Universidad Nacional

Sistemas de Estudios de Posgrado

Maestría en Administración de Tecnologías de Información

Énfasis en Administración de Proyectos

Metodología de implementación de aplicaciones de *software* en Amazon Web Services (AWS)

Miguel Alvarado Abarca

Heredia, Costa Rica, mayo, 2017

5 de mayo del año 2017

Universidad Nacional
Facultad de Ciencias Exactas y Naturales
Escuela de Informática
Posgrado en Gestión de la Tecnología de Información y Comunicación (ProGesTIC)

FORMULARIO DE DEPÓSITO LEGAL, AUTORIZACIÓN DE USO DE DERECHOS PATRIMONIALES DE AUTOR E INCORPORACIÓN A REPOSITORIOS INSTITUCIONALES DE INFORMACIÓN DE ACCESO PÚBLICO

La persona abajo firmante, en condición de estudiante de la maestría, **Miguel Alvarado Abarca** y autor del Trabajo final de graduación titulado: **Metodología de implementación de aplicaciones de software en Amazon Web Services (AWS)**, para optar al grado académico de Máster en: **Administración de Tecnología de la Información (MATI) con énfasis en Administración de Proyectos**, de conformidad con lo establecido en el documento de "Lineamientos generales para la realización del trabajo final de graduación" y demás normativa universitaria relacionada con estos trabajos de graduación, DECLARO BAJO FE DE JURAMENTO conociendo la responsabilidad civil, penal o administrativa en que podría incurrir al no decir la verdad, lo siguiente:

1. El documento, producto, obra audiovisual, software, resultado del trabajo final de graduación referido anteriormente es original, inédito y ha cumplido con todo el proceso de aprobación académico que confiere el grado académico postulado con esta obra.

2. El trabajo final de graduación referido anteriormente constituye una producción intelectual propia de la persona abajo firmante y a esta fecha no ha sido divulgado a terceros(as) de forma pública, por ningún medio de difusión impreso o digital.

3. Autorizo el depósito de un ejemplar en formato impreso y otro en formato digital (entregado en soporte de disco compacto), en la colección de trabajos finales de graduación del ProGesTIC de la Universidad Nacional, así como la realización de copias electrónicas adicionales para fines exclusivos de seguridad y conservación de la información.

4. En caso de que el trabajo final de graduación haya sido elaborado como obra en colaboración -bien se trate de obras en las que los autores(as) tienen el mismo grado de participación o aquellas en las que existe una persona autora principal y una o varias personas autoras secundarias-, todos(as) ellos(as) han contribuido intelectualmente en la elaboración del documento y en este acto, libero de responsabilidad a las autoridades del posgrado y a los funcionarios que custodian la

colección del ProGesTIC, en relación con el reconocimiento que se realiza respecto de los niveles de participación asignados por el propio autor del proyecto.

5. En caso de que el trabajo final de graduación haya sido elaborado como obras en colaboración (conforme a lo dispuesto en el punto 4), el autor abajo firmante designa a **Miguel Alvarado Abarca** como encargado(a) de recibir comunicaciones y representar con autoridad suficiente a los suscritos, en condición de agente autorizado(a) de los demás autores(as).

6. Reconozco que la colección de trabajos finales del ProGesTIC no emite criterios ni valoraciones académicas sobre lo planteado en el producto final del trabajo de graduación y autorizo a esta dependencia para que proceda a poner a disposición del público la obra en mención, a través de los espacios físicos o virtuales que se posea, así como a través del Repositorio Institucional; a partir del cual los usuarios de dichas plataformas puedan acceder al documento y hacer uso de este en el marco de los fines académicos, no lucrativos y de respeto a la integridad del contenido del mismo así como la mención del autor o poseedor de sus derechos.

7. Manifiesto que todos los datos de citas dentro de texto y sus respectivas referencias bibliográficas, así como las tablas y figuras (ilustraciones, fotografías, dibujos, mapas, esquemas u otros) tienen la fuente y el crédito debidamente identificados y se han respetado los derechos de autor.

8. Autorizo la licencia gratuita no exclusiva de los derechos patrimoniales de autor para reproducir, traducir, distribuir y poner a disposición pública en formato electrónico, el documento depositado, para fines académicos, no lucrativos y por plazo indefinido en favor de la Universidad Nacional, que incluye además los siguientes actos:

a. La publicación y reproducción íntegra de la obra o parte de esta, tanto por medios impresos como electrónicos, incluyendo Internet y cualquier otra tecnología conocida o por conocer.

b. La traducción a cualquier idioma o dialecto de la obra o parte de esta.

c. La adaptación de la obra a formatos de lectura, sonido, voz y cualquier otra representación o mecanismo técnico disponible, que posibilite su acceso para personas no videntes parcial o totalmente, o con alguna otra forma de capacidades especiales que les impida su acceso a la lectura convencional del proyecto.

c. La distribución y puesta a disposición de la obra al público, de tal forma que el público pueda tener acceso a ella desde el momento y lugar que cada quien elija, a través de los mecanismos físicos o electrónicos de que disponga.

d. Cualquier otra forma de utilización, proceso o sistema conocido o por conocerse que se relacione con las actividades y fines académicos a los

cuales se vincula la maestría, la colección de trabajos finales del ProGesTIC, la Escuela de Informática y la Universidad Nacional.

9. Reconozco que la colección de trabajos del ProGesTIC manifiesta actuar con diligencia para evitar la existencia en su sitio web de contenidos ilícitos y en caso de que tenga conocimiento efectivo de la existencia de infracciones a los derechos de propiedad intelectual, se reserva el derecho de proceder a bloquear el acceso durante el trámite del debido proceso para comprobar el incumplimiento y en caso de verificarse la falta, retirar definitivamente el acceso al proyecto depositado.

10. Acepto que la publicación y puesta a disposición del público del trabajo final de graduación, así como la presente autorización de uso de la obra, se regirá por la normativa institucional de la Universidad Nacional y la legislación de la República de Costa Rica. Adicionalmente, en caso de cualquier eventual diferencia de criterio o disputa futura, acepto que esta se dirimirá de acuerdo con los mecanismos de Resolución Alterna de Conflictos y la Jurisdicción Costarricense.

Autor: Miguel Alvarado Abarca

Firma: _____

Fecha de entrega: _____

Correo: alvarado.abarca@gmail.com

Índice general

Índice de figuras

Índice de cuadros

Índice de anexos

Resumen ejecutivo

Ante la constante creación e innovación de soluciones de software que utilizan los servicios de computación en nube, organizaciones, equipos de trabajo y profesionales en tecnologías de información; se encuentran ante el reto de proyectos de investigación, pruebas de concepto y capacitaciones para disminuir la curva de aprendizaje e incertidumbre de los procesos involucrados.

Por lo que el presente proyecto tiene como objetivo construir una metodología de implementación de aplicaciones de software utilizando el modelo de infraestructura como servicio de Amazon Web Services, metodología que se complementa con un plan de comunicaciones para la ejecución de las actividades involucradas, alineamiento de las actividades con las habilidades de TI requeridas, diagramas y plantillas de documentación.

Para el desarrollo del proyecto se realiza una investigación cualitativa, en la cual se exploran las áreas de infraestructura, seguridad, desarrollo de software, operación y monitoreo involucradas en el servicio en la nube de AWS. Además, se realiza un proceso de entrevistas con expertos en el tema, con el fin de obtener retroalimentación desde un enfoque práctico de las áreas previamente mencionadas.

Como producto final del proyecto, se obtiene una metodología estructurada como un conjunto de procesos y actividades, la cual define una guía y estandarización de los esfuerzos y elementos involucrados en la implementación de aplicaciones e infraestructura en AWS.

1. Capítulo I - El problema y su importancia

1.1. Antecedentes

Raven Software Solutions es una empresa de soluciones de tecnología información, fundada en el 2004, actualmente se encuentra localizada en Irving Texas y Jacksonville Florida, EUA (Raven, 2016).

La organización se encarga de proveer servicios de consultoría y desarrollo de aplicaciones en diversos sectores, en su cartera de servicios se incluye soluciones de comercio electrónico, aplicaciones empresariales, ingeniería de productos y desarrollo de *software*.

La misión de Raven Software Solutions consiste en: "*entender de manera detallada los requerimientos de los clientes y así proveer los adecuados y mejores recursos; para diseñar, desarrollar e implementar soluciones que permitan el crecimiento de las compañías*" (traducción propia).

Uno de los principales ejes de negocio de Raven Software Solutions, consiste en proveer a sus clientes, personal (recurso humano) especializado en diferentes áreas de tecnología de información, tales como: aseguramiento de la calidad, administración de sistemas, gestión de proyectos, administración de base de datos, servicios web, soporte de mesa de servicio, administración de redes y desarrollo de sistemas.

Adicionalmente, la empresa se enfoca en la creación de soluciones de reconocimiento de voz, respuesta de voz interactiva, integración de telefonía computacional y servicios de voz basados en web.

De acuerdo con el enfoque de Raven Software Solutions por incursionar en proyectos del área de *Cloud Computing*, surge el interés de la empresa en el proyecto, la cual se va a ver beneficiada con el producto final. Cabe resaltar que la información esencial para el desarrollo del proyecto reside en la documentación de modelo de infraestructura como servicio de la

computación en la nube y no específicamente de una unidad de negocio o departamento de la empresa.

1.1.1. Cloud Computing

Haciendo referencia propiamente al *Cloud Computing*, esta se ha convertido en una tecnología emergente y de rápido avance en el área de Tecnología de Información (TI), la cual brinda a las organizaciones la oportunidad de transformar sus modelos de negocio y obtener ventajas competitivas (Berman, Kesterson, Marshall, & Srivathsa, 2012).

Además, el *Cloud Computing* ha sido tema de interés en los amplios niveles de las organizaciones, desde los altos directivos hasta los usuarios finales (Salama & Shawish, 2014).

De acuerdo con El NIST (*US National Institute of Standards and Technology*) (2012) el *Cloud Computing* se define como "un modelo para habilitar de manera conveniente, un acceso por demanda de un conjunto compartido de recursos computacionales (redes, servidores, almacenamiento y servicios) que pueden ser rápidamente provisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de la nube".

A continuación, se detallan los principios de *Cloud Computing* (NIST, 2012):

- Servicio por demanda.
- Acceso global.
- Agrupamiento de recursos computacionales.
- Rapidez y elasticidad.
- Servicio controlado.

Existen tres modelos de servicios de *Cloud Computing*, los cuales se definen de la siguiente manera (Incorvaia, 2014):

- **Software como servicio**: modelo que provee acceso a *software* y sus funcionalidades de manera remota y mediante un servicio basado en la web. Este modelo permite a las organizaciones, acceder a funciones del negocio a un costo usualmente menor a un pago de licencias, además evita actividades de mantenimiento.

- **Plataforma como servicio**: plataforma computacional que permite la creación de aplicaciones web de manera rápida, fácil y sin la complejidad de compra y mantenimiento del software e infraestructura requerida.

- **Infraestructura como servicio**: modelo en el cual las organizaciones pueden asegurar hardware, almacenamiento, redes y otros servicios requeridos para realizar sus operaciones sin la necesidad de preocuparse de la compra o mantenimiento físico de equipo computacional.

El modelo de infraestructura como servicio, ha permitido a las organizaciones la creación de su propia infraestructura tecnológica en la nube bajo una modalidad de pago por uso (NTT Data, 2014).

La importancia del modelo de infraestructura como servicio reside en la factibilidad de construir aplicaciones de *software* robustas y de alta complejidad, las cuales pueden ser integradas con los servicios y productos internos de la organización o bien directamente con el cliente final, en el cual la organización tiene un control de los recursos computacionales utilizados (Gorelik, 2013).

Las principales áreas de tecnologías de información que deben ser consideradas por una organización ante la incorporación en un modelo de infraestructura como servicio son: hardware, redes, software y seguridad (Leimeister, Ried, Böhm, & Krcmar, 2010).

Según Gartner, Amazon Web Services es proveedor líder del modelo de infraestructura como servicio, superando a sus competidores próximos tales como Microsoft y Google. Para ello se evaluaron criterios de capacidad computacional, innovación en los servicios, agilidad y responsabilidad ante los cambios en el mercado (Gartner, 2015).

Amazon Web Services (2015) define su servicio como "una plataforma segura de servicios en la nube, que ofrece poder computacional, almacenamiento, entrega de contenido y otras funcionales para ayudar a la escalabilidad y crecimiento del negocio".

A continuación, se detallan los beneficios del uso de los servicios en la nube específicamente de Amazon Web Services (Sajee & Jinesh , 2014):

- Fácil uso.
- Económico.
- Flexibilidad.
- Confiable.
- Escalabilidad y alto rendimiento.
- Seguridad.

Actualmente, los servicios de AWS operan en 33 zonas de disponibilidad (centros de datos) en 12 regiones geográficas alrededor del mundo (AWS, 2016), logrando así tener 10 veces mayor capacidad computacional que la

sumatoria de la capacidad total de sus 14 competidores principales (Leong & Toombs & Gill, 2015).

Con base en la investigación de *451 Research Vendor Window*, en la cual participaron más de 1500 profesionales del área de tecnología de información y en la cual se evaluaron aspectos claves tales como nivel de adopción y rendimiento de los proveedores de servicios en la nube; Amazon Web Services se determina como líder en implementaciones de infraestructura como servicio, obteniendo un 57% del total de los consumidores considerados (451 Research, 2015).

Dada la naturaleza del proyecto, en el cual se va a investigar y desarrollar el conjunto de procesos y pasos requeridos al momento de implementar una aplicación de software en la nube, es importante mencionar que no se va realizar algún descubrimiento de diferencias o selección entre múltiples proveedores de infraestructura de computación en la nube, debido a que se está delimitando a Amazon Web Services como proveedor específico.

Esta delimitación se justifica con base en los intereses de la entidad patrocinadora del proyecto, además del continuo liderazgo que presenta Amazon Web Services como proveedor de capacidad computacional y servicios en la nube (Gartner, Magic Quadrant for Cloud Infrastructure as a Service, Worldwide, 2016).

1.2. Descripción y delimitación del problema

Las oportunidades a nivel técnico y de negocios que brindan los modelos de computación en la nube, organizaciones privadas y públicas, a nivel global, han incorporado en su estrategia el uso de estos servicios (451 Research , 2015).

La computación en la nube, al ser una tecnología emergente, implica una curva de aprendizaje tanto para la organización como para los recursos encargados de implementarla en un proyecto o servicio específico. Por tanto, se identifica la necesidad de crear proyectos de investigación, pruebas de concepto, capacitaciones o incluso contratar empresas o individuos con conocimiento especializado (Otieno & Njihia, 2014).

Específicamente, en el modelo de infraestructura como servicio, las organizaciones tienen mayor nivel de responsabilidad de los recursos computacionales utilizados, por lo tanto, existe un mayor nivel de complejidad en los procesos de implementación y operación de una aplicación de software. Complejidad que debe ser estimada por las organizaciones que desean innovar con este tipo de tecnología (Simorjay, 2016).

Por su parte, ante iniciativas de infraestructura como servicio utilizando la plataforma Amazon Web Services, se ha identificado que no hay una estandarización de las actividades requeridas en la implementación de una aplicación de software. A pesar que organizaciones, con la adquisición de conocimiento y lecciones aprendidas, han logrado adaptar mejores prácticas a sus procesos internos, estos no son de dominio público (Rowe & Sikes, 2006) (Jugdev, 2012).

El tener incertidumbre sobre cuáles son los procesos y las áreas involucradas al momento de implementar aplicaciones de software utilizando Amazon Web Services, implica, además, un nivel de riesgo que podría comprometer el éxito de los proyectos, por tanto, las organizaciones deben tomar la decisión de asumir el riesgo o no asumirlo (Attarzadeh, 2008).

Como consecuencia colateral a la ausencia de este tipo de estándar, se identifica los siguientes:

- Deficiente planeación de proyectos que involucran la implementación de aplicaciones en Amazon Web Services, debido a que no se tiene conocimiento previo del conjunto de actividades por realizar, roles y tipos de conocimientos que son requeridos por parte de los recursos involucrados; encadenando así un conjunto de dificultades en etapas posteriores (Laporte & Chevalier, 2016).
- Ante un panorama de la organización, programas y proyectos, se identifican consecuencias de aumento de los costos, tiempo de entrega o nivel de calidad, incluso podría implicar un cierre prematuro de proyectos u operaciones (Brantley, 2007) (Atkinson, 1999).

Por tanto, el problema de la investigación radica en la falta de una metodología, para estandarizar grupo de procesos y actividades que son requeridas ante la implementación de una aplicación de software en la plataforma de Amazon Web Services.

1.3. Justificación

Se identifica la oportunidad de construir una metodología que permita facilitar los procesos de implementación de aplicaciones de software en la plataforma de servicios de computación en la nube Amazon Web Services, además que permita resolver la problemática que actualmente se ha identificado.

1.3.1. Importancia

La principal motivación personal para el desarrollo de este proyecto, reside en un conjunto de retos encontrados en el ámbito laboral, en lo cual era necesario implementar una nueva solución de software basado en las tecnologías de computación en la nube, específicamente bajo el modelo de infraestructura como servicio. Para ese momento, en la organización era la

primera iniciativa de este tipo, por lo que se requirió un esfuerzo adicional de investigación y pruebas de concepto.

El haber contado en ese momento con una compilación de buenas prácticas o metodología que indicara cuales son las fases y actividades requeridas para este tipo de proyectos, hubiese disminuido la curva de aprendizaje técnico y organizacional, además de ventaja en procesos propios del desarrollo del software.

Con el desarrollo y finalización de este proyecto, se va a obtener en lo personal, un conocimiento de cada uno de los procesos, pasos, retos, riesgos y roles involucrados en el ciclo de vida de una implementación de *software* basado en tecnologías en la nuble y específicamente de los servicios de Amazon Web Services. Además de su integración con el ciclo de vida del desarrollo del *software* (*SDLC* por sus siglas en inglés).

Se identifica como producto final del proyecto, una metodología que detalla el conjunto de procesos y actividades requeridas en la implementación de aplicaciones de *software* basadas en el modelo de infraestructura como servicio del proveedor Amazon Web Services.

Dicha metodología está dirigida a organizaciones, cuyos proyectos se enfrentan al reto de implementar sus productos o servicios utilizando este tipo de tecnologías y servicios de computación en la nube, especialmente si la organización no cuenta con experiencia previa en este tipo de iniciativas.

A continuación, se detallan los beneficios que una organización, proyecto o servicio pueden obtener mediante el uso de esta nueva metodología:

- Identificación de las actividades requeridas para implementar un software que utiliza los servicios de infraestructura como servicio de Amazon Web Services (AWS).

- Identificación de los roles y responsabilidades que son requeridos en el proyecto.
- Plantillas de documentación de recursos computacionales requeridos, configuraciones, aspectos de seguridad y accesos de usuarios.
- Disminución de la curva de aprendizaje de iniciativas de implementación de software en AWS.
- Optimización de los procesos de la organización.
- Lenguaje común de términos, actividades y procesos con los interesados en la iniciativa de implementación de software en AWS.

1.3.2. Originalidad

La metodología obtenida con la finalización de este proyecto, va a servir de apoyo en el proceso de estandarización de actividades requeridas al momento de utilizar el modelo de infraestructura como servicio de AWS. Además, la metodología se visualiza de uso general para las organizaciones, ya que no está ligado a procesos, políticas o áreas de trabajo de una institución específica.

Una de las características del proyecto que es importante resaltar, es que mediante la creación y estandarización de conocimiento de tecnologías en la nube de AWS, se pretende promover en las organizaciones el uso de estos nuevos modelos y mitigar el riesgo asociado a proyectos de innovación en los cuales no se tiene experiencia previa.

En el producto final de este proyecto, se van a incorporar los conocimientos adquiridos de marcos de buenas prácticas en el área de servicios, procesos y proyectos; en los cuales se hace énfasis en elementos principales tales

como: comunicación, eficiente planeación, mejora continua, definición de roles y responsabilidades.

1.4. Objetivos generales y específicos

1.4.1. Objetivo general

Construir una metodología de implementación de aplicaciones de software en Amazon Web Services (AWS), mediante el desarrollo de una investigación, alineando los procesos requeridos en el modelo infraestructura como servicio y los servicios ofrecidos por AWS.

1.4.2. Objetivos específicos

1. Investigar los procesos de infraestructura, seguridad, implementación de software y monitoreo, mediante el desarrollo de una investigación, identificando cuáles son los componentes requeridos en la implementación de aplicaciones de software en la plataforma Amazon Web Services.

2. Identificar los roles y responsabilidades de tecnologías de información, mediante el análisis del modelo SFIA[1], creando una matriz de referencia con los procesos requeridos en la metodología de implementación de aplicaciones en AWS.

3. Identificar los departamentos y usuarios interesados, por medio del estudio de actividades requeridas en la implementación de aplicaciones en AWS, creando un plan de comunicación de los procesos establecidos en la metodología.

[1] Modelo de habilidades requeridas en los profesionales de Tecnologías de información.

4. Diseñar flujos de trabajo, mediante la identificación de las actividades requeridas en la implementación de aplicaciones en AWS, facilitando la comprensión de la metodología.

5. Crear plantillas de documentación, por medio del análisis de las actividades requeridas en la implementación de aplicaciones en AWS, facilitando el uso de la metodología.

2. Capítulo II – Marco Conceptual

2.1. Marco conceptual

En el presente marco conceptual se desarrolla la teoría de los procesos principales en un modelo en la nube de infraestructura como servicio, tales como lo son componentes de infraestructura para la creación de una red privada virtual, métodos de almacenamiento, herramientas que apoyan los procesos de implementación de software, servicios de monitoreo y mantenimiento, además de consideraciones de seguridad y control de acceso de usuarios y aplicaciones.

2.1.1. Infraestructura

2.1.1.1. Red privada en la nube (VPC)

La nube virtual privada (Virtual Private Cloud) es un servicio que permite la capacidad de provisionar de manera privada, aislada y controlada, recursos computacionales de AWS dentro de una red virtual. A continuación, se detallan los componentes requeridos en la creación de una VPC (Fortinet, 2015) (Sophos, 2014).

Los componentes iniciales de una VPC, se denominan tabla de direccionamiento (Route Tables) y subred (Subnet), los cuales indican el rango de IP´s que se encuentran disponibles en la red privada, además de las reglas de direccionamiento del tráfico dentro de la red. Existe una clasificación del tipo de subred, se define como subred publica aquella cuyo tráfico es dirigido por medio de una entrada de internet; se define como subred privada aquella que tiene comunicación únicamente con la red privada.

Para habilitar la comunicación de tráfico entre los recursos en la nube y una red interna corporativa, el servicio VPC cuenta con los componentes de entrada de cliente (Customer Gateway) y entrada virtual privada (Virtual

Private Gateway), los cuales actúan como receptor y emisor respectivamente, del tráfico enviado. Los anteriores, deben estar asociados a una red virtual privada (VPN), la cual se detalla en la sección de seguridad del presente documento.

Para el escenario en el cual es requerido que los servicios/aplicaciones de software en la nube sean accedidos por los usuarios mediante un dominio público, existen dos elementos principales que deben ser configurados. La creación de una dirección elástica (Elastic IP) permite crear un dominio público que puede ser accedido por medio de internet y que permite re direccionamiento del tráfico a los recursos en la nube de AWS. Este re direccionamiento se habilita mediante la creación de un NAT (Network Address Translation) y una entrada de internet (Internet Gateway), los cuales permiten la comunicación entre tráfico de internet público con la subred privada y sus respectivos recursos computacionales.

2.1.1.2. Elastic Cloud Computing (EC2)

Computación en la nube elástica (Elastic Cloud Computing, también conocido como EC2) es un servicio web que permite provisionar de manera flexible y escalable recursos computacionales, de los cuales el cliente de la nube tiene un control total. EC2 permite la creación de máquinas (servidores) virtuales denominadas instancias, las cuales pueden ser provisionadas con diferentes especificaciones computacionales y distribuciones de sistemas operativos. (Siegel & Gibbons, 2008) (Mohamed, 2013)

Existen diferentes tipos de instancias con base en las necesidades computacionales requeridas por el software o servicio, en términos de memoria, almacenamiento y procesamiento computacional (CPU). A continuación, se detallan las categorías de instancias que actualmente se encuentran disponibles (AWS, Tipo de instancias de Amazon EC2):

- Micro instancias.
- Propósito general.
- Memoria optimizada.
- Almacenamiento optimizado.
- Computación acelerada.
- Procesamiento optimizado.

En el momento que una instancia es creada, es necesario asociarla a diferentes recursos (previamente creados en la red privada) tales como sub-red, grupos de seguridad, almacenamiento y rol de acceso; cada uno de estos recursos se encuentra detallado en el presente documento. Es posible gestionar cada uno de los recursos de EC2 por medio de un modelo de etiquetas, las cuales permiten categorizar servicios, ambientes de desarrollo o módulos, con el fin de que estos puedan ser monitoreados o utilizados por otros servicios de manera separada, inclusive puede ser utilizados para administrar los costos de los recursos utilizados en la nube (AWS, Amazon Elastic Compute Cloud: User Guide for Linux Instances, 2016).

Con base en las necesidades de los servicios de tecnologías de información y densidad de tráfico de solicitudes de los diferentes recursos utilizados, EC2 provee servicios de balanceo de cargas (Elastic Load Balancer) y escalabilidad automatizada (AutoScaling) que permiten mayor disponibilidad de los servicios ofrecidos, además de una escalabilidad en tiempo real con base a la demanda. (Badwan, Tawfiq, Sleit, & Misk, 2013) (Tsz Lai, Trancong, & Goh, 2011)

2.1.1.3. Amazon Machine Images (AMI)

Amazon Machine Image (AMI) consiste en una plantilla de una máquina virtual en la cual se encuentra configurada de manera previa el sistema operativo, datos y aplicaciones de software. Cada una de estas plantillas puede ser configurada de manera personalizada con base a las necesidades de los servicios ofrecidos. Las AMI´s tienen como objetivo facilitar y agilizar el proceso de aprovisionamiento de nuevos recursos y ambientes computacionales en AWS. Amazon Web Services provee plantillas de manera pública para que puedan ser utilizadas por los usuarios, las cuales cuentan con servicios comunes tales como servidores de aplicaciones, aplicaciones web y base de datos, además de distribuciones de sistemas operativos. Las imágenes que son creadas por los usuarios en una red virtual privada también puede ser compartidas con otras cuentas, ambientes de desarrollo o de igual manera publicarla para cualquier usuario de la nube de AWS. (Balduzzi & Zaddach, 2012) (Bugie, Nürnberger, & Thomas, 2011)

El identificador de una AMI es uno de los principales parámetros para crear un servidor virtual (EC2), el cual además puede tener distintas configuraciones a nivel de capacidad de almacenamiento, grupos de seguridad, sub-red virtual y tipo de instancia EC2. Es posible crear N instancias EC2 basadas en la misma plantilla. (AWS, Amazon Elastic Compute Cloud: User Guide for Linux Instances, 2016)

2.1.1.4. Almacenamiento

A continuación, se detallan los principales métodos de almacenamiento de información que pueden ser utilizados en la infraestructura de Amazon Web Services.

2.1.1.4.1. Simple Storage Service (S3)

Amazon S3 (Simple Storage Service) es un servicio de almacenamiento de datos en la nube, los cuales pueden ser accedidos desde una infraestructura virtual privada, red corporativa o internet en general. S3 ofrece un servicio de alta redundancia, disponibilidad y replicación de los archivos almacenados, además el volumen de datos que se pueden almacenar es ilimitado. Sin embargo, se tiene límite para archivos individuales de 5 Terabytes.

S3 simula un sistema de archivos en el cual es posible listar, agregar, mover y eliminar los archivos, cada uno de estos archivos son almacenados como un objeto y estos objetos se encuentran agrupados es estructura denominadas "Buckets". El acceso y niveles autorización de cada uno los "Buckets" se encuentra determinados por las políticas de roles y usuarios definidos en IAM, además de las listas de control de acceso (definidas en la sección de seguridad del presente documento). (Brantner, Florescu, Graf, Kossmann, & Kraska, 2008) (Garfinkel, An Evaluation of Amazon's Grid Computing Services: EC2, S3, and SQS, 2007) (Garfinkel, commodity grid computing with Amazon´s S3 and EC2, 2007)

A continuación, se detallan las diferentes opciones de almacenamiento de S3 (AWS, Tipos de almacenamiento de Amazon S3, 2016):

- S3 estándar: Recomendado para archivos que deben ser accedidos frecuentemente y con disponibilidad inmediata.
- S3 Acceso poco frecuente: Recomendado para archivos deben ser accedidos con poca frecuencia, pero en caso de ser requeridos su tiempo de obtención debe ser mínimo. A diferencia del S3 estándar, este servicio de almacenamiento es más económico, sin embargo

existe una penalización si un porcentaje de los archivos almacenados son accedidos periódicamente.

- Glacier: Servicio de almacenamiento de datos con proyección largo plazo e infrecuente acceso. Es recomendado cuando el tiempo de recuperación de los archivos no es una prioridad, ya que es requerido un lapso 3 a 5 horas para un archivo especifico.

2.1.1.4.2. Elastic Block Storage (EBS)

Elastic Block Storage (EBS) es un volumen de almacenamiento a nivel de bloques, los cuales pueden ser asociados los a servidores virtuales (EC2) como discos de almacenamiento persistente y ser utilizados como sistema de archivo local. Cada uno de estos volúmenes posee un ciclo de vida separado de la instancia virtual por lo que pueden ser reutilizados en múltiples instancias. Sin embargo, existe la restricción que únicamente puede estar adjuntado a una instancia a la vez. Este tipo de almacenamiento es recomendado cuando se maneja información que cambia frecuentemente y que con persistencia de largo plazo. (Cloudera, 2016) (Sysfore Technologies, 2014) (Baron, 2010)

2.1.1.5. Base de datos

2.1.1.5.1. Servicio de base de datos relacional (RDS)

Relational DataBase Service (RDS) es un servicio web que permite la creación de una base de datos relacional en la nube, el cual facilita la instalación y operación de la base de datos. Dado a que está basado en la plataforma Elástica Cloud Computing (EC2), es posible seleccionar las capacidades de memoria, almacenamiento y rendimiento de lectura/escritura; con base a los requerimientos. (Sakhi, 2012) (Le Goaller, Conde, & Langha, 2013)

A continuación, se detallan unas de las principales características de este modelo de base de datos (Michel, 2010) (AWS, Amazon Relational Database Service User Guide, 2014):

- Permite una alta disponibilidad de servicio, debido a su replicación automática en diferentes zonas de disponibilidad.
- Fácil escalabilidad de los recursos computacionales.
- Automatización de actualización de versiones, copias de seguridad y recuperación de datos en caso de fallo.
- Soporta los siguientes motores de base de datos: mySQL, mariaDB, postgreSQL, Oracle y sqlServer

Algunas de las funciones adicionales del RDS, es la capacidad de encriptación de la base datos y copias de seguridad mediante "snapshots", las cuales se encuentran detalladas respectivamente en las secciones de encriptación, además de monitoreo y mantenimiento de este documento.

2.1.1.5.2. Aurora RDS

Amazon Aurora es un servicio basado en el modelo de base de datos RDS y compatible con el motor mySQL, el cual dado su arquitectura que permite tener un mayor rendimiento que las instancias RDS. Aurora provee un agrupamiento de instancias de base de datos la cuales van a dar soporte en conjunto al procesamiento de solicitudes, consiste en una instancia principal que se encarga de trabajos de lectura y escritura, además es posible agregar una o más instancias de replica que brindan apoyo en operaciones de lectura únicamente. De igual manera existe otro agrupamiento a nivel de volúmenes de almacenamiento los cuales se encuentran distribuidos en múltiples zonas de disponibilidad. Una de las principales características de aurora es su recuperación ante eventuales errores, en el cual su modelo de replicación y

alta disponibilidad permite que la detección y solución de errores no interrumpa en el procesamiento de solicitudes. (Associates Apps, 2015) (Littlefield, 2015)

2.1.1.5.3. DynamoDB

DynamoDB es un servicio de base datos no relacional, es cual se caracteriza por su rapidez de procesamiento, alta disponibilidad de servicio, almacenamiento ilimitado y fácil administración. Los principales parámetros al momento de utilizar una instancia de DynamoDB consisten en la capacidad de almacenamiento y rendimiento de procesamiento, para el caso de capacidad de almacenamiento el servicio brinda aprovisionamiento automático con base en el aumento de la cantidad de datos almacenados; con respecto a los valores de rendimiento, estos pueden ser modificados en tiempo de ejecución (sin afectar la disponibilidad o tiempos de respuesta de la base de datos) de acuerdo con los requerimientos, inclusive puede ser automatizado con base en el tráfico de solicitudes. (Bugiotti & Cabibbo, 2013) (Arcus Global, 2014) (Jafar, 2014)

2.1.1.5.4. Base de datos basadas en EC2

Este servicio de base de datos en la nube, se asimila al modelo tradicional de sistemas de base de datos en infraestructura local, en el cual es necesario realizar actividades manuales de configuración e instalación del motor de base de datos requerido. La arquitectura de servidores virtuales EC2 es la que permite la creación de este tipo de instancias de base de datos. Por lo tanto, para determinar el rendimiento, es requerido seleccionar el tipo de instancia EC2 a utilizar y capacidad de almacenamiento.

A diferencia del servicio de base de datos RDS, en este escenario es posible provisionar mayor variedad de motores de bases datos, ya que es posible que cada uno de los proveedores del software publiquen una plantilla (AMI)

de la aplicación, para que sea utilizada por cualquier usuario. Es necesario considerar al momento de utilizar este servicio, que los procesos de copia de seguridad, replicación, recuperación de datos, escalabilidad y optimización en general; deben ejecutarse de manera personalizada. Se recomienda este tipo de base de datos, cuando es requerido un control administrativo total a nivel de sistema operativo y de aplicación de software. (MySQL, 2009) (Arpitha, 2016)

2.1.2. Seguridad

En la presente sección se va a detallar los principales componentes de seguridad que deben ser configurados en la creación de una nueva infraestructura en la nube de AWS, además de los mecanismos para la gestión de usuarios y roles; y como pueden acceder a los diferentes servicios en la nube.

2.1.2.1. Red Virtual Privada (VPN)

Uno de los principales componentes de seguridad de la nube virtual privada (VPC) en AWS y parte de las actividades iniciales en proyectos de infraestructura en AWS, consiste en la creación de una red virtual privada (VPN), la cual permite crear uno o más canales privados para transferir información de manera segura entre la red privada corporativo (Centro de datos) y la nube virtual privada (VPC) de AWS. Este proceso se logra mediante la configuración de los elementos entrada virtual privada (Virtual Private Gateway) y entrada de cliente (Customer Gateway), los cuales se encuentran detallados en la sección de VPC del presente documento. (Detmer, 2015) (AWS, Amazon Virtual Private Cloud Network Administrator Guide, 2016) (AWS, Amazon Virtual Private Cloud User Guide, 2016)

Existen múltiples opciones para la configuración de una VPN en AWS:

- VPN mediante hardware: Consiste en la configuración del protocolo IPsec mediante el uso de un dispositivo físico de VPN dentro de la red interna corporativa.

- Conexión directa: Consiste en una conexión dedicada (física) desde la red interna corporativa y el centro de datos de AWS.

- VPN CloudHub: Esta opción permite configurar múltiples conexiones de redes internas corporativas con diferentes localidades con la nube virtual privada de AWS.

- VPN mediante software: Consiste en la configuración de una VPN mediante software, la cual se encuentra configurado dentro la red interna corporativa y es integrada con la nube virtual privada de AWS.

Para efectos de la metodología de implementación de aplicaciones en la nube que se va a desarrollar en este proyecto, se debe considerar el reto que podría implicar la creación una de VPN con la nube privada de AWS, esto debido a que dependiendo de la organización en la cual se estaría implementando, es necesario el trabajo en conjunto y comunicación entre el departamento de desarrollo con el departamento de infraestructura de la organización.

2.1.2.2. Acceso de usuarios y aplicaciones

2.1.2.2.1. Identity and Access Management (IAM)

La creación de usuarios acceso es uno de los primeros pasos que se debe realizar para utilizar la infraestructura de AWS, el cual es posible mediante el servicio IAM.

Amazon Identity and Access Management (IAM) es el servicio que gestiona el acceso por parte de usuarios y aplicaciones a los recursos computacionales de AWS, es posible la creación de usuarios individuales, grupos de usuarios, roles y políticas. Las políticas consisten en un conjunto de reglas que indican los recursos y tipos de operaciones que se autorizan a ejecutar. Para el caso de los roles estos se diferencia a los usuarios, en que los roles pueden ser asociados a los recursos que son creados y que no es necesario el uso de identificadores únicos o contraseñas. Cada uno de los

servicios de AWS que van a ser utilizados, deben estar asociado a un rol o un usuario con sus respectivas políticas de autorización. (Rackspace, 2016) (AWS, AWS Identity and Access Management User Guide, 2016)

2.1.2.2.2. Acceso y autorización

Existen tres opciones principales en la cuales los usuarios o aplicaciones de software pueden acceder y hacer uso de los recursos computacionales en la nube de AWS, mediante la interface web de AWS, mediante línea de comando y paquetes de desarrollo; o bien ingresando a los servidores virtuales EC2. Cada una de estas opciones se detalla a continuación.

Una vez que los usuarios hayan sido creados mediante el módulo de IAM, es posible el ingreso del equipo de trabajo a la interface web de AWS, la cual es denominada consola de AWS, en el cual el usuario puede crear y configurar los diferentes servicios en la nube de los cuales tenga autorización. Para lograr este acceso es necesaria la creación inicial de contraseña para los usuarios específicos, además es requerido proveer la dirección web única de la cuenta/ambiente de AWS previamente creado.

Para el caso de obtener acceso e integración de aplicaciones o usuarios a los servicios de AWS, mediante la interface de línea de comando o paquetes de desarrollo (SDK´s) de AWS, es necesario definir las llaves de acceso (Access key y Password Access Key) los cuales están asociados de manera única a los usuarios IAM. En el escenario que se utilice roles de autorización propiamente en los servidores virtuales (EC2), no es necesario definir usuarios o contraseñas, ya que de manera predeterminada el servidor identifica a que servicios se tiene autorización.

Para obtener acceso directo a los servidores virtuales (EC2) y su sistema de archivos (File System) de la infraestructura en la nube de AWS, es requerido crear una conexión SSH desde el ambiente local o red interna corporativa,

conexión que debe tener como parámetros un usuario previamente definido dentro del EC2 y la ruta del archivo que contiene la llave privada de autorización a ese servidor virtual específico. (Trinimbus, 2014) (MathWorks, 2014) (Wowza, 2016)

Con respecto al proceso de creación de una nueva aplicación de software en la nube, es importante definir roles y niveles de acceso en los cuales los usuarios interesados tengan autorización a cada uno de los componentes en los cuales deben tener interacción.

2.1.2.3. Grupos de seguridad

Los grupos de seguridad en la infraestructura computacional de AWS, se definen como la capa se seguridad que controla tráfico de entrada y salida de los servidores virtuales EC2 (Firewall). Estos grupos de seguridad deben ser asociados directamente como parámetro en la creación de nuevas instancias virtuales.

En la creación de un nuevo grupo de seguridad, por defecto todo el tráfico está restringido, por lo que se requiere definir reglas de entrada y salida del tipo de tráfico esperado. Para cada una de las reglas se debe especificar el tipo de protocolo de internet (TCP, UDP, ICMP), el puerto o rango de puertos permitidos, además el recurso de origen, este último puede ser la dirección IP especifica de una instancia EC2, un rango de direcciones IP o bien el identificador de otro grupo de seguridad.

Existe la flexibilidad de modificar las reglas de los grupos de seguridad y están van a surgir efecto en tiempo real en las instancias EC2 hayan sido creadas previamente y que estén asociadas a este grupo. Sin embargo, por otro lado, no se pueden eliminar o agregar grupos de seguridad en una instancia que haya sido inicializada. (Kiran, Shetty, & Hong, 2016) (Micro, 2013)

En las fases de planeación y diseño de nueva aplicación de software en AWS, es de vital importancia considerar cuales van a ser las reglas y grupos de seguridad que deben ser asignados a cada uno de los componentes y capas de la aplicación, ya que estos representan el flujo y servicios se van a comunicar.

2.1.2.4. Lista de acceso de red (ACL)

Amazon Access Control List (ACL) consiste en una capa adicional de seguridad del tráfico de entrada y salida en una red virtual privada, con la diferencia que los grupos de seguridad, operan a nivel de subred y no a nivel instancia virtual (EC2). De manera predetermina en los ACL, todo el tráfico de entrada o salida se encuentra denegado, por lo que es requerido definir reglas con la información de tipo de protocolo, rango de puertos, destino u origen, además si la regla es para permitir o denegar tráfico. (Citrix, 2013) (Overbond, 2015)

2.1.2.5. Cifrado de información

La seguridad de los datos almacenados en la nube, es una constante preocupación de las organizaciones que quieren hacer uso de la infraestructura de AWS, además debe existir un alineamiento de las políticas de seguridad de la organización con la arquitectura de los servicios desarrollados o que se pretenden desarrollar. Para facilitar estos procesos, AWS provee el servicio KMS.

Amazon Key Management Service (KMS) es un servicio en la nube que permite la gestión de llaves utilizadas para la encriptación y descifrado de información, el cual se encuentra integrado con múltiples servicios de AWS. A continuación se detalla las consideraciones de encriptación para los principales servicios de almacenamiento de AWS: (Hao, 2014) (Wynkoop,

2015) (Pragmatic) (AWS, AWS Key Management Service Developer Guide, 2016)

- S3: Es posible la protección de información que es almacenada en el servicio en la nube S3, mediante métodos de cifrado por el lado del cliente o bien por el lado del servidor. El enfoque de protección por el lado del cliente, consiste en procesos personalizados para cifrar la información previamente de que sea enviada a la nube y almacenada en S3. Por otro lado, el cifrado por el lado del servidor consiste en funcionalidades ya definidos en S3 que permiten que los datos sean automáticamente cifrados una vez que estos son cargados.

- EBS: Para el caso de los volúmenes de almacenamiento EBS, es posible la encriptación de los datos que se encuentran almacenados y también las copias de seguridad que sean creados con base en el volumen. En el proceso de creación del mismo volumen o bien de la instancia virtual EC2 es necesario la selección si el volumen deber ser cifrado o no.

- RDS: Para todos los motores de bases de datos disponibles en la tecnología RDS, también existe la opción de cifrado a nivel de disco, el cual mediante las funcionales de RDS únicamente es necesario la selección de la llave KMS que se desea utilizar.

Es importante considerar en el proceso de arquitectura del servicio en la nube, si existen componentes que requieren la integración de los servicios de KMS, además de si es necesario la creación de módulos personalizados para la gestión del cifrado de la información.

2.1.3. Implementación de Software

En la presente sección se detalla las diferentes herramientas y servicios en la nube de AWS que están enfocados para facilitar los procesos de desarrollo software y operación de los servicios.

2.1.3.1. Interface de línea de comandos (CLI)

Amazon Command line interface (CLI) es una herramienta que permite gestionar los servicios en la nube de AWS mediante línea de comandos, permitiendo un fácil acceso, automatización y control de los servicios utilizados, en la fase de desarrollo y operación del producto en la nube. (Amorin, NH, & AlAuf, 2015) (AWS, AWS Command Line Interface User Guide, 2016)

El nivel de acceso y tareas que son autorizadas de ejecutar con la herramienta, deben estar determinados por medio de los usuarios y roles definidos en el módulo de AWS IAM (Identity and Acesss management).

En caso de que el equipo de desarrollo del producto, este incursionando en el uso de la infraestructura de AWS y no tenga conocimiento previo de esta herramienta, es de gran importancia capacitarse en el uso de la misma, además de analizar si es requerido integrarla en el diseño del producto que se desea realizar.

2.1.3.2. Paquetes de desarrollo de software (SDK)

Una de las principales decisiones para migrar o crear aplicaciones de software bajo la infraestructura en la nube de AWS, consiste en verificar si existe una integración con las tecnologías, lenguajes de programación y ambiente de desarrollo que actualmente se trabajan en la organización o bien que se pretenden utilizar.

Actualmente AWS ofrece paquetes de desarrollo de software (Software Development kit) para las siguientes plataformas: Java, Android, JavaScript, IOS, .NET, Node,js, PHP, Python, Ruby, GO y C++. Permitiendo una integración directamente del software/procesos de la organización con los servicios de AWS. (AWS, Tools for Amazon Web Services, 2016)

Es importante resaltar que existe una amplia documentación técnica de cada uno de estos paquetes de desarrollo, por lo que es posible para los equipos de trabajo sin experiencia previa en la nube de AWS, disminuir su curva de aprendizaje.

2.1.3.3. AWS CodeCommit

Amazon CodeCommit es un servicio control de versiones en la nube que permite a los departamentos de Tecnologías de Información y desarrolladores crear repositorios del sistema GIT, comúnmente utilizados para gestionar los códigos fuentes o archivos binarios de las aplicaciones de software creadas. (Logic20/20, 2016)

Para la creación de un nuevo servicio o aplicación de software en la nube, no es estrictamente necesario hacer uso de CodeCommit y de igual manera se pueden utilizar los repositorios dentro de la infraestructura corporativa. Sin embargo, este servicio provee una fácil integración con otras herramientas encargadas del proceso automatizado de liberación de nuevas versiones y mejoras de software realizado; por lo que el uso de este servicio podría obtener ventajas.

2.1.4. Monitoreo y mantenimiento

2.1.4.1. CloudWatch

Amazon CloudWatch es un servicio que permite monitorear en tiempo real recursos computacionales de servidores virtuales (EC2), discos (EBS), instancias de base de datos (RDS) y balanceo de cargas; mediante la definición de métricas de los recursos utilizados (CPU, latencia, memoria), uso de red, operaciones de disco, entre otras. También es posible la creación de reglas personalizadas que se integren a los requerimientos del servicio que se quiere desarrollar. Cada uno de los resultados de estas métricas pueden ser representados de manera gráfica con sus respectivas estadísticas, o bien almacenadas en archivos de texto plano. (Park, Spetka, & Rasheed, 2013) (Kokkinos, Varvarigou, Kretsis, Soumplis, & Varvarigos, 2013) (Gandhi & Kumbharana, 2016)

Una de las principales ventajas de hacer uso de este servicio de monitoreo, consiste en llevar el término de elasticidad a un segundo nivel, en el cual es posible aumentar y disminuir los recursos de manera automática con base a los valores obtenidos en las métricas implementadas.

También es importante resaltar que una vez que sea desarrollo la aplicación de software y se encuentra en una fase de operación, los resultados de las métricas de monitoreo van apoyar los procesos de mejora continua e identificación de problemas.

2.1.4.2. Integraciones continuas

Debido a las necesidades del negocio y criticidad de las aplicaciones de software, organizaciones han tenido que automatizar los procesos de liberación de nuevas versiones de software y disminuir cualquier tarea

manual que conlleve a algún error no esperado, lo anterior se ha logrado mediante el apoyo de los procesos de integración continua de aplicaciones.

Martin Fowler define la integración continua como una práctica de desarrollo de software donde el equipo realiza integraciones constantes del trabajo y cada una de estas integraciones son verificadas mediante un proceso automático de implementación y prueba, con el fin de detectar la menor cantidad de errores posibles. (Fowler, 2007)

AWS provee los servicios en la nube de CodeDeploy y CodePipeline, los cuales en conjunto permiten a los usuarios definir sus flujos de integración continua con base a los respectivos requerimientos. Amazon CodeDeploy permite coordinar nuevas implementaciones de software y configuración en los servidores virtuales (EC2). Amazon CodePipeline tiene la capacidad para crear y automatizar grupos de trabajo, en los cuales se pueden incluir pruebas de integración de las nuevas versiones, además del ciclo de vida de liberación de software en múltiples ambientes de desarrollo. (Garnaat, 2016) (EntArchs, 2016)

2.1.4.3. Respaldos de información

Es necesario indicar en una metodología de implementaciones de aplicaciones en la nube, la importancia de definir procesos de respaldo de los datos que son utilizados en la infraestructura en la nube, esto con el objetivo de ser capaces de tener procesos de recuperación de información ante fallos no esperados, además tener la capacidad de duplicar datos en diferentes ambientes de desarrollo o servicios.

Para el caso de específico de los servicios de AWS, existe un concepto denominado “Snapshot”, el cual se considera con un respaldo o copia de un volumen de datos en un momento específico. La creación de una “Snapshot” está asociado a los volúmenes de almacenamiento EBS y se pueden realizar

ya sea de manera individual o bien si en encuentran asociados a un servidor virtual EC2, para este último el proceso de creación de plantillas de servidor virtuales (AMI´s) se encarga de realizar un "snapshot" de todos los EBS que tiene configurados.

Este proceso de respaldo también aplica para los servicios de base de datos en la nube RDS, los cuales a nivel macro, realizan una copia actual de toda la base de datos utilizada. El servicio provee de herramientas de automatización para realizar los "snapshots" con base en un horario específico, además de la posibilidad de definir reglas para restaurar las copias de seguridad. (Hogberg, 2012) (Digest, 2011) (AWS, Amazon Relational Database Service User Guide, 2014)

2.1.5. Roles de recursos Humanos

2.1.5.1. Modelo de habilidades (Roles y responsabilidades) de Tecnología de Información

Dado a uno de los objetivos específicos del proyecto, en el cual se van a analizar los roles y responsabilidades que son requeridos en cada uno de los procesos por definir en metodología, se toma como referencia el modelo de habilidades SFIA.

Skills Framework for the Information Age (SFIA) es un modelo establecido para identificar las habilidades de los profesionales de Tecnologías de información con base en los requerimientos del negocio. Este modelo permite un lenguaje común basado en las habilidades de TI, para mejorar la capacidad y planificación de los recursos; y gestión del rendimiento.

SFIA define un estándar de 97 habilidades de TI las cuales se encuentran en 7 categorías principales (Estrategia y arquitectura, Cambio en Negocio, Desarrollo e implementación de soluciones, Gestión del servicio, Gestión y aseguramiento de soporte, Comunicación con Cliente).

Además, cada una de las habilidades se establecen bajo un modelo de 7 niveles de responsabilidad (Seguir, asistir, aplicar, habilitar, asegurar/aconsejar, iniciar/influenciar e inspirar/definir estrategia), el cual contiene una definición detallada en términos de autonomía, complejidad, influencia y habilidades de negocio.

Actualmente SFIA se encuentra en su versión 6, la cual, de acuerdo a la madurez de sus versiones anteriores, experiencia de entidades con conocimiento en gestión de habilidades en ambientes corporativos y de educación, retroalimentaciones de las experiencias vividas por parte de los usuarios de SFIA; han incorporado cambios con base a las áreas de

habilidades digitales, seguridad cibernética, Big Data, Agile Cloud y gestión de la información.

SFIA es un modelo altamente aceptado a nivel internacional, cuenta con más de 2500 usuarios corporativos en más de 198 países, incluido el gobierno de Reino Unido. (SFIA, 2015) (Fundation, 2016)

3. Capítulo III - Marco metodológico

3.1. Alcance de la investigación

La presente es una investigación exploratoria con enfoque cualitativo, de acuerdo con Hernández, Fernández y Batista (2010) el enfoque cualitativo consiste en "comprender y profundizar los fenómenos, explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con el contexto". Por su parte, Burns y Grove (2001) define la investigación exploratoria como una "investigación realizada para obtener nuevas percepciones, descubrir nuevas ideas y/o incrementar el conocimiento de un fenómeno".

En este caso específico, se realiza una exploración de los procesos, componentes y servicios involucrados en la implementación de soluciones de software en la infraestructura en la nube de Amazon Web Services.

Se identificaron cinco áreas principales para iniciar la recolección información y que además van a permitir validar los resultados de la investigación. Se detallan a continuación:

- Componentes de arquitectura que deben ser utilizados para la creación de una infraestructura en la nube de AWS.
- Procesos de seguridad a considerar en la comunicación y protección de la información, por parte de los servicios o aplicaciones personalizadas.
- Herramientas que permite la implementación e integración de las aplicaciones de software con los servicios de AWS, además que faciliten las actividades en la fase desarrollo del software
- Componentes que permitan facilitar los procesos de monitoreo y mantenimiento en la fase de operación de las soluciones implementadas.

- Modelo de roles y responsabilidades de tecnologías de información que se encuentre alineado a las actividades involucradas de desarrollo e implementación de aplicaciones de software.

La documentación y conocimiento adquirido en el proceso de investigación se encuentra detallado en la sección de marco teórico del presente documento. Cada uno de los temas planteados, fueron sometidos a un proceso de análisis de las propuestas y definiciones de múltiples autores, con el objetivo de desarrollar una definición y aportes personales, con base en los objetivos y necesidades del proyecto.

3.2. Fuentes de información

3.2.1. Fuentes primarias

Se determina como fuente primaria de información, a profesionales a nivel global del área de tecnologías de información especialistas en infraestructura en la nube y tecnologías de Amazon Web Services. Hox y Boeije (2005) definen el concepto fuente primaria como "información que es recolectada para el problema específico de la investigación a mano, utilizando procedimientos que se adaptan al problema de investigación de la mejor manera".

La recolección de los datos se va a obtener mediante el método de entrevista semiestructurada, la cual se va aplicar a la muestra identificada en la presente investigación. Según Gill, Stewart, Treasure y Chadwick (2008) la entrevista semiestructura consiste en un "conjunto de preguntas principales que ayuda a definir las áreas a explorar, pero que también permite al entrevistador o el entrevistado divergir, con el objetivo de alcanzar una idea o responder en más detalle"

3.2.2. Fuentes secundarias

Se identifica como fuente secundaria, a los documentos en libros, publicaciones, artículos y documentos en línea, en los cuales múltiples autores presentan la teoría y conocimiento relevantes en esta investigación. Hernández, Fernández y Batista (2010) definen las fuentes secundarias como "compilaciones, resúmenes, y listados de referencias públicas en un área de conocimiento en particular, es decir reprocesan información de primera mano."

El método de recolección de información utilizado como fuente secundaria, consiste en la recopilación documental, la cual de acuerdo a Bowen (2009), se define como "un procedimiento sistemático para la revisión y evaluación de documentos de formato impreso o electrónico, los cuales deben ser analizados e interpretados para obtener entendimiento y desarrollar conocimiento empírico".

3.3. Población y Muestra

Se delimita como población de la investigación, al grupo de profesionales a nivel global del área de tecnologías de información, los cuales se determinan como especialistas en los servicios de infraestructura computacional en la nube y tecnologías de Amazon Web Services, además con experiencia a nivel de diseño y arquitectura de solución de software.

Con respecto a la muestra, esta se determina mediante muestro por oportunidad de un total de 7 personas con el perfil especificado en la población y a las cuales se les va a aplicar la entrevista definida en la presente investigación. El grupo seleccionado es especificado con respecto a las personas que estuvieron dispuestas a colaborar con la investigación, que contaban con la experticia deseada, además de disponibilidad a nivel tiempo.

Dörnyei (2007) define el concepto de muestro por oportunidad como "tipo de muestro no probabilistico o no aleatorio donde lo miembros de la población objetivo que cumplen ciertos criterios prácticos, tales como fácil accesibilidad, proximidad geografica, disponibilidad en un momento dado o la voluntad de participar; son incluidos para el proposito del estudio". Por su parte, Hernández, Fernández y Batista (2014) detalla que el muestro por conveniencia "están formados por los casos disponibles a los cuales tenemos acceso".

De acuerdo con Battaglia (2008) "el muestreo no probabilístico no intenta seleccionar una muestra no aleatoria de la población de interés".

3.4. Instrumentos de recolección de información

3.4.1. Entrevista

La aplicación de la entrevista semiestructurada tiene como objetivo contrarrestar la teoría encontrada en el proceso de recopilación documental del marco teórico.

La entrevista está compuesta por un total de 13 preguntas, las cuales se encuentran detalladas en el **apéndice 1** del presente documento.

4. Capítulo IV - Diagnóstico y análisis de resultados

Con respecto al diagnóstico y análisis de los datos obtenidos en el proceso de investigación, se detallan los principales hallazgos, a continuación:

4.1. Análisis de resultados

4.1.1. Componentes en la implementación de aplicaciones de software en AWS

Se identifica que en la infraestructura de la nube de AWS, existe la necesidad inicial de crear una nube virtual privada (VPC) la cual es la base de las subredes y componentes esenciales para hacer uso de los recursos computacionales. Recursos que se basan principalmente en la tecnología de computación elástica (EC2).

Para el caso de los servicios de almacenamiento de datos en la nube, se presentan las opciones de sistemas de objetos con almacenamiento infinito, volúmenes de almacenamiento a nivel de disco que pueden ser asociados a servidores virtuales, además de servicios propiamente de base de datos relacionales y no relacionales.

Cada uno de los servicios y recursos creados dentro de la nube privada se encuentran integrados a los procesos de autentificación por parte de usuarios y aplicaciones de software, permitiendo la gestión de múltiples niveles de acceso y modularidad que faciliten la integración y operación de los servicios de AWS utilizados.

Con respecto a la protección de las redes y recursos virtuales, se identifican capas de protección en la transferencia y autorización de flujo de datos. Además, se resalta la necesidad de establecer una conexión segura entre una infraestructura interna corporativa y la red virtual de AWS.

La gestión de llaves privadas para el cifrado de la información que se encuentra en la nube, genera un requerimiento para protocolos de protección directa de los datos y protección a nivel de disco de los recursos, asegurando la ilegibilidad en caso de manejo inapropiado de terceros.

Los procesos propiamente de la fase de desarrollo y operación se encuentran apoyados por gran variedad de paquetes de desarrollo (SDK) e interfaces de usuarios, además de herramientas que permiten la gestión de códigos fuentes e implementaciones de software.

Las soluciones que son implementadas en la nube de AWS, también pueden soportar procesos de implementación continua de aplicaciones de software, respaldos de seguridad automatizados, además de herramientas para monitorear con granularidad el comportamiento de los recursos computacionales que son utilizados.

Se resalta que la recolección de datos obtenida de cada uno de los procesos y sub procesos identificados en los objetivos específicos de este proyecto, nos brinda un flujo lógico de las actividades que son requeridas para poder crear o migrar soluciones de software utilizando la infraestructura en la nube de AWS.

4.1.2. Modelo de habilidades SFIA

La metodología SFIA revela la posibilidad asociar de manera detallada cuales son los perfiles y niveles de capacidad de los recursos humanos del área de tecnología de información, que son requeridos en cada uno de los procesos y actividades en la metodología que se va a obtener como resultado del presente proyecto.

4.2. Análisis de resultados de entrevista

A continuación, se detallan las categorías que se consideran principales en el listado de preguntas abiertas de la entrevista realizada y para cada una de ellas se presentan los vitales descubrimientos con respecto a los componentes de infraestructura, seguridad, desarrollo de software y monitoreo en la implementación de aplicaciones de software en AWS.

- Procedimiento para la creación de red privadas virtuales (VPC)
    - Se identifica la necesidad de realizar un análisis previo de las aplicaciones que son requeridas de soportar en la red privada, para poder realizar una distribución de los rangos de IP, representados en la tabla de direccionamiento y las sub-redes.
    - Se determina como buena práctica el diseño de sub-redes bajo un modelo de alta disponibilidad. Por tanto, se requiere utilizar múltiples zonas de disponibilidad.
    - Determinar la necesidad de utilizar sub-redes públicas y sub-redes privadas dentro de la red privada, con el fin de realizar la configuración y distribución óptima, sin comprometer las capas de seguridad.
    - Es necesario el involucramiento directo del equipo de infraestructura y equipo de dueños de la aplicación, en la toma de decisión del diseño de la red privada.
- Requerimiento de recursos computacionales (EC2) en la infraestructura virtual.
    - Se identifica la necesidad de identificar el tipo de recursos computacionales en las fases iniciales de diseño de la arquitectura,

con base en las necesidades de cada componente que va a ser utilizado. Sin embargo, es necesario el monitoreo constante en fases de pruebas de cargas y ambientes productivos para determinar si la medida debe ser re-evaluada.

- La innovación de la infraestructura en la nube conlleva la necesidad de evaluar servicios de activación automática de procesos, que no requieran uso de recursos computacionales, tales como AWS Lamda.

- Base de datos en la nube (relacionales y no relacionales), tecnología RDS.
  - Se identifica una tendencia del uso de la tecnología RDS para la base de datos en la nube de AWS, esto debido a su facilidad, alta disponibilidad y bajo nivel de mantenimiento.
  - Para propiamente uso de base de datos de software propietario, se idéntica el requerimiento de utilizar el modelo tradicional de configuración manual de los motores de base de datos en un servidor virtual, estos con base en la recomendaciones y especiaciones del vendedor.
- Tipos de red´s privada virtual (VPN) en la infraestructura en la nube.
  - La configuración de VPN por medio de hardware para la conexión con la red en la nube, se considera como tendencia a nivel corporativo. Sin embargo, para alta transferencia y comunicación la opción de Direct Connect (conexión física directa con AWS) se identifica como ideal.

- Para empresas pequeñas y con poco presupuesto el uso de VPN por medio de software se considera como óptima.

- Gestión de usuarios y autorizaciones (IAM).
    - Se idéntica una alta integración de los servicios ofrecidos por AWS IAM para la creación de roles y accesos, con herramientas establecidas a nivel corporativo para la autorización y monitoreo de los servicios en la nube. Software como SAML, SAMBA, Okta and Ping-Identity.

- Autorización de tráfico de datos en recursos y redes virtuales (Niveles de seguridad)
    - Se identifica gran aceptación de los grupos de seguridad y lista de acceso para determinar las capas de seguridad de la red, tanto a nivel de recursos virtuales y a nivel de tráfico de red.
    - Para los casos en el cual se define sub-redes públicas dentro de red en la nube, se considera como buena práctica la definición mínima y controlada de los puertos de tráfico de entrada.
    - Se recomienda la definición de un proceso robusto para la modificación de grupos de seguridad, para mitigar riesgos de seguridad.

- Encriptado de datos para la utilización en la infraestructura en la nube.
    - El uso del servicio de KMS para la gestión de llave privadas, se identifica como primordial en la información recolectada; Principalmente mediante el proceso automático de encriptación de los servicios de almacenamiento ofrecidos por AWS.

    - Se identifica como buena práctica la encriptación automática a nivel de disco de los volúmenes de datos y base datos RDS.

- Software de versión de control de código

    - Se identifica alta aceptación por parte de los servicios de versionamiento por AWS. Sin embargo, para los datos recolectados se utilizan repositorios privados y desligados de la infraestructura de AWS.

- Monitoreo de los recursos computacionales en AWS.

    - Se identifica el servicio CloudWatch como el más recomendado para el monitoreo de los recursos en la infraestructura de AWS.

5. Capítulo V – Solución del problema

5.1. Desarrollo de la solución

5.1.1. Introducción a la metodología

La presente metodología se define como un conjunto de procesos y actividades que guían al usuario de computación en la nube, en el ciclo de vida del desarrollo e implementación de soluciones de software utilizando los servicios de infraestructura de Amazon Web Services.

5.1.1.1. Procesos

Introducción a los procesos de la metodología.

5.1.1.2. Estructura

Se detalla la estructura que se va a desarrollar en cada uno de los procesos que se encuentran definidos en la presente metodología.

5.1.1.3. Objetivo

Descripción general de los entregables y expectativas que se van obtener como resultado del desarrollo de las actividades definidas en el proceso.

5.1.1.4. Supuestos

Conjunto de elementos que se asumen como verdaderos y que son requerimientos específicos para el desarrollo exitoso del proceso.

5.1.1.5. Actividades

Listado de las actividades que guían y facilitan al usuario, en cada uno de los entregables establecidos para el proceso especifico.

Consideraciones generales de las actividades:

- Tienen elementos de entrada y salida.

- Con base en los requerimientos de la solución de software, existen actividades opcionales.
- Existen dependencias de actividades dentro de un mismo proceso.
- Cada una de las actividades se encuentran identificados con un código único.

5.1.2. Procesos

5.1.2.1. Análisis de requerimientos

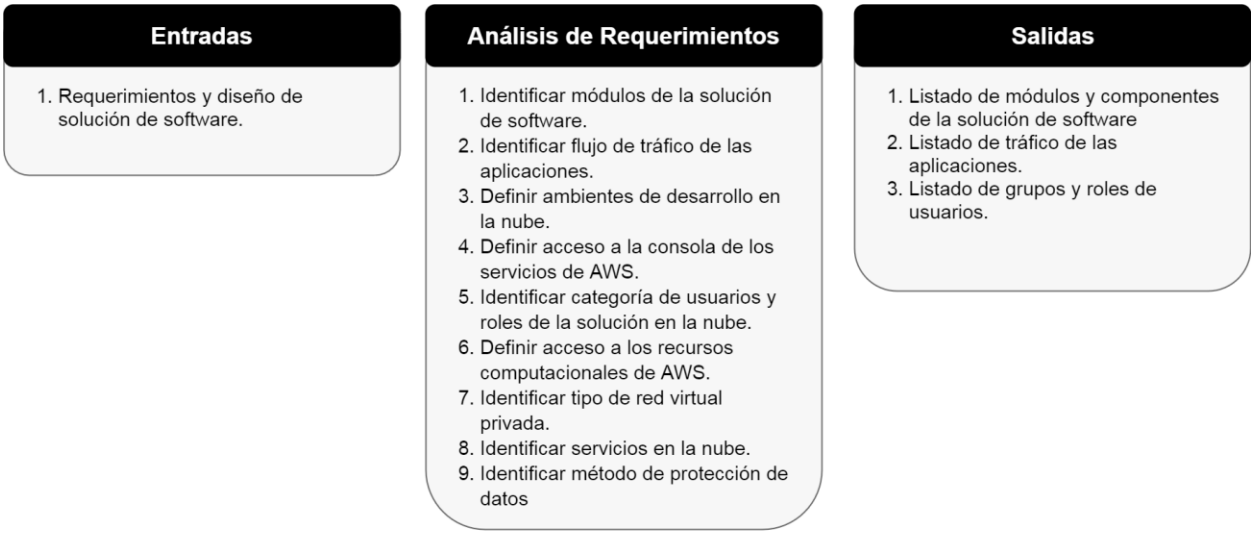


Figura 1 – Proceso de análisis de requerimientos

5.1.2.1.1. Objetivo

Proceso inicial que consisten en identificar y analizar los requerimientos de la solución de software, además de elementos de la infraestructura en la nube, los cuales definen la base para la creación de una red privada y servicios en la nube.

5.1.2.1.2. Supuestos

- Existen requerimientos de alto nivel y diseño de la solución de software que se pretende implementar.
- Conocimientos básicos de los servicios en la nube de AWS y capacidad de recursos computacionales.
- Conocimientos básicos de la consola de AWS (Interface gráfica Web) y el proceso de creación de nuevas cuentas para la utilización de infraestructura como servicio.

5.1.2.1.3. Actividades

Identificar módulos de la solución de software

Con base en los requerimientos y diseño de alto nivel del proyecto software, consiste en identificar los componentes o módulos que son requeridos implementar en la infraestructura en la nube, además se debe detallar las aplicaciones de software ya sea de terceros o personalizadas; que se van a implementar, integrar o desarrollar en cada uno de los módulos. También es requerido definir los componentes que se van a encontrar fuera de la infraestructura virtual de AWS, en caso de que sea necesario realizar llamadas externas a una infraestructura privada corporativa o bien por medio de protocolos de internet.

Una vez identificado los módulos y aplicaciones de software, es de alta utilidad identificar el tipo de procesamiento para cada uno de ellos, si el proceso es de tiempo real o procesamiento por lotes (batch); además de la frecuencia de uso (24/7, una vez al día, entre otros). Los datos anteriores van a facilitar la identificación del tipo de servicios en la nube que se integran con mayor facilidad, inclusive la estimación de los costos de los recursos computacionales en la nube por incurrir en la solución de software.

Identificar flujo de tráfico de las aplicaciones

Es necesario detallar el flujo de comunicación (tráfico de datos) entre cada una de las aplicaciones y componentes de software que van a estar involucrados en la solución, para cada uno de los enlaces de la comunicación se debe identificar el recurso origen, recurso destino, protocolo de intercambio de datos, además del puerto o rango de puertos utilizados.

Definir ambientes de desarrollo en la nube

Consiste en definir la cantidad y tipos de ambiente de desarrollo que son requeridos de implementar en la infraestructura de AWS. Por ejemplo: ambiente de desarrollo en el cual los recursos de desarrollo del software realizan las primeras versiones del software y realizan pruebas unitarias; ambiente de certificación en el cual se combinan los nuevos cambios del software y se involucra el departamento de aseguramiento de la calidad; ambiente de producción el cual impacta directamente la funcionalidad de los clientes y procesos asociados.

También es necesario identificar si las cuentas (ambientes de desarrollo) deben o no ser consolidadas a nivel de facturación de los gastos incurridos en la nube.

Definir acceso a la consola de los servicios de AWS (Interface de usuario)

Definir el protocolo de acceso por parte de los usuarios (equipo de desarrollo, aseguramiento de la calidad, operadores, entre otros.) a la consola de los servicios en la nube de AWS; con respecto a la gestión de usuarios y acceso único a la interface de usuario.

Se evalúa la implementación de métodos de autentificación multi-factor (Multi-Factor Authentication) para agregar una capacidad adicional de seguridad, además de usuario y contraseña; o bien implementación de

herramientas automatizadas e integradas con la red interna corporativa que permitan la autentificación y gestión de usuarios.

Identificar categoría de usuarios y roles

De acuerdo con los requerimientos de la solución de software y procesos establecidos de la organización, es necesarios realizar un listado de los roles y grupos de usuarios (tipos de usuario) que van a hacer uso de los recursos computacionales, además de la consola de servicios de AWS. Para ello se deben incluir los involucrados en fase de vida del desarrollo e implementación del software, además de la fase de operación y soporte del servicio. Para este caso particular no deben ser incluidos los usuarios/roles finales de la solución de software.

Definir acceso a los recursos computacionales de AWS

Se evalúa el tipo de acceso y protocolos de seguridad en el cual los usuarios ingresan desde los ambientes locales o red corporativa hacia los recursos computacionales EC2, en el cual se debe gestionar las llaves privadas de los recursos computacionales, cuentas de usuario de sistema operativo que deben ser autorizadas, además de las posibles reglas de seguridad (firewall) para establecer comunicación.

Identificar tipo de red virtual privada

Ante el requerimiento de habilitar una comunicación segura entre una red corporativa y la red privada en la nube (VPC), por medio de una red virtual privada (VPN), se debe evaluar el tipo de VPN a utilizar. A continuación, se detallan las actuales opciones:

- VPN mediante software
- VPN mediante hardware
- VPN CloudHub

- Conexión directa

Identificar servicios en la nube

En el detalle de las aplicaciones involucradas en la solución de software, se considera de vital importancia analizar cuáles van a ser los servicios en la nube de AWS (almacenamiento, recursos computacionales, balanceo de cargas, entre otros) que se adaptan de manera óptima a los requerimientos de cada una de las aplicaciones.

Identificar método de protección de datos

Se debe identificar para el listado de aplicaciones involucradas en la solución de software en la nube, el método de protección (encriptación, comunicación segura) de los datos transaccionales y de archivos de información involucrados.

Para el caso en que existan aplicaciones con envío, almacenamiento o lectura de datos por medio de archivos de información, se deben considerar los métodos de cifrado, los cuales se detallan a continuación:

- Cifrado por el lado del cliente, el cual implica un cifrado personalizado de los archivos antes de que estos sean enviados al ambiente de la nube privada, además de integración de procesos de descifrado en la lectura de los mismos
- Cifrado por el lado del servidor, el cual implica un cifrado a nivel de disco por parte de los servicios de almacenamiento de datos (base de datos RDS, S3, EBS, DynamoDB, entre otros) ofrecidos en la infraestructura de AWS. Por tanto, los archivos de información no son manipulado de manera externa y una vez que se encuentra en los servicios de almacenamientos, estos son cifrados de manera automática.

Con respecto al envío y obtención de datos a nivel transaccional es necesario evaluar los protocolos de comunicación segura (HTTPS, Certificados de seguridad), además de la implementación de servidores (Proxy Server) que intercepten las solicitudes cifradas.

Ante el requerimiento de cifrado de datos, se debe identificar la herramienta de gestión de llaves privadas, las cuales son utilizadas por las aplicaciones de software encargadas del cifrado y descifrado de información. Es posible utilizar el robusto servicio KMS (Key Management Services) de AWS o bien la integración de herramientas externas/personalizadas.

5.1.2.2. Gestión de roles y políticas

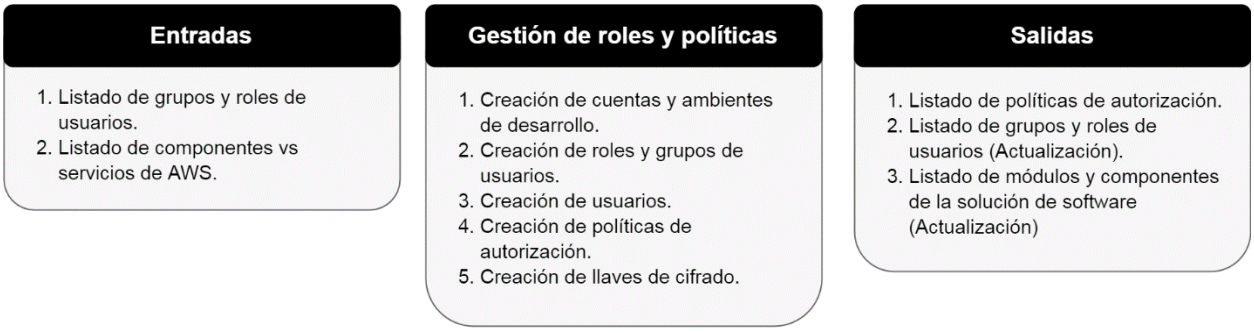


Figura 2 - Proceso de gestión de roles y políticas

5.1.2.2.1. Objetivo

El presente proceso tiene como objetivo la creación inicial de los ambientes de desarrollo en la nube que van a ser utilizados por la solución de software, además de la gestión de los roles, usuarios y políticas mediante el uso del módulo IAM. (Identity and Access Management).

5.1.2.2.2. Supuestos

- La organización cuenta con la información contable a la cual se va a asociar los gastos incurridos en el uso de los servicios e infraestructura en la nube.

- Se conoce de antemano los usuarios individuales (con un identificador único) que se encuentran asociados a los grupos/categorías de usuarios identificados, los cuales van a ser creados propiamente en la actividad *creación de usuarios*.

5.1.2.2.3. Actividades

Creación de cuentas y ambientes de desarrollo

Tomando como base la información obtenida en la actividad definir ambientes de desarrollo en la nube, la presente actividad consiste propiamente en la creación de cada uno de los ambientes de desarrollo identificados. Para ello se requiere detallar la información de la organización, además de la información contable en la cual se van a gestionar los cobros asociados.

Dado la creación de la cuenta de AWS, se obtiene un usuario con acceso total (usuario root), el cual cuenta inclusive con acceso a la información contable; por lo se recomienda la creación inicial de un usuario administrador, el cual posteriormente va a permitir la gestión de los roles y usuarios.

Es necesario estimar si es requerido o no tener una facturación consolidada, con respecto a todos los ambientes de desarrollo asociados a una organización, esto va a permitir obtener una facturación única de todos los recursos computacionales utilizados en el periodo.

Ante la creación de la(s) cuenta(s), es necesario evaluar el plan de soporte (brindado por parte del equipo de AWS) con respecto a los recursos y red privada en la nube. Dependiendo del plan seleccionado se puede incurrir en gastos adicionales.

Creación de roles y grupos de usuarios

Dado el **listado de grupos de usuarios y roles** los cuales detallan los tipos de usuarios/aplicaciones que van a utilizar los servicios, consola o recursos computacionales de AWS (tanto para la fase de desarrollo como la fase de operación de la solución de software en la nube).

La actividad consiste en la creación de cada uno de los roles y grupos de usuarios identificados, mediante el uso del módulo IAM (Identity Access Management).

Se recomienda la creación de roles a las aplicaciones de software que necesitan autorización a los diferentes servicios en la nube, además que van a ser utilizados mediante los recursos computacionales EC2 (Servidores virtuales). Los roles no tienen credenciales de acceso asociadas, por lo que se evita el almacenamiento de llaves privadas dentro del sistema de archivos del servidor virtual.

Por otro lado, se recomienda la creación de grupos de usuarios a todas esas categorías de usuarios finales en la cuales se identifica la necesidad de la gestión de llaves de acceso y contraseña para la utilización de los servicios en la nube.

Con el objetivo de definir un estándar en los nombres utilizados, se recomienda el siguiente formato:

- Grupos de usuarios
    - **{ Código de la Solución}_{Código de módulo}_{Nombre de grupo}**_Group
- Roles
    - **{ Código de la Solución}_{Código de módulo}_{Nombre de rol}**_Role

Es importante resaltar que la creación de roles, grupos de usuarios y usuarios se deben realizar para cada uno de los ambientes de desarrollo que fueron creados, ya que estos no pueden ser compartidos entre ellos. Por tanto, la presente actividad tiende a ser realiza más de una vez.

Creación de usuarios

Consiste en la creación de los usuarios que deben tener acceso a los servicios, consola o recursos computacionales de AWS. Una vez que han sido creados los usuarios, se debe asociar cada uno de ellos a los grupos de usuarios definidos en las actividades previas.

Es necesario definir el protocolo en el cual se va a hacer entrega de las llaves privadas (obtenidas en la creación de cada usuario) a los usuarios finales.

Para el caso en la cual exista una integración de herramientas para la autentificación y gestión de usuarios, la creación de usuarios se establece mediante el procedimiento establecido por la organización y no precisamente mediante el uso del módulo IAM (Identity and Access Management).

Se recomienda el siguiente formato para el nombre de cada uno de los usuarios por crear:

- **{Código de la Solución}_{código del módulo}_{Nombre o ID de usuario}**_User

Creación de políticas de autorización

Las políticas de autorización permiten brindar o limitar niveles de acceso para los diferentes servicios de la nube de AWS, por lo que presente actividad consiste en la creación de las políticas de autorización que van a

ser asociadas a los usuarios, grupos de usuarios y roles que fueron definidos en actividades previas.

Dado la recomendación para crear grupos de usuarios, se presenta la facilidad de que las políticas de autorización se deben asociar únicamente a los grupos y automáticamente estas se van ver reflejadas en todos los usuarios relacionados al grupo.

En la creación de las políticas es necesario definir los tipos de servicios a los cuales se debe de tener acceso, además del tipo de acciones (descripción de recursos, creación de recursos, entre otros.) para cada uno de ellos. Las políticas también permiten filtrar las autorizaciones por recursos computacionales específicos, por lo que, una vez creado los recursos, las políticas pueden ser actualizadas para obtener mayor rigurosidad en los accesos.

Una vez finalizada la creación de las políticas de autorización, se debe proceder a asociar/configurar cada una de ellas con los grupos de usuarios y roles identificados en el **listado de grupos y roles de usuario**.

El módulo de IAM provee de manera predeterminada un conjunto de roles que pueden ser utilizados, sin embargo, también estas pueden ser creadas de manera personalizadas con base en los requerimientos y solución de software que se desea implementar.

Se recomienda el siguiente formato para el nombre de cada uno de las políticas por crear:

- **{Código de la Solución}_{Código de módulo}_{Nombre de la política}**_Policy

Creación de llaves de cifrado

De acuerdo al listado de aplicaciones de la solución de software en la nube, para las cuales se identificó la necesidad de definir un método de cifrado para la lectura, escritura o almacenamiento de los datos, la actividad consiste en la creación de las llaves de cifrado para cada una de ellas. Se recomienda la creación de las llaves de manera separada para cada aplicación involucrada.

5.1.2.3. Red virtual en la nube

Figura 3 – Proceso de red privada virtual

5.1.2.3.1. Objetivo

Consiste en la creación y configuración de los componentes que permiten establecer una red privada en la nube, en los cuales además se incluye la definición de las capas de seguridad con respecto la transferencia de datos, subred y recursos computacionales.

5.1.2.3.2. Supuestos

- Se cuenta con personal capacitado o soporte por parte del equipo de infraestructura de la organización, para la asignación de direcciones IP en la privada en nube, o bien para la creación y configuración de la red virtual privada (VPN) en caso de que sea necesario.

5.1.2.3.3. Actividades

Creación de red privada en la nube

La presente actividad consiste en la creación de la red privada en la nube (VPC, por sus siglas en inglés), la cual se considera uno de los componentes base para la creación y configuración de la infraestructura en la cual se va a provisionar los recursos computacionales en la nube. Se recomienda de creación de una única VPC para cada uno de los ambientes de desarrollo disponibles.

Para ello, es necesario definir el rango de direcciones IP disponibles (preferiblemente rango de direcciones privadas), el cual se debe especificar mediante un bloque de direccionamiento de IP´s (CIDR block), una máscara de red entre "/16" y "/24", lo anterior mediante el estándar RFC 4632.

Es importante resaltar que el bloque CIDR no puede ser modificado una vez que se haya finalizado la creación de la VPC, por lo que se debe realizar un análisis detallado este dato, tomando en cuenta la capacidad de la presente solución en la nube y el crecimiento futuro. Es recomendable abarcar la mayor cantidad posible de direcciones IP.

Para el caso de en el cual es necesario asociar una red virtual privada (VPN) de la red interna corporativa, se debe tomar en cuenta las siguientes consideraciones en la creación de la VPC:

- Es necesario la creación de una entrada virtual privada (Virtual Private Gateway), la cual va actuar como un túnel que reside en el lado de la infraestructura de AWS para el intercambio de comunicación con la red interna corporativa.
- El rango de direcciones de IP que va a ser definida en la VPC, debe ser analizada en conjunto con la configuración disponible de la red interna

corporativa y de VPN, con el objetivo de verificar que no haya algún conflicto entre ellas.

Para el caso en el cual se requiere el acceso de trafico proveniente de internet, se requiere la configuración de una entrada de internet (Internet gateway) en la red privada en la nube; la cual posteriormente debe ser asociada a una subred de tipo pública para permitir el trafico entrante.

Creación de red virtual privada

La creación de una red virtual privada (VPN, por sus siglas en inglés) procede con respecto al análisis obtenido en la actividad de identificación de tipo de red virtual privada, la cual puede ser opcional dependiendo de los requerimientos establecidos en la solución de software en la nube.

Se recomienda la configuración de una VPN para establecer un acceso y comunicación segura entre los recursos computacionales definidos en la nube y la red interna corporativa.

Para la creación de la VPN y su respectiva integración con la red virtual privada (VPC) es necesario estimar el esfuerzo requerido por el equipo de infraestructura de la organización para la creación o configuración de una VPN mediante software, hardware o conexión directa.

Es necesario la creación de una entrada de cliente (Customer Gateway), la cual actúa como túnel por parte de la red interna corporativa, para permitir la comunicación segura con AWS. La creación y configuración de la entrada de cliente reside principalmente en la VPN de la red interna de la organización y una vez finalizada es necesario asociar en la VPC de AWS la información de IP de la entrada de cliente, además del tipo de direccionamiento el cual puede ser estático o dinámico (mediante el uso de del protocolo Border Gateway Protocol).

Creación de subredes

Consiste en la creación de las subredes requeridas en la red privada en la nube, la cual define el rango de direcciones de IP directamente asociadas a los recursos computacionales y la cual es un subconjunto del bloque de direccionamiento de IP´s (CIDR block) que fue definido para la VPC.

Se recomienda la definición de las subredes con base al **listado de módulos y componentes de la solución de software**, creando una subred por cada módulo identificado en los requerimientos de la solución.

Al igual que en la VPC, es necesario realizar un análisis detallado del bloque de direccionamiento (CIDR) que va a ser utilizado, con el objetivo de que este acorde a la capacidad estimada, además que no haya conflictos de escalabilidad en el futuro. Además, se debe estimar que no haya ningún solapamiento con el rango de direcciones IP establecidas para las demás subredes.

Cada una de las subredes debe asociarse a una única zona de disponibilidad (Availability Zones), por lo que sí existe el requerimiento de componentes de la solución que van a ser provisionadas en más de una zona de disponibilidad, se debe estimar la creación de una o más subredes.

Con respecto al **listado de tráfico de las aplicaciones**, es posible identificar los componentes que requieren comunicación con internet (fuera de la red virtual privada), por lo en la creación de estas subredes específicas, es necesario especificar el componente de entrada de internet (internet gateway) creado en la VPC. El conjunto de subredes que tiene asociado una entrada de internet se consideran como subredes públicas, las que no cumple con este caracteriza se considera subredes privadas.

Es importante resaltar que del bloque de direcciones IP asignado a la subred, las primeras 4 direcciones IP y la última dirección se encuentran reservadas para el uso propiamente de AWS, por lo que no pueden ser utilizadas por los recursos.

Se recomienda el siguiente formato del nombre de las subredes:

- **{Código de la Solución}_{Código del módulo}_{Código de zona de disponibilidad}**

Creación de dominios

La presente actividad consistente en la creación de los dominios y direcciones IP públicas para permitir el acceso proveniente de internet, por parte de los usuarios a las aplicaciones de software en la nube. Con respecto a los requerimientos de la solución, esta actividad puede ser opcional.

Es requerido el uso del módulo Route 53 para registrar los dominios públicos y legibles a los usuarios finales, además se identifica el uso del componente de direcciones IP elásticas (Elastic IP) para la creación de direcciones IP públicas. Una vez definidos, el tráfico puede ser re-direccionado a los recursos de balanceo de carga o instancias virtuales de manera directa, las cuales contienen las aplicaciones de software específicas.

Se recomienda re-direccionar el tráfico proveniente de internet a los recursos computacionales que se encuentran en las subredes públicas definidas para la VPC. Por su parte, es importante resaltar que el uso de direcciones IP publicas asignadas directamente a los recursos EC2, no definen IP pública estática y el cambio de estado de las instancias virtuales puede provocar un cambio de IP.

Creación de tablas de direccionamiento

La actividad consiste en la creación y configuración las tablas de direccionamiento (route tables), las cuales permite definir reglas para el direccionamiento del tráfico de red.

Con la configuración inicial de la VPC, se obtiene de por defecto una tabla principal de direccionamiento (main route table). Sin embargo, se recomienda la creación personalizada de las tablas de direccionamiento con respecto a las subredes previamente definidas. Especialmente si se han configurado subredes públicas, ya que es necesario definir una tabla de direccionamiento personalizada asociada a la entrada de internet (internet gateway).

Las subredes por defecto son asociadas a la tabla principal de direccionamiento, por lo que es necesario actualizar cada una de las subredes con los nuevos datos obtenidos en la presente actividad.

Propiamente en la configuración de las tablas de direccionamiento, es necesario definir el rango de direcciones IP donde proviene el tráfico y el componente donde debe ser redirigido el trafico (target).

Creación de grupos de seguridad

Tomando como base el **listado de tráfico de las aplicaciones**, en el cual se encuentra detallado el flujo de comunicación de la solución de software en la nube, la actividad consiste en la creación de los grupos de seguridad (security groups), los cuales proveen una capa de seguridad para controlar el tráfico de entrada y salida los recursos computacionales (EC2) asociados a cada una de las aplicaciones.

Se recomienda la creación de un grupo de seguridad para cada una de las aplicaciones identificadas previamente.

En la creación de los grupos de seguros, es necesario definir de manera separada las reglas de entrada y las reglas de salida. A continuación, se detallan los datos requeridos en la creación de cada regla del grupo de seguridad:

- Tipo.
- Protocolo de Internet.
- Puerto o rango de puertos.
- Recurso destino u origen.

Con respecto a la información de recurso destino u origen, este puede ser detallado en términos de dirección IP, rango de direcciones IP (CIDR Block) o bien el identificador de un grupo de seguridad.

Es importante resaltar, que por defecto los grupos de seguridad restringen el tráfico de entrada o salida a los recursos computacionales asociados, por lo que las reglas se definen para permitir el tipo de tráfico esperado.

Se recomienda el siguiente formato en los nombres de los grupos de seguridad:

- **{Código de la Solución}_{Código del módulo}_{Nombre de la aplicación}_SG**

Creación de lista de acceso de red

Con el objetivo de agregar una capa adicional de seguridad a nivel de subred (a diferencia de los grupos de seguridad que operan a nivel de servidores virtuales EC2), es posible crear listas de acceso de red (ACL) para controlar el tráfico de entrada y salida de la subred.

Al igual que los grupos de seguridad, es necesario detallar el tipo de protocolo internet, puerto o rango de puertos y recurso. Sin embargo, para

el ACL se debe detallar si la regla es definida para denegar o para permitir el tráfico.

El **listado de tráfico de aplicaciones** se determina como insumo principal para la creación y configuración de estas listadas de acceso. No obstante, se resalta que las listas de acceso pueden ser opcionales y es posible utilizar la configuración por defecto, la cual permite todo el tráfico de la red.

Creación de llaves de acceso

Las llaves de acceso (Amazon EC2 key pairs) utilizan información criptográfica para permitir una autorización de forma segura a los recursos computacionales EC2 (servidores virtuales), se logra así acceder de manera directa a los recursos mediante el protocolo SSH.

Por lo que, la presente actividad consiste en la creación de las llaves de acceso para cada uno de las aplicaciones identificadas en el **listado de módulos y componentes de la solución de software**.

Una vez finalizado la creación de cada una de las llaves de acceso, se obtiene un archivo de formato ".pem", el cual contiene las llaves de confianza, las cuales posteriormente deben ser configuradas en los servidores virtuales EC2 a utilizar por la solución en la nube.

Se recomienda el siguiente formato para el nombre de las llaves de acceso:

- **{Código de la Solución}_{Código del módulo}_{Nombre de la aplicación}_KP**

5.1.2.4. Implementación de software

Figura 4 – Proceso de implementación de software

5.1.2.4.1. Objetivo

El presente proceso tiene como objetivo el desarrollo e implementación de las aplicaciones que se han identificado en los requerimientos de la solución de software en la nube, para lo cual se requiere un análisis y creación de la infraestructura a utilizar, además de identificar las dependencias para el inicio del desarrollo.

5.1.2.4.2. Supuestos

- Se tiene conocimiento la(s) tecnología(s) y lenguaje(s) de programación que van a ser utilizados en las actividades de desarrollo e implementación de las aplicaciones de software.
- Se tiene conocimiento del presupuesto que se encuentra asignado para los recursos computacionales de la solución de software en la nube.

5.1.2.4.3. Actividades

Identificación de tipos de recursos computacionales

Con respecto al **listado de módulos y componentes de la solución de software**, la presente actividad tiene como objetivo identificar las

especificaciones de los recursos computacionales para cada una de las aplicaciones involucradas en la solución de software.

Las especificaciones de los recursos computacionales se determinan con respecto a la capacidad de CPU, memoria, acho de banda, tipo y cantidad de almacenamiento; las cuales se encuentran categorizadas en los tipos de recursos EC2 disponibles.

Para el caso en el cual se utilice otros servicios de AWS (RDS, DynamoDB, S3 etc), las especificaciones de cada uno de ellos también deben ser incluidas en el análisis.

Es necesario resaltar que las especificaciones de los recursos requeridos, se deben realizar para cada uno de los ambientes de desarrollo disponibles, enfocándose principalmente en el ambiente productivo, el cual se asume que requiere mayor capacidad computacional, con respecto a los ambientes de pruebas.

Durante el análisis de los tipos de recursos computacionales, se recomienda la evaluación de la escalabilidad horizontal de la aplicación de software.

Estimación de costos computacionales

La actividad de estimación de costos computacionales consiste en evaluar los gastos mensuales que conllevan el uso de los recursos computacionales requeridos en la solución de software en la nube. Para la evaluación se requiere los insumos del **listado de tipos de recursos computacionales**, además del **listado de módulos y componentes de la solución de software**.

Se resalta que esta actividad puede ser opcional, sin embargo, es importante realizar un análisis del presupuesto asignado a la solución en la nube, con respecto al estimado de costos.

Para determinar los costos asociados, es requerido asociar el costo del tipo y especificaciones de los recursos computacionales, con respecto a la frecuencia de uso estimada.

También es necesario incluir otros servicios requeridos en la solución, los cuales tienen un costo asociado y no están contemplados en los costos de los recursos computacionales (servidores virtuales), tales como almacenamiento S3, balanceos de cargas (ELB), dominios, entre otros.

Con respecto a los resultados obtenidos en la estimación de los costos, puede existir una restructuración de los tipos de recursos computacionales identificados.

Creación de recursos computacionales

La presente actividad consiste propiamente en la creación de los recursos computacionales, los cuales fueron identificados y analizados en actividades previas. Para ello se toma como insumo la información detallada en el **listado de tipos de recursos computacionales, listado de subredes**, **listado de módulos y componentes de la solución de software**.

Es posible la creación de los recursos de manera manual (utilizado la interface web de AWS, línea de comandos o integración con los servicios de AWS). Sin embargo, se recomienda el uso de servicios que permiten la creación automática de los recursos computacionales, tales como cloud formation, contenedores de aplicaciones, entre otros.

Para la creación de los recursos computacionales, es requerido utilizar como parámetros las configuraciones previamente realizadas para cada una de las aplicaciones de la solución de software, tales como nombre de rol, identificador de la red privada en la nube (VPC), subred o subredes, grupo(s) de seguridad, además de las llaves de acceso.

Además de la creación de los recursos EC2, también es necesario la creación o configuración de servicios y componentes de AWS que se consideran necesario en la infraestructura de la solución en la nube. Tales como base de datos, estructura de almacenamiento en la nube, componentes de balanceo de cargas, entre otros.

Con respecto a los datos obtenidos en la actividad identificación de métodos de protección, en la cual se determina si es requerido el método cifrado de datos por el lado del servidor; es necesario tomar en cuenta esta información en la creación y configuración de los volúmenes de datos de EC2, base de datos en la nube, almacenamiento S3, entre otros.

Es importante resaltar que la creación de los recursos computacionales se debe realizar para cada uno de los ambientes de desarrollo disponibles. Sin embargo, se recomienda que la creación de los recursos se encuentre alineada con respecto a la finalización de cada una de las fases de desarrollo.

Identificación de paquetes de desarrollo

La actividad tiene como objetivo identificar los paquetes de desarrollo, que son requeridos para el desarrollo de las aplicaciones de software en la nube, los cuales van a permitir integrar la solución con diferentes servicios de la infraestructura de AWS. Para ello se toma como base el **listado de módulos y componentes de la solución de software**.

Es necesario realizar un análisis de las tecnologías, ecosistemas (framework´s) y tipos de lenguajes de programación que van a ser utilizados en la solución en la nube; con el objetivo de verificar compatibilidad e integración con los paquetes de desarrollo requeridos.

Con la identificación previa de los paquetes de desarrollo SDK, herramientas a nivel de línea comandos y componentes para facilitar el uso e integración de los servicios de AWS; se facilita en proceso propiamente del desarrollo de la solución en la nube.

Desarrollo de aplicaciones de software

La presente actividad consiste en el desarrollo de las aplicaciones de software que han sido identificadas en la solución en la nube, y las cuales han sido la base para efectuar las actividades previas de la presente metodología. Para ello se deben ejecutar los procesos propiamente del ciclo de vida del desarrollo del software establecidos en la organización.

Además del desarrollo de la lógica de negocios en la solución en la nube, es necesario el desarrollo de los componentes para integrar la aplicación con los servicios de infraestructura de AWS.

Para la ejecución de la actividad es necesario analizar información esencial que se ha recopilado al momento, los cuales se detallan a continuación:

- Listado de módulos y componentes de la solución de software.
- Listado de tráfico de las aplicaciones.
- Listado de grupos y roles de usuarios.

Es necesario resaltar que, para cada una de las aplicaciones de software identificadas, se debe hacer efectivos los métodos de protección de datos que ha identificado previamente en la presente metodología.

Implementación de aplicaciones

La actividad implementación de aplicaciones consiste en definir e implementar el proceso de liberación de versiones de las aplicaciones de

software desarrolladas hacia los recursos computacionales que se han definido en la infraestructura en la nube.

El proceso de liberación de nuevas versiones puede ser tan simple como un conjunto de pasos manuales en el cual la aplicación de software se almacena en los servidores virtuales EC2, imágenes AMI, entre otros.

Sin embargo, se recomienda la implementación de herramientas integración continua, en el cual es posible automatizar los procesos liberación de versiones entre los múltiples ambientes de desarrollo que se encuentren disponibles. Es posible el uso de herramientas tales como CodeDeploy, CodePipeline, entre otros. Además, se evalúa la integración con repositorios de código fuentes que se encuentre de manera local o en la nube.

Para el caso en el cual se cuenta con múltiples ambientes de desarrollo, es necesario definir el proceso para liberar o migrar las nuevas versiones del software entre ambientes.

Para la liberación de nuevas aplicaciones en la cual se requiere generar una nueva imagen AMI con la nueva versión del código fuente o configuración, es necesario definir la gestión de las AMI´s con versiones previas, por lo que se debe definir la cantidad de copias, período de retención, entre otros.

Aseguramiento de calidad

La presente actividad consiste en definir los pasos de aseguramiento de calidad para validar la funcionalidad de las aplicaciones de software que han sido desarrolladas e implementadas en actividades previas.

Para el caso, en el cual es requerido definir procesos o herramientas de integración continua, se debe evaluar la integración del anterior con propiamente el procedimiento del aseguramiento de calidad, en el cual se

puede realizar pruebas automáticas o manuales con respecto a las nuevas versiones liberadas de las aplicaciones de software.

5.1.2.5. Operación y monitoreo

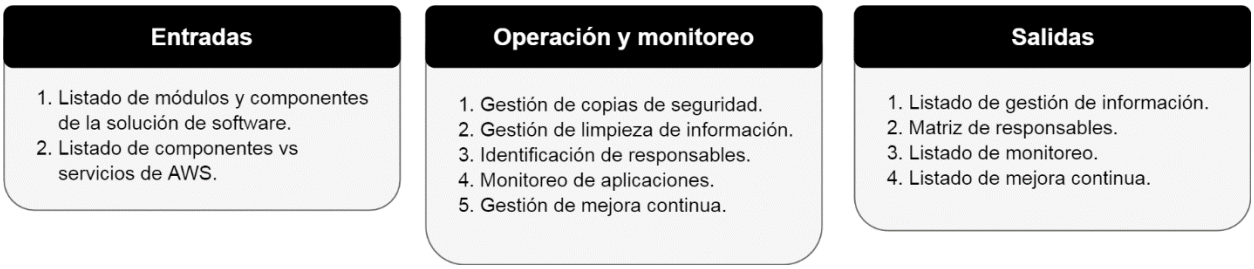


Figura 5 – Proceso de operación y monitoreo

5.1.2.5.1. Objetivo

El proceso de operación y monitoreo tiene como objetivo definir los procedimientos que se deben ejecutar de manera continua, una vez que la solución de software en la nube se encuentre en la fase de operación. En los cuales se debe detallar la gestión de copias de seguridad y limpieza de la información, además de identificar los componentes de la solución que requieren monitorear de su comportamiento.

5.1.2.5.2. Supuestos

- Es posible la integración, configuración o modificación de la infraestructura y aplicaciones de software para cumplir con los requerimientos de gestión de copias de seguridad, limpieza de datos o monitoreo a identificar en las presentes actividades.

5.1.2.5.3. Actividades

Gestión de copias de seguridad

La presente actividad consiste en definir el procedimiento para la gestión de copias de seguridad de la información e infraestructura correspondientes a la solución en la nube.

Con respecto al **Listado de módulos y componentes de la solución de software**, es necesario analizar cuáles son los componentes (Base de datos, volúmenes de almacenamiento, archivos de información, servidores virtuales, entre otros) que tienen el requerimiento de crear copias de seguridad.

Para cado uno de los componentes identificados se debe definir:

- Frecuencia en la creación de copias de seguridad.
- Como se va a realizar la copia de seguridad.
- Período de retención de las copias de seguridad.

Para el caso, en el cual es requerido hacer uso de los procesos automáticos (para la creación de copias de seguridad) de servicios específicos de AWS, es necesario realizar la configuración especifica en cada uno de los recursos.

Gestión de limpieza de información

La actividad consiste en definir el procedimiento de limpieza o borrado de información que va a ser recopilada en la solución de software en la nube, en el cual se incluye la información almacenada en instancias de base de datos, información en volúmenes de servidores virtuales, registros de aplicaciones (Log´s), entre otros.

Con respecto al **Listado de módulos y componentes de la solución de software**, es necesario identificar la información asociada a cada uno de los componentes de software, con el objetivo de definir la frecuencia de limpiado de datos, período de retención de la información, además de cómo se va a realizar la limpieza.

Ante la flexibilidad de los servicios de almacenamiento en la nube (S3, Glacier, entre otros), es posible evaluar la posibilidad de mover los datos que no desean ser eliminados o bien que van a tener un acceso poco

frecuente, a otras opciones de almacenamiento que tienen un costo asociado menor.

Se recomienda la creación de procesos automatizados para la limpieza de los datos, además de notificaciones con el objetivo de informar a los dueños de la aplicación si el volumen de información sobrepasada lo permitido.

Identificación de responsables

La identificación de responsables tiene como objetivo identificar a los departamentos, equipos de trabajo o personas que son responsables de brindar soporte o toma de decisiones a las aplicaciones de software en la nube, ante alguna eventualidad.

Tomando como base el **Listado de módulos y componentes de la solución de software**, es necesario generar una matriz con el listado de aplicaciones de software vs los responsables identificados, la cual va a ser de gran ayuda en la fase de operación y ciclo de vida del servicio, especialmente si es una solución de software con gran impacto en la organización.

Monitoreo de aplicaciones

La presente actividad consiste en identificar las aplicaciones de software para las cuales es requerido realizar un monitoreo a nivel de infraestructura, de aplicación, registros de datos (Log´s), entre otros. Para ello se toma como base el **Listado de módulos y componentes de la solución de software,** en el cual se detallan los componentes principales de la solución en la nube.

Se recomienda el uso de CloudWatch como herramienta de monitoreo, debido a su integración con los recursos computacionales de AWS. Sin

embargo, también es posible la implementación de herramientas externas para el monitoreo.

Para cada una de las aplicaciones de software identificadas (que se desean monitorear), es requerido definir cuáles van a ser los datos específicos que se desea llevar registro y frecuencia en q se va a monitorear. Además de realizar la configuración o desarrollo especifico (en caso de que aplique) en la aplicación, con el fin de obtener los datos identificados.

Es necesario analizar si para cada una de la información monitoreada, es requerido generar alertas de notificación una vez que estos se encuentren fuera de un rango establecido.

Es importante mencionar que esta actividad puede ser opcional, sin embargo, se considera de gran importancia tener registros del comportamiento de la solución en la nube.

Gestión de mejora continúa

La actividad de mejora continua consiste en definir un procedimiento de recolección de datos, con el fin de identificar áreas de mejoras a nivel funcional y de rendimiento de las aplicaciones de software en la nube. Al igual que la actividad de monitoreo, la mejora continua se considera actividad opcional.

Es necesario identificar cuáles van a ser los componentes de software a los cuales se desea incluir en la actividad de mejora continua, tomando como base el **Listado de módulos y componentes de la solución de software.** Para cada uno de los anteriores se debe detallar lo siguiente:

- Que se va a medir.
- Cuales datos se van a recolectar.
- Como se van a analizar los datos obtenidos.

- Como se van a presentar los datos.

Una vez que se haya encontrado un área de mejora o bien los datos encontrados no se encuentran dentro del rango establecido, es necesario comunicar a los involucrados correspondientes para analizar y realizar las correcciones respectivas.

La presente actividad se encuentra directamente ligada a la actividad de monitoreo, ya que esta última es la que va a brindar los datos de insumos para su respectivo análisis.

5.1.3. Flujo de actividades de la metodología

A continuación, se presenta el diagrama de flujo de las actividades definidas en la metodología, en el cual se idéntica el conjunto de dependencias para cada uno de los procesos y actividades requeridos en la implementación de aplicaciones de software en AWS.

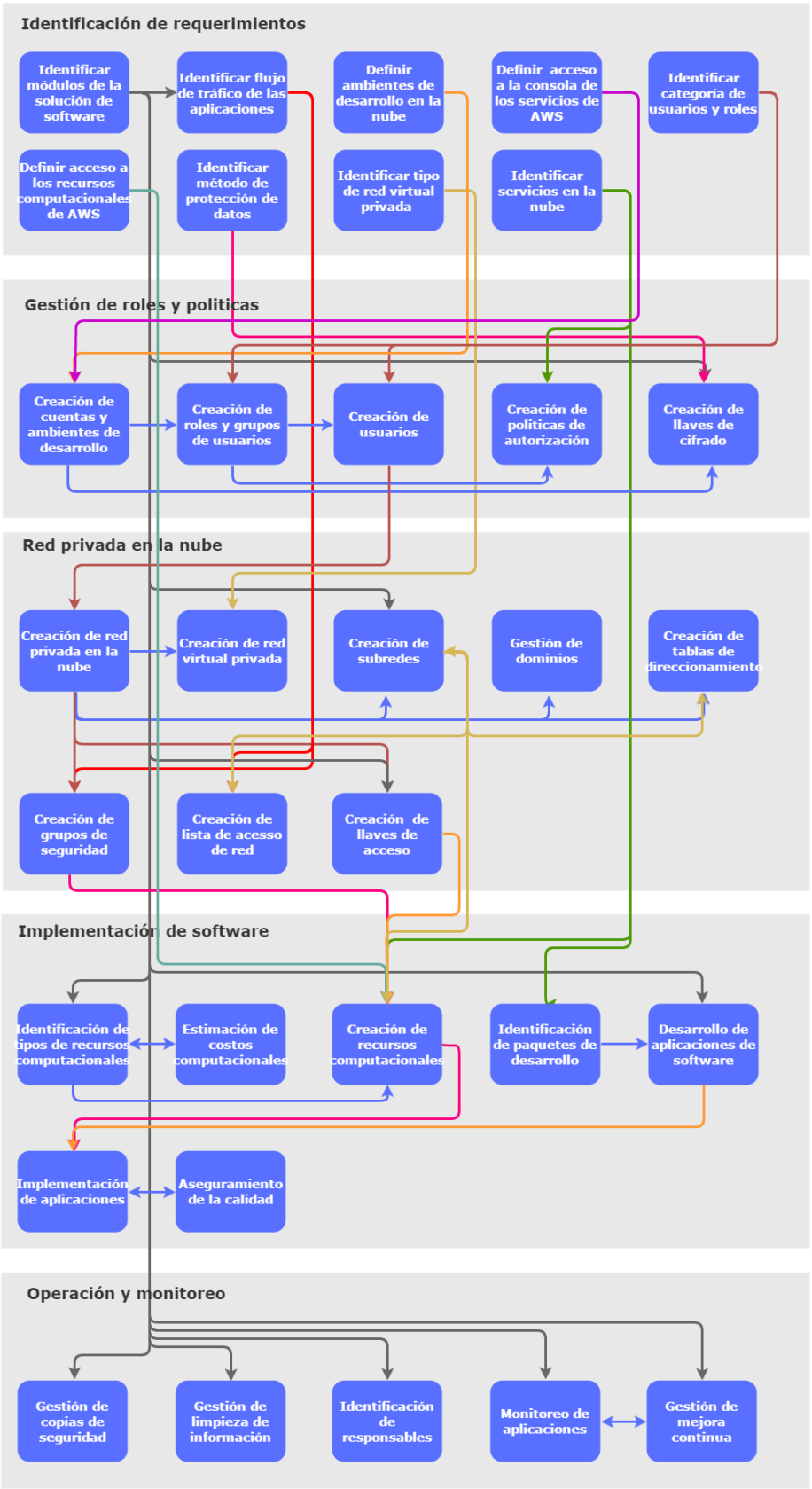


Figura 6 – Flujo de actividades de la metodología.

5.1.4. Plantillas de documentación

A continuación, se realiza el detalle de las plantillas de documentación (documentos de salida) de las principales actividades identificadas en la metodología.

Listado de módulos y componentes de la solución

El listado de módulos de la solución de software es uno de los principales documentos de salida de la metodología, el cual, con base en los resultados obtenidos en el proceso de análisis de requerimientos, se detallan el listado de los módulos de la solución de software, aplicaciones asociadas a cada módulo, descripción breve de cada aplicación, el tipo de procesamiento (si es una aplicación en línea, por lotes, entre otros), la frecuencia en que se estima ser utilizada, los servicios o infraestructura propiamente de AWS que va a estar asociada a cada una de las aplicaciones, además para el caso que sea necesario se debe detallar el método de protección de datos de cada aplicación.

En procesos posteriores de la metodología, este documento es actualizado para detallar las llaves de acceso (EC2 Keys pairs) para las aplicaciones identificadas, subredes asociadas, rango de direcciones IP disponible en la subred, además de las llaves de cifrado en el escenario que sea requerido.

La plantilla se encuentra representada en el anexo *4.1 Listado de módulos y componentes de la solución.*

Listado de tráfico de las aplicaciones

El presente documento de salida representa el flujo del todo el tráfico de entrada y salida asociado a la solución de software en la nube, incluyendo el tráfico de herramientas externas a la red privada que se integran o consumen información de la solución. Para cada una de las aplicaciones

identificadas se detallar el recurso de origen, recurso destino, el tipo de protocolo de intercambio de información, además del puerto o rango de puertos que van a ser utilizados.

La plantilla se encuentra representada en el anexo *4.2 Listado de tráfico de las aplicaciones*.

Listado de grupos y roles de usuarios

El listado de grupos y roles de usuarios consiste en el detalle de los actores (identificados en las fases de desarrollo, implementación y operación de la solución de software) y aplicaciones de software que requieren tener acceso a los servicios o infraestructura de AWS. Para cada una de los registros identificados se debe detallar el nombre del rol o grupo de usuarios, el tipo (propiamente si es un grupo de usuario o un rol), aplicación asociada (este dato puede ser opcional para los grupos de usuarios) y área de la organización asociada (aplica únicamente para los grupos de usuarios).

Posteriormente a la creación de los roles y grupos de usuarios, el documento debe ser actualizado con el nombre con el que fue creado en el módulo IAM, políticas de autorización asociadas, además para el caso que fuese necesario los nombres de los usuarios asociados a los grupos creados.

La plantilla se encuentra representada en el anexo 4.3 Listado de grupos y roles de usuarios.

Listado de políticas de autorización

El presente documento de salida detalla las políticas de autorización que van a estar asociadas a los grupos de usuarios y roles que van a ser utilizados en la infraestructura de AWS, logrando así dar acceso a las diferentes funcionalidades de los servicios de AWS. Para el documento se debe detallar el nombre de la política de autorización, el nombre con el que fue creado en

el módulo IAM, el nivel de acceso de la política (lectura, escritura, entre otros), los servicios de AWS asociados a la política, además de manera opcional se puede ingresar los identificadores de los recursos (ARN) a los cuales únicamente se autoriza el uso de la política.

La plantilla se encuentra representada en el anexo *4.4 Listado de políticas de autorización*.

Listado de subredes

El presente documento detalla la información de las subredes creadas, con respecto al ambiente de desarrollo en el cual fue creado, nombre del módulo, nombre de la subred, identificador de la subred (obtenido en el módulo IAM, una vez que se haya creado), además del bloque de direcciones IP asignado.

La plantilla se encuentra representada en el anexo *4.5 Listado de subredes*.

Listado de grupos de seguridad

El listado de grupos de seguridad consiste en el detalle de las reglas de tráfico de entrada y salida que se encuentra asociado a cada uno de los recursos computacionales EC2. Para cada una de las reglas del grupo de seguridad se debe definir el nombre de la aplicación de software asociada, nombre del grupo de seguridad (tal como fue definido en la creación en el módulo EC2), identificar del grupo de seguridad (se obtiene una vez finalizada la creación), tipo de regla (si es regla para entrada o salida de trafico), tipo de comunicación, protocolo, puerto o rango de puertos y recurso de origen o destino.

La plantilla se encuentra representada en el anexo *4.6 Listado de grupos de seguridad*.

Listado de tipos de recursos computacionales

El presente documento de salida detalla las especificaciones de los recursos computacionales que son requeridos en la solución en la nube. Para cada uno de los recursos se debe detallar el ambiente de desarrollo que pertenece, nombre de la aplicación a la cual se encuentra asociada, el nombre del recurso computacional, el tipo de recurso (si es un servidor EC2, base de datos RDS, DynamoDB, entre otros), el tamaño del recurso (t2.nano, entre otros), especificación técnicas del recurso, además de la cantidad de recursos que son requeridos.

La plantilla se encuentra representada en el anexo *4.7 Listado de tipos de recursos computacionales*.

Listado de gestión de información

El listado de gestión de información contiene el detalle de los procesos de respaldo de información o limpieza de datos asociados a la solución en la nube, los cuales deben ser ejecutados continuamente en la fase de operación. Es requerido definir el ambiente de desarrollo en el cual se va a realizar la copia de seguridad o limpieza, la aplicación asociada, el nombre del proceso, tipo de gestión (limpieza de información o respaldo de información), la frecuencia que se debe realizar, el período de retención, nombre de los recursos computacionales involucrados, además el nombre de los procesos que se encargan de la automatización de la gestión (en caso de que sea necesario).

La plantilla se encuentra representada en el anexo *4.8 Listado de gestión de información*.

Matriz de responsables

El presente documento detalla mediante una matriz de responsables, los roles de la organización que está interesados en la solución en la nube. Para cada una de las aplicaciones de software identificadas, se debe detallar los roles que son encargados, responsables, consultados e informados.

La plantilla se encuentra representada en el anexo *4.9 Matriz de responsables*.

Listado de monitoreo

El listado de monitoreo contiene el detalle de los componentes de la solución en la nube que requieren llevar registro de su comportamiento (monitorear) en la fase de operación. Es requerido definir el ambiente de desarrollo en el cual se va a realizar, la aplicación de software asociada, el nombre del componente que se pretende monitorear, el tipo de componente (infraestructura, funcionalidad de aplicación, archivos log´s, entre otros), cuales los datos específicos que se deben monitorear, la frecuencia de monitoreo, cuales son los procesos asociados o encargados del monitoreo, además de tipo de acción (envió de alerta, aumentar capacidad aplicación, entro otros) a realizar una vez que se haya identificado alguna anormalidad.

La plantilla se encuentra representada en el anexo *4.10 Listado de monitoreo*.

Listado de mejora continúa

El documento de listado de mejora continua consiste en definir los componentes de la solución en la nube que requieren ser monitoreados con el fin de identificar defectos u optimizaciones con respecto a un proceso de mejora continua. Es necesario detallar el nombre de la aplicación que se encuentra asociada, el nombre del componente de mejora continua, el

nombre del componente(s) de monitoreo (el cual va a brindar la información de los datos que se están monitoreando), cuál va a ser el protocolo de análisis de datos una vez que se haya obtenidos resultados, además del protocolo de presentación de los datos a los interesados respectivos para las posibles acciones correctivas.

La plantilla se encuentra representada en el anexo *4.11 Listado de mejora continua*.

5.1.5. Matriz de referencia

Tomando como base el modelo SFIA (Skills Framework for the information Age), el cual permite identificar las habilidades de los profesionales de tecnologías de información. A continuación, se presenta una matriz de referencia entre las actividades definidas en la presente metodología y las habilidades de TI que se consideran esenciales para la ejecución de dicha actividad. Además, para cada una de las habilidades identificadas, se detalla el nivel de responsabilidad que se considera necesario.

En el anexo 3 *Habilidades y niveles de responsabilidad SFIA*, se detalla cada una de las habilidades identificadas en la matriz de referencia.

Nombre de Actividad	Habilidades y niveles responsabilidad SFIA									
	Diseño de sistemas	Análisis de datos	Diseño de redes	Administración de la seguridad	Configuración de software	Infraestructura TI	Desarrollo de software	Lanzamiento y despliegue	Realización de pruebas	Gestión del almacenamiento
	4 - 5	3 - 4	5	4 - 5	3 - 4	2 - 3	2 - 5	3 - 5	3 - 5	3-4
Identificación de requerimientos										
Identificar módulos de la solución de software	X									
Identificar flujo de tráfico de las aplicaciones	X									
Definir ambientes de desarrollo en la nube	X									
Definir acceso a la consola de los servicios de AWS	X			X						
Identificar categoría de usuarios y roles		X								
Definir acceso a los recursos computacionales de AWS	X		X	X						
Identificar método de protección de datos				X						
Identificar tipo de red virtual privada			X							
Identificar servicios en la nube	X									
Gestión de roles y politicas										
Creación de cuentas y ambientes de desarrollo					X					
Creación de roles y grupos de usuarios					X					
Creación de usuarios					X					
Creación de politicas de autorización				X	X					
Creación de llaves de cifrado					X					
Red privada virtual										
Creación de red privada en la nube						X				
Creación de red virtual privada						X				
Creación de subredes						X				
Creación de tablas de direccionamiento						X				
Creación de grupos de seguridad						X				
Creación de lista de accesso de red						X				
Creación de llaves de acceso						X				
Implementación de software										
Identificación de tipos de recursos computacionales	X						X			
Estimación de costos computacionales	X									
Creación de recursos computacionales						X				
Identificación de paquetes de desarrollo							X			
Desarrollo de aplicaciones de software							X			
Implementación de aplicaciones								X	X	
Aseguramiento de la calidad									X	
Operación y monitoreo										
Gestión de copias de seguridad										X
Gestión de limpieza de información										X
Identificación de responsables	X									
Monitoreo de aplicaciones	X									
Gestión de mejora continua	X									

Figura 7 – Matriz de referencia actividades metodología vs habilidades SFIA.

5.1.6. Plan de comunicación

A continuación, se detalla el plan de comunicación de la presente metodología, el cual consiste en detallar para cada una de las actividades, cual es la información esencial que debe ser comunicada una vez que está es finalizada, además de cuáles son los departamentos de la organización que tienen interés o necesidad de la información respectiva. Además, en la sección de notas, se especifica la relación de la información por presentar con las plantillas definidas en la metodología.

Actividad	Objetivo	Audiencia /Interesados	Notas
Identificación de requerimientos			
Identificar módulos de la solución de software	Informe de los módulos y aplicaciones de software por modulo que fueron identificados en los requerimientos de la solución de software.	Gerencia Equipo Desarrollo	Se toma como base del informe la plantilla *Listado de módulos y componentes de la solución de software.*
Identificar flujo de tráfico de las aplicaciones	Informe detallado del flujo de comunicación y transferencia de datos de las aplicaciones en la solución.	Equipo Desarrollo Equipo de infraestructura	Se toma como base del informe la plantilla *Listado de tráfico de las aplicaciones.*
Definir ambientes de desarrollo en la nube	Comunicar la cantidad de ambientes de desarrollo definidos para la infraestructura de la red privada en la nube.	Gerencia Equipo Desarrollo	

Definir acceso a la consola de los servicios de AWS	Envió de los pasos a seguir para que los usuarios puedan acceder a la interface de usuario de AWS para cada uno de los ambientes de desarrollo identificados, además de los requisitos que se deben gestionar.	Gerencia Equipo Desarrollo Equipo de infraestructura Equipo de seguridad	
Identificar categoría de usuarios y roles	Informe de los grupos de usuarios y roles que se identificaron requeridos para el desarrollo y operación de la solución.	Equipo de infraestructura	Se toma como base del informe la plantilla *Listado de grupos y roles de usuarios*.
Definir acceso a los recursos computacionales de AWS	Envió del protocolo a seguir por parte del equipo de desarrollo para poder ingresar a los recursos computacionales de AWS, además de los requisitos que se deben gestionar.	Gerencia Equipo Desarrollo Equipo de infraestructura Equipo de seguridad	
Identificar método de protección de datos	Informe de las políticas de seguridad que van a ser utilizadas en cada una de las aplicaciones de software, así cómo se van a proteger los datos utilizados	Gerencia Equipo Desarrollo Equipo de infraestructura Equipo de seguridad	La información se debe detallar/actualizar para cada una de las aplicaciones en el Listado de módulos y componentes de la solución de software
Identificar tipo de red virtual privada	Comunicación del diseño de red virtual privada que se adapta de mayor manera a los requerimientos e infraestructura en AWS	Equipo Desarrollo	
Identificar servicios en la nube	Envió del detalle de los servicios e infraestructura en la nube de AWS que van a ser utilizados en integrados en la solución.	Equipo Desarrollo Equipo de infraestructura	La información se debe detallar/actualizar para cada una de las aplicaciones en el Listado de módulos y componentes de la solución de software

Gestión de roles y políticas			
Creación de cuentas y ambientes de desarrollo	Comunicación de la información (incluyendo el número de cuenta) de las cuentas creadas en AWS.	Gerencia Equipo Desarrollo Equipo de infraestructura	
Creación de roles y grupos de usuarios	Actualización de nombres de los roles y grupos de usuarios con que fueron creados mediante el módulo de IAM.	Equipo de infraestructura	Se toma como base del informe la actualización de la plantilla *Listado de grupos y roles de usuarios*.
Creación de usuarios	Actualización de nombres de los usuarios con que fueron creados mediante el módulo de IAM.	Equipo de infraestructura	Se toma como base del informe la actualización de la plantilla *Listado de grupos y roles de usuarios*.
Creación de políticas de autorización	Comunicación del detalle de las políticas de autorización creadas para los roles y grupos de seguridad identificados en la solución.	Equipo de infraestructura	Se toma como base del informe la plantilla *Listado de políticas de autorización*.
Creación de llaves de cifrado	Actualización de los identificadores de las llaves de cifrado para la protección de datos de las aplicaciones de software en que sean requeridos.	Equipo de infraestructura	La información se debe detallar/actualizar para cada una de las aplicaciones en el *Listado de módulos y componentes de la solución de software.*
Red privada virtual			
Creación de red privada en la nube	Comunicación de la creación exitosa de la red privada en la nube (VPC), así como la información esencial de identificadores y rango de IP utilizados.	Equipo de infraestructura	

Creación de red virtual privada	Comunicación de la configuración realizada en la creación de la VPN, además de información requerida para la infraestructura en la nube.	Equipo de infraestructura	
Creación de subredes	Informe de los datos de nombres e identificadores de las subredes creadas en la cuenta de AWS, además los rangos de direcciones IP utilizados.	Equipo de infraestructura Equipo de desarrollo	La información se debe detallar/actualizar para cada una de las aplicaciones en el *Listado de módulos y componentes de la solución de software.*
Creación de tablas de direccionamiento	Envió de los detalles utilizados en la creación de las tablas de direccionamiento y como estas se encuentran asociada a las subredes y recursos orígenes y destinos del tráfico de información.	Equipo de infraestructura	
Creación de grupos de seguridad	Comunicación del detalle de los grupos de seguridad que fueron creados para la solución en la nube y que van a ser utilizados en la creación de los recursos computacionales.	Equipo de infraestructura Equipo de desarrollo	Se toma como base del informe la plantilla *Listado de grupos de seguridad*.
Creación de lista de acceso de red	Envió de los detalles utilizados en la creación de las listas de acceso.	Equipo de infraestructura	
Creación de llaves de acceso	Actualización del nombre con que fueron creadas las llaves de acceso para cada una de las aplicaciones identificadas en la solución.	Equipo de infraestructura Equipo de desarrollo	La información se debe detallar/actualizar para cada una de las aplicaciones en el *Listado de módulos y componentes de la solución de software.*
Implementación de software			

Identificación de tipos de recursos computacionales	Informe del detalle de los recursos computacionales que se identificaron como requeridos para cumplir los requerimientos de la solución en la nube.	Equipo de infraestructura Equipo de desarrollo	Se toma como base del informe la plantilla *Listado de tipos de recursos computacionales*.
Estimación de costos computacionales	Comunicación de los costos asociados a la utilización de los recursos computacionales, así como el balance con el presupuesto estimado.	Gerencia	
Creación de recursos computacionales	Informe de la creación exitosa de los recursos computacionales identificados, además de información de identificadores o rutas que se consideren requeridas.	Equipo de desarrollo	
Identificación de paquetes de desarrollo	Envió del análisis realizado de las dependencias técnicas que son requeridas para el inicio de la fase del desarrollo del software, además de rutas de repositorios o archivos que se consideren necesarios para el equipo de desarrollo.	Equipo de desarrollo	
Desarrollo de aplicaciones de software	Comunicación constante del avance y finalización de los entregables identificados en la fase de desarrollo de las aplicaciones de software.	Equipo de desarrollo	

Implementación de aplicaciones	Informe del procedimiento a utilizar para la implementación de las aplicaciones en la infraestructura de AWS, además del detalle de las posibles herramientas o procesos de automatización que deben ser configurados para su utilización en la fase de operación.	Equipo de desarrollo Equipo de gestión de liberaciones	
Aseguramiento de la calidad	Informe del procedimiento de aseguramiento de la calidad que va a ser utilizado en la solución en la nube, además del detalle de las posibles herramientas o procesos de automatización que deben ser configurados para su utilización en la fase de operación.	Equipo de desarrollo Equipo de aseguramiento de la calidad	
Operación y monitoreo			
Gestión de copias de seguridad	Informe de los componentes que requieren la creación de copias de seguridad de la información utilizada en la solución, además que deben ser ejecutados de manera constante en la fase de operación.	Equipo de infraestructura	Se toma como base del informe la plantilla *Listado gestión de información*.
Gestión de limpieza de información	Informe de los componentes que requieren una gestión de borrado de información que ya no va ser utilizada por las diferentes aplicaciones de la solución en la nube, además que deben ser ejecutados de manera constante en la fase de operación.	Equipo de desarrollo Equipo de infraestructura	Se toma como base del informe la plantilla *Listado gestión de información*.

Identificación de responsables	Envió de una matriz de responsables, con el detalle de los individuos u organización referentes para cada una de las aplicaciones de software que fueron implementadas.	Gerencia Equipo de desarrollo Equipo de infraestructura	Se toma como base del informe la plantilla *Matriz de responsables*.
Monitoreo de aplicaciones	Informe de los componentes (infraestructura, aplicaciones) que requieren ser monitoreados para obtener información específica, además de que deben ser ejecutados de manera constante en la fase de operación.	Equipo de desarrollo Equipo de infraestructura	Se toma como base del informe la plantilla *Listado de monitoreo*.
Gestión de mejora continua	Informe de los componentes (y su respectivo detalle) que van a ser utilizados en los procedimientos de mejora continua de la solución en la nube, además cuyas actividades deben ser ejecutadas de manera constante en la fase de operación.	Equipo de desarrollo Equipo de infraestructura	Se toma como base del informe la plantilla *Listado de mejora continua*.

Cuadro 1 - Plan de comunicación

5.2. Procedimiento de implementación

5.2.1. Procedimiento

Como procedimiento para ejecutar plan piloto del proyecto, se define conjunto de requerimientos funcionales y técnicos para la implementación de una solución de software en la nube de AWS, solución que va a permitir la gestión de visitantes en un condominio residencial.

Con respecto a estos requerimientos, se procede a ejecutar las actividades establecidas en los procesos de análisis de requerimientos, gestión e roles y políticas, red virtual en la nube, implementación de software, operación y monitoreo; establecidos en la metodología de implementación de aplicaciones obtenida como producto final del presente proyecto.

En la sección de pruebas y resultados se presenta la evidencia e información obtenida con la ejecución de cada una de las actividades, además del detalle de los descubrimientos identificados y correcciones respectivas.

5.2.2. Requerimientos funcionales

Se requiere la creación de una solución de software en la nube, la cual va a permitir el registro de visitantes en un condominio residencial. Para ello se debe contar con una interfaz gráfica en el cual los usuarios finales (personal de seguridad) pueden insertar, actualizar, consultar o borrar los datos de visitantes. También es posible el ingreso de visitantes al software por medio de un archivo con formato CSV, permitiendo la inserción de múltiples visitantes, teniendo como límite un máximo de 100 registros por archivo.

Se debe ingresar la información de cedula de visitante, nombre de visitante, fecha y hora de visita, además del número de casa a la cual se autorizó el ingreso.

Los datos recolectados deben permanecer almacenados por un periodo de dos años, después de ese período los registros deben ser eliminados.

5.2.3. Requerimientos técnicos

- Es requerido el uso de la infraestructura en la nube de AWS.
- Es requerido la creación de una aplicación web utilizando tecnología java.
- Los registros se deben almacenar en un motor de base de datos Mysql.
- Se requiere un plazo de dos años para la retención de la información en la base de datos.
- Se debe realizar un respaldo temporal de los registros de las aplicaciones (logs).
- Dado el tráfico de usuarios esperado (20 usuarios), no se requiere la cantidad se servidores virtuales son fijos y no se requiere escalamiento automático de los recursos computacionales.
- No se requiere VPN para la conexión con la red en la nube, sin embargo, se requiere la habilitación/autorización de un único IP de la red de la organización

5.3. Pruebas y resultados

5.3.1. Aplicación de la metodología

5.3.1.1. Análisis de requerimientos

Identificar módulos de la solución de software

Con respecto a los requerimientos para crear una solución de software de gestión de visitantes a condominio residencial, se identifica un único módulo el cual se va a denominar gestión de visitantes. El siguiente cuadro detalla las aplicaciones que se identifican para ese módulo.

Nombre de Módulo	Nombre de Aplicación	Descripción de Aplicación	Tipo Procesamiento	Frecuencia de Uso
Gestión de visitantes	Registro Individual de visitantes	Catálogo de consulta, inserción y actualización de datos de visitantes.	Tiempo real	24x7
Gestión de visitantes	Registro Masivo de visitantes	Mantenimiento para inclusión de archivo .csv para carga masiva de datos.	Tiempo real	24x7
Gestión de visitantes	Base de datos	Almacenamiento de registros de visitantes.	Tiempo real	24x7

Cuadro 2- Plan Piloto - módulos y aplicaciones de software

Identificar flujo de tráfico de las aplicaciones

A continuación, se detalla el tráfico esperado de las 3 aplicaciones para el módulo de gestión de visitantes.

Nombre de aplicación	Recurso Origen	Recurso Destino	Protocolo	Rango de puertos
Registro Individual de visitantes	186.177.56.12	Red Interna	HTTPS	443
Registro Masivo de visitantes	186.177.56.12	Red Interna	HTTPS	443
Base de datos	Registro individual / Masivo	Registro individual / Masivo	TCP	3306

Cuadro 3- Plan Piloto - tráfico de las aplicaciones

Definir ambientes de desarrollo en la nube

Para la presente solución, se identifica la necesidad de crear los siguientes ambientes de desarrollo:

- Desarrollo.
- Certificación (Staging).
- Producción.

Cada uno de los ambientes debe de tener su propia cuenta de AWS, por tanto, se van a crear 3 cuentas, las cuales se deben consolidar para generar una facturación única.

Definir acceso a la consola de los servicios de AWS

A continuación, se detalla del procedimiento necesario para que los usuarios que requieren los servicios de AWS puedan obtener ingresar a la consola.

- Mediante el uso del módulo IAM, se va a realizar de manera manual la creación de los usuarios requeridos, los cuales deben ser respectivamente asociados a las políticas de autorización necesarios.
- Una vez que el usuario es creado, se debe enviar la información de cuenta y credenciales respectivas a cada uno de los usuarios, incluyendo la contraseña inicial para el ingreso a la consola de AWS. Esta contraseña debe ser actualizada en la primera autentificación.
- Para cada usuario se debe habilitar un dispositivo virtual (Google Authenticator) que permita la autentificación de factor múltiple (MFA, Multi-Factor Authentication), por lo tanto, para acceder a la consola es requerido ingresar la contraseña y un código único generado de manera aleatoria por el dispositivo virtual.

Identificar categoría de usuarios y roles

Con respecto a la plantilla listado de grupos y roles de usuarios, el siguiente cuadro detalla los grupos de usuarios y roles del módulo de gestión de visitantes que deben ser creados en AWS.

Nombre	Tipo (Grupo usuarios / rol)	Área	Aplicación
Administradores de sistemas	Grupo de usuario	Infraestructura	
Desarrolladores	Grupo de usuario	Desarrollo de software	

Infraestructura	Grupo de usuario	Infraestructura	
QA	Grupo de usuario	Aseguramiento de la calidad	
Gestión Individual de visitantes	Rol		Registro individual de visitantes
Gestión Masiva de visitantes	Rol		Registro masivo de visitantes
Base de datos	Rol		Base de datos

Cuadro 4 - Plan Piloto - grupo de usuarios y roles

Definir acceso a los recursos computacionales de AWS

A continuación, se detalla el procedimiento para el acceso directo de los usuarios (desarrolladores, administradores de sistemas, entre otros) a los servidores virtuales en la red en la nube de AWS.

- Para cada uno de los ambientes de desarrollo establecidos para la solución de AWS, es necesario crear un servidor virtual para acceso único (JumpBox), por tanto, de manera inicial todos los usuarios deben conectarse a este servidor especifico desde su local, para posteriormente poder acceder al servidor virtual deseado. La creación del servidor acceso único permite habilitar la conexión SSH desde el internet a un único servidor virtual en la red, separando de los recursos de la red privada.
- Para el ingreso al servidor de acceso único, se requiere crear una sesión con un cliente SSH, al cual se le debe configurar el IP del servidor, además de la llave privada que fue proveída al usuario.
- Para el ingreso desde el servidor de acceso único al servidor deseado, se debe utilizar el protocolo SHH con la dirección IP privada del servidor destino.

Identificar tipo de red virtual privada

Con respecto a los requerimientos del módulo de gestión de visitantes, no se requiere la configuración de una VPN para la red privada de AWS.

Identificar servicios en la nube

Con respecto a las aplicaciones identificadas para el módulo de gestión de visitantes, el siguiente cuadro detalla los servicios de AWS que se identifican necesarios y que deben ser configurados/integrados a la aplicación específica.

Nombre de Módulo	Nombre de Aplicación	Servicios de AWS
Gestión de visitantes	Registro Individual de visitantes	EC2, Volúmenes EBS, Almacenamiento S3
Gestión de visitantes	Registro Masivo de visitantes	EC2, Volúmenes EBS, Almacenamiento S3
Gestión de visitantes	Base de datos	RDS

Cuadro 5 - Plan piloto - servicios de AWS

Identificar método de protección de datos

La protección de las solicitudes de las aplicaciones de gestión de visitantes se va a realizar por medio de una comunicación HTTPS. Para el caso de la base de datos se va a utilizar el cifrado de disco a nivel de disco. A continuación, se realiza el detalle con respecto a los datos de la plantilla de módulos y componentes de la solución.

Nombre de Módulo	Nombre de Aplicación	Método de protección de datos
Gestión de visitantes	Registro Individual de visitantes	HTTPS
Gestión de visitantes	Registro Masivo de visitantes	HTTPS

Gestión de visitantes	Base de datos	Cifrado a nivel disco por medio del proceso automático de RDS.

Cuadro 6 - Plan Piloto - métodos de protección de datos

5.3.1.2. Gestión de roles y políticas

Creación de cuentas y ambientes de desarrollo

Se procede a la creación de los 3 ambientes de desarrollo identificados en las actividades previas y los cuales fueron consolidados para obtener una única facturación de los gastos incurridos. Con respecto al tipo de soporte de las cuentas, se utiliza el plan básico.

A continuación, se detallan los números de cuenta para cada uno de los ambientes.

Ambiente	Nombre de cuenta	Número de cuenta
Desarrollo	GestionVisitantes_Desarrollo	664696267192
Certificación	GestionVisitantes_Certificacion	838086963765
Producción	GestionVisitantes_Produccion	133053031746

Cuadro 7 - Plan piloto - ambientes de desarrollo

Creación de roles y grupos de usuarios

La siguiente información detalla el nombre de los roles y grupos de usuarios que fueron creados con el módulo IAM. Cabe resaltar que cada uno de ellos fueron creados en los 3 ambientes de desarrollo de AWS.

Nombre	Nombre IAM
Administradores de sistemas	VM_Administrator_Group
Desarrolladores	VM_Developer_Group
Infraestructura	VM_Infraestructure_Group
QA	VM_QA_Group
Gestión individual de visitantes	VM_IndividualManagement_Role

Gestión masiva de visitantes	VM_MassiveManagement_Role
Base de datos	VM_DataBase_Role

Cuadro 8 - Plan piloto - grupos de usuarios y roles IAM

En la figura 7 y 8, se presentan respectivamente los registros de los grupos de usuarios y roles creados en el módulo IAM.

Group Name	Users	Inline Policy	Creation Time
VM_Administrator_Group	0		2017-03-25 23:04 CST
VM_Developer_Group	0		2017-03-25 23:04 CST
VM_Infraestructure_Group	0		2017-03-25 23:05 CST
VM_QA_Group	0		2017-03-25 23:05 CST

Figura 8 – Grupos de usuarios.

Role Name	Creation Time
VM_DataBase_Role	2017-03-25 23:12 CST
VM_IndividualManagement_Role	2017-03-25 23:11 CST
VM_MassiveManagement_Role	2017-03-25 23:12 CST

Figura 9 – Roles de usuarios.

Creación de usuarios

Para la solución de gestión de visitantes se identifican 6 usuarios (los cuales van a hacer uso de la consola de AWS) en total, 1 usuario para el grupo de administradores de sistemas, 3 usuarios desarrolladores, 1 usuarios encargado de la infraestructura, además 1 usuario en el grupo de aseguramiento de la calidad. Cada uno de estos usuarios tiene un identificador único de 8 dígitos y el cual va a ser utilizado en el nombre de usuario creado en AWS. Para el presente caso, se utiliza los mismos datos de usuarios para los tres ambientes de AWS.

Ante la creación de los usuarios, se debe de realizar los siguientes pasos para el envío de la información obtenida:

- Configuración y envió de la contraseña inicial del usuario, la cual debe ser actualizada de manera posterior a la primera autentificación.
- Creación y envió de las llaves privadas (Access Key ID y Secret Access key).
- También se debe proveer al usuario la dirección (URL) en la cual se debe autentificar para el ingreso a la consola de AWS. (La dirección es única para cada una de las cuentas creadas).

El siguiente cuadro detalla los nombres de los usuarios creados utilizando el módulo IAM, los cuales también fueron asociados al grupo de usuario respectivo.

Nombre	Tipo (Grupo usuarios / rol)	Nombre IAM	Usuarios IAM
Administradores de sistemas	Grupo de usuario	VM_Administrator_Group	VM_22548974_User
Desarrolladores	Grupo de usuario	VM_Developer_Group	VM_22543675_User VM_22514789_User VM_22543394_User
Infraestructura	Grupo de usuario	VM_Infraestructure_Group	VM_22503366_User
QA	Grupo de usuario	VM_QA_Group	VM_22543301_User

Cuadro 9 - Plan piloto - Usuarios IAM

En la figura 10 – Usuarios, se presentan los usuarios propiamente creados en el módulo IAM.

User name	Groups	Password	Last sign-in	Access keys	Creation time
VM_22503366_User	0	✔	Never	1 active	2017-03-25 23:21 CST
VM_22514789_User	0	✔	Never	1 active	2017-03-25 23:20 CST
VM_22543301_User	0		N/A	1 active	2017-03-25 23:24 CST
VM_22543394_User	0	✔	Never	1 active	2017-03-25 23:20 CST
VM_22543675_User	0	✔	Never	1 active	2017-03-25 23:19 CST
VM_22548974_User	0	✔	Never	1 active	2017-03-25 23:15 CST

Figura 10 – Usuarios.

Creación de políticas de autorización

El siguiente cuadro detalla las políticas de autorización que fueron creadas, con respecto a los servicios y niveles de acceso requeridos en la solución en la nube. Además, se realiza la asociación de las políticas con cada uno de los grupos de seguridad y roles previamente definidos. Los usuarios al estar ligado a los grupos de seguridad, obteniendo directamente las mismas políticas asignadas a los grupos.

Nombre Política	Nombre Política IAM	Nivel de acceso	Servicios AWS
Lectura EC2	VM_ReadEC2_Policy	Lectura	EC2
Escritura EC2	VM_FullEC2_Policy	Lectura, Escritura	EC2
Lectura S3	VM_ReadS3_Policy	Lectura	S3
Escritura S3	VM_FullS3_Policy	Lectura, Escritura	S3
Lectura RDS	VM_ReadRDS_Policy	Lectura	RDS
Escritura RDS	VM_FullRDS_Policy	Lectura, Escritura	RDS

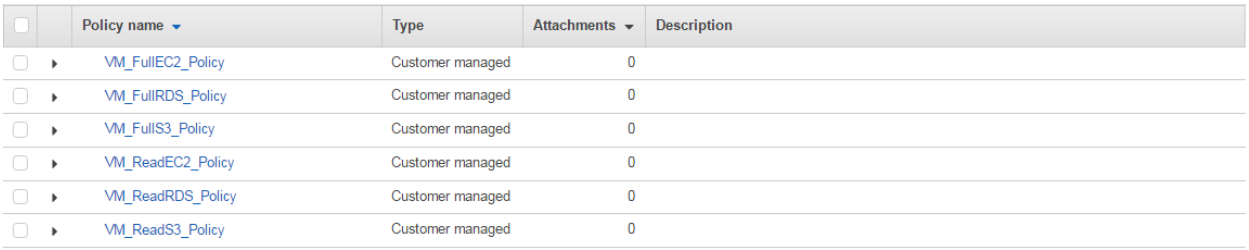
Cuadro 10 - Plan piloto - políticas IAM

Nombre	Nombre IAM	Políticas de autorización
Administradores de sistemas	VM_Administrator_Group	VM_FullEC2_Policy VM_FullS3_Policy VM_FullRDS_Policy
Desarrolladores	VM_Developer_Group	VM_ReadEC2_Policy VM_FullS3_Policy VM_ReadRDS_Policy
Infraestructura	VM_Infraestructure_Group	VM_FullEC2_Policy VM_FullS3_Policy VM_FullRDS_Policy
QA	VM_QA_Group	VM_ReadEC2_Policy VM_ReadS3_Policy VM_ReadRDS_Policy
Gestión individual de visitantes	VM_IndividualManagement_Role	VM_FullS3_Policy VM_ReadEC2_Policy

		VM_ReadRDS_Policy
Gestión masiva de visitantes	VM_MassiveManagement_Role	VM_FullS3_Policy VM_ReadEC2_Policy VM_ReadRDS_Policy
Base de datos	VM_DataBase_Role	VM_FullRDS_Policy

Cuadro 11 - Plan piloto - políticas IAM vs roles y grupos de usuarios

En la figura 11 – Políticas de autorización, se presentan las politicas propiamente creados en el módulo IAM.



Policy name	Type	Attachments	Description
VM_FullEC2_Policy	Customer managed	0	
VM_FullRDS_Policy	Customer managed	0	
VM_FullS3_Policy	Customer managed	0	
VM_ReadEC2_Policy	Customer managed	0	
VM_ReadRDS_Policy	Customer managed	0	
VM_ReadS3_Policy	Customer managed	0	

Figura 11 – Políticas de autorización.

Creación de llaves de cifrado

Dado los requerimientos y métodos de protección de datos para la solución de gestión de visitantes, no es requerida la creación de llaves de cifrado. Para el caso del cifrado a nivel de disco de la base de datos RDS, se va a hacer uso de la llave por defecto que el servicio de RDS configura en su proceso automatizado.

5.3.1.3. Red virtual en la nube

Creación de red privada en la nube

Se procede a la creación de la red privada en la nube (VPC), con respecto a los requerimientos de módulo de gestión de visitantes, se identifica la necesidad de crear una única VPC por cada uno de los ambientes de desarrollo.

A continuación, se detallan los identificadores y rango de IP utilizados para cada VPC.

Ambiente	Identificador de VPC	Bloque de direcciones IP
Desarrollo	vpc-62eba405	10.0.0.0/22
Certificación	vpc-7b99d31c	10.0.4.0/22
Producción	vpc-d28dc6b5	10.0.8.0/22

Cuadro 12 - Plan piloto - redes privadas en la nube

En la figura 12 – Red virtual privada, se presenta el registro de la red privada en la nube creada en el módulo VPC de AWS.

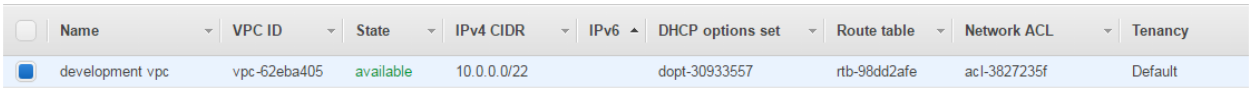


Figura 12 – Red virtual privada (VPC).

Dado de la creación de la VPC, se procede a la creación de la entrada de internet, lo cual va a permitir el tráfico entrante de internet. El registro se presenta en la figura 13 – Entrada de internet.

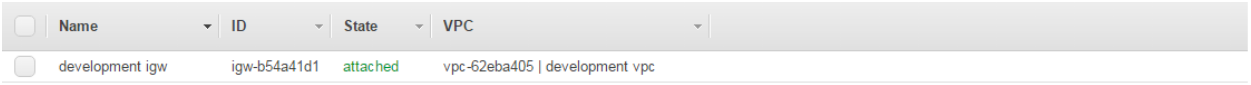


Figura 13 – Entrada de internet (Internet Gateway).

Creación de red virtual privada

Dado los requerimientos de la solución, no se requieren la creación de una red virtual privada (VPN) en la red privada de AWS.

Creación de tablas de direccionamiento

Para el caso de la subred privada, se va a hacer uso de la tabla de direccionamiento por defecto de la VPC. Sin embargo, para el caso de la red pública, es necesario a la creación de una nueva tabla de direccionamiento la

cual va a recibir en tráfico de una IP específica de internet y el cual va a ser direccionado a la red privada de AWS.

A continuación, se detalla la información para cada uno de los ambientes de desarrollo:

Ambiente	Nombre	ID	Origen	Destino
Desarrollo	Tabla para subred publica	rtb-76d82f10	186.177.56.12	igw-b54a41d1
Certificación	Tabla para subred publica	rtb-70a85516	186.177.56.12	igw-a64156c2
Producción	Tabla para subred publica	rtb-f7609391	186.177.56.12	igw-5f697d3b

Cuadro 13 - Plan piloto - tablas de direccionamiento

En la figura 14 – Tabla de direccionamiento, se presenta el registro de la tabla creada en el módulo VPC de AWS.

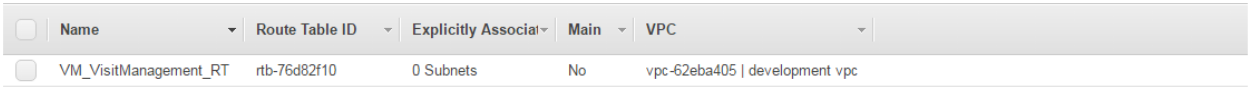


Figura 14 – Tabla de direccionamiento.

Creación de subredes

Se procede a la creación de las subredes del módulo de gestión de visitantes, se identifica la necesidad de crear dos subredes en cada uno de los ambientes de desarrollo, utilizando us-west-2 como única zona de disponibilidad.
De las dos subredes, una va a ser de tipo pública (por tanto, va a estar asociada al internet gateway) y la cual va a contener las aplicaciones para que puedan accedidas por medio de internet; la segunda subred es de tipo privada, la cual va contener la base de datos.

A continuación, se detalla los identificadores de las subredes y bloque de direcciones IP utilizadas.

Ambiente de desarrollo	Modulo	Nombre	Identificador	Bloque de direcciones IP
Desarrollo	Gestión de visitantes	VM_us-west-2	Subnet-08786850	10.0.0.0/24
Desarrollo	Gestión de visitantes	VM_Public_us-west-2	Subnet-c477679c	10.0.1.0/24
Certificación	Gestión de visitantes	VM_us-west-2	subnet-32d8c56a	10.0.4.0/24
Certificación	Gestión de visitantes	VM_Public_us-west-2	subnet-1ddac745	10.0.5.0/24
Producción	Gestión de visitantes	VM_us-west-2	subnet-3aa61d73	10.0.8.0/24
Producción	Gestión de visitantes	VM_Public_us-west-2	subnet-5ea61d17	10.0.9.0/24

Cuadro 14 - Plan Piloto - subredes

En la figura 15 – subredes, se presenta las subredes creadas en el módulo EC2 y la cuales se encuentran asociadas a la VPC previamente creada.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Availability Zone	Route Table
VM_Public_us-west-2	subnet-c477679c	available	vpc-62eba405 | development vpc	10.0.1.0/24	251	us-west-2c	rtb-76d82f10 | VM_Vi...
VM_us-west-2	subnet-08786850	available	vpc-62eba405 | development vpc	10.0.0.0/24	251	us-west-2c	rtb-98dd2afe

Figura 15 – Subredes.

Creación de grupos de seguridad

A continuación, se detalla las reglas de los grupos de seguridad requeridos en las aplicaciones del módulo de gestión de visitantes:

Ambiente	Nombre de grupo de seguridad	Id SG	Tipo regla	Tipo	Protocolo	Rango de puertos	Recurso
Desarrollo	VM_IndividualManagement_SG	sg-88cd2df3	Entrada	HTTPS	TCP	443	186.177.56.12
Desarrollo	VM_IndividualManagement_SG	sg-88cd2df3	Entrada	SSH	TCP	22	sg-0acf2f71
Desarrollo	VM_IndividualManagement_SG	sg-88cd2df3	Salida	Custom TCP Rule	TCP	3306	sg-9bd232e0
Desarrollo	VM_MassiveManagement_SG	sg-9ad535e1	Entrada	HTTPS	TCP	443	186.177.56.12
Desarrollo	VM_MassiveManagement_SG	sg-9ad535e1	Entrada	SSH	TCP	22	sg-0acf2f71
Desarrollo	VM_MassiveManagement_SG	sg-9ad535e1	Salida	Custom TCP Rule	TCP	3306	sg-9bd232e0
Desarrollo	VM_DataBase_SG	sg-9bd232e0	Entrada	Custom TCP Rule	TCP	3306	sg-88cd2df3
Desarrollo	VM_DataBase_SG	sg-9bd232e0	Entrada	Custom TCP Rule	TCP	3306	sg-9ad535e1
Desarrollo	VM_JumpBox_SG	sg-0acf2f71	Entrada	SSH	TCP	22	186.177.56.12
Desarrollo	VM_JumpBox_SG	sg-0acf2f71	Salida	SSH	TCP	22	sg-88cd2df3
Desarrollo	VM_JumpBox_SG	sg-0acf2f71	Salida	SSH	TCP	22	sg-9ad535e1
Certificación	VM_IndividualManagement_SG	sg-5916e322	Entrada	HTTPS	TCP	443	186.177.56.12
Certificación	VM_IndividualManagement_SG	sg-5916e322	Entrada	SSH	TCP	22	sg-8d16e3f6
Certificación	VM_IndividualManagement_SG	sg-5916e322	Salida	Custom TCP Rule	TCP	3306	sg-d814e1a3

Certificación	VM_MassiveManagement_SG	sg-8214e1f9	Entrada	HTTPS	TCP	443	186.177.56.12
Certificación	VM_MassiveManagement_SG	sg-8214e1f9	Entrada	SSH	TCP	22	sg-8d16e3f6
Certificación	VM_MassiveManagement_SG	sg-8214e1f9	Salida	Custom TCP Rule	TCP	3306	sg-d814e1a3
Certificación	VM_DataBase_SG	sg-d814e1a3	Entrada	Custom TCP Rule	TCP	3306	sg-5916e322
Certificación	VM_DataBase_SG	sg-d814e1a3	Entrada	Custom TCP Rule	TCP	3306	sg-8214e1f9
Certificación	VM_JumpBox_SG	sg-8d16e3f6	Entrada	SSH	TCP	22	186.177.56.12
Certificación	VM_JumpBox_SG	sg-8d16e3f6	Salida	SSH	TCP	22	sg-5916e322
Certificación	VM_JumpBox_SG	sg-8d16e3f6	Salida	SSH	TCP	22	sg-8214e1f9
Producción	VM_IndividualManagement_SG	sg-7834c103	Entrada	HTTPS	TCP	443	186.177.56.12
Producción	VM_IndividualManagement_SG	sg-7834c103	Entrada	SSH	TCP	22	sg-ae34c1d5
Producción	VM_IndividualManagement_SG	sg-7834c103	Salida	Custom TCP Rule	TCP	3306	sg-9730c5ec
Producción	VM_MassiveManagement_SG	sg-9437c2ef	Entrada	HTTPS	TCP	443	186.177.56.12
Producción	VM_MassiveManagement_SG	sg-9437c2ef	Entrada	SSH	TCP	22	sg-ae34c1d5
Producción	VM_MassiveManagement_SG	sg-9437c2ef	Salida	Custom TCP Rule	TCP	3306	sg-9730c5ec
Producción	VM_DataBase_SG	sg-9730c5ec	Entrada	Custom TCP Rule	TCP	3306	sg-7834c103
Producción	VM_DataBase_SG	sg-9730c5ec	Entrada	Custom TCP Rule	TCP	3306	sg-9437c2ef
Producción	VM_JumpBox_SG	sg-ae34c1d5	Entrada	SSH	TCP	22	186.177.56.12

Producción	VM_JumpBox_SG	sg-ae34c1d5	Salida	SSH	TCP	22	sg-7834c103
Producción	VM_JumpBox_SG	sg-ae34c1d5	Salida	SSH	TCP	22	sg-9437c2ef

Cuadro 15 - Plan piloto - grupos de seguridad

En la figura 16 – Grupos de seguridad, se presentan los registros de grupo de seguridad creados en el módulo VPC de AWS.

Name tag	Group ID	Group Name	VPC	Description
VM_MassiveManagement_SG	sg-9ad535e1	VM_MassiveManagement_SG	vpc-62eba405	VM_MassiveManagement_SG
VM_JumpBox_SG	sg-0acf2f71	VM_JumpBox_SG	vpc-62eba405	VM_JumpBox_SG
VM_IndividualManagement_SG	sg-88cd2df3	VM_IndividualManagement_SG	vpc-62eba405	VM_IndividualManagement_SG
VM_DataBase_SG	sg-9bd232e0	VM_DataBase_SG	vpc-62eba405	VM_DataBase_SG

Figura 16 – Grupos de seguridad.

Creación de lista de acceso de red

Se procede a utilizar la lista de acceso por defecto para cada una de las subredes definidas en la VPC.

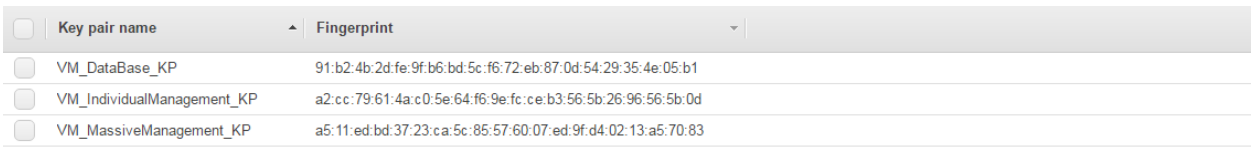
Creación de llaves de acceso

Se procede a la creación de las llaves de acceso (Key pairs) para cada una de las aplicaciones del módulo de gestión de visitantes, A continuación, se detalla la información utilizada.

Nombre de Módulo	Nombre de Aplicación	Llaves de acceso
Gestión de visitantes	Registro Individual de visitantes	VM_IndividualManagement_KP
Gestión de visitantes	Registro Masivo de visitantes	VM_MassiveManagement_KP
Gestión de visitantes	Base de datos	VM_DataBase_KP

Cuadro 16 - Plan piloto - llaves de acceso

En la figura 17 – Llaves de acceso, se presentan los registros creados en la plataforma de AWS.



Key pair name	Fingerprint
VM_DataBase_KP	91:b2:4b:2d:fe:9f:b6:bd:5c:f6:72:eb:87:0d:54:29:35:4e:05:b1
VM_IndividualManagement_KP	a2:cc:79:61:4a:c0:5e:64:f6:9e:fc:ce:b3:56:5b:26:96:56:5b:0d
VM_MassiveManagement_KP	a5:11:ed:bd:37:23:ca:5c:85:57:60:07:ed:9f:d4:02:13:a5:70:83

Figura 17 – Llaves de acceso (Key pairs).

5.3.1.4. Implementación de software

Identificación de tipos de recursos computacionales

A continuación, se detallan los recursos computacionales y sus respectivas especificaciones, los cuales son requeridos en los tres ambientes de desarrollo para la solución de gestión de visitantes.

Ambiente de desarrollo	Aplicación	Nombre Recurso	Tipo de Recurso	Tamaño de recurso	Especificaciones de recurso	Cantidad de recursos
Desarrollo	Registro Individual de visitantes	Jboss	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1
Desarrollo	Registro Masivo de visitantes	Jboss	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1
Desarollo	Registro Visitantes	JumpBox	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1
Desarrollo	Base de datos	Mysql RDS	RDS	db.t2.micro	1 CPU / 1 GB Memoria	1
Desarrollo	Registro Visitantes	Bucket para logs	S3	---------	1 GB de almacenamiento estimado	1
Certificación	Registro Individual de visitantes	Jboss	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1
Certificación	Registro Masivo de visitantes	Jboss	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1

Certificación	Registro Visitantes	JumpBox	EC2	t2.micro	1 CPU / 1 GB Memoria / 1GB volumen EBS	1
Certificación	Base de datos	Mysql RDS	RDS	db.t2.micro	1 CPU / 1 GB Memoria	1
Certificación	Registro Visitantes	Bucket para logs	S3	---------	1 GB de almacenamiento estimado	1
Producción	Registro Individual de visitantes	Jboss	EC2	t2.medium	2 CPU / 4 GB Memoria / 6GB volumen EBS	1
Producción	Registro Masivo de visitantes	Jboss	EC2	t2.medium	2 CPU / 4 GB Memoria / 6GB volumen EBS	1
Producción	Registro Visitantes	JumpBox	EC2	t2.micro	2 CPU / 4 GB Memoria / 1GB volumen EBS	1
Producción	Base de datos	Mysql RDS	RDS	db.t2.medium	2 CPU / 4 GB Memoria	1
Producción	Registro Visitantes	Bucket para logs	S3	---------	6 GB de almacenamiento estimado	1

Cuadro 17 - Plan piloto - tipos de recursos computacionales

Estimación de costos computacionales

Se procede a la estimación de los costos asociados a los recursos computacionales requeridos para la solución de gestión de visitantes.

Ambiente	Detalle por recursos	Total Mensual
Desarrollo	3 x t2.micro = 0.012 / hora 1 x db.t2.micro = 0.017 / hora S3 1 GB = 0.023 / mes EBS 3 GB = 0.10 / mes	$ 38.483
Certificación	3 x t2.micro = 0.012 / hora 1 x db.t2.micro = 0.017 / hora S3 1 GB = 0.023 / mes EBS 3 GB = 0.10 / mes	$ 38.483
Producción	2 x t2.medium = 0.047 / hora 1 x t2.micro = 0.012 / hora 1 x db.t2.medium = 0.068 / hora S3 6 GB = 0.023 / mes EBS 13 GB = 0.10 / mes	$ 125.418

Cuadro 18 - Plan piloto - estimación de costos computacionales

Creación de recursos computacionales

La creación de los recursos computacionales no se incluye como parte del alcance del plan piloto. Sin embargo, se detalla toda la información previamente definida para cada aplicación del módulo de gestión de visitantes y que es utilizada en la creación de los recursos computacionales.

Ambiente	Aplicación	Tipo de recurso	Parámetros
Desarrollo	Registro Individual de visitantes	EC2 t2.micro	Vpc id: vpc-62eba405 Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_IndividualManagement_SG Llave de acceso: VM_IndividualManagement_KP
Desarrollo	Registro Masivo de visitantes	EC2 t2.micro	Vpc id: vpc-62eba405 Rol: VM_MassiveManagement_Role

			Subred: VM_Public_us-west-2 Grupo seguridad: VM_MassiveManagement_SG Llave de acceso: VM_MassiveManagement_KP
Desarrollo	Base de datos	RDS db.t2.micro	Vpc id: vpc-62eba405 Rol: VM_DataBase_Role Subred: VM_us-west-2 Grupo seguridad: VM_DataBase _SG Llave de acceso: VM_DataBase _KP
Desarrollo	Registro Visitantes	EC2 t2.micro	Vpc id: vpc-62eba405 Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_JumpBox_SG Llave de acceso: VM_IndividualManagement_KP
Certificación	Registro Individual de visitantes	EC2 t2.micro	Vpc id: vpc-7b99d31c Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_IndividualManagement_SG Llave de acceso: VM_IndividualManagement_KP
Certificación	Registro Masivo de visitantes	EC2 t2.micro	Vpc id: vpc-7b99d31c Rol: VM_MassiveManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_MassiveManagement_SG Llave de acceso: VM_MassiveManagement_KP
Certificación	Base de datos	RDS db.t2.micro	Vpc id: vpc-7b99d31c Rol: VM_DataBase_Role Subred: VM_us-west-2 Grupo seguridad: VM_DataBase _SG Llave de acceso: VM_DataBase _KP
Certificación	Registro Visitantes	EC2 t2.micro	Vpc id: vpc-7b99d31c Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_JumpBox_SG Llave de acceso: VM_IndividualManagement_KP
Producción	Registro Individual	EC2 t2.	Vpc id: vpc-d28dc6b5

	de visitantes	medium	Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_IndividualManagement_SG Llave de acceso: VM_IndividualManagement_KP
Producción	Registro Masivo de visitantes	EC2 t2. medium	Vpc id: vpc-d28dc6b5 Rol: VM_MassiveManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_MassiveManagement_SG Llave de acceso: VM_MassiveManagement_KP
Producción	Base de datos	RDS db.t2. medium	Vpc id: vpc-d28dc6b5 Rol: VM_DataBase_Role Subred: VM_us-west-2 Grupo seguridad: VM_DataBase _SG Llave de acceso: VM_DataBase _KP
Producción	Registro Visitantes	EC2 t2.micro	Vpc id: vpc-d28dc6b5 Rol: VM_IndividualManagement_Role Subred: VM_Public_us-west-2 Grupo seguridad: VM_JumpBox_SG Llave de acceso: VM_IndividualManagement_KP

Cuadro 19 - Plan piloto - Creación de recursos computacionales

Identificación de paquetes de desarrollo

El siguiente listado detallada los paquetes de desarrollo requeridos para la fase de desarrollo de las aplicaciones del módulo de gestión de visitantes.

- Java 7 JDK
- Jboss 5.1
- Librería Mysql 5.6
- AWS java sdk 1.11.105

Desarrollo de aplicaciones de software

El desarrollo (creación de código fuente) propiamente de las aplicaciones no se incluye como parte del alcance del plan piloto.

Implementación de aplicaciones

Para el módulo de gestión de visitantes, se define un procedimiento manual para la implementación/liberación de las aplicaciones en los recursos computacionales de la red privada de AWS. A continuación, se detalla el procedimiento a seguir:

- Seguido de la creación o actualización del código fuente de las aplicaciones, se procede a la liberación de la aplicación en el ambiente de AWS.
- La implementación de las aplicaciones se debe realizar de manera local, en la cual se va a obtener un archivo de formato ".war" con la aplicación Java.
- El archivo debe ser enviado mediante el protocolo FTP al servidor de acceso único para el ambiente de desarrollo específico que se esté trabajando.
- El archivo se debe trasladar mediante SSH, del servidor de acceso único al servidor configurado para la aplicación.
- Ya en el servidor destino, se debe reciclar el aplicativo con la nueva versión de la aplicación.
- La implementación de las aplicaciones en los ambientes de certificación y producción, se debe obtener la aprobación por parte del equipo de aseguramiento de calidad, en la cual se detalla el éxito de las pruebas funcionales en el ambiente de desarrollo previo.

Aseguramiento de calidad

Con respecto al aseguramiento de la calidad de las aplicaciones involucradas en el módulo de gestión de visitantes, se detalla el procedimiento a realizar por parte el equipo de calidad:

- La actividad de aseguramiento de la calidad se va a realizar de manera secuencial con la fase de desarrollo de las aplicaciones.
- El conjunto de pruebas se debe realizar con respecto a los ambientes de desarrollo establecidos, se inicia con el ambiente de certificación, con respecto a los resultados obtenidos se procede o no al ambiente de producción.
- Una vez finalizado la implementación/liberación de la aplicación específica en el ambiente de AWS, se procede al inicio de pruebas funcionales de la aplicación. Para ello se debe recibir una notificación por parte del equipo encargado que la implementación ha se completado.
- El conjunto de pruebas se va a realizar de manera manual por parte del o los miembros del equipo de aseguramiento de la calidad.
- Se deben ejecutar el conjunto de casos de pruebas definidos para la aplicación específica. La ejecución de las pruebas se debe realizar de manera local, apuntando a las direcciones (URL) en el ambiente de AWS correspondientes para la aplicación.
- Para el caso en que los casos de pruebas sean exitosos se procede a la aprobación de las aplicaciones, para el escenario contrario, se debe reportar la excepción al equipo de desarrollo para su respectiva corrección.

5.3.1.5. Operación y monitoreo

Gestión de copias de seguridad

Con respecto a las copias de seguridad para el módulo de gestión de visitantes, se identifica el requerimiento de realizar copias de seguridad para la base de datos en la nube (RDS) en la cual se va almacenar los datos transaccionales de la solución. El proceso se va a realizar únicamente para el ambiente de producción, además se va a utilizar a la configuración automática que provee RDS para la gestión de respaldos.

También se requiere una copia de seguridad de los archivos de registros de las aplicaciones (Log´s), los cuales va a ser depositados en el servicio de almacenamiento S3.

A continuación, se detalla la información con respecto a la plantilla gestión de información:

Ambiente	Nombre	Tipo	Frecuencia	Periodo retención	Recursos	Procesos
Producción	Respaldo RDS	Respaldo	Diario a las 11 pm	Un mes	RDS	Configuración en RDS para respaldo automático.
Desarrollo / Certificación / Producción	Respaldo de log´s	Respaldo	Diario 10 pm	15 Días	S3 Bucket	Script bash de copiado de los log´s del día al bucket de S3.

Cuadro 20 - Plan piloto - copias de seguridad

Creación de limpieza de información

Con respecto a los requerimientos del módulo de gestión de visitantes, se identifica la necesidad de borrar los datos transaccionales de los visitantes que se encuentran almacenados en la base de datos con una antigüedad mayor a dos años; además se requiere el borrado de los archivos de registros de las aplicaciones (Log´s).

A continuación, se presenta el detalla de cada uno de ellos:

Ambiente	Nombre	Tipo	Frecuencia	Periodo	Recursos	Procesos
Desarrollo /Certificación /Producción	Borrado de log´s de aplicaciones	Limpieza de información	Diario a las 10:30 pm	1 día.	Servidores EC2 de la aplicación	Script bash de borrado del log diario, una vez que se haya finalizado la copia a S3.
Producción	Borrado de registros con antigüedad de dos años	Limpieza de información	Diario a las 10 pm.	2 años.	RDS	Script Python con conexión RDS y borrado de todos los registros con fecha de ingreso mayor a dos años.

Cuadro 21 - Plan piloto - limpieza de información

Identificación de responsables

La siguiente matriz detalla los equipos responsables de las aplicaciones desarrolladas en el módulo gestión de visitantes:

Aplicaciones	Equipo de desarrollo 1	Equipo de desarrollo 2	Equipo de infraestructura
Registro Individual de visitantes	X		
Registro Masivo de visitantes		X	
Base de datos			X

Cuadro 22 - Plan piloto - matriz de responsables de aplicación

Monitoreo de aplicaciones

Para el monitoreo de las aplicaciones del módulo de gestión de visitantes, se identifica la necesidad de monitorear el comportamiento del espacio disponible en la base de datos RDS, para el caso en que se supere el 85 % de la capacidad, se requiere él envió de correos de notificación.

A continuación de detalla la información con respecto a la plantilla monitoreo de aplicaciones:

Ambiente	Aplicación	Nombre	Tipo	Datos a monitorear	Frecuencia	Procesos	Acción
Producción	Base de datos	Monitoreo Capacidad de RDS	Informativo	Espacio de almacenamiento disponible. Se activa en caso de que el espacio utilizado sea mayor a 85 % de la capacidad.	Cada 30 minutos	Configuración de alerta cloudwatch en la instancia de base de datos RDS.	Envió de alerta por correo

Cuadro 23 - Plan piloto - monitoreo de aplicaciones

Gestión de mejora continua

Con respecto a los requerimientos y alcance del módulo de gestión de visitantes, no se definen componentes para la actividad de mejora continua.

5.3.2. Resultados

Nombre de actividad	Resultados
Identificación de requerimientos	
Identificar módulos de la solución de software	Se evalúa la inclusión de información en la cual se describa de forma breve cada una de las aplicaciones identificadas para la solución. Se agrega una nueva columna "Descripción" en la plantilla respectiva.
Identificar flujo de tráfico de las aplicaciones	Se ejecuta de manera exitosa.
Definir ambientes de desarrollo en la nube	Se ejecuta de manera exitosa.
Definir acceso a la consola de los servicios de AWS	Se ejecuta de manera exitosa.
Identificar categoría de usuarios y roles	Se debe resaltar que el dato *de aplicación asociada* es un dato opcional para los registros de tipo grupo de usuarios, además el dato *de área en la organización* únicamente aplica para los grupos de usuarios.
Definir acceso a los recursos computacionales de AWS	Se ejecuta de manera exitosa.
Identificar tipo de red virtual privada	Se ejecuta de manera exitosa.
Identificar servicios en la nube	Se ejecuta de manera exitosa.
Identificar método de protección de datos	Se ejecuta de manera exitosa.
Gestión de roles y políticas	
Creación de cuentas y ambientes de desarrollo	Es necesario incluir en la actividad, el análisis del plan de soporte que es requerido por parte del equipo de AWS, para las cuentas de la organización.
Creación de roles y grupos de usuarios	Se replantea el formato recomendado para el nombre del grupo de usuario, en el cual se incluye el código del módulo en el cual se encuentra asociada, además del nombre propiamente asignado al grupo de usuario.
Creación de usuarios	Para la creación de usuarios es requerido conocer cuáles son los usuarios específicos que van a estar involucrados en la solución en la nube, por lo que se procede a agregar la acotación en la sección de supuestos del proceso. Se procede a replantear el formato recomendado del tipo de usuario a crear en el módulo IAM, en el cual se elimina el tipo de usuario y se agrega el código del módulo asociado.
Creación de políticas de autorización	Dado que las políticas de autorización

	pueden definir acciones de múltiples servicios de AWS, se procede a cambiar el nombre de servicio del estándar recomendado y se agrega el código del módulo. Se identifica la necesidad de agregar en la plantilla una columna en el cual se puede agregar de manera opcional los identificadores de los recursos (ARN) que tienen autorización a utilizar la política.
Creación de llaves de cifrado	Se ejecuta de manera exitosa.
Red privada virtual	
Creación de red privada en la nube	Se identifica la necesidad de agregar la información del componente entrada de internet (Internet gateway), el cual debe ser configurado para el caso de soluciones en la nube que esperan tráfico proveniente de internet, por ende, se deben crear subredes públicas.
Creación de red virtual privada	Se ejecuta de manera exitosa.
Creación de subredes	Se considera la necesidad de resaltar en el detalle de la actividad, las direcciones IP que se encuentran reservas por parte de AWS para cada una de las subredes. Dado que pueden existir más de una subred por modulo o aplicación de la solución en la nube, se procede a separar de la plantilla *Listado módulos y aplicaciones*, los datos de subred y rango de direcciones IP, por lo q se crear la plantilla *Listado de subredes.*
Creación de tablas de direccionamiento	Se identifica la necesidad de mover la actividad de creación de tablas de direccionamiento, antes de la actividad de creación de subredes. Para el caso en la cual se ocupan subredes publica, es necesario configurar de antemano la tabla de direccionamiento asociada a la entrada de internet (Internet gateway). Se corrigen los datos de destino y origen en la configuración de tablas direccionamiento, ya que se presentabas de manera inversa.
Creación de grupos de seguridad	Se identifica la necesidad de agregar el identificador del grupo de seguridad en la información del documento de salida; identificar que se obtiene una vez creado el grupo de seguridad en AWS.
Creación de lista de acceso de red	Se ejecuta de manera exitosa.

Creación de llaves de acceso	Se procede a resaltar en el detalle de la actividad, los datos de llaves de confianza que se obtienen al finalizar la creación de las llaves de acceso; además en que momento deben ser utilizadas.
Implementación de software	
Identificación de tipos de recursos computacionales	Se ejecuta de manera exitosa.
Estimación de costos computacionales	Se ejecuta de manera exitosa.
Creación de recursos computacionales	Se ejecuta de manera exitosa.
Identificación de paquetes de desarrollo	Se ejecuta de manera exitosa.
Desarrollo de aplicaciones de software	Se ejecuta de manera exitosa.
Implementación de aplicaciones	Se procede agregar en la especificación de la tarea, el escenario en el cual se deben gestionar las versiones anteriores de imágenes AMI.
Aseguramiento de la calidad	Se ejecuta de manera exitosa.
Operación y monitoreo	Se ejecuta de manera exitosa.
Gestión de copias de seguridad	Se ejecuta de manera exitosa.
Gestión de limpieza de información	Se ejecuta de manera exitosa.
Identificación de responsables	Se ejecuta de manera exitosa.
Monitoreo de aplicaciones	Se ejecuta de manera exitosa.
Gestión de mejora continua	Se ejecuta de manera exitosa.

Cuadro 24 - Plan Piloto - Resultados

6. Capítulo VI – Análisis Financiero

6.1. Análisis de ingresos

El detalle de los ingresos del análisis financiero, se va a determinar con respecto al ahorro que conlleva el uso de la metodología de implementación de aplicaciones de software en Amazon Web Services, en los proyectos estimados para el período en estudio; contrarrestado con el costo estimado de los proyectos ejecutados sin la metodología.

El ahorro de los costos asociados a los proyectos que utilizan la metodología, se determina de acuerdo la disminución de la curva de aprendizaje (por parte del equipo de trabajo) de los procesos de infraestructura, seguridad, implementación de software, monitoreo y mantenimiento; utilizando de los servicios en nube de AWS. Además del ahorro de tiempo al utilizar las actividades estandarizadas definidas en la metodología.

Con respecto a la estrategia de la organización patrocinadora, se estima la ejecución de 2 proyectos anuales, los cuales se categorizan como proyectos pequeños o proyectos mediados, de acuerdo con la cantidad de recursos y tiempo de ejecución. Para este caso específico se estima la ejecución anual de 1 proyecto pequeño y 1 proyecto mediano.

Con base en el juicio de un experto, el ahorro en los costos incurridos del proyecto utilizando la metodología, se determina con respecto al tiempo que no consumido en las tareas de investigación y pruebas de concepto en el cronograma del proyecto. Por lo que se procede a realizar una estimación de actividades para proyectos de tipo pequeño y mediano, en los cuales se estiman las tareas totales, además propiamente de las tareas de investigación.

A continuación, se detallan los costos estimados para las categorías de proyecto.

Proyectos	Cantidad recursos	Tiempo Estimado	Costo Estimado	Ahorros
Pequeño	2	2 meses	$21,280.00	$4,480.00
Mediano	4	2 meses	$44,520.00	$5,320.00

Cuadro 25 - Categoría de proyectos

6.2. Análisis de inversión inicial

A continuación, se presenta el conjunto de tareas involucradas en el desarrollo del proyecto, las cuales determinan la inversión inicial que se debe incluir en el flujo de caja.

Nombre	Duración	Cantidad de Horas
Capítulo V - Solución del Problema	**56d**	**336**
Desarrollo de la Solución	**41d**	**246**
Procesos de metodología	**24d**	**144**
Identificación de requerimientos	4d	24
Gestión de políticas y roles	5d	30
Infraestructura	5d	30
Implementación de software	5d	30
Operación y monitoreo	5d	30
Flujos de actividades de metodología	5d	30
Plantillas de documentación	4d	24
Matriz de referencia (roles TI vs procesos metodología)	4d	24
Plan de comunicación	4d	24
Procedimiento de Implementación	10d	60
Pruebas y resultados	3d	18
Capacitación y acompañamiento	15d	90

Cuadro 26 - Tareas de desarrollo de proyecto

El costo del recurso humano encargado de la ejecución de las tareas tiene un costo por hora de $30, costo que incluyen los gastos fijos (internet, electricidad, oficina, entre otros) incurridos para el desarrollo del proyecto.

Dado un total de 336 horas para el desarrollo del proyecto, se determina que la inversión inicial de $10,080.00 (336 horas x $30).

6.3. Datos

A continuación, se presenta el detalle de los valores que son utilizados en el flujo de caja.

Descripción	Valor
Periodo de Flujo de caja	6 años
Inversión Inicial	$10,080.00
Inflación	5%
Tasa de descuento	5%
Ahorro de costos para periodo inicial	$9,800.00

Cuadro 27 - Datos de flujo de caja

6.4. Flujo de caja

Periodo	0	1	2	3	4	5	6
Ahorro en costos		9800	10,290.00	10,804.50	11,344.73	11,911.96	12,507.56
Ingresos Totales		**9,800.00**	**10,290.00**	**10,804.50**	**11,344.73**	**11,911.96**	**12,507.56**
Inversión Inicial	10080						
Egresos	**(10,080.00)**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
Utilidad		9,800.00	10,290.00	10,804.50	11,344.73	11,911.96	12,507.56
Utilidad Neta	**(10,080.00)**	**9,800.00**	**10,290.00**	**10,804.50**	**11,344.73**	**11,911.96**	**12,507.56**
Periodo de recuperación		(280.00)	10,010.00	20,814.50	32,159.23	44,071.19	56,578.75
Indicadores Financieros							
PER			**0.33**				
VAN		**$45,920.00**					
TIR		100%					

ID (índice de deseabilidad)		$4.56					

Cuadro 28 - Flujo de caja

6.5. Resultados

Con respecto a los datos anteriores, se obtienen los siguientes resultados:

- El tiempo requerido para recuperar la inversión inicial (periodo de recuperación) se encuentra en el mes **0.33 del año 2**.
- Con respecto a la utilidad neta de los 6 periodos identificados en el flujo de caja y tasa de descuento de un 5%, se determina que el Valor Actual Neto (VAN) del proyecto es de **$45,920.00**.
- La tasa máxima de interés (TIR) que el proyecto soporta es de un **100%**.
- El índice de deseabilidad por cada dólar invertido es de **$4.56**.
- De acuerdo con los indicadores financieros obtenidos, en los cuales se demuestra una ganancia con respecto a la inversión realizada, además se considera aceptable el tiempo requerido para recuperar la inversión; se determina que el proyecto es financieramente factible.

7. Capítulo VII - Conclusiones y recomendaciones

7.1. Conclusiones

1. Con base en la información recolectada en la investigación y desarrollo de la metodología, se identifica el proceso de infraestructura como pilar para la creación de una red privada y solución de software en la nube de AWS. Por lo que el estado de las actividades definidas para el equipo de infraestructura tiene un impacto superior en desarrollo de un proyecto específico.
2. Además de las ventajas identificadas del modelo SFIA en los objetivos del proyecto, en la cual se asocia las actividades definidas en la metodología con las habilidades de tecnología de información requeridas por parte del equipo de trabajo; es posible analizar los departamentos de la organización y su respectiva línea de tiempo, en la cual deben ser involucrados en el desarrollo de la solución en la nube.
3. Con el análisis de la investigación teórica y metodológica del proyecto, con respecto a los procesos de infraestructura, seguridad, desarrollo de software, monitoreo y mantenimiento para el desarrollo de soluciones en la nube de AWS; se resalta la importancia de una arquitectura de alta disponibilidad en las aplicaciones de software, lo cual se trató de reflejar en las actividades definidas en la metodología y el uso respectivo de las zonas de disponibilidad de AWS para soportar este escenario.
4. Con respecto al modelo de infraestructura como servicio de AWS, se identifica una variable constante para optimizar o reducir los costos asociados al uso de los recursos computacionales. Lo cual se encuentra directamente ligado a la innovación de herramientas para automatizar la creación de los recursos a demanda, además de servicios para evitar el uso innecesario de servidores virtuales.

7.2. Recomendaciones

1. Tener un enfoque constante de técnicas de seguridad en la totalidad de las actividades involucradas en el desarrollo de una aplicación de software en la nube. Esto a pesar de que en la metodología se definen actividades específicas para definir los métodos de protección de datos y tráfico de la red privada virtual.
2. Involucrar múltiples áreas de la organización (desarrollo de software, infraestructura, operaciones, gerencia) en el uso de la metodología, desde la etapa inicial de la iniciativa, esto por parte de los equipos de trabajo específicos; con el fin de evitar conflictos de comunicación e identificación de responsabilidades.
3. Incluir un enfoque en la metodología, en el cual se pueda identificar o evaluar el nivel de maduración de las soluciones en la nube, especialmente para organizaciones que tienen experiencia previa en la nube de AWS y han logrado superar la curva de aprendizaje. Se identifica un proceso de maduración en el uso del modelo de infraestructura en la nube de AWS, en la cual se optimiza el uso y creación recursos computacionales.
4. Evaluar modelos de ciclos de vida del servicio que aporten información de estándares y mejoras prácticas para el desarrollo y constante evaluación de los elementos identificados. Esto con respecto a las actividades de monitoreo y operación de la solución en la nube, en las cuales se indican cuales elementos son requeridos en esta fase especifica.

8. Capítulo VIII – Análisis Retrospectivo

El desarrollo del proyecto presentó un reto personal y profesional, en el cual fue posible expandir los conocimientos de infraestructura, seguridad y red en la nube de AWS, los cuales implican experticia de múltiples áreas de tecnologías de información y no únicamente del desarrollo del software. Además, se logra tener una visión global de los componentes, habilidades y equipos de trabajo que se encuentran involucrados en iniciativas de soluciones en la nube.

El poder plantear ese conocimiento adquirido en una metodología, fue de gran importancia, ya que es posible facilitar el esfuerzo de curva de aprendizaje de organizaciones y profesionales de TI, que se encuentran incursionando en las tecnologías de AWS.

Con respecto a los objetivos establecidos en el plan inicial, estos se cumplieron de manera exitosa, obteniendo como resultado el desarrollo de la metodología, incluyendo un plan de comunicación en la ejecución de las actividades específicas y una matriz de referencia en el cual se recomienda las habilidades que el equipo de tecnología de información debe tener para la ejecución de la metodología.

El proceso investigación de áreas de infraestructura, seguridad, desarrollo de software, operación y monitoreo de la nube de AWS, en conjunto con los insumos obtenidos de manera directa con expertos en arquitectura en soluciones en la nube: permitió tener una visión clara del esfuerzo holístico que con lleva la implementación de aplicaciones utilizando la infraestructura como servicio de AWS, lo cual se trató de plantear en los procesos y actividades definidos en la metodología.

En el desarrollo del proyecto y ejecución del plan piloto, no se identificó ninguna variación o dificultad que comprometiera la trayectoria del proyecto, propiamente en los resultados del plan piloto, se identifican áreas de mejora

para facilitar el uso de la metodología, las cuales se modificaron de manera inmediata en el detalle de las actividades.

9. Referencias bibliográficas

451 Research . (2015). *451 Research.* 451 Research Vendor Window.

Amorin, K., NH, S., & AlAuf, L. (2015). *CloudWhip: A Tool for Provisioning Cyber Security Labs in the Amazon Cloud.* Northeastern University, Boston.

Arcus Global. (2014). *Amazon DynamoDB.* Arcus Global Ltd.

Arpitha, M. (2016). *The Performance Computing of Oracle Database on AWS Cloud Storage.* IJCST.

Associates Apps. (2015). *Amazon Aurora - A Fast, Affordable and Powerful RDBMS.* Apps Associates LLC.

Atkinson, R. (1999). Project management: cost, time and quality, two best guesses and a phenomenon, its time to accept other success criteria. *International Journal of Project Management*, Vol. 17, No. 6, pp. 337-342.

Attarzadeh, I. (2008). *Project Management Practices: The Criteria for Success or Failure.* International Business Information.

AWS. (2014). *Amazon Relational Database Service User Guide.* Amazon Web Services, Inc.

AWS. (2014). *Amazon Relational Database Service User Guide.* Amazon Web Services, Inc.

AWS. (2015). *Cloud Computing withAmazon Web Services*. Obtenido de https://aws.amazon.com/what-is-aws/.

AWS. (2016). Amazon Elastic Compute Cloud: User Guide for Linux Instances. Amazon Web Services, Inc.

AWS. (2016). *Amazon Virtual Private Cloud Network Administrator Guide.* Amazon Web Services, Inc.

AWS. (2016). *Amazon Virtual Private Cloud User Guide.* Amazon Web Services, Inc.

AWS. (2016). *AWS Command Line Interface User Guide.* Amazon Web Services, Inc.

AWS. (2016). *AWS Identity and Access Management User Guide.* Amazon Web Services, Inc.

AWS. (2016). *AWS Key Management Service Developer Guide.* Amazon Web Services, Inc.

AWS. (2016). *Tipos de almacenamiento de Amazon S3.* Recuperado el 11 de 10 de 2016, de https://aws.amazon.com/s3/storage-classes/

AWS. (2016). *Tipos de instancias de Amazon EC2.* Recuperado el 10 de Octubre de 2016, de Amazon Web Services: https://aws.amazon.com/ec2/instance-types/

AWS. (2016). *Tools for Amazon Web Services*. Recuperado el 22 de 10 de 2016, de https://aws.amazon.com/tools/

AWS. (s.f.). *Tipo de instancias de Amazon EC2.* Recuperado el 10 de Octubre de 2016, de https://aws.amazon.com/ec2/instance-types/

Badwan, F., Tawfiq, K., Sleit, A., & Misk, N. (2013). *Cloud Computing challenges with emphasis on Amazon EC2 and Windows Azure.* International Journal of Computer Networks & Communications.

Balduzzi, M., & Zaddach, J. (2012). *A Security Analysis of Amazon's Elastic Compute Cloud Service.* Eurocom.

Baron, J. (2010). *Storage Options in the AWS Cloud.* Amazon Web Services.

Battaglia, M. (2008). Nonprobability Sampling. En P. Lavrakas, *Encyclopedia of Surbey Research Methods.* SAGE Publications.

Berman, S., Kesterson, L., Marshall, A., & Srivathsa, R. (2012). *The power of cloud - Driving business model innovation.* IBM Institute for Business Value.

Bondi, A. (2000). haracteristics of scalability and their impact on performance. Proceedings of the second international workshop on Software and performance. *WOSP '00*, Pages 195-203 .

Boudriga, N. (2010). Security of mobile communications. *CRC Press*, pp. 32–33.

Bourke, C. (2015). *Introduction to Git.* Lincoln,: University of Nebraska–Lincoln.

Bowen, G. (2009). *Document Analysis as a Qualitative.* Qualitative Research Journal.

Brantley, W. (2007). *The Five Secrets to Project Success.* Villanova University.

Brantner, M., Florescu, D., Graf, D., Kossmann, D., & Kraska, T. (2008). *Building a Database on S3.* Research Gate.

Bugie, S., Nürnberger, S., & Thomas, P. (2011). *AmazonIA: When Elasticity Snaps Back.* Information Security & Cryptography Group.

Bugiotti, F., & Cabibbo, L. (2013). *A Comparison of Data Models and APIs of NoSQL Datastores.* Universit`a Roma Tre.

Burns, N., & Grove, S. (2001). *The Practice of Nursing Research: Conduct, Critique & Utilization.* Pennsylvania: Saunders.

Citrix. (2013). *Citrix XenApp on AWS: Reference Architecture.* Citrix Systems, Inc.

Cloudera. (2016). *Cloudera Enterprise Reference Architecture for AWS Deployments.* Cloudera Inc.

Comer, D. (2009). *Computer Networks and Internets.* New Jersey: Pearson Education, Inc.

Detmer, E. (2015). *Connecting On-Premise Systems to Cloud Infrastructure.* Decision First Technologies.

Digest, T. A. (2011). *Amazon's Availability Zones.* Sombers Associates, Inc.

Dörnyei, Z. (2007). *Comparison of Convenience Sampling and Purposive Sampling.* New York: Oxford University Press.

EntArchs. (2016). *DevOp(tion)s for Enterprises.* EntArchs Agile Architecture Consulting.

Fortinet. (2015). *FortiGate-AWS Deployment Guide.* Fortinet.

Fowler, M. (2007). *Continuous Integration*. Recuperado el 26 de 10 de 2016, de http://www.martinfowler.com/articles/continuousIntegration.html

Frankel , S., Kent , K., Lewkowski , R., Orebaugh , A., Ritchey, R., & Sharma, S. (2005). *Guide to IPsec VPNs.* Gaithersburg: National Institute of Standards and Technology.

Fundation, S. (2016). *What is SFIA.* Recuperado el 01 de 10 de 2016, de http://www.sfia-online.org/about-sfia/what-is-sfia/

Gandhi, V., & Kumbharana, C. (2016). *Comparative study of Amazon EC2 and Microsoft Azure cloud architecture.* International Journal of Advanced Networking Applications.

Garfinkel, S. (2007). *An Evaluation of Amazon's Grid Computing Services: EC2, S3, and SQS.* Harvard Computer.

Garfinkel, S. (2007). *commodity grid computing with Amazon´s S3 and EC2.* Usenix.

Garnaat, M. (2016). *boto Documentation.* Boto.

Gartner. (2015). *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide.*

Gartner. (2016). *Magic Quadrant for Cloud Infrastructure as a Service, Worldwide.* Gartner.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, 204: 291-295.

Gorelik, E. (2013). *Cloud Computing Models.* Massachusetts Institute of Technology.

Group, N. W. (2006). *The Secure Shell (SSH) Protocol Architecture.* SSH Communications Security Corp.

Hao, C. (2014). *A Survey and Classification of Privacy-Preservation Mechanisms for Cloud Data Management.* University Magdeburg.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la investigación.* México D.F: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación.* México D.F: McGraw-Hill.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de La Investigación.*

Hogberg, D. (2012). *An Applied Evaluation and Assessment of Cloud Computing Platforms.* Umea University.

Hox, J., & Boeije, H. (2005). Data Collection, Primary vs. Secondary. En L. Kimberly, *Encyclopedia of social measurement* (págs. 593-560). Elsevier Inc.

Incorvaia, L. (2014). *Cloud Computing Deployment and Service Models.* Reliable Solutions Group.

Institute, P. M. (2004). *A guide to the project management body of knowledge (PMBOK guide).* Newtown square: Project Management Institute.

Jafar, A. (2014). *The Research Study on DynamoDB – NoSQL Database Service.* International Journal of Computer Science and Information Technology.

Jugdev, K. (2012). Learning from Lessons Learned: Project Management Research Program. *American Journal of Economics and Business Administration*, 4 (1): 13-22.

Kiran, S., Shetty, S., & Hong, L. (2016). *Generation of Labelled Datasets to Quantify the Impact of Security Threats to Cloud Data Centers.* Scientific Research Publishing Inc.

Kokkinos, P., Varvarigou, T., Kretsis, A., Soumplis, P., & Varvarigos, E. (2013). *Cost and Utilization Optimization of Amazon EC2 instances.* IEEE Computer Society.

KPMG. (2011). *The Cloud - Changing the Business Ecosystem.*

Laporte, C., & Chevalier, F. (2016). An Innovative Approach to the Development of Project Management Processes for Small-Scale Projects in aLarge Engineering Company. En K. Jakobs, *Effective Standardization Management in Corporate Settings.* IGI Global.

Le Goaller, J.-P., Conde, C., & Langha, S. (2013). *RDBMS in the Cloud: Oracle Database on AWS.* Amazon Web Services.

Leimeister, S., Ried, C., Böhm, M., & Krcmar, H. (2010). *The Bussiness perspective of cloud computing: actors, roles and value networks.* European Conference on Information System.

Littlefield, C. (2015). *Introducing Amazon RDS for Aurora.* Global Knowledge Training LLC.

Logic20/20. (2016). *Cloud Collaboration and Storage Services.* Logic20/20, Inc.

MathWorks. (2014). *MATLAB on EC2 Instructions Guide.* The MathWorks, Inc.

Michel, D. (2010). *Databases in the Cloud.* HSR University.

Micro, T. (2013). *Best Practices for Security and Compliance with Amazon Web Services.* Trend Micro Inc.

Mohamed, A. (2013). *An Introduction to Cloud Computing Concepts.* Software Engineering Competence Center.

MySQL. (2009). *Best Practices Guide for MySQL on Amazon EC2.* Sun Microsystems .

NIST. (2012). *Cloud Computing, review of feature, benefits and risk, and recommendations for secure, efficient, implementation.*

NTT Data. (2014). *Cloud Computing: Transforming the Enterprise.* NTT DATA, Inc.

Otieno, J., & Njihia, J. (2014). Challenges of Cloud Computing in Business: Towards New Organizational Competencies. *International Journal of Business and Social Science*, Vol. 5 No. 3; March 2014.

Overbond. (2015). *Overbond Digital, Transparent & Secure .* Overbond Inc.

Park, J., Spetka, E., & Rasheed, H. (2013). *Near-Real-Time Cloud Auditing for Rapid Response.* Distribution Unlimited Publisher.

Pragmatic. (s.f.). *AWS HIPAA Compliance.* Pragmatic Inc.

Rackspace. (2016). *Patterns, challenges and best practices for AWS accounts in your cloud strategy.* Rackspace US, Inc.

Raven. (2016). *About Us*. Recuperado el 12 de 6 de 2016, de http://ravensoftwaresolutions.com/index.php/about-us/

Real Academia Española, R. (2014). *Diccionario de la lengua española.* Madrid: Espasa Libros, S. L. U.

Rowe, S., & Sikes, S. (2006). *Lessons Learned: Taking it to the Next Level.* Washington: PMI Global Congress Proceedings.

Sajee , M., & Jinesh , V. (2014). *Overview of Amazon Web Services.* Amazon Web Services.

Sakhi, I. (2012). *Database security in the cloud.*

Salama, M., & Shawish, A. (2014). *Cloud Computing: Paradigms.* Cairo: Springer-Verlag Berlin Heidelberg.

SFIA. (2015). *SFIA6 The complete reference guide.* SFIA Foundation.

Siegel, M., & Gibbons, F. (2008). *Amazon enters the cloud computing business.* Stanford University Case Publisher.

Simorjay, F. (2016). *Shared Responsibilities For Cloud Computing.* Microsoft.

Sophos. (2014). *Sophos UTM on AWS Overview and Deployment Guide.* Sophos Group.

Sysfore Technologies. (2014). *Microsoft Azure vs. Amazon Web Services.* Sysfore Technologies Pvt. Ltd.

Tanenbaum, A., & Wetherall, D. (2011). *Computer networks.* Seattle: Prentice.

Trinimbus. (2014). *Securing Your Amazon Web Services Account Using Identity and Access Management.* Trinimbus Cloud Management Solution.

Tsz Lai, W., Trancong, H., & Goh, S. (2011). Cloud Computing. En D. C, *A Fresh Graduate's Guide to Software Development Tools and Technologies.* National University of Singapore.

van der Veen, A., & van Bon, J. (2007). *Foundations of ITIL V3.* Van Haren Publishing.

Wirzenius, L., Oja, J., Stafford, S., & Weeks, A. (2004). *The Linux System Administrator's Guide.* Linux Documentation Project.

Wowza. (2016). *Wowza Streaming Engine for Amazon EC2.* Wowza Media Systems.

Wynkoop, S. (2015). *How to Meet Best Practices for Protecting Information in AWS.* Townsend Security.

10. Apéndice

10.1. Apéndice 1. Entrevista

1. Con base a su experiencia previa, ¿cuál ha sido el proceso o protocolo para determinar las subredes requeridas en la creación de una red privada en la nube (VPC), además de la definición del rango de direcciones IP disponibles? ¿Considera necesaria la comunicación con el equipo interno de infraestructura para determinar este análisis? ¿Utiliza algún método (buena práctica) para categorizar las subredes en base a los requerimientos, módulos o aplicaciones de la solución por implementar?
2. ¿En qué fase del desarrollo de una solución de software utilizando la infraestructura de AWS, considera necesario determinar el tipo de capacidad computacional (Tipos de EC2) que es requerida para cada uno de los componentes? ¿Considera algunos escenarios en el cual no sea necesario la utilización de la tecnología EC2 y cuales serían estos servicios computacionales de AWS con el cual se podrían remplazar?
3. Para los componentes/módulos de la solución de software que han requerido un sistema base de datos en la nube, ha utilizados los motores disponibles en la tecnología RDS (Amazon relational Database service) o bien base de datos no relacionales tal como DynamoDB. ¿Qué tipo de ventajas ha identificado en el uso de estos servicios de Base datos, en comparación al modelo de base de datos basado en instancias EC2?
4. En la creación de una red privada en la nube (VPC) en conjunto con la red privada corporativa, ¿Qué tipo de VPN (Hardware, Software, conexión directa, CloudHub) ha utilizado? ¿Cuál considera usted que debería ser la o las consideraciones principales para definir cuál tipo de VPN se adapta a los requerimientos?

5. Con respecto a la gestión de usuarios para otorgar acceso a la consola de AWS (interface web) y hacer uso de los servicios en la nube, ¿Qué tipo de proceso ha utilizado anteriormente, gestión manual o bien mediante el uso de herramientas externas que se encuentran integradas a los servicios de la red interna corporativa?
6. Con respecto a las capas de seguridad para controlar el tráfico entrante y saliente a nivel de instancias virtuales (EC2) y red, ¿considera alguna buena práctica para facilitar la creación y el uso de los grupos de seguridad y listas de acceso?
7. Con respecto a los archivos de información, los cuales son enviados a la infraestructura de AWS, ¿Ha utilizado usted algún proceso de cifrado de información, de ser así, el proceso de cifrado se ha realiza antes de ser enviados a la nube (personalizado en la red corporativo) o bien mediante los servicios de cifrado automático que proveen los servicios de AWS? ¿Para ello utilizo KMS para gestión la de llaves privadas o bien alguna otra herramienta externa?
8. ¿Utiliza el proceso automático de cifrado a nivel de disco para los recursos de volúmenes de datos (EBS) y sistema base de datos (RDS)?
9. En el desarrollo de una solución de software en la infraestructura de AWS, ¿Ha utilizado algún paquete de desarrollo (SDK) que permita la integración del proceso personalizado con los servicios de AWS, de ser así, que tipo de lenguaje de programación ha utilizado con mayor frecuencia?
10. Con respecto a software de control de versiones para el desarrollo y liberaciones de software, ¿Cuáles ha utilizado en proyectos en la nube de AWS? ¿Considera necesario que este tipo de herramientas se encuentren en la red privada corporativa o que es encuentre basada en su totalidad en servicios en la nube?

11. ¿Qué servicios o herramientas ha utilizado para el monitoreo de los recursos computacionales de AWS? ¿Qué beneficios le ha proporcionado el uso de las mismas?
12. ¿Tiene alguna experiencia previa en la implementación de herramientas de integración continua y automatización de liberación de nuevas versiones de códigos fuentes?
13. ¿Considera/utiliza alguna métrica de creación de copias de seguridad a nivel de volúmenes de datos (EBS), base de datos RDS, además de plantillas de servidores virtuales(AMI´s); que pueden obtener beneficios en las fases de desarrollo y operación de la solución de software en la nube?

11. Glosario

Nombre	Significado
Software	Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. (Real Academia Española, 2014)
Computación en la nube	Modelo para habilitar de manera conveniente, un acceso por demanda de un conjunto compartido de recursos computacionales (redes, servidores, almacenamiento y servicios) que pueden ser rápidamente provisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de la nube. (NIST, 2012)
Escalabilidad	Capacidad que tiene un sistema, red o proceso de manejar aumento de volumen para alcanzar las necesidades del usuario. (Bondi, 2000)
Gestión de Proyectos	Aplicación de conocimientos, habilidades, herramientas, y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. (Institute, 2004)
Infraestructura de tecnologías de información.	Conjunto de hardware, software, red, instalaciones, entre otros (incluyendo toda la tecnología de información), en orden para desarrollar, probar, entregar, monitorear, controlar y brindar soporte de los servicios de TI. (van der Veen & van Bon, 2007)
GIT	Sistema de control de versiones utilizado para el desarrollo de software y otras tareas de control de versiones. (Bourke, 2015)
DNS	Esquema jerárquico, basado en nombres de dominios, utilizados para asociar direcciones IP con nombres de servidores. (Tanenbaum & Wetherall, 2011)
Latencia	Tiempo requerido para transferir información a través de una red. (Comer, 2009)
IPsec	Ecosistema de estándares abiertos para asegurar comunicaciones privadas en redes públicas. (Frankel , y otros, 2005)

SSH	Protocolo criptográfico de red para operar servicios de red de manera segura. (Group, 2006)
File System	Método y estructura de datos que es utilizado por un sistema operativo para llevar registro de los archivos en un volumen de datos o partición. (Wirzenius, Oja, Stafford, & Weeks, 2004)
Firewall	Sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente, basado en un conjunto de reglas predeterminadas. (Boudriga, 2010)

12. Anexos

Anexo 1 - Carta de aceptación de la empresa interesada

Date: 03/06/2016

To,

MaestríaenAdministración de Tecnologías de Información

Universidad Nacional de Costa Rica

The goal of the current letter is to indicate the interest of the final product of the project "**Methodology to implement software applications in Amazon Web Services (AWS)**" to be developed by Miguel Alvarado Abarca, in order to support the thesis of the Master degree program.

It´s important to highlight that the project is not going to include the process information or business Knowledge of the organization.

If you have any questions/concerns you may call us on (001)-214-254-3373.

Regards,

Venkat Pailla,
President,
Raven Software Solutions Inc.

Raven Software Solutions Inc.
4425 W Airport Freeway, Suite 595, Irving, Texas 75062. P: 214-254-3373| F: 214-254-3373|
E: hr@ravensoftwaresolutions.com

Anexo 2 - Siglas y acrónimos

Siglas y acrónimos	Significado
AWS	Amazon Web Services
MATI	Maestría en Administración de Tecnología de la Información
NIST	National Institute of Standards and Technology
SDLC	Ciclo de Vida del Desarrollo del Software (por sus siglas en inglés)
TI	Tecnología de Información
WBS	Work Breakdown Structure
DNS	Domain Name System
CPU	Central Processing Unit
IPSEC	Internet Protocol security
SSH	Secure Shell

Anexo 3 - Habilidades y niveles de responsabilidad SFIA

Modelo de habilidades y niveles de responsabilidad de profesionales de tecnologías de información, utilizado para desarrollar una matriz de referencia entre las actividades definidas en la presente metodología y sus respectivas habilidades identificadas en el modelo SFIA.

Habilidad	Descripción Habilidad
Diseño de sistemas	Corresponde a la especificación y el diseño de sistemas de información para satisfacer las necesidades empresariales definidas en cualquier contexto público o privado, incluido el contexto comercial, industrial, científico y lúdico y de ocio. La identificación de conceptos y su transformación en

	un diseño aplicable. El diseño o la selección de componentes. El mantenimiento de la compatibilidad con las arquitecturas empresariales y de solución, y el cumplimiento de las normas corporativas dentro de los límites de costes, seguridad y sostenibilidad.
Análisis de datos	Corresponde a la investigación, la evaluación, la interpretación y la clasificación de datos, a fin de definir y aclarar las estructuras de información que describan las relaciones entre entidades del mundo real. Estas estructuras facilitan el desarrollo de sistemas informáticos, enlaces entre sistemas o actividades de recuperación.
Diseño de redes	Se refiere a la producción de diseños de redes y políticas, estrategias, arquitecturas y documentación de diseño, que abarcan voz, datos, texto, correo electrónico, fax e imagen, para respaldar las estrategias y los requisitos empresariales en cuanto a conectividad, interconexión, seguridad, resistencia, recuperación, acceso y acceso remoto. Esto podría incorporar todos los aspectos de la infraestructura de comunicaciones, ya sean internos o externos, móviles, públicos o privados, Internet, intranet o centros de llamadas.
Ingeniería de seguridad	Corresponde a la aplicación de métodos adecuados para garantizar la seguridad durante todas las fases del ciclo de vida de desarrollos de sistemas relacionados con la seguridad, incluidos el mantenimiento y la reutilización. Estos incluyen riesgos de seguridad y análisis de riesgo, especificación de requisitos de seguridad, diseño arquitectónico de sistemas relacionados con la seguridad, diseño de métodos formales, verificación y validación de la

	seguridad, y preparación del estudio de seguridad.
Configuración de software	Se refiere a la configuración de productos de software en entornos/plataformas de software nuevos o existentes.
Infraestructura de las TI	Corresponde a la operación y el control de la infraestructura de las TI (generalmente hardware, software, datos almacenados en varios medios y todos los equipos dentro de las redes locales o de área amplia) necesarios para prestar y respaldar correctamente los servicios y productos de las TI a fin de satisfacer las necesidades de una empresa. Incluye la preparación para servicios nuevos o modificados; el funcionamiento del proceso de modificación; el mantenimiento de estándares reguladores, legales y profesionales; la creación y gestión de sistemas y componentes en entornos informáticos virtualizados; y la supervisión del rendimiento de los sistemas y servicios en relación con su contribución al rendimiento de negocio, su seguridad y su sostenibilidad.
Desarrollo de software	Corresponde al diseño, la creación, la realización de pruebas y la documentación de componentes de software nuevos y modificados a partir de especificaciones suministradas de conformidad con las normas y los procesos de desarrollo y seguridad acordados.
Lanzamiento y despliegue	Se refiere a la gestión de procesos, sistemas y funciones para englobar, construir, probar y aplicar cambios y actualizaciones (que están vinculados como

	"lanzamientos") en un entorno activo, estableciendo o continuando el servicio especificado, para permitir la entrega controlada y eficaz al departamento de Operaciones y la comunidad de usuarios.
Realización de pruebas	Se refiere a la planificación, el diseño, la gestión, la ejecución y la presentación de informes sobre pruebas mediante el uso de herramientas y técnicas apropiadas de realización de pruebas y conforme a las normas de procesos acordadas y las regulaciones específicas de la industria. El objetivo de la realización de pruebas es garantizar que los sistemas, configuraciones, paquetes o servicios nuevos y modificados, junto con cualquier interfaz, funcionen tal como esté especificado (incluidos los requisitos de seguridad), y que los riesgos asociados a su despliegue se conozcan y documenten correctamente. La realización de pruebas incluye el proceso de ingeniería, utilización y mantenimiento de testware (casos de pruebas, guiones de pruebas, informes de pruebas, planes de pruebas, etc.) para medir y mejorar la calidad del software que se está probando.
Gestión del almacenamiento	Se refiere a la planificación, la implementación, la configuración y el ajuste del hardware y software de almacenamiento, abarcando el almacenamiento de datos en línea, fuera de línea, remotos y fuera de las instalaciones (copias de seguridad, archivado y recuperación de desastres) y garantizando el cumplimiento de requisitos reguladores y de seguridad.

Anexo 4 - Plantillas de documentación

4.1 - Listado de módulos y componentes de la solución

Nombre de Módulo	Nombre de Aplicación	Descripción Aplicación	Tipo Procesamiento	Frecuencia de Uso	Servicios AWS	Método Protección de datos	Llaves de Cifrado	Llaves de acceso

4.2 - Listado de tráfico de las aplicaciones

Nombre de aplicación	Recurso Origen	Recurso Destino	Protocolo	Rango de puertos

4.3 - Listado de grupos y roles de usuarios

Nombre	Tipo (Grupo usuarios / rol)	Aplicación	Área	Nombre IAM	Usuarios IAM Asociados	Políticas de autorización

4.4 – Listado de políticas de autorización.

Nombre Política	Nombre Política IAM	Nivel de acceso	Servicios AWS	Recursos (ARN) permitidos

4.5 – Listado de subredes

Ambiente de desarrollo	Modulo	Nombre	Identificador	Bloque de direcciones IP

4.6 – Listado de grupos de seguridad.

Aplicación	Nombre de grupo de seguridad	Identificador	Tipo regla	Tipo	Protocolo	Rango de puertos	Recurso

4.7 – Listado de tipos de recursos computacionales.

Ambiente de desarrollo	Aplicación	Nombre Recurso	Tipo de Recurso	Tamaño de recurso	Especificaciones de recurso	Cantidad de recursos

4.8 – Listado gestión de información.

Ambiente de desarrollo	Aplicación	Nombre	Tipo	Frecuencia	Periodo retención	Recursos Computacionales	Procesos

4.9 – Matriz de responsables.

Aplicaciones	Rol 1	Rol 2	Rol 3	Rol 4
Aplicación 1				
Aplicación 2				
Aplicación 3				
Aplicación 4				

4.10 – Listado de monitoreo.

Ambiente de desarrollo	Aplicación	Nombre	Tipo	Datos a monitorear	Frecuencia	Procesos	Acción

4.11 – Listado de mejora continúa.

Aplicación	Nombre	Componentes de monitoreo	Análisis de datos	Presentación de datos

Anexo 5 - Carta de aceptación del proyecto

Date: 05/18/2017

To,

Maestría en Administración de Tecnologías de Información,

Universidad Nacional de Costa Rica.

The goal of the current letter is to indicate the acceptance of the project **"Methodology *to implement software applications in Amazon Web Services (AWS)*"** developed by Miguel Alvarado Abarca, in order to support the thesis of the Master degree program. In which, the goals were achieved.

If you have any questions/concerns you may call us on (001)-214-254-3373

Regards,

Venkat Pailla,

President of,

Raven Software Solutions Inc.

Raven Software Solutions Inc.
4425 W Airport Freeway, Suite 595, Irving, Texas 75062. P: 214-254-3373| F: 214-254-3373|
E: hr@ravensoftwaresolutions.com

Anexo 6 - Carta de aprobación filóloga

EDUCATESIS, hace constar que se realizó la revisión del presente trabajo, se analizó la construcción de párrafos, vicios del lenguaje, ortografía, puntuación y otros relacionados a la Corrección de Estilo, sin alterar la intencionalidad del autor y el enfoque del tema. Por lo tanto, **CERTIFICA**, la revisión y corrección de la tesis para optar por el Grado Académico de:

Maestría en maestría en Administración de Tecnologías de Información
Énfasis en Administración de Proyectos
UNIVERSIDAD NACIONAL

Tema:

Metodología de implementación de aplicaciones de *software* en Amazon Web Services (AWS).

Elaborado por: ***Miguel Alvarado Abarca***

Se extiende la presente en San José, 22 de mayo del 2017.

Atentamente:

LICDA. JACQUELINE RÍOS A.
COORDINADORA GENERAL DE FILÓLOGOS
EDUCATESIS
C/616

educatesis@hotmail.com
8762-2302