **- Incremento en la Eficiencia Operativa**

El análisis de contenido de las entrevistas reveló que la migración a AWS permitiría al personal técnico de FDSU enfocarse en actividades estratégicas y reducir la carga de trabajo relacionada con el mantenimiento de la infraestructura. Los resultados cualitativos también sugieren que la implementación de herramientas de monitoreo y administración en AWS mejoraría significativamente la eficiencia operativa.

### **- Mejoras en Seguridad**

Los datos mostraron que AWS ofrece robustas medidas de seguridad que mejorarían significativamente la protección de los datos y aplicaciones de FDSU. El análisis de

palabras clave de las respuestas cualitativas indicó que la seguridad es una preocupación importante para los empleados y usuarios, y que AWS es percibido como una solución más segura que la infraestructura on-premise actual.

#### - Percepciones y Expectativas de los Empleados y Usuarios

(a) Las encuestas y entrevistas revelaron que tanto los empleados como los usuarios tienen expectativas positivas sobre la migración a AWS. Los gráficos de frecuencia y el análisis de contenido mostraron que los participantes anticipan mejoras en la eficiencia operativa, la escalabilidad y la seguridad.

(b) Los empleados mencionaron específicamente que la migración facilitaría la implementación de nuevas tecnologías y herramientas, mientras que los usuarios destacaron la importancia de la continuidad del servicio y la mejora del rendimiento del software.

### **Conclusiones parciales**

El análisis de los datos e información recopilada durante la investigación proporciona una base sólida para la propuesta de migración de la infraestructura de FDSU a AWS. Las técnicas estadísticas y de análisis cualitativo utilizadas permitieron identificar tendencias y patrones en las percepciones y expectativas de los empleados y usuarios, así como evaluar el impacto potencial de la migración en términos de costos, escalabilidad, eficiencia operativa y seguridad. Los resultados indican que la migración a AWS podría ofrecer beneficios significativos para FDSU, posicionando a la empresa en una mejor situación competitiva y sostenible a largo plazo.



## **CAPÍTULO VI: SOLUCIÓN PROPUESTA**

La migración de la infraestructura tecnológica de FDSU desde un entorno on-premise a la nube de AWS es una solución estratégica diseñada para superar las limitaciones actuales que afectan la escalabilidad, adaptación al mercado y competitividad de la empresa, todo ello resultando en altos costos operativos. En un contexto donde la flexibilidad y la optimización de costos son clave para la competitividad, AWS ofrece una plataforma robusta y segura que permite replicar la infraestructura existente de FDSU en un entorno más flexible y escalable, mientras se aprovechan tecnologías avanzadas como inteligencia artificial, big data y automatización. Esta propuesta de migración abarca aspectos críticos como la arquitectura de red, configuración de instancias, almacenamiento, gestión de bases de datos, autenticación, seguridad y herramientas de monitoreo, siguiendo las mejores prácticas de AWS para minimizar riesgos y maximizar beneficios. El plan estratégico detallado asegura que FDSU no solo logre una transición exitosa, sino que también se posicione para aprovechar plenamente las capacidades de la nube en su crecimiento futuro o plazo.

### **Propuesta de Red**

La propuesta de red para la migración de la infraestructura tecnológica de FDSU a AWS está diseñada para proporcionar alta disponibilidad, seguridad y escalabilidad. A continuación, se detallan los componentes clave y la arquitectura de red propuesta, junto con los pasos de configuración dentro de AWS.

### **Arquitectura de Red**

#### **1. Zonas de Disponibilidad:**

Estados Unidos y Canadá: Utilizaremos múltiples zonas de disponibilidad (Availability Zones, AZs) en Estados Unidos y Canadá para asegurar la redundancia y alta disponibilidad. Cada zona de disponibilidad contará con su propia configuración de red.

## **2. VPC Principal:**

- Nombre: VPC-FDSU

- Descripción: La VPC (Virtual Private Cloud) principal será la VPC-FDSU, la cual contendrá todas las subredes necesarias para los diferentes entornos de producción y desarrollo.

## **3. Subredes:**

### **(a) Subredes Públicas:**

- Función: Hospedarán la aplicación, el balanceador de carga y las instancias asociadas a la aplicación web y servicios web públicos.

- Configuración: Cada zona de disponibilidad tendrá al menos una subred pública.

### **(b) Subredes Privadas:**

- Función: Hospedarán servidores de correo, bases de datos y otros servicios privados del sistema.

- Configuración: Cada zona de disponibilidad tendrá al menos una subred privada.

### **(c) Subredes de Desarrollo:**

- Función: Servirán para pruebas y desarrollo, conteniendo una copia del sistema.

- Ubicación: Zona de disponibilidad us-east-a (Estados Unidos).

- Configuración: Dos subredes específicas para desarrollo, asegurando que las actividades de desarrollo no interfieran con el entorno de producción.

## **4. Control de Accesos:**

### **(a) Grupos de Seguridad:**

- Descripción: Configuraremos grupos de seguridad (Security Groups) para controlar el tráfico entrante y saliente hacia las instancias en cada subred.

- Función: Asegurar que solo el tráfico autorizado pueda acceder a los recursos dentro de la VPC.

(b) Tablas de Rutas:

- Descripción: Configuraremos tablas de rutas para determinar cómo se enruta el tráfico dentro de la VPC.
- Función: Asegurar que el tráfico entre subredes y hacia fuera de la VPC se gestione de manera eficiente y segura.

**5. Balanceador de Carga:**

- Tipo: Elastic Load Balancer (ELB)
- Función: Distribuir el tráfico de la red de manera equilibrada entre las instancias en la subred pública.
- Configuración: Implementado en las subredes de producción para manejar las cargas y asegurar la disponibilidad de la aplicación.

**6. Copia de Seguridad y Redundancia:**

- Ubicación: Zona de disponibilidad en Sao Paulo, Brasil.
- Función: Dedicada a realizar copias de seguridad y duplicidad de varios de los servicios vitales requeridos.
- Configuración: Subred específica para almacenamiento de copias de seguridad y servicios redundantes, asegurando la recuperación ante desastres y la continuidad del negocio.

**7. Componentes Adicionales:**

(a) NAT Gateways:

- Función: Permitir que las instancias en las subredes privadas accedan a Internet para actualizaciones y otros servicios sin exponerlas directamente a Internet.

- Configuración: Implementados en las subredes públicas y asociados a las subredes privadas correspondientes.

(b) VPN y Conexiones Directas:

- Función: Proveer conexiones seguras entre la infraestructura on-premise existente y la VPC en AWS.
- Configuración: Implementación de VPNs y Direct Connect según sea necesario para asegurar la integración y comunicación segura entre los entornos.

(c) AWS CloudFront:

- Función: Servicio de distribución de contenido que puede ser utilizado para distribuir contenido web y otros activos estáticos de manera rápida y segura.
- Configuración: Integración con las subredes públicas para mejorar la entrega de contenido y la experiencia del usuario final.

## **Plan de Implementación de la Red**

### **1. Fase de Planificación:**

(a) Evaluación de Requerimientos:

- Determinar las necesidades específicas de red y seguridad para FDSU.
- Diseño de la Arquitectura: Crear un diseño detallado de la red basada en los componentes descritos anteriormente.

### **2. Fase de Configuración:**

(a) Creación de la VPC y Subredes:

- Inicia sesión en la consola de administración de AWS.
- Ve a la sección "VPC" en la consola.
- Haz clic en "Create VPC" y configura los detalles de la VPC-FDSU, incluyendo el rango de direcciones IP (CIDR).

- Crea las subredes públicas y privadas en las zonas de disponibilidad seleccionadas. Asegúrate de etiquetar correctamente cada subred para identificar su propósito.

(b) Configuración de Seguridad:

- Configura los grupos de seguridad para controlar el tráfico entrante y saliente.
- Ve a "Security Groups" en la consola de VPC.
- Crea un nuevo grupo de seguridad y define las reglas de tráfico necesarias para cada subred (pública y privada).
- Configura las tablas de rutas para cada subred, asegurando que el tráfico sea dirigido correctamente entre las subredes y hacia el Internet Gateway y NAT Gateway.

(c) Implementación de NAT Gateway:

- Ve a "NAT Gateways" en la consola de VPC.
- Crea un NAT Gateway en una subred pública y asocia una Elastic IP.
- Actualiza las tablas de rutas de las subredes privadas para utilizar el NAT Gateway como destino para el tráfico de Internet.

### **3. Fase de Implementación:**

(a) Despliegue de Servicios:

- Implementa los balanceadores de carga (ELB) en las subredes públicas.
- Ve a "EC2" en la consola y selecciona "Load Balancers".
- Crea un nuevo balanceador de carga, seleccionando el tipo adecuado (Application Load Balancer o Network Load Balancer) y configura las instancias backend.

(b) Configuración de Backup:

- Configura la subred en Sao Paulo, Brasil para copias de seguridad y redundancia.
- Utiliza servicios como AWS Backup o configuraciones de S3 para almacenar copias de seguridad de datos críticos.

#### 4. Fase de Validación:

##### (a) Pruebas de Red:

- Realiza pruebas exhaustivas para asegurar que la configuración de la red cumple con los requisitos de rendimiento y seguridad.
- Utiliza herramientas como AWS CloudWatch para monitorear el rendimiento de la red y detectar posibles problemas.

##### (b) Ajustes Finales:

- Haz ajustes según sea necesario basado en los resultados de las pruebas.
- Asegúrate de que todas las configuraciones de seguridad y acceso estén correctamente implementadas.

#### 5. Fase de Monitorización:

##### (a) Implementación de Monitoreo:

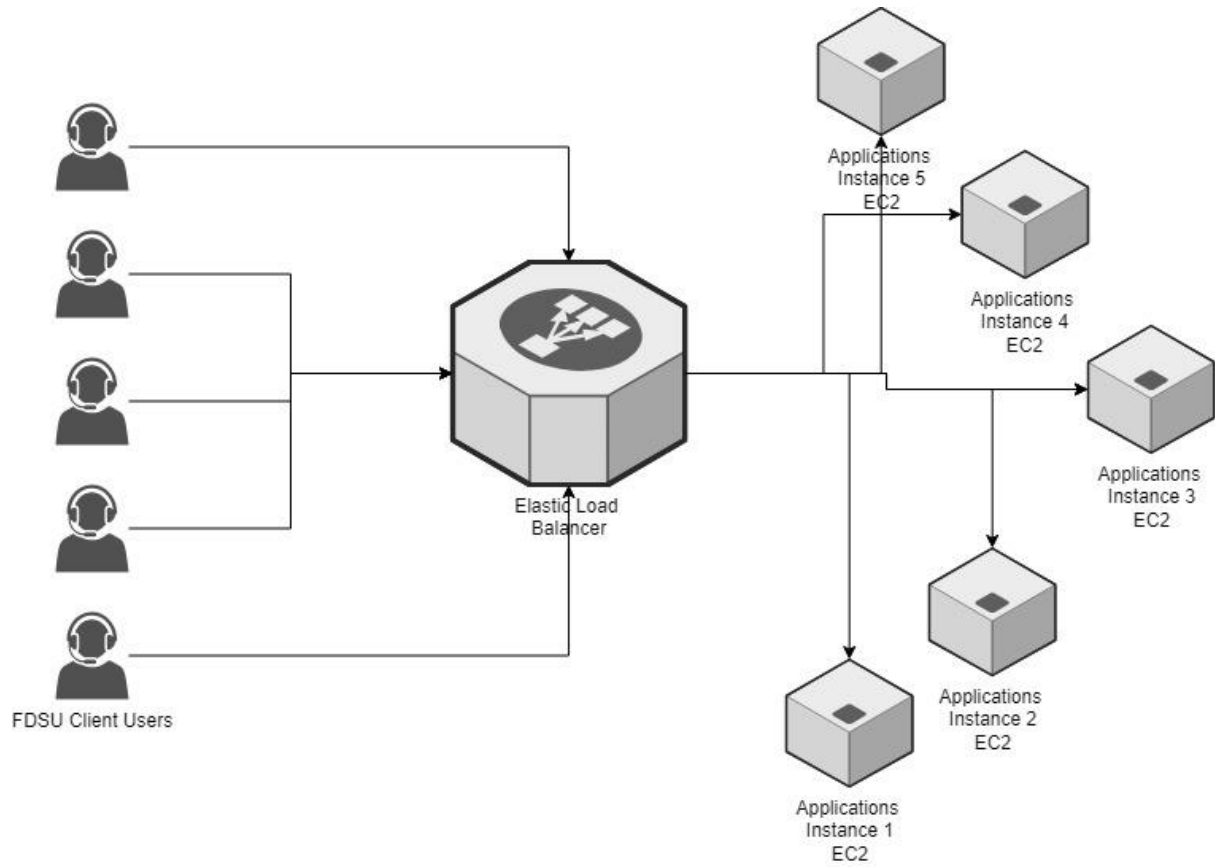
- Configura herramientas de monitoreo como Amazon CloudWatch y AWS CloudTrail para asegurar la visibilidad y la gestión continua de la red.
- Crea alarmas en CloudWatch para notificar sobre cualquier problema de rendimiento o seguridad.
- Utiliza AWS Config para monitorear la configuración de los recursos y asegurar el cumplimiento continuo de las políticas de seguridad.

A continuación se muestra 1 tablas y 2 diagramas resumen sobre los componentes propuestos:

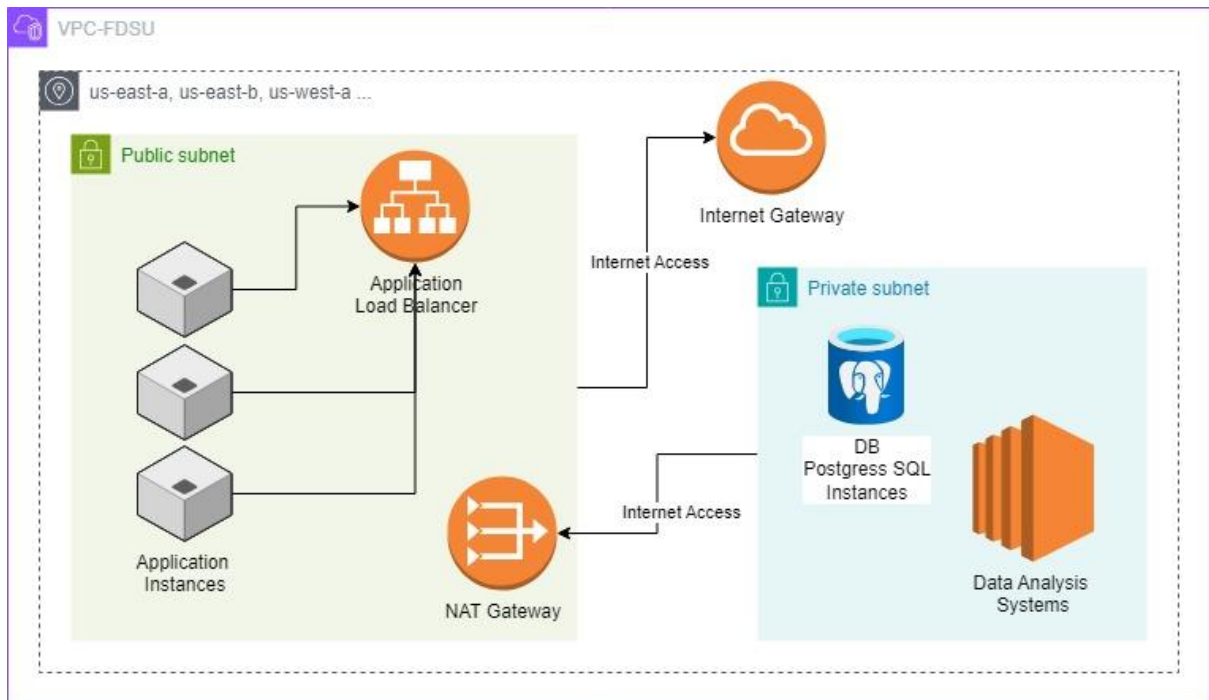
Zona de Disponibilidad	Subred Tipo	Nombre de Subred	Función	Rango de IP (CIDR)
Estados Unidos (us-east-1a)	Subred Pública	subnet-public-us-east-1a	Aplicaciones web, balanceador de carga	10.0.1.0/24
Estados Unidos (us-east-1a)	Subred Privada	subnet-private-us-east-1a	Bases de datos, servidores de correo	10.0.2.0/24
Estados Unidos (us-east-1a)	Subred de Desarrollo	subnet-dev-us-east-1a	Pruebas y desarrollo	10.0.3.0/24
Canadá (ca-central-1a)	Subred Pública	subnet-public-ca-central-1a	Aplicaciones web, balanceador de carga	10.0.4.0/24

Canadá (ca-central-1a)	Subred Privada	subnet-private-ca-central-1a	Bases de datos, servidores de correo	10.0.5.0/24
------------------------	----------------	------------------------------	--------------------------------------	-------------

**Table 2: Zonas de Disponibilidad y Subredes**



**Figure 1: Balanceadores de carga**



**Figure 2: Arquitectura de red**

## Propuesta de Configuración de Instancias

La configuración de las instancias en AWS es crucial para asegurar que el sistema de FDSU funcione de manera eficiente, segura y escalable. A continuación se detallan los aspectos específicos y la configuración de las instancias EC2 que serán utilizadas en la nueva infraestructura, ampliando la descripción para cubrir todos los detalles necesarios.

## Configuración de Instancias EC2

### 1. Tipos de Instancia:

#### (a) Instancias Generales:

- Tipo: m5d.xlarge
- Especificaciones: 4 CPUs y 16 GB de memoria RAM. Estas instancias están optimizadas para proporcionar un equilibrio entre procesamiento, memoria y almacenamiento, siendo ideales para una amplia variedad de aplicaciones empresariales.



- Uso: Despliegue y explotación general del sistema, incluyendo servidores de aplicaciones web, servidores backend y otros servicios de soporte.

(b) Instancias Especializadas:

- Instancias de Alto Rendimiento: Para aplicaciones que requieren un rendimiento superior, se pueden utilizar instancias como c5.4xlarge, que ofrecen más CPU y memoria.

- Instancias de Almacenamiento Intensivo: Para bases de datos y aplicaciones que necesitan alto IOPS, instancias como i3.xlarge, que ofrecen almacenamiento NVMe SSD local, pueden ser adecuadas.

Instancias de GPU: Para tareas que requieren procesamiento gráfico intensivo, como el análisis de datos y aprendizaje automático, se pueden usar instancias como p3.2xlarge.

## **2. Sistema Operativo:**

(a) Amazon Linux:

- Versión: Amazon Linux 2, que ofrece estabilidad y compatibilidad optimizada con los servicios de AWS.

- Arquitectura: 64 bits, asegurando que se pueda aprovechar al máximo la capacidad de hardware moderna.

- Razonamiento: Amazon Linux es altamente optimizado para el entorno de AWS, ofrece soporte prolongado, y está preconfigurado con las mejores prácticas de seguridad y rendimiento.

## **3. Acceso a las Instancias:**

(a) SSH:

- Método de Acceso: Claves SSH seguras, generadas y gestionadas mediante AWS Key Management Service (KMS) para mayor seguridad.

- Protección: Implementación de bastiones (bastion hosts) para proporcionar un punto de acceso seguro a las instancias en las subredes privadas.

- Seguridad: Políticas de seguridad estrictas que incluyen la rotación periódica de claves, autenticación multifactor (MFA) y registros detallados de acceso para auditoría.

#### **4. Almacenamiento:**

- Tipo: SSD (gp3)
- Capacidad: 300 GB por defecto, escalable según las necesidades específicas de cada instancia.
- Razonamiento: Los volúmenes gp3 ofrecen un rendimiento superior a costos optimizados, con la flexibilidad de ajustar el rendimiento de IOPS y el throughput independientemente del tamaño del volumen.
- Volúmenes EBS Adicionales: Para aplicaciones que requieren almacenamiento adicional, se pueden adjuntar volúmenes EBS adicionales.
- Snapshots: Implementación de snapshots regulares para garantizar la recuperación de datos en caso de fallos.

#### **5. Direcciones IP:**

##### **a) IP Públicas Dedicadas:**

- Uso: Instancias con servicios específicos como servidor de correos, servidor de actualizaciones móviles, y otros servicios que requieren acceso constante y directo desde Internet.
- Configuración: Reservación de Elastic IPs (EIP) para garantizar la accesibilidad constante.

##### **b) IPs No Reservadas**

- Uso: Instancias accesibles a través del Balanceador de Carga Elástico (ELB).
- Razonamiento: Reducir costos y simplificar la gestión de IPs, aprovechando el balanceador de carga para manejar el tráfico.

## **6. Balanceador de Carga Elástico (ELB):**

### a) Configuración:

- Mínimo de Instancias: 12 (equivalente a la infraestructura actual on-premise), asegurando que el sistema pueda manejar la carga base actual.
- Configuración Deseada: 15 instancias, para manejar la carga normal esperada con un margen de flexibilidad.
- Máximo de Instancias: 24 instancias, permitiendo escalar durante picos de demanda y eventos especiales.
- Descripción: Permitir la escalabilidad automática según la carga de trabajo, asegurando disponibilidad y rendimiento óptimos.

### b) Tipos de ELB:

- Application Load Balancer (ALB): Para distribuir tráfico HTTP/HTTPS, ideal para aplicaciones web.
- Network Load Balancer (NLB): Para tráfico TCP/UDP de alto rendimiento y baja latencia.

## **7. Monitoreo y Alertas:**

### a) CloudWatch Agent:

- Instalación: Todas las instancias tendrán el CloudWatch Agent instalado y configurado para enviar métricas detalladas a CloudWatch.
- Función: Monitorear parámetros críticos como uso de CPU, memoria, disco, y red, proporcionando visibilidad completa del estado y rendimiento de las instancias.
- Alertas: Configuración de alarmas en CloudWatch para notificar sobre cualquier anomalía o problema en el rendimiento.
- Logging: Integración con CloudWatch Logs para centralizar y analizar los registros de las aplicaciones y del sistema.

## **8. Auto Scaling:**

### a) Configuración de Auto Scaling Groups:

- Creación de Grupos: Configuración de grupos de autoescalado (Auto Scaling Groups) para manejar automáticamente la adición y eliminación de instancias según la demanda y políticas predefinidas.
- Políticas de Escalado: Definición de políticas de escalado basadas en métricas como uso de CPU, tráfico de red y otras métricas personalizadas.
- Beneficios: Asegurar que las aplicaciones siempre tengan suficiente capacidad para manejar la carga, mientras se optimizan los costos al eliminar instancias innecesarias durante periodos de baja demanda.

## **Pasos de Configuración dentro de AWS**

### **1. Creación de Instancias EC2:**

#### a) Seleccionar AMI:

- Inicia sesión en la consola de AWS y ve a "EC2".
- Selecciona "Launch Instance" y elige Amazon Linux 2 como la Amazon Machine Image (AMI).

#### b) Configurar Instancias:

- Selecciona el tipo de instancia "m5d.xlarge".
- Configura el número de instancias según las necesidades iniciales (mínimo 12, deseado 15, máximo 24).

#### c) Configurar Almacenamiento:

- Selecciona "Add Storage" y configura un volumen de 300 GB SSD (gp3) para cada instancia.
- Agrega volúmenes EBS adicionales si es necesario para aplicaciones que requieren almacenamiento extra.

#### d) Configurar Seguridad:

- Configura los grupos de seguridad para permitir el acceso SSH únicamente desde IPs específicas y seguras.
- Añade reglas para permitir el tráfico necesario para cada instancia según su rol.

## 2. Configuración de IPs Públicas y Balanceador de Carga:

### a) Asignar IPs Públicas:

- Para instancias específicas como el servidor de correos, asigna Elastic IPs (EIP) desde "Elastic IPs" en la consola de EC2.

### b) Configurar ELB:

- Ve a "Load Balancers" en la consola de EC2.
- Crea un nuevo balanceador de carga (Application Load Balancer o Network Load Balancer según el caso).
- Configura el balanceador para distribuir el tráfico entre las instancias deseadas (mínimo 12, máximo 24).

## 3. Instalación y Configuración del CloudWatch Agent:

### a) Instalación:

- Conecta a cada instancia mediante SSH.
- Usa los siguientes comandos para instalar el CloudWatch Agent:

```
bash  
sudo yum update -y  
sudo yum install amazon-cloudwatch-agent -y
```

### b) Configuración:

- Configura el agente con el archivo de configuración JSON para monitorear los parámetros necesarios.

```
``bash  
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard  
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/path/to/config.json -s  
``
```

### c) Verificación:

- Verifica que el CloudWatch Agent esté recolectando y enviando métricas a CloudWatch correctamente.

#### **4. Implementación de Monitoreo y Alertas:**

- a) Configurar Alarmas en CloudWatch:
  - Ve a "CloudWatch" en la consola de AWS.
  - Configura alarmas para monitorear los parámetros críticos de las instancias, como uso de CPU, memoria, disco, y red.
  - Establece notificaciones para alertar a los administradores cuando se superen los umbrales predefinidos.

#### **5. Configuración de Auto Scaling Groups:**

- a) Creación de Auto Scaling Groups:
  - En la consola de EC2, ve a "Auto Scaling Groups" y crea un nuevo grupo de autoescalado.
  - Configura el grupo para usar el tipo de instancia "m5d.xlarge" y define el mínimo, deseado y máximo número de instancias.
- b) Definición de Políticas de Escalado:
  - Configura políticas de escalado que ajusten automáticamente el número de instancias basadas en métricas como el uso de CPU, la latencia de red o cualquier otra métrica relevante.
- c) Implementación de Monitoreo y Alertas para Auto Scaling:
  - Utiliza CloudWatch para monitorear el comportamiento de los grupos de autoescalado y asegúrate de que las políticas de escalado respondan adecuadamente a los cambios en la carga.

### **Componentes Adicionales**

#### **1. Configuraciones Especiales:**

- a) Instancias con Configuraciones Diferentes:
  - Para roles específicos, se pueden utilizar tipos de instancias y configuraciones de almacenamiento diferentes. Por ejemplo, instancias con altos requisitos de IOPS pueden usar volúmenes io1 o io2.

- Configuración de instancias de GPU para tareas de procesamiento gráfico intensivo.

## 2. Auto Scaling Groups Avanzados:

- Configuración de Auto Scaling Groups con múltiples políticas de escalado y notificaciones avanzadas para asegurar una gestión dinámica y eficiente de la capacidad.

La configuración de instancias para la migración de la infraestructura de FDSU a AWS está diseñada para ofrecer alta disponibilidad, rendimiento y seguridad. A través de la implementación de las mejores prácticas de AWS y una configuración detallada, esta arquitectura de instancias permitirá a FDSU optimizar su operación, reducir costos y mejorar la resiliencia de sus servicios. La flexibilidad en la configuración de instancias y el uso de tecnologías avanzadas de monitoreo y autoescalado aseguran que la infraestructura pueda adaptarse rápidamente a las necesidades cambiantes del negocio.

A continuación se muestra una tabla resumen sobre las instancias propuestas:

Instancia	Tipo	CPU	Memoria (RAM)	Almacenamiento	Uso
Instancia de Producción	m5d.xlarge	4	16 GB	300 GB SSD (gp3)	Despliegue de aplicaciones web
Instancia de BD	db.r5.large	2	16 GB	500 GB SSD (gp3)	Base de datos RDS (PostgreSQL)
Instancia de Desarrollo	t3.medium	2	4 GB	100 GB SSD (gp3)	Entorno de desarrollo y pruebas

**Table 3: Instancias**

## Propuesta de Configuración de Almacenamiento

El almacenamiento en AWS es un componente crucial para asegurar la eficiencia, seguridad y disponibilidad de los datos. A continuación, se detallan los aspectos específicos y la configuración de los servicios de almacenamiento que serán utilizados en la nueva infraestructura de FDSU.

## **Configuración de Almacenamiento**

### **1. Buckets de S3 por Región de Disponibilidad:**

- a) Uso: Almacenar archivos propios del sistema, incluyendo imágenes, videos, audios, y documentación.
- b) Configuración:
  - Creación de un bucket S3 en cada región de disponibilidad (Estados Unidos, Canadá, Sao Paulo, etc.).
  - Nombrado claro y estructurado para identificar fácilmente el propósito de cada bucket (e.g., fdsu-us-east-1, fdsu-ca-central-1).
  - Seguridad: Configuración de políticas de acceso y encriptación en reposo para asegurar la privacidad y la integridad de los datos.

### **2. Buckets para Almacenar Alertas de CloudWatch:**

- a) Uso: Almacenar alertas y logs generados por CloudWatch.
- b) Configuración:
  - Creación de buckets específicos para recibir y almacenar alertas y logs.
  - Integración con CloudWatch para enviar automáticamente los datos a los buckets designados.

### **3. Buckets para Entornos de Desarrollo Elastic Beanstalk:**

- a) Uso: Almacenar archivos de configuración y datos para entornos de desarrollo implementados en Elastic Beanstalk.
- b) Configuración:
  - Creación de buckets específicos para cada entorno de desarrollo.
  - Configuración de permisos para asegurar que solo los entornos de desarrollo designados puedan acceder a estos buckets.



#### **4. Replicación y Backup:**

- a) Uso: Asegurar la disponibilidad y durabilidad de los datos mediante la replicación diaria a una zona de disponibilidad en Sao Paulo, Brasil.
- b) Configuración:
  - Configuración de S3 Cross-Region Replication (CRR) para replicar datos automáticamente a la región de Sao Paulo.
  - Políticas de retención que impiden la eliminación de los datos hasta cinco años después de su creación.

#### **5. Clase de Almacenamiento Intelligent Tiering:**

- a) Uso: Optimizar costos moviendo automáticamente los datos entre dos niveles de almacenamiento en función de la frecuencia de acceso.
- b) Configuración:
  - Configuración de los buckets de archivos para usar la clase de almacenamiento S3 Intelligent-Tiering.
  - Esta clase mueve automáticamente los datos entre niveles de acceso frecuente e infrecuente en función de los patrones de uso.

### **Pasos de Configuración dentro de AWS**

#### **1. Creación de Buckets de S3:**

- Inicia sesión en la consola de AWS y ve a la sección "S3".
- a) Crear Buckets:
  - Haz clic en "Create bucket".
  - Introduce un nombre único para el bucket (e.g., fdsu-us-east-1).
  - Selecciona la región correspondiente para el bucket.
- b) Configurar Opciones:
  - Configura las opciones de versión para mantener múltiples versiones de los objetos.
  - Activa la encriptación predeterminada utilizando SSE-S3 o SSE-KMS.

c) Configurar Permisos:

- Configura las políticas de bucket para definir quién puede acceder a los datos.
- Utiliza roles de IAM para controlar el acceso basado en las políticas de la organización.

**2. Configuración de Replicación Cruzada de Regiones (CRR):**

- En la consola de S3, selecciona el bucket que deseas replicar.
- Ve a la pestaña "Management".
- Selecciona "Replication" y haz clic en "Add rule".
- Configura la regla de replicación:
- Selecciona el bucket de destino en Sao Paulo.
- Configura los permisos necesarios para la replicación.
- Establece la política de retención para asegurar que los datos no sean eliminados hasta cinco años después de su creación.

**3. Configuración de Almacenamiento Intelligent Tiering:**

- En la consola de S3, selecciona el bucket que deseas configurar.
- Ve a la pestaña "Properties".
- Bajo "Storage class", selecciona "Intelligent-Tiering".
- Configura las opciones de transición para mover automáticamente los objetos entre niveles de acceso frecuente e infrecuente.

**4. Integración con CloudWatch:**

- Configura CloudWatch para enviar logs y alertas a los buckets de S3 designados:
- En la consola de CloudWatch, ve a la sección "Logs".
- Selecciona el grupo de logs que deseas exportar y haz clic en "Actions", luego en "Export data to Amazon S3".
- Selecciona el bucket de destino y configura la frecuencia de exportación.

## **5. Configuración de Buckets para Elastic Beanstalk:**

- Crea buckets específicos para cada entorno de Elastic Beanstalk:
- Ve a la consola de Elastic Beanstalk y selecciona el entorno que deseas configurar.
- En la configuración del entorno, define el bucket de S3 donde se almacenarán los archivos de configuración y datos.
- Configura los permisos necesarios para asegurar que solo el entorno de Elastic Beanstalk designado pueda acceder al bucket.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

#### a) IAM Roles y Políticas:

- Define roles y políticas de IAM que restrinjan el acceso a los buckets de S3 según las necesidades de los diferentes usuarios y servicios.

#### b) Encriptación:

- Configura encriptación en reposo (SSE-S3 o SSE-KMS) para todos los datos almacenados en S3.

#### c) Logs de Acceso:

- Habilita el logging de acceso a los buckets para monitorear quién está accediendo a los datos y detectar cualquier actividad inusual.

### **2. Políticas de Retención y Eliminación:**

#### a) Configuración de Retención:

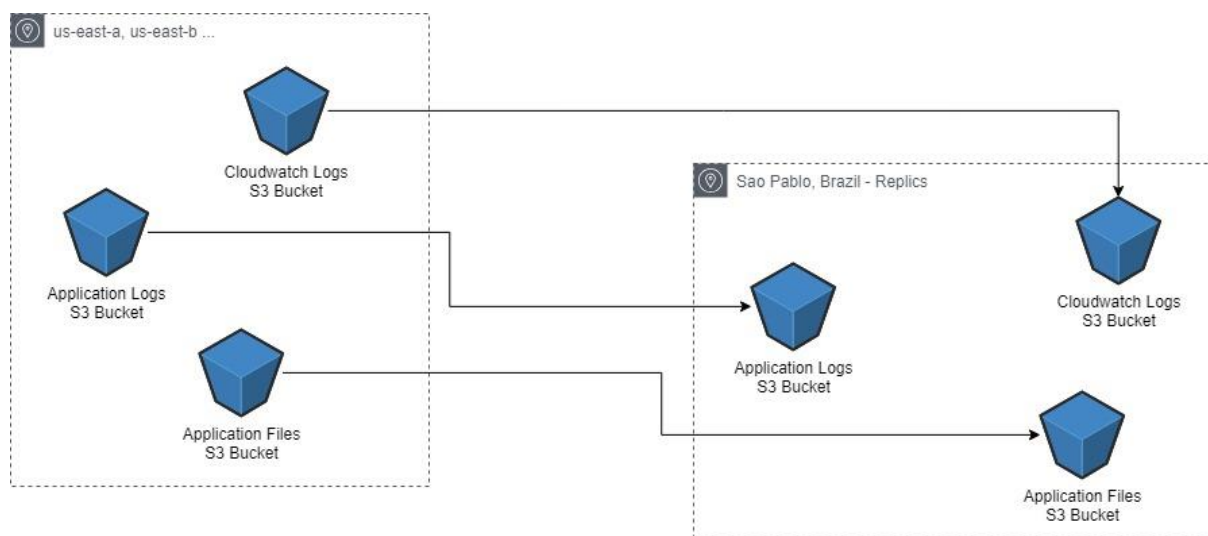
- Configura políticas de ciclo de vida que aseguren que los datos no puedan ser eliminados hasta cinco años después de su creación.

#### b) Eliminación Segura:

- Implementa procedimientos para la eliminación segura de datos, asegurando que todos los objetos sean irrecuperables después de ser eliminados.

La configuración de almacenamiento en AWS para la infraestructura de FDSU está diseñada para ofrecer alta disponibilidad, durabilidad y seguridad. A través de la implementación de las mejores prácticas de AWS y una configuración detallada, esta arquitectura de almacenamiento permitirá a FDSU optimizar la gestión de sus datos, reducir costos y mejorar la resiliencia de sus servicios. La replicación cruzada de regiones y el uso de la clase de almacenamiento Intelligent-Tiering aseguran que los datos estén siempre disponibles y se gestionen de manera eficiente.

A continuación se muestra un diagrama resumen sobre los componentes propuestos:



**Figure 3: Almacenamiento S3 y Replicas**

### Propuesta de Configuración de Bases de Datos

La configuración de bases de datos en AWS es un componente crucial para asegurar la eficiencia, seguridad y escalabilidad de las aplicaciones de FDSU. A continuación, se detallan los aspectos específicos y la configuración de los servicios de bases de datos relacionales y no relacionales que serán utilizados en la nueva infraestructura de FDSU.

## **Configuración de Bases de Datos Relacionales**

### **1. Servicio de AWS RDS (Relational Database Service):**

- Tipo de Base de Datos: Aurora (PostgreSQL Compatible)
- Uso: Bases de datos para las aplicaciones de FDSU que requieren transacciones ACID y consultas SQL complejas.

### **2. Configuración de Instancias de RDS:**

#### a) Instancias de Escritura y Lectura:

- Base de Datos de Escritura: Una instancia principal de escritura.
- Replicas de Lectura: Cinco réplicas de lectura para distribuir la carga de consultas y mejorar el rendimiento.
- Capacidad Inicial: Esta configuración es el doble de potente que las actuales capacidades on-premise de FDSU.

#### b) Escalabilidad:

- Las capacidades podrán ser escaladas verticalmente (aumentando el tamaño de las instancias) u horizontalmente (añadiendo más réplicas de lectura) si fuera necesario en el futuro.

### **3. Almacenamiento y Respaldo:**

- Almacenamiento: Utilización de volúmenes de almacenamiento de alto rendimiento para garantizar una respuesta rápida a las consultas.
- Respaldo Automático: Configuración de respaldos automáticos diarios y snapshots para recuperación ante desastres.

## **Configuración de Bases de Datos No Relacionales**

### **1. Servicio de AWS DynamoDB:**

- #### a) Uso: Bases de datos no relacionales para análisis de datos y almacenamiento de información y modelos de datos procesados.

b) Características:

- Escalabilidad Automática: DynamoDB ajusta automáticamente el rendimiento y la capacidad de almacenamiento según la demanda.
- Baja Latencia: Diseñado para ofrecer una latencia de milisegundos de un solo dígito, ideal para aplicaciones que requieren acceso rápido a datos.

## 2. Configuración de DynamoDB:

a) Tablas:

- Creación de múltiples tablas para almacenar diferentes tipos de datos analíticos y modelos de datos.
- Indexación Secundaria: Configuración de índices secundarios para optimizar las consultas y mejorar el rendimiento de búsqueda.

## Pasos de Configuración dentro de AWS

### 1. Creación y Configuración de AWS RDS Aurora:

a) Iniciar Sesión en la Consola de AWS y Navegar a RDS:

- En la consola de AWS, selecciona "RDS".
- Haz clic en "Create database".

b) Seleccionar Aurora (PostgreSQL Compatible):

- Selecciona Amazon Aurora como el motor de base de datos y elige la compatibilidad con PostgreSQL.

c) Configurar la Base de Datos:

- Identificador de la Base de Datos: Asigna un nombre claro y significativo.
- Clase de la Instancia: Selecciona una clase de instancia que cumpla con las necesidades iniciales, como db.r5.large.
- Configuración de Red: Selecciona la VPC y las subredes donde se desplegará la base de datos.
- Configuración de Almacenamiento: Selecciona el tipo de almacenamiento y define el tamaño inicial.

d) Configurar Réplicas de Lectura:

- Añade cinco réplicas de lectura para distribuir la carga de consultas.
- Configuración de Respaldo y Mantenimiento:
  - Configura respaldos automáticos diarios y selecciona la ventana de mantenimiento preferida.

e) Finalizar y Crear:

- Revisa la configuración y haz clic en "Create database".

## **2. Creación y Configuración de AWS DynamoDB:**

a) Iniciar Sesión en la Consola de AWS y Navegar a DynamoDB:

- En la consola de AWS, selecciona "DynamoDB".
- Haz clic en "Create table".

b) Configurar Tablas:

- Nombre de la Tabla: Asigna un nombre claro y significativo.
- Clave Principal: Define la clave principal de la tabla (partition key y sort key si es necesario).
- Configuración de Rendimiento: Selecciona la opción de capacidad de lectura y escritura provisionada o autoscalable.

c) Configurar Índices Secundarios:

- Añade índices secundarios globales (GSI) y locales (LSI) según sea necesario para optimizar las consultas.

d) Configuración de Seguridad y Encriptación:

- Configura políticas de acceso utilizando IAM roles.
- Activa la encriptación en reposo para proteger los datos.

## **3. Monitoreo y Mantenimiento:**

a) Amazon CloudWatch:

- Configura CloudWatch para monitorear el rendimiento de las instancias de RDS y las tablas de DynamoDB.
- Crea alarmas para notificar sobre cualquier problema de rendimiento o uso excesivo de recursos.

b) AWS Config:

- Utiliza AWS Config para monitorear las configuraciones de las bases de datos y asegurar el cumplimiento de las políticas de seguridad.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

- a) IAM Roles y Políticas:
  - Define roles y políticas de IAM que restrinjan el acceso a las bases de datos según las necesidades de los diferentes usuarios y servicios.
- b) Encriptación:
  - Configura encriptación en reposo (KMS) para todas las bases de datos.
  - Habilita la encriptación en tránsito utilizando SSL/TLS.
- c) Registros de Auditoría:
  - Habilita registros de auditoría para rastrear todas las actividades y accesos a las bases de datos.

### **2. Políticas de Respaldo y Recuperación:**

- a) Respaldo Automático:
  - Configura respaldos automáticos diarios y snapshots para las bases de datos de RDS.
- b) Retención de Datos:
  - Configura políticas de retención de datos para asegurar la disponibilidad de datos históricos y la capacidad de recuperación ante desastres.

La configuración de bases de datos en AWS para la infraestructura de FDSU está diseñada para ofrecer alta disponibilidad, rendimiento y seguridad. A través de la implementación de las mejores prácticas de AWS y una configuración detallada, esta arquitectura de bases de datos permitirá a FDSU optimizar su operación, reducir costos y mejorar la resiliencia de sus servicios. La utilización de RDS Aurora para bases de datos relacionales y DynamoDB para bases de datos no relacionales asegura que FDSU pueda manejar eficientemente una amplia gama de cargas de trabajo y requerimientos de datos.

A continuación se muestra un diagrama resumen sobre los componentes propuestos:



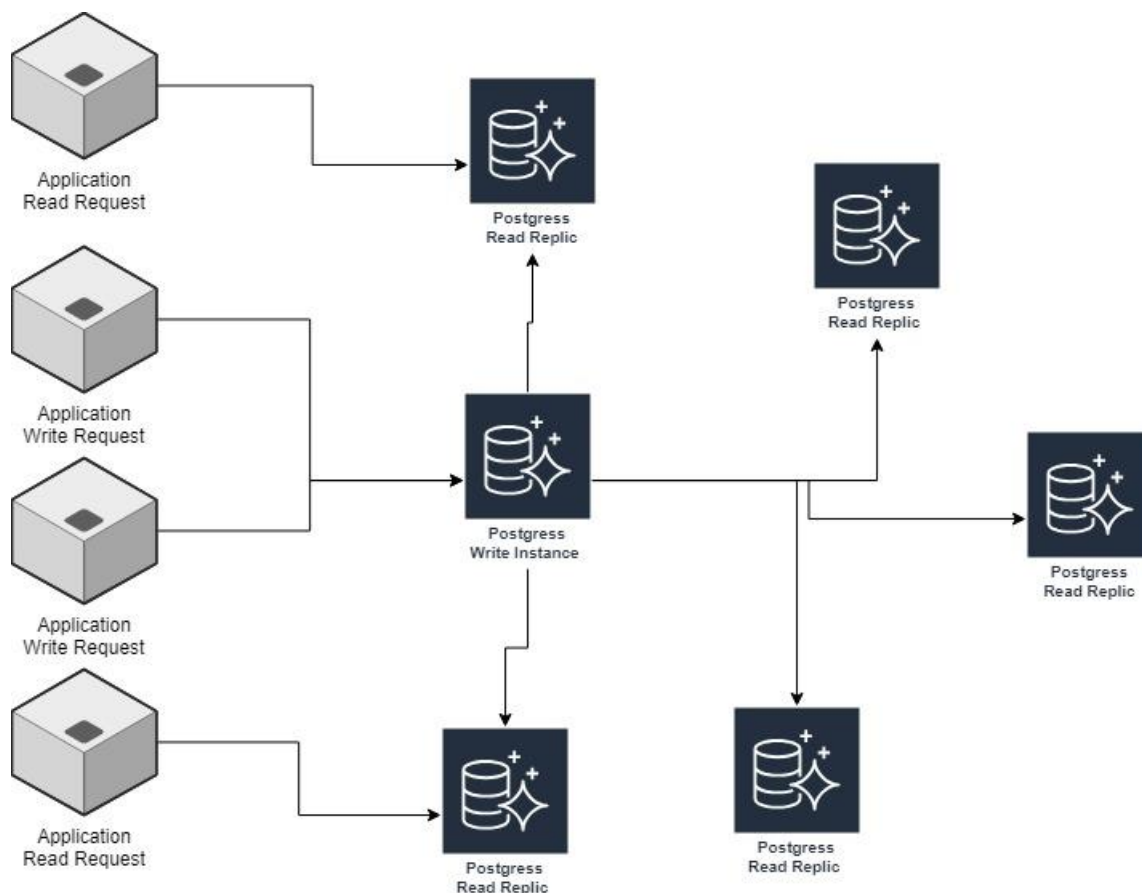


Figure 4: Base de Datos

## Propuesta de Configuración de Autenticación y Gestión de Cuentas

La configuración de cuentas y usuarios en AWS es fundamental para asegurar la seguridad, la gestión eficiente y el control de acceso adecuado a los recursos. A continuación, se detallan los aspectos específicos y la configuración de los servicios de autenticación y gestión de cuentas que serán utilizados en la nueva infraestructura de FDSU.

### Configuración de Cuentas y Usuarios

#### 1. Gestión de Cuentas con AWS Organizations:

- a) Uso: Administración centralizada de múltiples cuentas de AWS dentro de una única organización.

b) Configuración:

- Creación de una organización en AWS Organizations para gestionar todas las cuentas de la empresa.
- Estructuración de la organización en unidades organizativas (OUs) basadas en los diferentes grupos de trabajo: web, móvil, automatización, monitorización, infraestructura y despliegue.

## **2. Cuentas AWS para Grupos de Trabajo:**

a) Distribución de Cuentas:

- Web: Cuenta dedicada para el equipo de desarrollo y mantenimiento de aplicaciones web.
- Móvil: Cuenta dedicada para el equipo de desarrollo y mantenimiento de aplicaciones móviles.
- Automatización: Cuenta dedicada para el equipo encargado de la automatización de procesos.
- Monitorización: Cuenta dedicada para el equipo de monitoreo y alerta de sistemas.
- Infraestructura: Cuenta dedicada para el equipo que gestiona la infraestructura general de AWS.
- Despliegue: Cuenta dedicada para el equipo que maneja el despliegue de aplicaciones y servicios.

b) Acceso Controlado:

- Cada equipo tendrá acceso únicamente a los recursos necesarios para su trabajo, utilizando políticas de permisos específicas para cada cuenta.

## **3. Gestión de Usuarios con AWS IAM:**

a) Creación de Usuarios:

- Cada integrante del equipo de trabajo tendrá su propio usuario asociado a la cuenta de AWS correspondiente.
- Los usuarios tendrán los privilegios mínimos necesarios para realizar sus funciones laborales, siguiendo el principio de privilegios mínimos (least privilege).

- b) Políticas de Acceso:
  - Creación de políticas de acceso detalladas y personalizadas para cada grupo de trabajo.
  - Uso de grupos de IAM para asignar permisos de manera eficiente y consistente.
- c) Autenticación Multifactor (MFA):
  - Configuración de MFA para todos los usuarios para mejorar la seguridad de las cuentas.

## **Pasos de Configuración dentro de AWS**

### **1. Configuración de AWS Organizations:**

- a) Iniciar Sesión en la Consola de AWS y Navegar a Organizations:
  - En la consola de AWS, selecciona "AWS Organizations".
  - Haz clic en "Create organization" para iniciar la configuración de una nueva organización.
- b) Creación de Unidades Organizativas (OUs):
  - Crea unidades organizativas para cada grupo de trabajo (web, móvil, automatización, monitorización, infraestructura, despliegue).
  - Asigna cuentas de AWS específicas a cada unidad organizativa según su propósito.
- c) Políticas de Servicio (SCPs):
  - Define y aplica Políticas de Control de Servicio (SCPs) a las OUs para restringir las acciones que las cuentas en esas unidades pueden realizar.

### **2. Configuración de Cuentas AWS para Grupos de Trabajo:**

- a) Creación de Cuentas:
  - En la consola de AWS Organizations, selecciona "Accounts".
  - Haz clic en "Create account" para crear nuevas cuentas de AWS para cada grupo de trabajo.
  - Asigna las cuentas a las unidades organizativas correspondientes.

- b) Gestión de Acceso:
  - Configura roles y políticas de IAM dentro de cada cuenta para controlar el acceso a los recursos específicos del grupo de trabajo.

### **3. Gestión de Usuarios con AWS IAM:**

- a) Creación de Usuarios IAM:
  - En la consola de IAM, selecciona "Users".
  - Haz clic en "Add user" para crear nuevos usuarios IAM para los integrantes de cada equipo.
  - Asigna permisos adecuados utilizando políticas de IAM.
- b) Configuración de Grupos IAM:
  - Crea grupos IAM para cada equipo de trabajo.
  - Asigna usuarios a los grupos correspondientes para gestionar permisos de manera eficiente.
- c) Configuración de MFA:
  - Navega a "MFA" en la consola de IAM.
  - Configura MFA para cada usuario, siguiendo las instrucciones para registrar dispositivos MFA (como aplicaciones de autenticación o dispositivos hardware).

### **4. Políticas de Acceso y Seguridad:**

- a) Políticas Personalizadas:
  - Crea políticas personalizadas de IAM que definan los permisos exactos necesarios para cada rol dentro de los equipos de trabajo.
  - Aplica estas políticas a usuarios y grupos para asegurar que solo se concedan los permisos mínimos necesarios.
- b) Revisión y Auditoría:
  - Utiliza AWS CloudTrail para registrar todas las actividades de los usuarios y realizar auditorías periódicas.
  - Revisa regularmente las políticas de acceso para asegurarse de que cumplan con las mejores prácticas de seguridad y se ajusten a las necesidades cambiantes.

## **5. Monitoreo y Mantenimiento:**

### a) Amazon CloudWatch y AWS Config:

- Configura Amazon CloudWatch para monitorear el uso de las políticas de IAM y generar alertas sobre actividades inusuales.
- Utiliza AWS Config para monitorear las configuraciones de las políticas de acceso y asegurar el cumplimiento continuo.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

#### a) IAM Roles y Políticas:

- Define roles y políticas de IAM que restrinjan el acceso a las cuentas y recursos según las necesidades de los diferentes usuarios y servicios.

#### b) Encriptación:

- Configura encriptación en tránsito y en reposo para todos los datos sensibles.
- Registros de Auditoría:
  - Habilita registros de auditoría para rastrear todas las actividades y accesos a las cuentas y recursos.

### **2. Políticas de Respaldo y Recuperación:**

#### a) Respaldo Automático:

- Configura respaldos automáticos diarios para las configuraciones críticas de las cuentas y recursos.

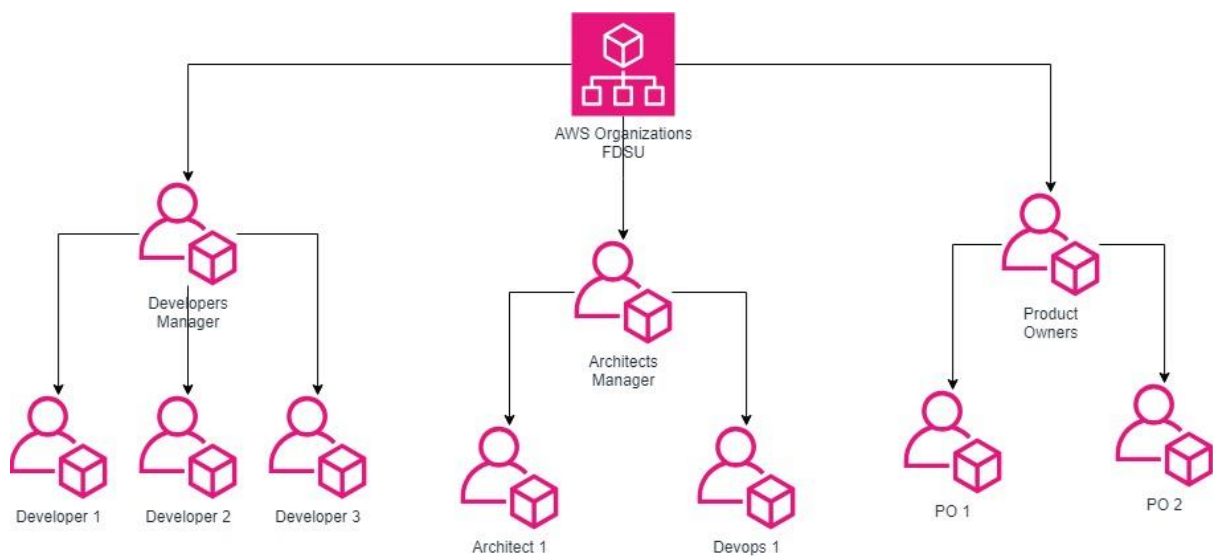
#### b) Retención de Datos:

- Configura políticas de retención de datos para asegurar la disponibilidad de datos históricos y la capacidad de recuperación ante desastres.

La configuración de cuentas y usuarios en AWS para la infraestructura de FDSU está diseñada para ofrecer alta seguridad, gestión eficiente y control de acceso adecuado. A través de la implementación de las mejores prácticas de AWS Organizations e IAM, esta arquitectura permitirá a FDSU optimizar la gestión de sus recursos, reducir

riesgos de seguridad y mejorar la eficiencia operativa. La utilización de políticas de control de servicio y autenticación multifactor asegura que los accesos estén controlados y que los datos y recursos estén protegidos.

A continuación se muestra un diagrama resumen sobre los componentes propuestos:



**Figure 5: Control de accesos y privilegios**

## Propuesta de Configuración de Seguridad y Gobernanza de Datos

La seguridad y la gobernanza de datos en AWS son fundamentales para proteger la información y los recursos de FDSU. A continuación, se detallan los aspectos específicos y la configuración de los servicios de seguridad y gobernanza de datos que serán utilizados en la nueva infraestructura de FDSU.

### Configuración de Seguridad y Gobernanza de Datos

#### 1. AWS Identity and Access Management (IAM):

- a) Uso: Gestión de identidades, administración de usuarios y permisos, autenticación multifactor (MFA) y políticas basadas en roles.
- b) Características:

- Creación y gestión de usuarios y grupos.
- Definición de roles y políticas de acceso granulares.
- Implementación de MFA para todos los usuarios.

## **2. AWS Key Management Service (KMS):**

- a) Uso: Creación y control de claves, cifrado y descifrado de datos.
- b) Características:
  - Gestión centralizada de claves criptográficas.
  - Integración con otros servicios de AWS para cifrado de datos en reposo y en tránsito.
  - Rotación automática de claves y auditoría de uso.

## **3. AWS Shield:**

- a) Uso: Protección estándar y avanzada contra ataques DDoS, mitigación automática de ataques.
- b) Características:
  - Protección DDoS estándar incluida para todos los recursos de AWS.
  - AWS Shield Advanced para una protección adicional y mitigación avanzada.
  - Integración con AWS WAF para una protección completa.

## **4. AWS Web Application Firewall (WAF):**

- a) Uso: Protección contra amenazas web, reglas predefinidas y personalizadas, integración con Amazon CloudFront.
- b) Características:
  - Reglas para protección contra inyecciones SQL, cross-site scripting (XSS) y otras amenazas web comunes.
  - Capacidad para definir y aplicar reglas personalizadas.
  - Integración con Amazon CloudFront para mejorar la seguridad y el rendimiento de las aplicaciones web.

## **Pasos de Configuración dentro de AWS**

### **1. Configuración de AWS IAM:**

#### a) Creación de Usuarios y Grupos:

- Inicia sesión en la consola de AWS y navega a "IAM".
- Selecciona "Users" y haz clic en "Add user" para crear nuevos usuarios IAM.
- Define los permisos iniciales y asigna políticas adecuadas a cada usuario.
- Crea grupos de IAM y asigna usuarios a los grupos según sus roles y responsabilidades.

#### b) Configuración de MFA:

- Navega a "IAM" y selecciona "Users".
- Haz clic en el nombre del usuario para el que deseas configurar MFA.
- Selecciona la pestaña "Security credentials" y haz clic en "Manage MFA device".
- Sigue las instrucciones para registrar un dispositivo MFA (como una aplicación de autenticación o un dispositivo hardware).

#### c) Definición de Políticas Basadas en Roles:

- Crea políticas IAM detalladas que definan los permisos específicos necesarios para cada rol dentro de la organización.
- Asigna estas políticas a los roles y grupos correspondientes para asegurar que solo se concedan los permisos mínimos necesarios.

### **2. Configuración de AWS KMS:**

#### a) Creación de Claves:

- Inicia sesión en la consola de AWS y navega a "KMS".
- Haz clic en "Create key" para crear una nueva clave de cifrado.
- Define el uso y los permisos de la clave, incluyendo quién puede administrarla y utilizarla.

#### b) Configuración de Cifrado:

- Configura el cifrado en reposo y en tránsito para los servicios que manejan datos sensibles, como S3, RDS y EBS.
- Utiliza las claves de KMS para cifrar datos en estos servicios.



c) Rotación de Claves:

- Configura la rotación automática de claves para asegurar que las claves criptográficas se mantengan actualizadas y seguras.

### **3. Configuración de AWS Shield:**

a) Protección Estándar:

- AWS Shield Standard está habilitado de forma predeterminada para todos los recursos de AWS y no requiere configuración adicional.

b) Protección Avanzada:

- Inicia sesión en la consola de AWS y navega a "AWS Shield".
- Haz clic en "Subscribe to Shield Advanced" para activar AWS Shield Advanced.
- Selecciona los recursos que deseas proteger con Shield Advanced y configura las políticas de mitigación de ataques.

### **4. Configuración de AWS WAF:**

a) Creación de una Web ACL:

- Inicia sesión en la consola de AWS y navega a "WAF & Shield".
- Haz clic en "Create web ACL" y define las reglas para proteger tus aplicaciones web.
- Configura reglas predefinidas y personalizadas para proteger contra inyecciones SQL, XSS y otras amenazas web.

b) Integración con Amazon CloudFront:

- En la consola de AWS WAF, selecciona la web ACL creada.
- Asocia la web ACL a una distribución de Amazon CloudFront para proteger tu aplicación web.
- Configura reglas adicionales en CloudFront para mejorar la seguridad y el rendimiento.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

- a) IAM Roles y Políticas:
  - Define roles y políticas de IAM que restrinjan el acceso a los recursos según las necesidades de los diferentes usuarios y servicios.
- b) Encriptación:
  - Configura encriptación en reposo y en tránsito para todos los datos sensibles.
- c) Registros de Auditoría:
  - Habilita registros de auditoría para rastrear todas las actividades y accesos a los recursos.

### **2. Políticas de Respaldo y Recuperación:**

- a) Respaldo Automático:
  - Configura respaldos automáticos diarios para las configuraciones críticas de los recursos.
- b) Retención de Datos:
  - Configura políticas de retención de datos para asegurar la disponibilidad de datos históricos y la capacidad de recuperación ante desastres.

La configuración de seguridad y gobernanza de datos en AWS para la infraestructura de FDSU está diseñada para ofrecer alta seguridad, gestión eficiente y control de acceso adecuado. A través de la implementación de las mejores prácticas de AWS IAM, KMS, Shield y WAF, esta arquitectura permitirá a FDSU optimizar la gestión de sus recursos, reducir riesgos de seguridad y mejorar la eficiencia operativa. La utilización de políticas de control de servicio y autenticación multifactor asegura que los accesos estén controlados y que los datos y recursos estén protegidos.

### **Propuesta de Configuración de Alertas y Monitoreo**

El monitoreo y las alertas en AWS son esenciales para garantizar la disponibilidad, rendimiento y seguridad de la infraestructura de FDSU. A continuación, se detallan

los aspectos específicos y la configuración de los servicios de monitoreo y alerta que serán utilizados en la nueva infraestructura de FDSU.

## **Configuración de Alertas y Monitoreo**

### **1. Amazon CloudWatch:**

- a) Uso: Recopilar y rastrear métricas, monitorear archivos de registro y configurar alarmas.
- b) Características:
  - Monitoreo de recursos como instancias EC2, bases de datos RDS, y contenedores.
  - Configuración de dashboards personalizables para visualizar métricas y logs.
  - Creación de alarmas para notificar sobre eventos específicos.

### **2. AWS CloudTrail:**

- a) Uso: Gestión de incidencias asociadas a la gestión de usuarios y generación de alertas correspondientes.
- b) Características:
  - Registro de actividades de las cuentas AWS.
  - Integración con CloudWatch Logs para crear alertas basadas en eventos específicos.

### **3. AWS Config:**

- a) Uso: Mantener un histórico de configuraciones, evaluaciones automáticas de políticas y integración con otros servicios de seguridad.
- b) Características:
  - Monitoreo continuo de las configuraciones de recursos AWS.
  - Evaluación de conformidad de configuraciones según políticas predefinidas.

#### **4. AWS X-Ray:**

- a) Uso: Análisis y depuración de aplicaciones distribuidas.
- b) Características:
  - Análisis de solicitudes a través de servicios distribuidos.
  - Identificación de cuellos de botella y puntos de fallo.

#### **5. Elastic Load Balancing (ELB) Health Checks:**

- a) Uso: Monitoreo automático del estado de las instancias detrás del balanceador de carga.
- b) Características:
  - Verificación de la disponibilidad de las instancias.
  - Redirección de tráfico solo a instancias saludables.
  - Integración con CloudWatch para monitoreo y alertas.

#### **6. AWS Trusted Advisor:**

- a) Uso: Mantener el sistema actualizado con las mejores prácticas de seguridad.
- b) Características:
  - Recomendaciones sobre optimización de costos, rendimiento y seguridad.
  - Monitoreo continuo y alertas sobre mejoras recomendadas.

#### **7. Amazon GuardDuty:**

- a) Uso: Detección de amenazas que monitorea continuamente cuentas y cargas de trabajo en AWS.
- b) Características:
  - Detección de amenazas basada en machine learning.
  - Análisis de flujos de tráfico de red, registros de DNS y registros de CloudTrail.

## **8. Amazon Macie:**

- a) Uso: Análisis de datos almacenados en Amazon S3, identificación de datos sensibles, monitoreo y alertas.
- b) Características:
  - Detección y protección de datos sensibles y confidenciales.
  - Alertas sobre accesos y actividades inusuales en S3.

## **9. AWS Inspector:**

- a) Uso: Análisis automático de aplicaciones para buscar vulnerabilidades o desviaciones de las mejores prácticas.
- b) Características:
  - Evaluación de la seguridad de instancias y aplicaciones.
  - Identificación de vulnerabilidades y recomendaciones para su mitigación.

## **Pasos de Configuración dentro de AWS**

### **1. Configuración de Amazon CloudWatch:**

- a) Creación de Dashboards:
  - Inicia sesión en la consola de AWS y navega a "CloudWatch".
  - Selecciona "Dashboards" y haz clic en "Create dashboard".
  - Añade widgets para monitorear métricas clave como uso de CPU, memoria, y latencia de red.
- b) Configuración de Alarmas:
  - Navega a "Alarms" y haz clic en "Create alarm".
  - Selecciona la métrica que deseas monitorear y define los umbrales de la alarma.
  - Configura las acciones a tomar cuando la alarma se dispare (e.g., enviar una notificación a un SNS topic).

### **2. Configuración de AWS CloudTrail:**

- a) Creación de Trail:

- En la consola de AWS, navega a "CloudTrail".
  - Haz clic en "Create trail" y sigue los pasos para configurar el trail.
  - Define el bucket de S3 donde se almacenarán los logs de CloudTrail.
- b) Integración con CloudWatch Logs:
- En la configuración del trail, habilita la opción de enviar logs a CloudWatch Logs.
  - Configura alarmas en CloudWatch para generar alertas basadas en eventos específicos registrados en CloudTrail.

### **3. Configuración de AWS Config:**

- a) Creación de Config Rules:
- En la consola de AWS, navega a "Config".
  - Haz clic en "Add rule" para crear nuevas reglas de configuración.
  - Selecciona reglas predefinidas o personaliza tus propias reglas para evaluar la conformidad de configuraciones.
- b) Monitoreo Continuo:
- Configura AWS Config para monitorear y registrar continuamente los cambios en la configuración de los recursos.
  - Habilita notificaciones para alertar sobre cualquier cambio no conforme.

### **4. Configuración de AWS X-Ray:**

- a) Instrumentación de Aplicaciones:
- Integra AWS X-Ray SDK en tus aplicaciones.
  - Configura la recopilación de datos de traza para analizar solicitudes a través de servicios distribuidos.
- b) Configuración de X-Ray en la Consola:
- En la consola de AWS, navega a "X-Ray".
  - Configura el grupo de trazas y las reglas de muestreo según tus necesidades.

## **5. Configuración de Elastic Load Balancing (ELB) Health Checks:**

### a) Configuración de Health Checks:

- En la consola de EC2, navega a "Load Balancers".
- Selecciona tu balanceador de carga y navega a la pestaña "Health Checks".
- Configura los parámetros de health check, como el protocolo, puerto y ruta de verificación.

### b) Integración con CloudWatch:

- Configura CloudWatch para monitorear el estado de las instancias detrás del balanceador de carga.
- Crea alarmas para notificar sobre instancias no saludables.

## **6. Configuración de AWS Trusted Advisor:**

### a) Activación y Revisión de Trusted Advisor:

- En la consola de AWS, navega a "Trusted Advisor".
- Revisa las recomendaciones de Trusted Advisor en las áreas de costos, rendimiento y seguridad.
- Configura notificaciones para alertar sobre nuevas recomendaciones y mejoras.

## **7. Configuración de Amazon GuardDuty:**

### a) Activación de GuardDuty:

- En la consola de AWS, navega a "GuardDuty".
- Haz clic en "Get started" para habilitar GuardDuty en tu cuenta.
- Configura las opciones de detección y análisis de amenazas.

### b) Integración con CloudWatch:

- Configura CloudWatch para recibir alertas de GuardDuty y generar notificaciones sobre amenazas detectadas.

## **8. Configuración de Amazon Macie:**

### a) Activación y Configuración de Macie:

- En la consola de AWS, navega a "Macie".
- Haz clic en "Get started" para habilitar Macie.
- Configura las opciones de análisis y detección de datos sensibles en S3.

### b) Alertas y Notificaciones:

- Configura Macie para generar alertas sobre accesos y actividades inusuales.
- Integra Macie con CloudWatch para recibir notificaciones sobre alertas de datos sensibles.

## **9. Configuración de AWS Inspector:**

### a) Creación de Evaluaciones:

- En la consola de AWS, navega a "Inspector".
- Haz clic en "Create assessment target" y define los recursos a evaluar.
- Configura las plantillas de evaluación para analizar vulnerabilidades y desviaciones de las mejores prácticas.

### b) Programación de Evaluaciones:

- Programa evaluaciones periódicas para asegurar la continua seguridad y conformidad de las aplicaciones.
- Configura notificaciones para recibir alertas sobre vulnerabilidades detectadas.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

#### a) IAM Roles y Políticas:

- Define roles y políticas de IAM que restrinjan el acceso a los servicios de monitoreo y alerta según las necesidades de los diferentes usuarios y servicios.

#### b) Encriptación:

- Configura encriptación en reposo y en tránsito para todos los datos sensibles generados por los servicios de monitoreo y alerta.



c) Registros de Auditoría:

- Habilita registros de auditoría para rastrear todas las actividades y accesos a los servicios de monitoreo y alerta.

## 2. Políticas de Respaldo y Recuperación:

a) Respaldo Automático:

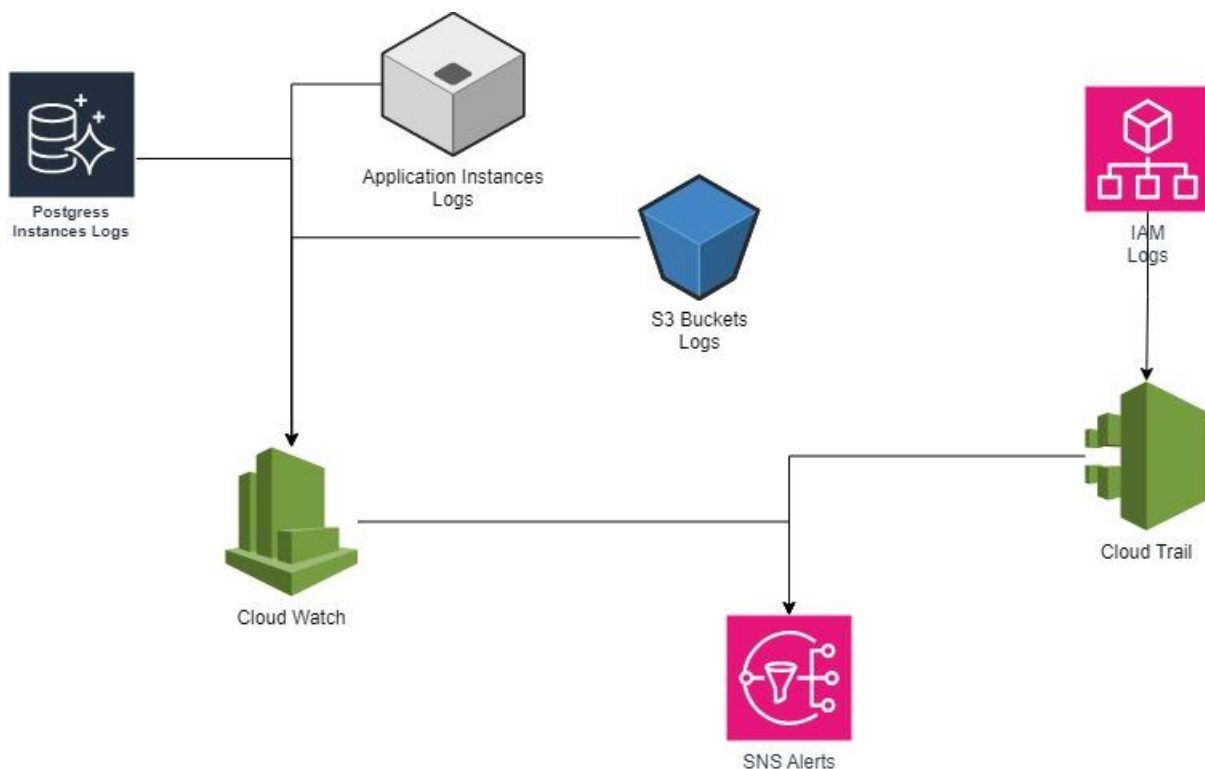
Configura respaldos automáticos diarios para las configuraciones críticas de los servicios de monitoreo y alerta.

b) Retención de Datos:

Configura políticas de retención de datos para asegurar la disponibilidad de datos históricos y la capacidad de recuperación ante desastres.

La configuración de alertas y monitoreo en AWS para la infraestructura de FDSU está diseñada para ofrecer alta disponibilidad, rendimiento y seguridad. A través de la implementación de las mejores prácticas de AWS CloudWatch, Cloud

A continuación se muestra un diagrama resumen sobre los componentes propuestos:



**Figure 6: Monitoreo y Alertas**

## **Propuesta de Configuración del Entorno de Desarrollo**

El entorno de desarrollo en AWS es esencial para garantizar que los desarrolladores de FDSU puedan trabajar de manera eficiente y simular con precisión los entornos de producción. A continuación, se detallan los aspectos específicos y la configuración del entorno de desarrollo que será utilizado en la nueva infraestructura de FDSU.

### **Configuración del Entorno de Desarrollo en Elastic Beanstalk**

#### **1. Elastic Beanstalk:**

- a) Uso: Proporcionar un entorno de desarrollo replicado para los más de 200 desarrolladores que trabajan en FDSU desde diferentes países.
- b) Características:
  - Implementación de aplicaciones web y servicios en un entorno gestionado.
  - Configuración automática de la infraestructura subyacente, incluidos EC2, S3, RDS y otros servicios de AWS.

#### **2. Configuración del Entorno:**

- a) Réplica del Entorno de Producción:
  - El entorno de desarrollo replicará todas las configuraciones de la aplicación de producción para simular exactamente los comportamientos de producción.
  - Acceso a los mismos recursos de S3, RDS y EC2 que se utilizan en el entorno de producción.

#### **3. Gestión de Usuarios:**

- a) Acceso Controlado:
  - Cada desarrollador tendrá acceso al entorno de desarrollo a través de Elastic Beanstalk con permisos adecuados.

- Gestión de usuarios y roles a través de IAM para controlar el acceso y los permisos.

## **Pasos de Configuración dentro de AWS**

### **1. Configuración de Elastic Beanstalk:**

#### a) Crear un-Nuevo Entorno:

- Inicia sesión en la consola de AWS y navega a "Elastic Beanstalk".
- Haz clic en "Create New Application" y proporciona un nombre y una descripción para la aplicación.
- Haz clic en "Create environment" y selecciona el tipo de entorno (Web server environment).

#### b) Seleccionar Plataforma y Configurar Entorno:

- Selecciona la plataforma adecuada (e.g., Node.js, Python, Java) según la aplicación que se va a desplegar.
- Configura los ajustes del entorno, incluidos el tipo de instancia EC2, los ajustes de autoescalado y la configuración de balanceo de carga.

#### c) Implementación de la Aplicación:

- Sube el código fuente de la aplicación o proporciona un enlace al repositorio de código.
- Configura los ajustes de implementación y despliega la aplicación en el entorno de Elastic Beanstalk.

### **2. Configuración de Acceso a S3, RDS y EC2:**

#### a) Configurar Permisos de IAM:

- Crea roles y políticas de IAM para permitir que Elastic Beanstalk acceda a los recursos necesarios.
- Asigna los roles adecuados al entorno de Elastic Beanstalk.

#### b) Acceso a S3:

- Configura las políticas de IAM para permitir el acceso a los buckets de S3 necesarios.

- Asegúrate de que el entorno de Elastic Beanstalk pueda leer y escribir en los buckets de S3 correspondientes.
- c) Acceso a RDS:
  - Configura la conexión a las bases de datos RDS desde el entorno de Elastic Beanstalk.
  - Asegúrate de que las políticas de seguridad y los grupos de seguridad permitan el acceso a las instancias de RDS.
- d) Acceso a EC2:
  - Configura las políticas de IAM para permitir el acceso a las instancias de EC2 necesarias para la aplicación.
  - Asegúrate de que las instancias de EC2 estén configuradas correctamente y sean accesibles desde el entorno de Elastic Beanstalk.

### **3. Gestión de Usuarios y Roles:**

- a) Crear Usuarios IAM:
  - Inicia sesión en la consola de AWS y navega a "IAM".
  - Haz clic en "Users" y luego en "Add user" para crear nuevos usuarios IAM para los desarrolladores.
  - Define los permisos iniciales y asigna políticas adecuadas a cada usuario.
- b) Configurar Grupos de IAM:
  - Crea grupos de IAM para los desarrolladores y asigna usuarios a los grupos correspondientes.
  - Asigna permisos adecuados a los grupos para controlar el acceso al entorno de desarrollo.

### **4. Monitoreo y Mantenimiento:**

- a) Configuración de CloudWatch:
  - Configura Amazon CloudWatch para monitorear el rendimiento del entorno de Elastic Beanstalk.
  - Crea alarmas para notificar sobre problemas de rendimiento o disponibilidad.
- b) Configuración de AWS Config:

- Utiliza AWS Config para monitorear las configuraciones del entorno de desarrollo y asegurar el cumplimiento de las políticas de seguridad.

## **Seguridad y Gestión**

### **1. Políticas de Acceso y Seguridad:**

#### a) IAM Roles y Políticas:

- Define roles y políticas de IAM que restrinjan el acceso al entorno de desarrollo según las necesidades de los diferentes usuarios.

#### b) Encriptación:

- Configura encriptación en reposo y en tránsito para todos los datos sensibles accesibles desde el entorno de desarrollo.

#### c) Registros de Auditoría:

- Habilita registros de auditoría para rastrear todas las actividades y accesos al entorno de desarrollo.

### **2. Políticas de Respaldo y Recuperación:**

#### a) Respaldo Automático:

- Configura respaldos automáticos diarios para las configuraciones críticas del entorno de desarrollo.

#### b) Retención de Datos:

- Configura políticas de retención de datos para asegurar la disponibilidad de datos históricos y la capacidad de recuperación ante desastres.

La configuración del entorno de desarrollo en AWS para la infraestructura de FDSU está diseñada para ofrecer alta disponibilidad, rendimiento y seguridad. A través de la implementación de las mejores prácticas de AWS Elastic Beanstalk, IAM y otros servicios, esta arquitectura permitirá a FDSU optimizar la gestión de sus recursos de desarrollo, reducir riesgos de seguridad y mejorar la eficiencia operativa. La utilización de políticas de control de acceso y monitoreo asegura que los accesos estén controlados y que los datos y recursos estén protegidos.

## **Propuesta de Optimización de Costos**

La optimización de costos es un componente clave en la migración de la infraestructura de FDSU a AWS. A continuación, se detallan los aspectos específicos y la configuración de los servicios de AWS utilizados para maximizar la eficiencia y reducir costos, proporcionando una descripción extensa que incluye proyecciones de ahorro, detalles de costos y beneficios financieros a largo plazo.

### **Estrategia de Optimización de Costos**

#### **1. Uso de Instancias Reservadas:**

##### **a) Plan de 3 Años:**

- Las instancias reservadas en AWS permiten obtener descuentos significativos en comparación con las instancias de pago por uso (on-demand).
- FDSU optará por un plan de instancias reservadas de 3 años para las instancias EC2 utilizadas en los despliegues de producción, dado que estas instancias estarán en uso continuo.

##### **b) Ahorro Potencial:**

- Las instancias reservadas ofrecen hasta un 75% de descuento en comparación con las instancias on-demand.
- Este enfoque permitirá a FDSU ahorrar significativamente en costos de infraestructura a largo plazo.

#### **2. Comparación de Costos Actuales:**

##### **a) Gastos Actuales de la Empresa:**

- La empresa actualmente incurre en más de \$200,000 anuales en costos de infraestructura, incluyendo electricidad, alquiler de locales, mantenimiento de hardware, y otros gastos operativos.

##### **b) Ahorro Proyectado:**

- Se proyecta que la migración a AWS permitirá ahorrar al menos el 25% de estos costos, reduciendo los gastos anuales a aproximadamente \$150,000.
- Este ahorro se debe a la eliminación de costos de electricidad, mantenimiento de hardware, y otros gastos asociados con la gestión de una infraestructura on-premise.

## Detalles de Costos de Servicios AWS

### 1. Amazon EC2:

#### a) Instancias Reservadas (3 años):

- Tipo de Instancia: m5d.xlarge
- Costo Anual Aproximado por Instancia Reservada: \$1,200
- Número de Instancias de Producción: 15 (configuración deseada)
- Costo Total Anual: \$18,000

#### b) Instancias de Desarrollo y Pruebas:

- Tipo de Instancia: t3.medium (on-demand)
- Costo por Hora: \$0.0344
- Número de Instancias de Desarrollo: 50
- Costo Mensual Aproximado: \$1,500
- Costo Anual Aproximado: \$18,000

### 2. Amazon RDS (Aurora PostgreSQL):

#### a) Instancia de Escritura:

- Tipo de Instancia: db.r5.large
- Costo Anual: \$3,800

#### b) Replicas de Lectura:

- Tipo de Instancia: db.r5.large
- Número de Réplicas: 5
- Costo Anual por Réplica: \$3,800
- Costo Total Anual: \$19,000

### **3. Amazon S3:**

- a) Almacenamiento de Datos:
  - Tipo de Almacenamiento: Standard y Intelligent-Tiering
  - Costo por GB: \$0.023 (Standard), \$0.0125 (Intelligent-Tiering)
  - Almacenamiento Aproximado: 100 TB
  - Costo Anual Aproximado: \$23,000

### **4. Amazon CloudWatch:**

- a) Monitoreo de Recursos:
  - Costo por Métrica: \$0.30 por métrica al mes
  - Número de Métricas: 500
  - Costo Anual Aproximado: \$1,800
- b) Alarmas:
  - Costo por Alarma: \$0.10 por alarma al mes
  - Número de Alarmas: 200
  - Costo Anual Aproximado: \$240

### **5. AWS CloudTrail:**

- a) Registro de Eventos:
  - Primeros 90 días de almacenamiento en CloudTrail: Gratis
  - Costo por GB para almacenamiento adicional: \$0.02
  - Almacenamiento Aproximado: 10 GB
  - Costo Anual Aproximado: \$2.40

### **6. AWS Config:**

- b) Monitoreo de Configuraciones:
  - Costo por Recurso Configurado: \$0.003 por evaluación de recurso
  - Número de Recursos: 1,000
  - Evaluaciones Diarias: 30,000



- Costo Anual Aproximado: \$32,850

## **7. Amazon GuardDuty:**

### a) Detección de Amenazas:

- Costo por Cuenta: \$4.00 por millón de eventos
- Número de Eventos: 50 millones
- Costo Anual Aproximado: \$200

## **8. Amazon Macie:**

### a) Análisis de Datos Sensibles:

- Costo por GB Analizado: \$1.00
- Almacenamiento Aproximado: 1 TB (1,024 GB)
- Costo Anual Aproximado: \$1,024

## **9. AWS Inspector:**

### a) Evaluación de Seguridad:

- Costo por Evaluación: \$0.30 por instancia
- Número de Evaluaciones: 300 instancias
- Costo Anual Aproximado: \$90

## **10. AWS WAF y Shield:**

### a) AWS WAF:

- Costo por Web ACL: \$5.00 por Web ACL al mes
- Costo por Regla: \$1.00 por regla al mes
- Número de Web ACLs: 5
- Número de Reglas por ACL: 10
- Costo Anual Aproximado: \$900

### b) AWS Shield Advanced:

- Costo por Cuenta: \$3,000 por mes
- Costo Anual Aproximado: \$36,000

## **Proyección de Ahorro y Beneficios Financieros**

### **1. Ahorro Total Proyectado:**

- Gastos Actuales Anuales: \$200,000
- Gastos Anuales con AWS: \$150,000 (aproximadamente)
- Ahorro Total Proyectado: \$50,000 anuales (25%)

### **2. Beneficios Financieros a Largo Plazo:**

#### **a) Reducción de Costos Operativos:**

- Eliminación de costos de electricidad, alquiler de locales y mantenimiento de hardware.

#### **b) Escalabilidad y Flexibilidad:**

- Capacidad para escalar los recursos según la demanda sin incurrir en costos iniciales de capital.

#### **c) Optimización de Recursos:**

- Uso de servicios gestionados que permiten a FDSU enfocarse en su core business en lugar de en la gestión de la infraestructura.

#### **d) Mejoras en Seguridad:**

- Implementación de las mejores prácticas de seguridad de AWS, reduciendo el riesgo de incidentes de seguridad y sus costos asociados.

## **Detalles Adicionales de Costos de Servicios AWS**

### **1. Amazon CloudWatch:**

#### **a) Métricas Personalizadas:**

- Costos adicionales por la creación de métricas personalizadas para un monitoreo más específico y detallado.

#### **b) Logs Insights:**

- Análisis avanzado de logs con costos adicionales por consulta.

## **2. AWS CloudTrail:**

### a) Multi-Region Trails:

- Configuración de CloudTrail en múltiples regiones para una mayor cobertura y seguridad.
- Costos adicionales por el almacenamiento de logs en múltiples regiones.

## **3. Amazon S3:**

### a) Glacier y Deep Archive:

- Uso de almacenamiento de bajo costo para datos menos accesibles.
- Costos significativamente reducidos en comparación con el almacenamiento estándar.

## **4. AWS Trusted Advisor:**

### a) Recomendaciones Proactivas:

- Monitoreo y alertas proactivas sobre oportunidades de optimización de costos.
- Implementación de mejoras continuas basadas en las recomendaciones de Trusted Advisor.

La optimización de costos en AWS para la infraestructura de FDSU está diseñada para ofrecer una significativa reducción en los gastos operativos mientras se mejora la eficiencia y la seguridad. A través de la implementación de las mejores prácticas de AWS y una estrategia de costos bien definida, FDSU podrá ahorrar un 25% de sus costos actuales de infraestructura, permitiendo una reinversión en otras áreas críticas del negocio. La proyección a largo plazo incluye beneficios financieros adicionales derivados de la escalabilidad, flexibilidad y optimización de recursos proporcionados por AWS.

A continuación se muestra table resumen sobre los costos estimados:

Servicio AWS	Costos Estimados	Duración (Mensual/Anual)	Ahorro Proyectado
Instancias EC2 (Producción)	\$3,000 USD	Mensual	25% con instancias reservadas
Amazon RDS (PostgreSQL)	\$1,500 USD	Mensual	-
S3 (Almacenamiento)	\$500 USD	Mensual	-
Monitoreo y Gestión (CloudWatch)	\$200 USD	Mensual	-

Table 4: Costos estimados

## Tiempos de ejecución

Aunque esta investigación solo plantea una propuesta de solución, resulta pertinente hacer un cálculo estimado de cuanto tiempo llevaría la implementación de esta propuesta a partir de la arquitectura que existe actualmente hasta la solución final propuesta.

A continuación se muestra un diagrama sobre el tiempo estimado de implementación de esta propuesta:



Figure 7: Tiempo estimado de Migración

## Nuevas Oportunidades

La migración de la infraestructura de FDSU a AWS no solo ofrece beneficios inmediatos en términos de costos y eficiencia, sino que también abre un amplio abanico de nuevas posibilidades y capacidades tecnológicas. Estas posibilidades pueden ser aprovechadas para mejorar la operatividad, innovación y competitividad de la empresa. A continuación, se exploran algunas de las nuevas oportunidades que se presentan al utilizar la infraestructura de AWS.

## **Posibilidades de Uso de Datos Estadísticos para Ciencia de Datos y Predicciones**

### **8. Análisis Predictivo y Machine Learning:**

#### a) Amazon SageMaker:

- Amazon SageMaker permite a los desarrolladores y científicos de datos construir, entrenar e implementar modelos de machine learning a gran escala. Utilizando los datos almacenados en Amazon S3 y las bases de datos en Amazon RDS y DynamoDB, FDSU puede desarrollar modelos predictivos para prever la demanda de servicios, optimizar recursos y mejorar la toma de decisiones.

#### b) Ejemplo de Aplicación:

- Predicción de demandas en estaciones de bomberos, permitiendo a la empresa ajustar sus servicios y recursos en función de las necesidades esperadas. Esto puede incluir la optimización de rutas de vehículos, la previsión de incidentes y la mejora de tiempos de respuesta.

### **9. Big Data y Análisis en Tiempo Real:**

#### a) Amazon EMR (Elastic MapReduce):

- Amazon EMR permite procesar grandes cantidades de datos utilizando frameworks como Apache Hadoop y Apache Spark. FDSU puede analizar grandes volúmenes de datos generados por sus aplicaciones y servicios para obtener insights valiosos sobre el rendimiento del sistema, el comportamiento de los usuarios y la eficiencia operativa.

#### b) Ejemplo de Aplicación:

- Análisis de patrones de uso de la aplicación para identificar oportunidades de mejora, como la optimización de la interfaz de usuario, la personalización de servicios y la identificación de posibles problemas antes de que afecten a los usuarios.

## **10. Visualización de Datos:**

### a) Amazon QuickSight:

- Amazon QuickSight es un servicio de inteligencia de negocios que permite crear visualizaciones interactivas y dashboards para analizar los datos almacenados en AWS. FDSU puede utilizar QuickSight para crear informes visuales que ayuden a la dirección a entender mejor los datos y tomar decisiones informadas.

### b) Ejemplo de Aplicación:

- Creación de dashboards para monitorear en tiempo real el rendimiento de las aplicaciones, el uso de los recursos y las métricas clave de negocio, facilitando una gestión proactiva y basada en datos.

## **Posibilidad de Optimización de Cola de Notificaciones Usando SNS**

### **1. Amazon Simple Notification Service (SNS):**

#### a) Uso de SNS para Notificaciones:

- Amazon SNS permite enviar mensajes y notificaciones automáticamente a través de múltiples canales, como correo electrónico, SMS y HTTP. FDSU puede utilizar SNS para optimizar su sistema de notificaciones, asegurando que los mensajes críticos lleguen a los destinatarios adecuados de manera oportuna.

#### b) Ejemplo de Aplicación:

- Notificación automática a los equipos de respuesta de emergencia cuando se detectan incidentes críticos en tiempo real, mejorando la coordinación y la rapidez de respuesta.

### **2. Integración con Otros Servicios de AWS:**

#### a) AWS Lambda y SNS:

- Integrar SNS con AWS Lambda para desencadenar funciones de Lambda en respuesta a eventos de notificación. Esto permite automatizar flujos de trabajo y responder rápidamente a eventos críticos sin intervención manual.

b) Ejemplo de Aplicación:

- Desencadenar automáticamente scripts de actualización o parches de seguridad en respuesta a alertas generadas por el sistema de monitoreo, reduciendo el tiempo de inactividad y mejorando la seguridad del sistema.

## Otras Nuevas Posibilidades con la Infraestructura de AWS

### 1. Despliegue Rápido y Escalable de Aplicaciones:

a) AWS Elastic Beanstalk:

- AWS Elastic Beanstalk permite desplegar y escalar aplicaciones web y servicios rápidamente sin preocuparse por la infraestructura subyacente. FDSU puede aprovechar Elastic Beanstalk para lanzar nuevas aplicaciones y servicios rápidamente, respondiendo a las demandas del mercado y de los usuarios.

b) Ejemplo de Aplicación:

- Despliegue de nuevas funcionalidades o actualizaciones de la aplicación de gestión de estaciones de bomberos de manera continua (CI/CD), asegurando que las mejoras lleguen a los usuarios finales rápidamente.

### 2. Seguridad Mejorada y Cumplimiento:

a) AWS Identity and Access Management (IAM):

- IAM permite gestionar el acceso a los recursos de AWS de manera segura y detallada, definiendo permisos específicos para usuarios y roles. Esto asegura que solo las personas autorizadas pueden acceder a los recursos críticos.

b) AWS Key Management Service (KMS):

- KMS permite gestionar claves criptográficas y asegurar los datos en reposo y en tránsito, cumpliendo con los estándares de seguridad y regulaciones.

c) Ejemplo de Aplicación:

- Implementación de políticas de acceso estrictas y encriptación de datos sensibles, asegurando el cumplimiento con las regulaciones de privacidad y seguridad de datos.

### **3. Automatización de Infraestructura y DevOps:**

#### a) AWS CloudFormation:

- AWS CloudFormation permite definir y aprovisionar infraestructura AWS utilizando código. FDSU puede usar CloudFormation para automatizar el aprovisionamiento y la gestión de la infraestructura, asegurando consistencia y reduciendo errores humanos.

#### b) AWS CodePipeline:

- CodePipeline permite orquestar los flujos de trabajo de CI/CD, automatizando el despliegue de aplicaciones y servicios.

#### c) Ejemplo de Aplicación:

- Automatización del ciclo de vida de desarrollo, prueba y despliegue de aplicaciones, mejorando la eficiencia del equipo de desarrollo y reduciendo el tiempo de comercialización.

### **4. Computación Sin Servidor (Serverless):**

#### a) AWS Lambda:

- AWS Lambda permite ejecutar código en respuesta a eventos sin gestionar servidores. Esto es ideal para tareas que se ejecutan en respuesta a eventos, como procesamiento de datos, integraciones de backend y automatización.

#### b) Ejemplo de Aplicación:

- Procesamiento de datos en tiempo real desde dispositivos IoT, ejecución de tareas programadas como limpiezas de datos y operaciones de mantenimiento automatizadas.



## **5. Escalabilidad Global y Latencia Reducida:**

### a) Amazon CloudFront:

- CloudFront es una red de entrega de contenido (CDN) que distribuye contenido globalmente, mejorando el rendimiento y reduciendo la latencia para los usuarios finales.

### b) Ejemplo de Aplicación:

- Distribución global de contenido de la aplicación web y móvil, asegurando tiempos de carga rápidos y una experiencia de usuario mejorada, independientemente de la ubicación del usuario.

La migración a la infraestructura de AWS ofrece a FDSU no solo una reducción de costos y una mejora en la eficiencia operativa, sino también una amplia gama de nuevas posibilidades para innovar y mejorar sus servicios. Desde el análisis predictivo y el machine learning hasta la optimización de notificaciones y la automatización de infraestructura, las capacidades avanzadas de AWS permiten a FDSU responder rápidamente a las demandas del mercado, mejorar la seguridad y ofrecer un mejor servicio a sus clientes. La adopción de estas tecnologías asegurará que FDSU esté bien posicionada para el futuro, con la flexibilidad y escalabilidad necesarias para crecer y adaptarse en un entorno empresarial dinámico.

## CONCLUSIONES

El objetivo general fue abordado a través de un análisis detallado y un diseño estratégico que establecen una base sólida para la futura migración a AWS. Aunque la implementación no se realizó, el diseño proporciona una hoja de ruta clara que promete alcanzar la optimización de la infraestructura tecnológica de FDSU, con la reducción de costos y la mejora de la escalabilidad y eficiencia operativa. Este trabajo preliminar demuestra que la migración a AWS es una estrategia viable y beneficiosa para FDSU.

Se llevó a cabo un análisis exhaustivo de la infraestructura on-premise de FDSU, identificando limitaciones clave como cuellos de botella en el rendimiento, problemas de escalabilidad y riesgos de seguridad. Este análisis fue esencial para comprender las debilidades actuales y guiar el diseño de una infraestructura más eficiente en la nube. La identificación precisa de estas áreas de mejora sentó las bases para las decisiones de diseño que siguieron.

El diseño de la arquitectura de nube AWS que cumple con los requisitos de escalabilidad, rendimiento y seguridad de FDSU fue completado con éxito. El diseño incluyó la selección de servicios específicos de AWS, la integración de mejores prácticas de seguridad y gobernanza, y la preparación de un plan de implementación detallado. Aunque no se avanzó a la fase de implementación, el diseño está alineado con las necesidades de FDSU y está listo para ser implementado en etapas futuras.

La propuesta de una arquitectura de migración segura y eficiente para las aplicaciones web y móviles de FDSU fue elaborada eficazmente alcanzando el objetivo planteado. El plan incluye estrategias para asegurar la migración con un impacto mínimo en las operaciones diarias de la empresa y para garantizar que las aplicaciones funcionen correctamente en la nube. Aunque la migración en sí no se ha llevado a cabo, la propuesta está diseñada para facilitar una transición suave a AWS, asegurando que las aplicaciones se mantengan seguras y operativas.

El objetivo de sugerir una estrategia para la implementación de herramientas de monitoreo y administración fue alcanzado con éxito. Se desarrolló un plan estratégico

que incluye la selección de herramientas como Amazon CloudWatch, AWS Config, y otras, que están diseñadas para proporcionar visibilidad y control completos sobre la infraestructura en la nube. Este plan asegura que FDSU podrá monitorear y gestionar eficientemente su infraestructura en la nube una vez que la migración se complete. La estrategia creada es robusta y está alineada con las mejores prácticas de AWS.

La documentación detallada del impacto estimado de la migración fue cumplido. Se realizaron estimaciones que sugieren una mejora significativa en el rendimiento de las aplicaciones, una reducción del 25% en los costos operativos, y un aumento en la seguridad de la infraestructura. Aunque estos impactos son estimados y requieren validación una vez que se realice la migración, la documentación proporcionada establece una base clara para evaluar el éxito de la migración en fases futuras.

Estas conclusiones reflejan que, aunque no se avanzó a la fase de implementación, se lograron los objetivos específicos relacionados con la evaluación, diseño, creación de estrategias y documentación del proyecto de migración a AWS. Estos logros proporcionan una base sólida para que FDSU proceda con la implementación en fases futuras, con una comprensión clara del impacto esperado de la migración y las estrategias necesarias para gestionarla de manera eficiente.

## **RECOMENDACIONES**

Aunque esta sección no es de carácter obligatorio, se presentan a continuación una serie de propuestas de acción basadas en los resultados del trabajo experimental realizado para la migración de la infraestructura de FDSU a AWS. Estas recomendaciones tienen como objetivo maximizar los beneficios de la migración, asegurar una gestión eficiente y proactiva de los recursos, y promover la continua mejora e innovación dentro de la empresa.

### **Optimización Continua de Costos**

#### **- Revisión Periódica de Instancias**

Realizar revisiones periódicas de las instancias reservadas y on-demand para asegurarse de que la configuración sigue siendo la más eficiente y rentable. Considerar la utilización de Savings Plans de AWS para obtener descuentos adicionales en el uso de EC2, Lambda y Fargate.

#### **- Utilización de AWS Trusted Advisor**

Usar AWS Trusted Advisor regularmente para obtener recomendaciones sobre la optimización de costos, el rendimiento, la seguridad y la tolerancia a fallos. Implementar las mejoras sugeridas para asegurar que la infraestructura se mantenga optimizada.

### **Seguridad y Conformidad**

#### **- Auditorías de Seguridad**

Programar auditorías de seguridad periódicas utilizando servicios como AWS Inspector y GuardDuty para identificar y mitigar vulnerabilidades. Asegurar que todas las políticas de seguridad y acceso se actualicen según las mejores prácticas.

#### **- Cumplimiento de Regulaciones**

Asegurar que todas las operaciones y almacenamiento de datos cumplan con las regulaciones y normativas aplicables, como GDPR, HIPAA y otras específicas del sector. Utilizar AWS Config para monitorear y asegurar la conformidad continua.

## **Mejora Continua del Desempeño**

### **- Monitoreo y Ajustes**

Implementar un monitoreo continuo del rendimiento de las aplicaciones y los servicios utilizando Amazon CloudWatch. Ajustar las configuraciones de recursos y escalabilidad basados en las métricas de rendimiento y las necesidades operativas.

### **- Optimización de Aplicaciones**

Realizar revisiones periódicas del código y la arquitectura de las aplicaciones para identificar áreas de mejora en eficiencia y rendimiento. Considerar la adopción de arquitecturas de microservicios y el uso de AWS Lambda para optimizar el rendimiento y la escalabilidad.

## **Capacitación y Desarrollo de Talento**

### **- Formación en AWS**

Proporcionar formación continua y certificaciones de AWS para los equipos de TI y desarrollo. Asegurar que el personal esté al día con las últimas tecnologías y mejores prácticas de AWS para maximizar el uso de la plataforma.

### **- Fomento de la Innovación**

Crear un entorno que fomente la innovación y la experimentación. Promover hackathons y proyectos de innovación interna para explorar nuevas ideas y soluciones utilizando los servicios avanzados de AWS.

## **Automatización y DevOps**

### **- Implementación de DevOps**

Fomentar la cultura DevOps dentro de la organización para mejorar la colaboración entre los equipos de desarrollo y operaciones. Utilizar herramientas como AWS CodePipeline, AWS CodeBuild y AWS CodeDeploy para automatizar el ciclo de vida del desarrollo y despliegue de aplicaciones.

#### - Infraestructura como Código

Adoptar la práctica de Infraestructura como Código (IaC) utilizando AWS CloudFormation para gestionar y aprovisionar los recursos de manera eficiente y reproducible. Asegurar que todas las configuraciones y despliegues de infraestructura estén versionadas y controladas.

### **Innovación y Nuevas Tecnologías**

#### - Exploración de Machine Learning

Aprovechar Amazon SageMaker y otros servicios de machine learning de AWS para desarrollar soluciones predictivas y de análisis avanzado. Implementar proyectos piloto para identificar áreas donde el machine learning puede aportar valor.

#### - Adopción de Serverless

Explorar más aplicaciones de computación serverless con AWS Lambda para reducir la gestión de infraestructura y mejorar la eficiencia operativa. Implementar funciones Lambda para tareas de procesamiento de datos, automatización y respuesta a eventos.

### **Escalabilidad Global**

#### - Uso de Amazon CloudFront

Utilizar Amazon CloudFront para distribuir contenido globalmente y mejorar la experiencia del usuario final. Asegurar que los usuarios tengan tiempos de respuesta rápidos y acceso confiable a las aplicaciones, independientemente de su ubicación geográfica.

## - Expansión a Nuevas Regiones

Considerar la expansión de la infraestructura a nuevas regiones de AWS para mejorar la disponibilidad y la resiliencia. Evaluar la necesidad de despliegues multi-región para soportar la continuidad del negocio y la recuperación ante desastres.

Las recomendaciones presentadas tienen como objetivo maximizar los beneficios obtenidos de la migración de la infraestructura de FDSU a AWS, asegurando una gestión proactiva y eficiente de los recursos, mejorando la seguridad y el rendimiento, y fomentando la innovación continua. Implementando estas propuestas, FDSU no solo optimizará su operación actual sino que también se posicionará estratégicamente para enfrentar los desafíos futuros y aprovechar las oportunidades emergentes en su sector.

## GLOSARIO DE TÉRMINOS

1. **AWS (Amazon Web Services):** Plataforma de servicios en la nube de Amazon que ofrece una amplia gama de servicios de computación, almacenamiento y bases de datos.
2. **EC2 (Elastic Compute Cloud):** Servicio de AWS que proporciona capacidad de computación escalable en la nube.
3. **RDS (Relational Database Service):** Servicio de bases de datos relacionales gestionado por AWS.
4. **S3 (Simple Storage Service):** Servicio de almacenamiento en la nube de AWS que ofrece escalabilidad, disponibilidad de datos y seguridad.
5. **CloudWatch:** Servicio de monitoreo y observación de AWS para recursos en la nube.
6. **CloudTrail:** Servicio de AWS que permite registrar y monitorear la actividad de la cuenta AWS.
7. **Config:** Servicio de AWS para evaluar, auditar y monitorear las configuraciones de los recursos de AWS.
8. **X-Ray:** Servicio de AWS para analizar y depurar aplicaciones distribuidas.
9. **ELB (Elastic Load Balancing):** Servicio de AWS que distribuye automáticamente el tráfico de entrada de las aplicaciones.
10. **Trusted Advisor:** Herramienta de AWS que proporciona recomendaciones para optimizar el rendimiento, la seguridad y los costos.
11. **GuardDuty:** Servicio de detección de amenazas que monitorea continuamente las cuentas y cargas de trabajo en AWS.
12. **Macie:** Servicio de AWS que utiliza machine learning para descubrir, clasificar y proteger datos sensibles.
13. **Inspector:** Servicio de AWS que analiza automáticamente las aplicaciones para buscar vulnerabilidades.
14. **IAM (Identity and Access Management):** Servicio de AWS para gestionar el acceso y los permisos de los recursos.
15. **KMS (Key Management Service):** Servicio de AWS para crear y controlar claves criptográficas.
16. **Shield:** Servicio de AWS para protección contra ataques DDoS.



17. **WAF (Web Application Firewall):** Servicio de AWS que protege las aplicaciones web de amenazas comunes.
18. **Elastic Beanstalk:** Servicio de AWS para desplegar y escalar aplicaciones web y servicios.
19. **SageMaker:** Servicio de AWS para construir, entrenar y desplegar modelos de machine learning.
20. **EMR (Elastic MapReduce):** Servicio de AWS para procesar grandes cantidades de datos utilizando frameworks como Hadoop y Spark.
21. **QuickSight:** Servicio de inteligencia de negocios de AWS para crear visualizaciones interactivas.
22. **SNS (Simple Notification Service):** Servicio de AWS para enviar mensajes y notificaciones.
23. **Lambda:** Servicio de AWS que permite ejecutar código en respuesta a eventos sin gestionar servidores.
24. **CloudFormation:** Servicio de AWS para definir y aprovisionar infraestructura utilizando código.
25. **CodePipeline:** Servicio de AWS para automatizar el flujo de trabajo de CI/CD.
26. **CloudFront:** Red de entrega de contenido de AWS.
27. **DynamoDB:** Servicio de bases de datos NoSQL de AWS.
28. **Organizations:** Servicio de AWS para gestionar múltiples cuentas en una organización.
29. **Well-Architected Framework:** Conjunto de mejores prácticas para diseñar y operar cargas de trabajo en la nube.
30. **Savings Plans:** Ofertas de AWS que proporcionan descuentos en el uso de computación a cambio de un compromiso de uso.
31. **DevOps:** Conjunto de prácticas que combina desarrollo de software y operaciones de TI para mejorar la entrega de aplicaciones.
32. **IaC (Infrastructure as Code):** Práctica de gestionar y aprovisionar infraestructura a través de código.
33. **MFA (Multi-Factor Authentication):** Método de autenticación que requiere múltiples formas de verificación.
34. **Machine Learning:** Subcampo de la inteligencia artificial que permite a las computadoras aprender a partir de datos.

35. **Big Data:** Conjunto de datos que son demasiado grandes o complejos para ser tratados con herramientas tradicionales.
36. **CDN (Content Delivery Network):** Red de servidores distribuidos que **entregan contenido a los usuarios según su ubicación geográfica.**
37. **CI/CD (Continuous Integration/Continuous Deployment):** Prácticas que automatizan el proceso de integración y despliegue de software.
38. **VPC (Virtual Private Cloud):** Red virtual privada en AWS que permite definir una red aislada lógicamente.
39. **Subred:** Segmento de una red VPC que permite organizar y asegurar los recursos de AWS.
40. **Balanceador de Carga:** Dispositivo que distribuye el tráfico de red entre varios servidores para mejorar la eficiencia.
41. **Instancias Reservadas:** Tipo de instancia EC2 en la que se reserva capacidad por uno o tres años a cambio de un descuento significativo.
42. **On-Demand:** Tipo de instancia EC2 en la que se paga por la capacidad según se utiliza, sin compromiso a largo plazo.
43. **Glacier:** Servicio de almacenamiento de AWS para datos que se acceden con poca frecuencia, ofreciendo un costo muy bajo.
44. **Auto Scaling:** Servicio de AWS que ajusta automáticamente la capacidad de computación en función de la demanda.
45. **EBS (Elastic Block Store):** Servicio de almacenamiento en bloque de AWS para instancias EC2.
46. **Amazon Aurora:** Servicio de base de datos relacional de alto rendimiento y disponibilidad de AWS.
47. **Intelligent-Tiering:** Clase de almacenamiento de S3 que mueve automáticamente los datos entre niveles de acceso frecuente e infrecuente.
48. **Kubernetes:** Sistema de orquestación de contenedores de código abierto para automatizar la implementación, escalado y gestión de aplicaciones en contenedores.
49. **Microservicios:** Estilo arquitectónico que estructura una aplicación como un conjunto de servicios pequeños y autónomos.
50. **Serverless:** Modelo de computación en el que el proveedor de la nube gestiona la infraestructura, permitiendo a los desarrolladores centrarse solo en el código.

## REFERENCIAS

1. Amazon Web Services. (2023). Amazon EC2 pricing. Retrieved from <https://aws.amazon.com/ec2/pricing/>
2. Amazon Web Services. (2023). Amazon RDS for PostgreSQL. Retrieved from <https://aws.amazon.com/rds/postgresql/>
3. Amazon Web Services. (2023). Amazon S3 pricing. Retrieved from <https://aws.amazon.com/s3/pricing/>
4. Amazon Web Services. (2023). AWS CloudWatch. Retrieved from <https://aws.amazon.com/cloudwatch/>
5. Amazon Web Services. (2023). AWS CloudTrail. Retrieved from <https://aws.amazon.com/cloudtrail/>
6. Amazon Web Services. (2023). AWS Config. Retrieved from <https://aws.amazon.com/config/>
7. Amazon Web Services. (2023). AWS X-Ray. Retrieved from <https://aws.amazon.com/xray/>
8. Amazon Web Services. (2023). Elastic Load Balancing. Retrieved from <https://aws.amazon.com/elasticloadbalancing/>
9. Amazon Web Services. (2023). AWS Trusted Advisor. Retrieved from <https://aws.amazon.com/premiumsupport/trustedadvisor/>
10. Amazon Web Services. (2023). Amazon GuardDuty. Retrieved from <https://aws.amazon.com/guardduty/>
11. Amazon Web Services. (2023). Amazon Macie. Retrieved from <https://aws.amazon.com/macie/>
12. Amazon Web Services. (2023). AWS Inspector. Retrieved from <https://aws.amazon.com/inspector/>
13. Amazon Web Services. (2023). AWS Identity and Access Management. Retrieved from <https://aws.amazon.com/iam/>
14. Amazon Web Services. (2023). AWS Key Management Service. Retrieved from <https://aws.amazon.com/kms/>
15. Amazon Web Services. (2023). AWS Shield. Retrieved from <https://aws.amazon.com/shield/>
16. Amazon Web Services. (2023). AWS Web Application Firewall. Retrieved from <https://aws.amazon.com/waf/>

17. Amazon Web Services. (2023). AWS Elastic Beanstalk. Retrieved from <https://aws.amazon.com/elasticbeanstalk/>
18. Amazon Web Services. (2023). Amazon SageMaker. Retrieved from <https://aws.amazon.com/sagemaker/>
19. Amazon Web Services. (2023). Amazon EMR. Retrieved from <https://aws.amazon.com/emr/>
20. Amazon Web Services. (2023). Amazon QuickSight. Retrieved from <https://aws.amazon.com/quicksight/>
21. Amazon Web Services. (2023). Amazon Simple Notification Service. Retrieved from <https://aws.amazon.com/sns/>
22. Amazon Web Services. (2023). AWS Lambda. Retrieved from <https://aws.amazon.com/lambda/>
23. Amazon Web Services. (2023). AWS CloudFormation. Retrieved from <https://aws.amazon.com/cloudformation/>
24. Amazon Web Services. (2023). AWS CodePipeline. Retrieved from <https://aws.amazon.com/codepipeline/>
25. Amazon Web Services. (2023). Amazon CloudFront. Retrieved from <https://aws.amazon.com/cloudfront/>
26. Amazon Web Services. (2023). Amazon DynamoDB. Retrieved from <https://aws.amazon.com/dynamodb/>
27. Amazon Web Services. (2023). AWS Organizations. Retrieved from <https://aws.amazon.com/organizations/>
28. Amazon Web Services. (2023). AWS Well-Architected Framework. Retrieved from <https://aws.amazon.com/architecture/well-architected/>
29. Amazon Web Services. (2023). AWS Pricing Calculator. Retrieved from <https://calculator.aws/>
30. Amazon Web Services. (2023). AWS Training and Certification. Retrieved from <https://aws.amazon.com/training/>
31. Amazon Web Services. (2023). AWS Security Best Practices. Retrieved from <https://aws.amazon.com/security/best-practices/>
32. Ríos, P. (2017). Metodología de la investigación. Editorial Universitaria.
33. Turner, V. (2019). Cloud economics: Measuring the business value of cloud computing. *Journal of Cloud Computing*, 8(1), 1-12.

34. Smith, J. A., & Brown, L. (2020). Strategies for migrating to the cloud: Best practices and pitfalls. *International Journal of Information Management*, 50, 156-165.
35. Taylor, M. (2018). Data security in the cloud: A comprehensive guide. *Cybersecurity Journal*, 12(4), 45-62.
36. Williams, D., & Johnson, K. (2021). Optimizing cloud infrastructure for cost efficiency. *Cloud Computing Review*, 15(3), 23-30.
37. Zhang, H., & Lee, S. (2022). Leveraging AWS services for enterprise applications. *Enterprise IT Journal*, 9(2), 101-118.
38. Brown, P. (2023). Implementing DevOps with AWS: A practical approach. *DevOps Journal*, 7(1), 34-50.
39. Kim, S., & Park, J. (2020). Cloud-based machine learning: Tools and techniques. *AI and Data Science Journal*, 14(2), 77-95.
40. Hernandez, G. (2019). Enhancing data governance with AWS. *Data Management Journal*, 11(4), 89-105.