



MAESTRÍA EN GERENCIA DE SISTEMAS Y TECNOLOGÍAS DE
INFORMACIÓN

ESTUDIO PARA OPTIMIZAR MEDIANTE CLOUD COMPUTING LA
INFRAESTRUCTURA DE CÓMPUTO CENTRAL DE LOS SISTEMAS DE
INFORMACIÓN QUE SOPORTAN LOS 67 PROCESOS CRÍTICOS DE
NEGOCIO EN LA EMBOTELLADORA DE BEBIDAS ARCA CONTINENTAL
ECUADOR

Trabajo de Titulación presentado en conformidad a los requisitos establecidos
para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de
Información

Profesor guía
MBA. Jaime Vinueza

Autor
Jaime José Gallegos Oleas

Año
2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

MBA. Jaime Vinueza

CI: 1716028509

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Jaime José Gallegos Oleas

CI: 1713538286

AGRADECIMIENTOS

A la organización Arca Continental Ecuador por el apoyo prestado para la realización del trabajo de titulación.

A mi tutor Jaime Vinuesa por su guía constante y profesional con la cual se logró culminar este documento.

A mis padres y hermanos por inculcarme valores y preceptos que me han formado como persona de bien.

DEDICATORIA

A mi esposa y mis hijos que son la motivación para lograr todos los objetivos que me he trazado en mi vida. Gracias por su amor, apoyo, consideración y comprensión en este tiempo que duro la realización del trabajo de titulación.

RESUMEN

Este estudio logro identificar soluciones importantes a necesidades de los procesos del negocio respecto al uso de la infraestructura de cómputo central que requiere de un proceso de renovación y consolidación, esto se puede lograr mediante el uso de servicios en cloud computing con costos muy convenientes y soluciones tecnológicas que mejoraran la disponibilidad y escalabilidad de los servicios computacionales.

Logrando un aprovisionamiento de la infraestructura en tiempos cortos y permitiendo que nuevas iniciativas del negocio fluyan rápidamente, de esta forma el área de Tecnologías de Información estará enfocada en optimizar los procesos del negocio relaciones a la sistematización de los mismos, en donde la infraestructura no será más una limitante para lograr los objetivos estratégicos de la organización.

ABSTRACT

This study identified important achievement needs solutions to business processes regarding the use of central computing infrastructure that requires a process of renewal and consolidation, this can be achieved through the use of cloud computing services with very good rates and solutions technology to improve the availability and scalability of computational services.

Achieving a provisioning infrastructure in a short time and allowing new business initiatives flow rapidly, thus the area of Information Technology will focus on optimizing business processes relationships systematizing them, where the infrastructure is not more limiting to achieve the strategic objectives of the organization.

INDICE

1. CAPITULO I. Definiciones y Alcance.....	1
1.1 Antecedentes	1
1.2 Objetivos.....	3
1.3 Justificación.....	4
1.4 Alcance.	5
2. CAPITULO II. Procesos de Negocio.	6
2.1 Descripción de los mapas de procesos del negocio.	6
2.2 Identificación de los procesos críticos y la cadena de valor.....	15
2.3 Análisis de los procesos del negocio actuales.....	16
2.4 Necesidades de los procesos del negocio enfocados a su automatización y del catálogo de servicios asociado...	19
3. CAPITULO III. Cloud Computing.	33
3.1 Definiciones y características.....	33
3.2 Tipos de <i>cloud computing</i>	38
3.3 Comparación del <i>cloud computing</i> frente a entornos tradicionales	40
3.4 Ventajas y Desventajas de <i>cloud computing</i>	42
3.5 Seguridad en <i>cloud computing</i>	44
3.6 Marco de referencia de Implementaciones en <i>cloud computing</i>	45
3.7 Proveedores de soluciones de <i>cloud computing</i>	47
4. CAPITULO IV. Diseño de la solución.....	55
4.1 Arquitectura de la propuesta	55

4.2 Costos de la solución propuesta y retorno sobre la inversión.	76
4.3 Análisis de Impacto en el negocio de la solución Propuesta.....	94
4.4 Comparación de la solución con aprovisionamiento de infraestructura interna.....	95
CONCLUSIONES.....	104
RECOMENDACIONES.....	109
REFERENCIAS.....	110
ANEXOS.....	112

CAPITULO I. DEFINICIONES Y ALCANCE

1.1 Antecedentes

La embotelladora de bebidas es una empresa dedicada a la producción, distribución y venta de bebidas refrescantes.

La organización tiene tres centros de cómputo ubicados en las ciudades de Quito y Guayaquil. Dos de estos centros de cómputo están ubicados en Quito, uno de ellos está localizado en el edificio corporativo de la organización en el sector de Calderón y el otro está ubicado en el edificio de IBM del Ecuador, el tercer centro de cómputo está localizado en la planta embotelladora en Guayaquil.

La infraestructura tecnológica central de la organización se encuentra en plataformas no homogéneas y en diferentes realidades geográficas, por lo tanto la administración es compleja, descentralizada y costosa.

El área de Tecnología y Sistemas tiene un número limitado de recursos que brindan el soporte a la infraestructura y servicios que brinda al negocio, esto hace que el monitoreo de los sistemas de información no sea el acorde y exista incidentes que afecten el normal funcionamiento de las aplicaciones.

En nuestro país existen empresas locales y extranjeras que están promoviendo servicios de *cloud computing* para todo tipo de necesidades de negocio como son: *IBM, TelcoNet* con infraestructura propia instalada en centros de cómputo que se encuentran en ciudades como Quito y Guayaquil. También *Level3, HP, Google* que brinda estos servicios desde fuera de nuestro territorio.

A continuación describo algunos servicios que nos pueden ofrecer estas organizaciones:

Migración de los sistemas de información que están en ambientes de producción, desarrollo y pruebas a *cloud computing*.

Respecto al almacenamiento de la información también son servicios que se ofrece en *cloud computing* respecto a las copias de respaldos y archivo de la información de la organización.

También estos servicios están enfocados a herramientas colaborativas como el uso del correo electrónico, calendario, chat, compartir archivos, video y audio conferencia, entre otras. (Level3, s.f.)

Otro grupo de soluciones que se están proporcionando van en la línea del análisis de la información que está consolidada en los sistemas de información como son: *ERP* (Sistemas informáticos destinados a la administración de recursos en una organización) (SAP s.f.), *CRM* (Sistemas informáticos para la administración de la relación con los clientes), *BPM* (Sistemas informáticos para administración por procesos del negocio), *EPM* (Sistemas informáticos para la administración de proyectos empresariales), sistemas internos.

El manejo de planes de recuperación de desastres mediante el uso de *cloud computing* nos permitirá analizar y comprobar la hipótesis del caso de estudio planteado, con niveles de disponibilidad que antes la organización no podía lograrlos sino se invertía ingentes recursos económicos.

La gama de servicios que se ofrecen en *cloud computing* es muy amplia y cada día va evolucionando para soportar la mayoría de necesidades que tiene la organización esto logrará bajos costos, ahorros para la empresa. Configurando y poniendo en marcha iniciativas o requerimientos de la empresa que se cumplan en tiempos muy cortos permitiendo acceder a la información del negocio desde cualquier lugar y dispositivo en el mundo (Gartner, 2011).

El crecimiento económico que ha logrado el Ecuador en los últimos años y el proceso de modernización que está realizando el estado en diferentes ámbitos han permitido que la empresa privada también crezca en sus necesidades de automatizar sus procesos, lo que finalmente conlleva a requerir mayores servicios en línea.

Nuestro país está inmerso en un modelo de desarrollo, esto ha permitido que las tecnologías como el *cloud computing* según (Gartner, 2014) sean un soporte a las necesidades de las organizaciones permitiendo crecimiento sostenible en el tiempo mediante la flexibilidad (Amplitud del recurso para intercambiar información), costos accesibles, escalabilidad (Mejorar recursos sin perder calidad de servicio) y personalización a los requerimientos que demanden las instituciones, de esta forma se consolide como un conjunto de herramientas para el desarrollo.

1.2 Objetivos

1.2.1 Objetivo general

Diseñar una estrategia de consolidación óptima mediante *cloud computing* que permita soportar los procesos y el crecimiento del negocio brindando: disponibilidad, confiabilidad, seguridad y estandarización de su infraestructura informática central enfocada a los sistemas de información que tiene la organización.

1.2.1 Objetivos específicos

- Identificar los servicios críticos de la organización que requieran ser migrados a *cloud computing* apalancados en los procesos de negocio.
- Describir y realizar un análisis comparativo de la infraestructura en *cloud computing* frente a la tradicional y extrapolar las ventajas competitivas enmarcadas bajo la realidad de la empresa del presente caso de estudio.

- Presentar y dimensionar un modelo de crecimiento respecto a los sistemas y servicios de TI que soportarán las necesidades de la organización.
- Proponer la arquitectura en *cloud computing* para que optimice los recursos y requerimientos del negocio.

1.3 Justificación

La organización está en expansión constante esto ha ocasionado requerimientos en varios ámbitos tecnológicos como son: sistemas de información, infraestructura, servicios informáticos por lo tanto requiere consolidar estas necesidades en plataformas robustas (Sistema que permite al usuario recuperar la información con facilidad), bajo demanda, elásticas, flexibles, ágiles y a bajos costos que permitan satisfacer los requerimientos del negocio y su crecimiento.

Existen necesidades que requieren respuestas rápidas en menor tiempo del que actualmente se ejecuta respecto a la provisión de sistemas de información y sus demandantes capacidades en los procesos del negocio.

Los requerimientos del negocio van enfocados al aprovechamiento de la información que generan los diferentes procesos y que haya disponibilidad de la misma en todo momento para que la toma de decisiones sea oportuna y brinde una ventaja competitiva sobre sus competidores bajo el marco de las nuevas tendencias tecnológicas como es el *cloud computing*.

1.4 Alcance

Analizar los servicios críticos del negocio para desarrollar una arquitectura de consolidación de los sistemas centrales de Arca Continental Ecuador que se encuentran funcionando en las ubicaciones: Guayaquil Planta, Quito Calderón e *IBM (International Business Machine*, empresa multinacional estadounidense que fabrica y comercializa hardware y software con filiales en varios países) del Ecuador que están soportando los 67 procesos críticos del negocio identificando cuáles de ellos puedan ser migrados a *cloud computing*.

Realizar un análisis comparativo sobre los costos de aprovisionamiento interno de la infraestructura que soporta las aplicaciones del negocio versus migrarla a *cloud computing*.

Realizar un análisis de impacto en el negocio y retorno de la inversión de la solución propuesta.

Dimensionar un modelo de crecimiento donde se describa un plan de capacidad para las necesidades de la organización en un ambiente de *cloud computing*.

CAPITULO II. PROCESOS DE NEGOCIO

2.1 Descripción de los mapas de procesos del negocio

La organización receipta los requerimientos de los clientes y de los consumidores, requiere de insumos para los procesos de producción que ejecuta.

Se rige a las leyes, reglamentos del Estado Ecuatoriano, también a las directrices de Arca Continental en México y *The Coca Cola Company* (Corporación multinacional dedicada a la elaboración de bebidas). Se encuentra financiada por los recursos de los accionistas.

De esta forma mediante la ejecución de sus procesos se logra productos terminados de la más alta calidad del mercado con servicios de valor agregado y equipamiento para nuestros clientes y consumidores.

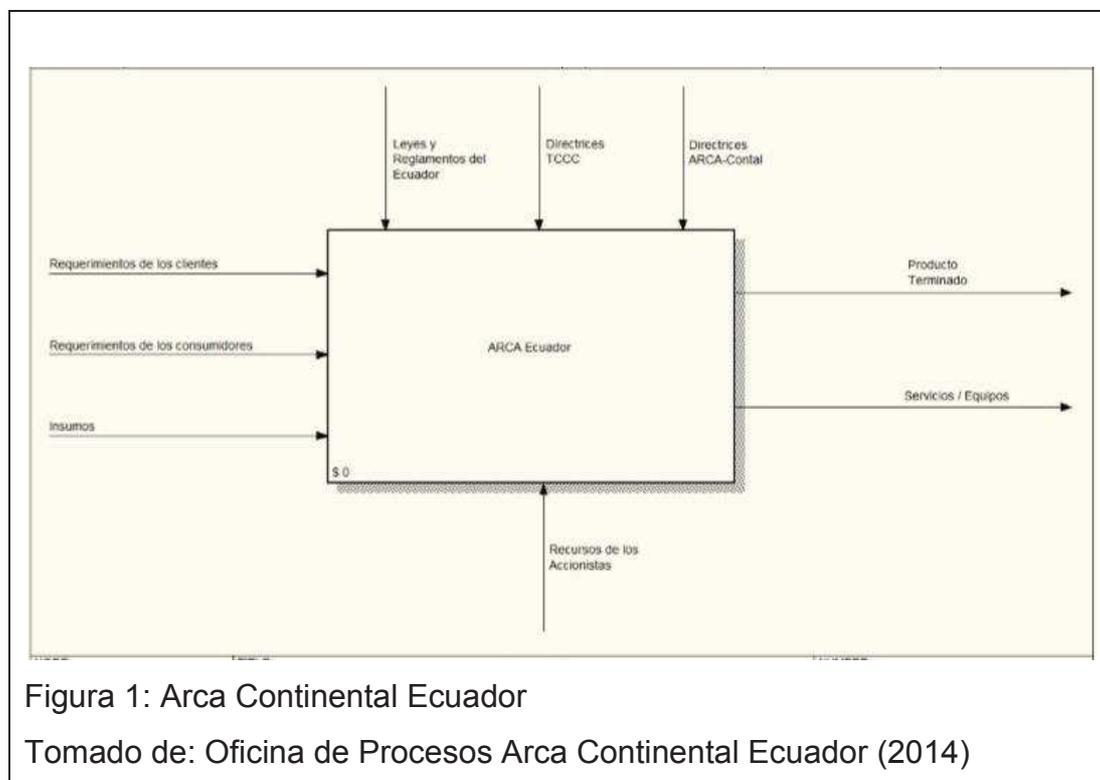


Figura 1: Arca Continental Ecuador

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

Los macro procesos de la organización están enfocados en: la responsabilidad de la dirección, la gestión de los recursos, realización del producto, medición, análisis y mejora de los procesos del negocio.

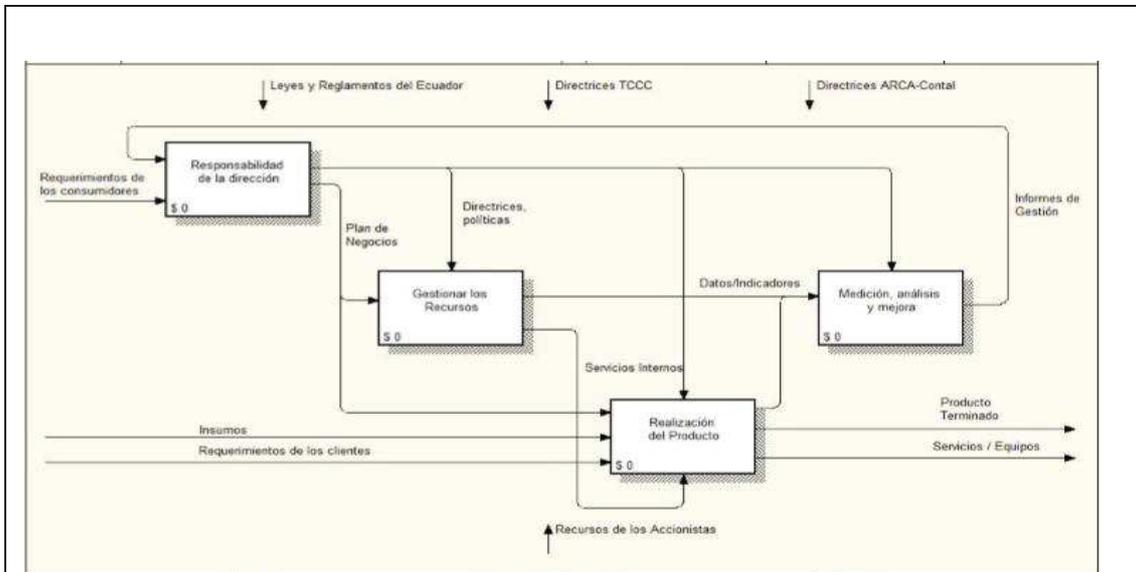


Figura 2: Macro Procesos Arca Continental Ecuador

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1 Macro Proceso responsabilidad de la dirección

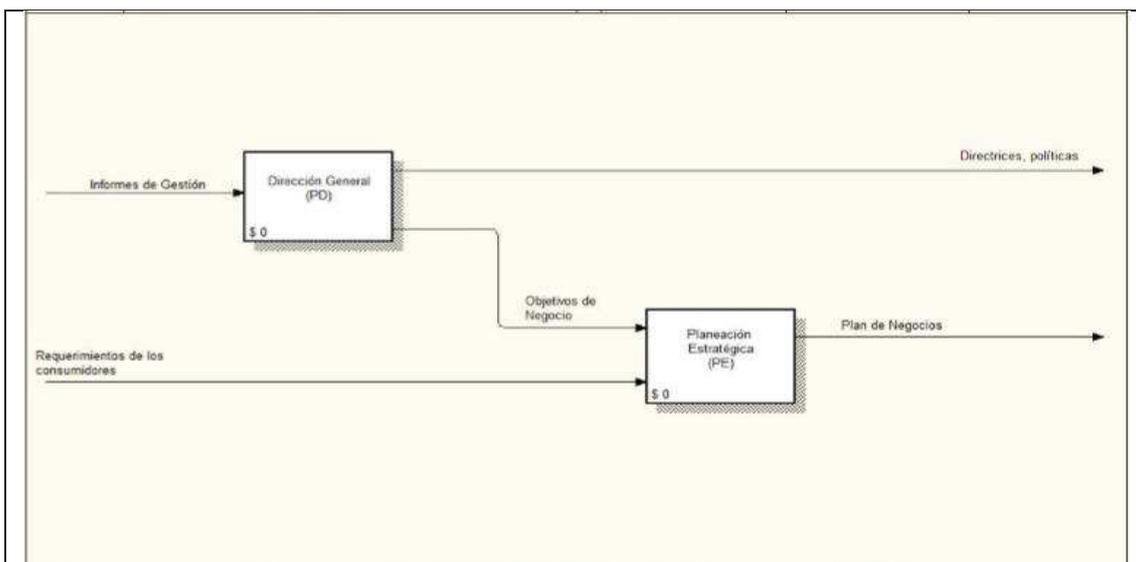


Figura 3: Macro Proceso responsabilidad de la dirección

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.1 Proceso dirección general

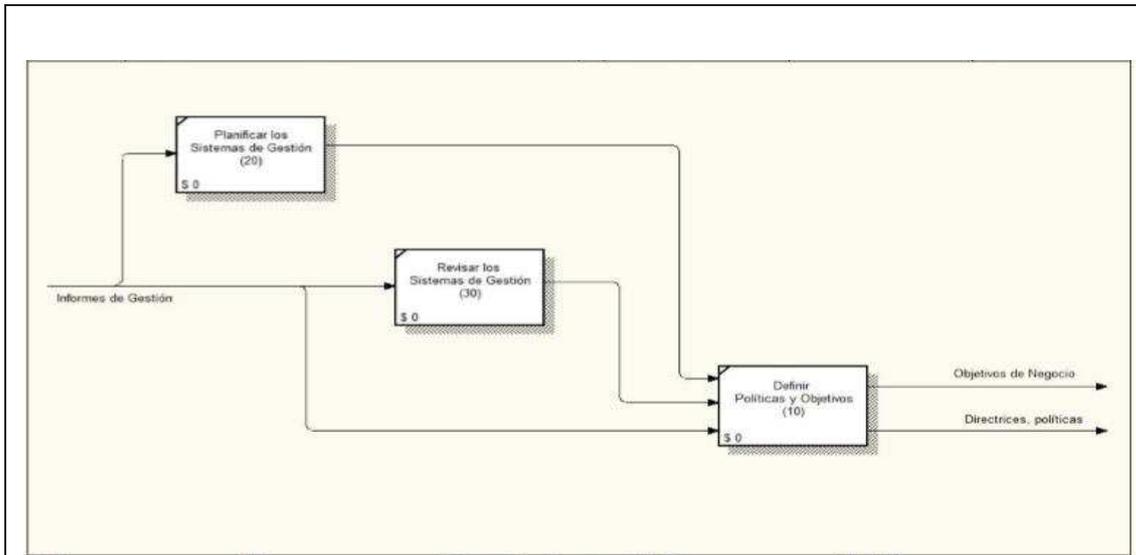


Figura 4: Proceso dirección general

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.2 Proceso planeación estratégica

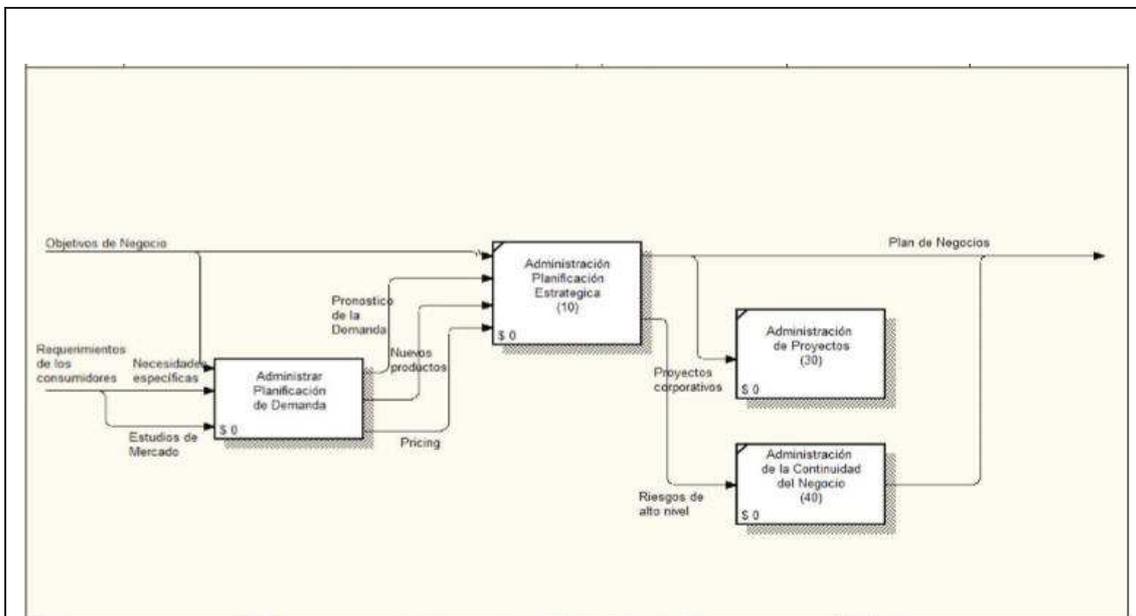


Figura 5: Proceso planeación estratégica

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.2 Macro Proceso gestionar los recursos

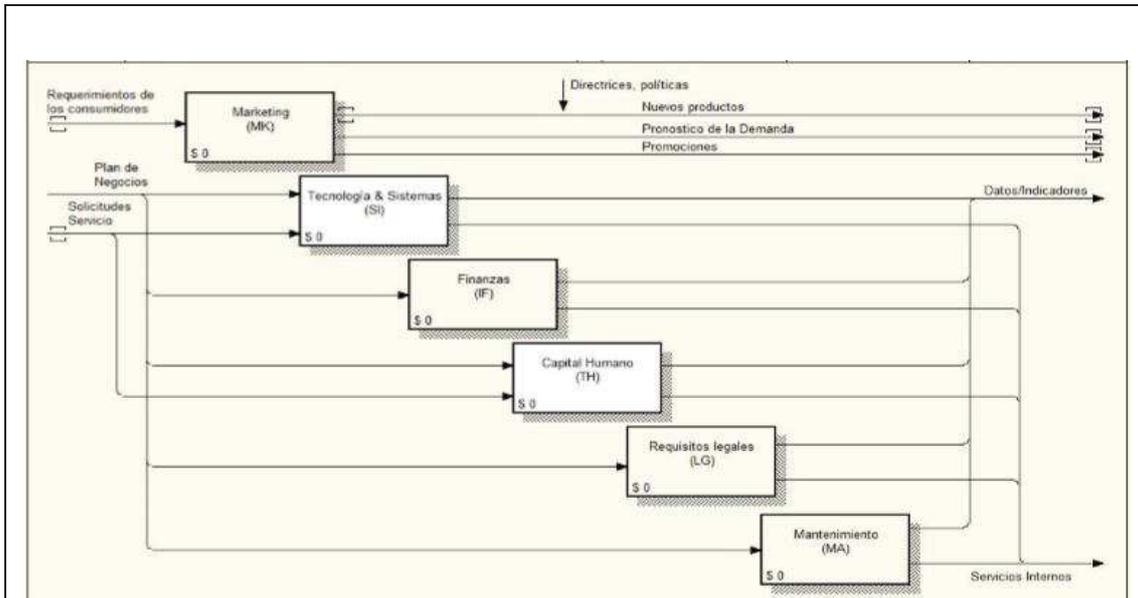


Figura 6: Macro Proceso gestionar los recursos

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.3 Proceso marketing

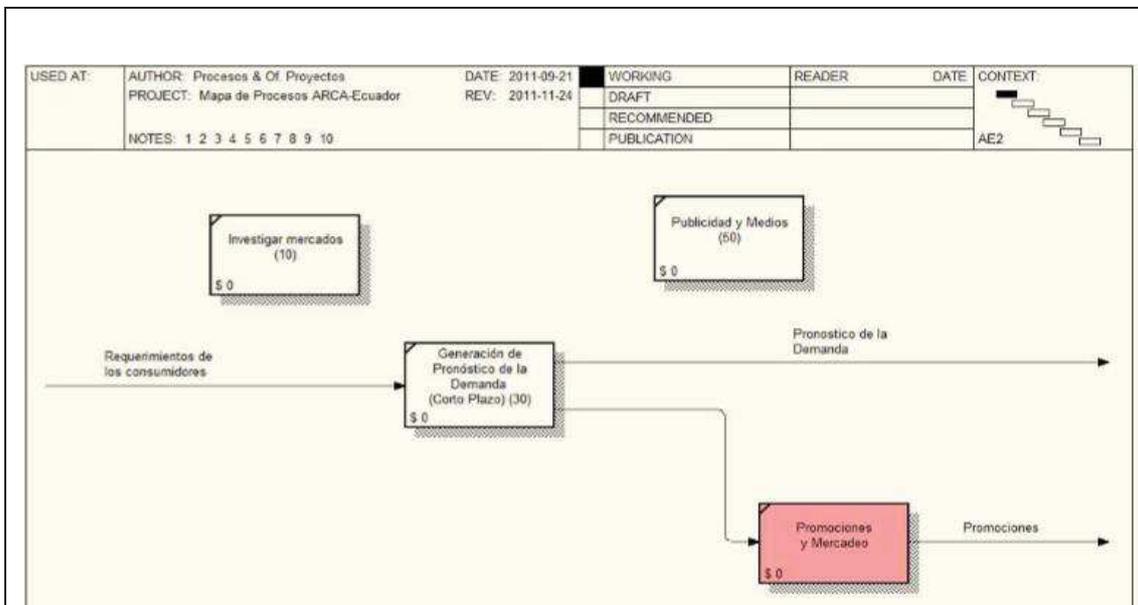


Figura 7: Proceso Marketing

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.4 Proceso tecnología y sistemas

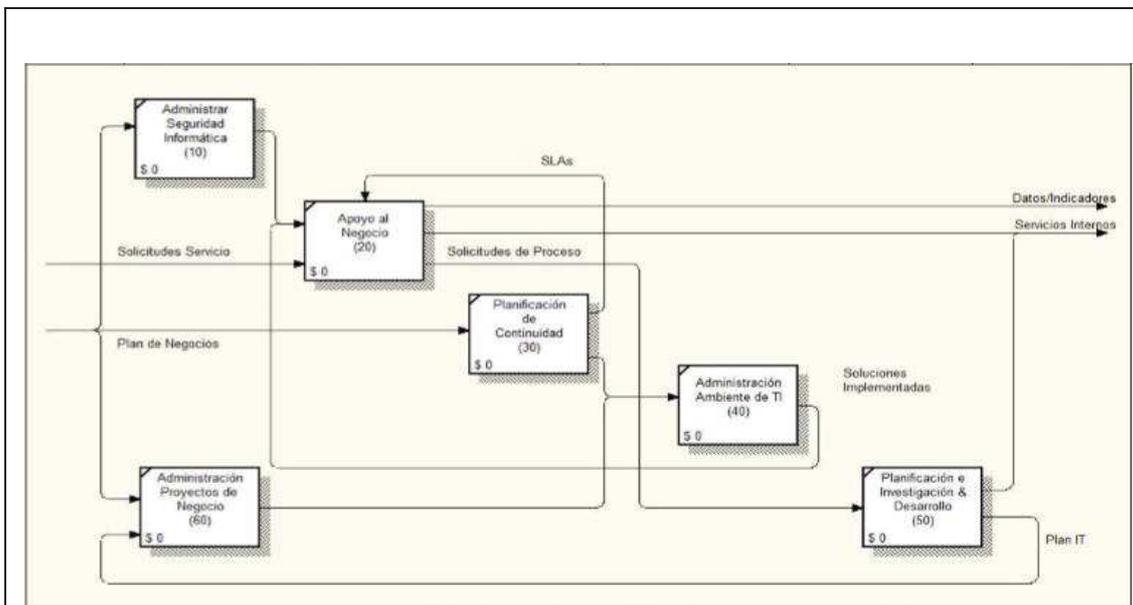


Figura 8: Proceso de tecnología y sistemas

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.5 Proceso finanzas

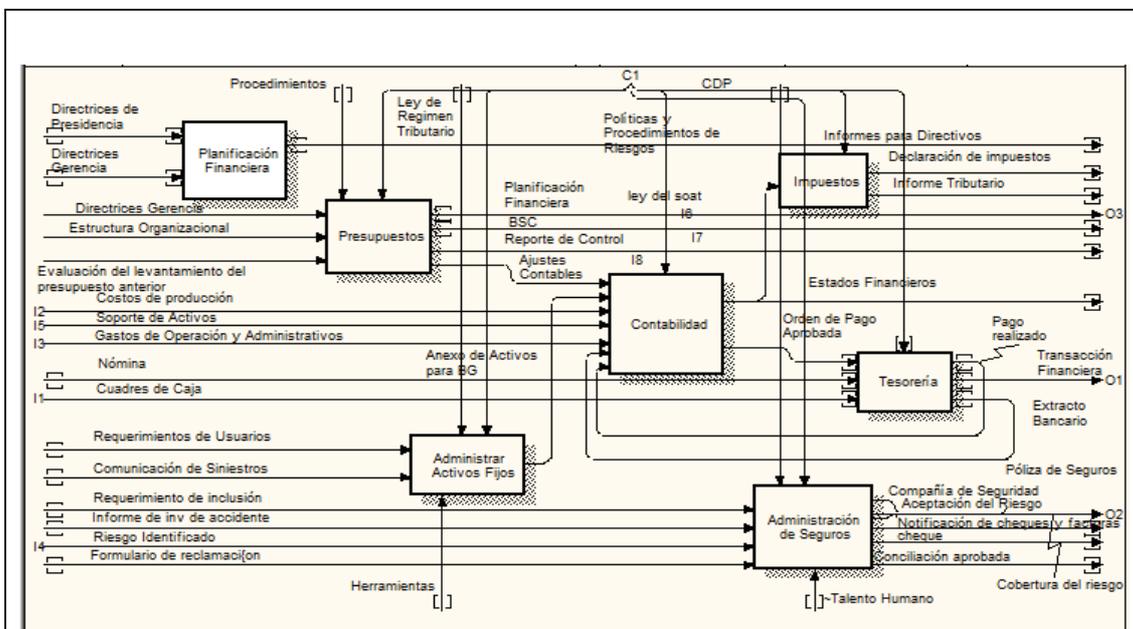


Figura 9: Proceso finanzas

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.6 Proceso capital humano

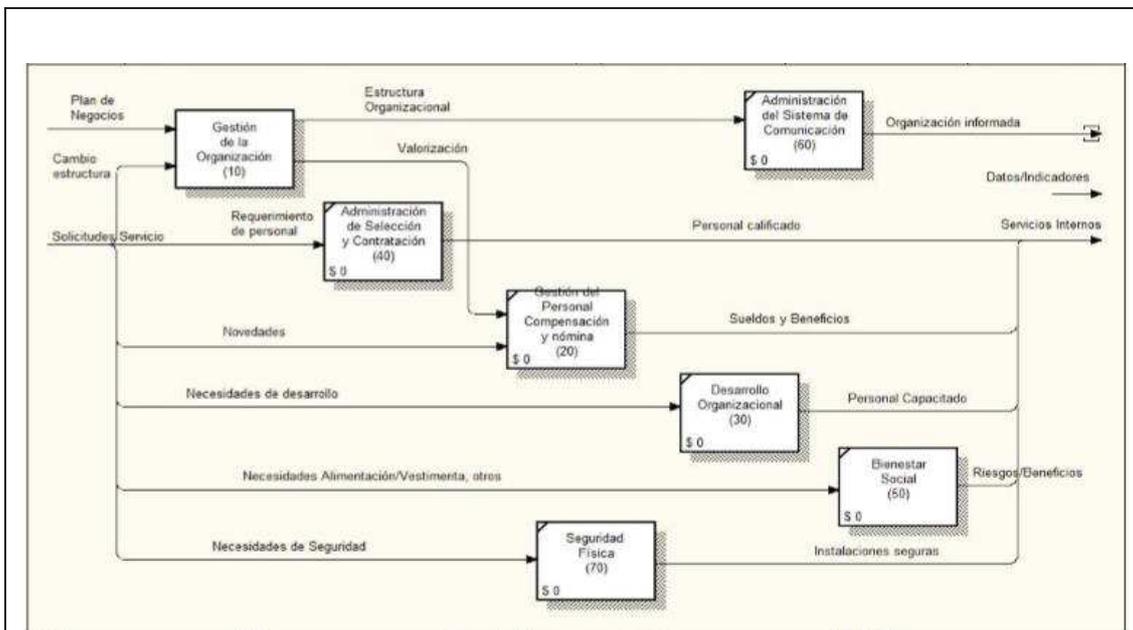


Figura 10: Proceso capital humano

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.7 Proceso requisitos legales

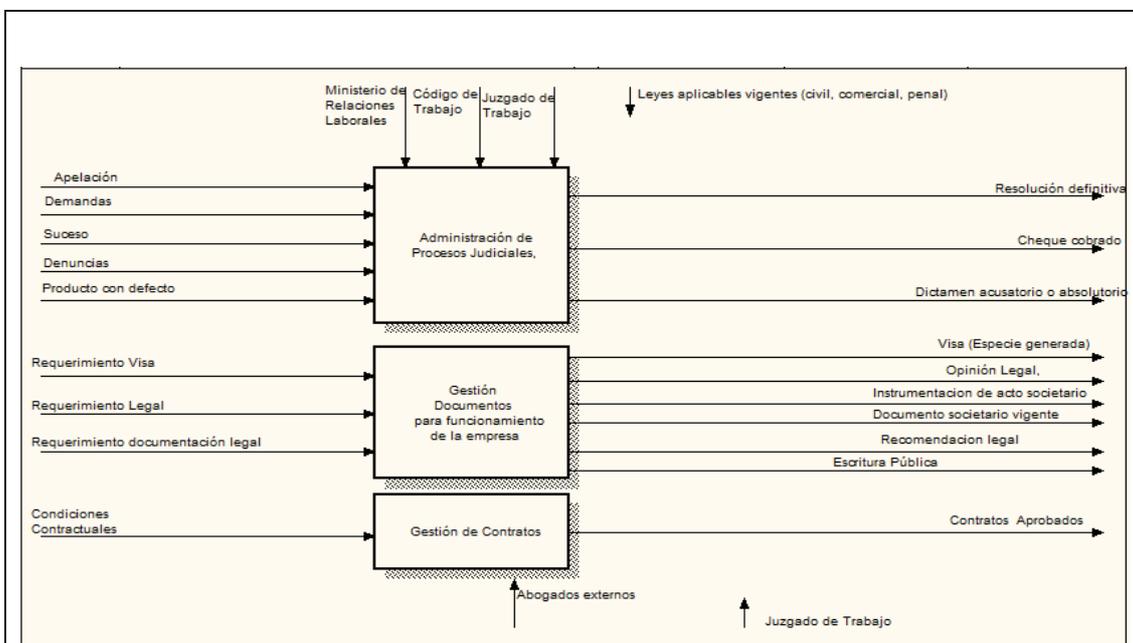


Figura 11: Proceso requisitos legales

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.8 Proceso mantenimiento

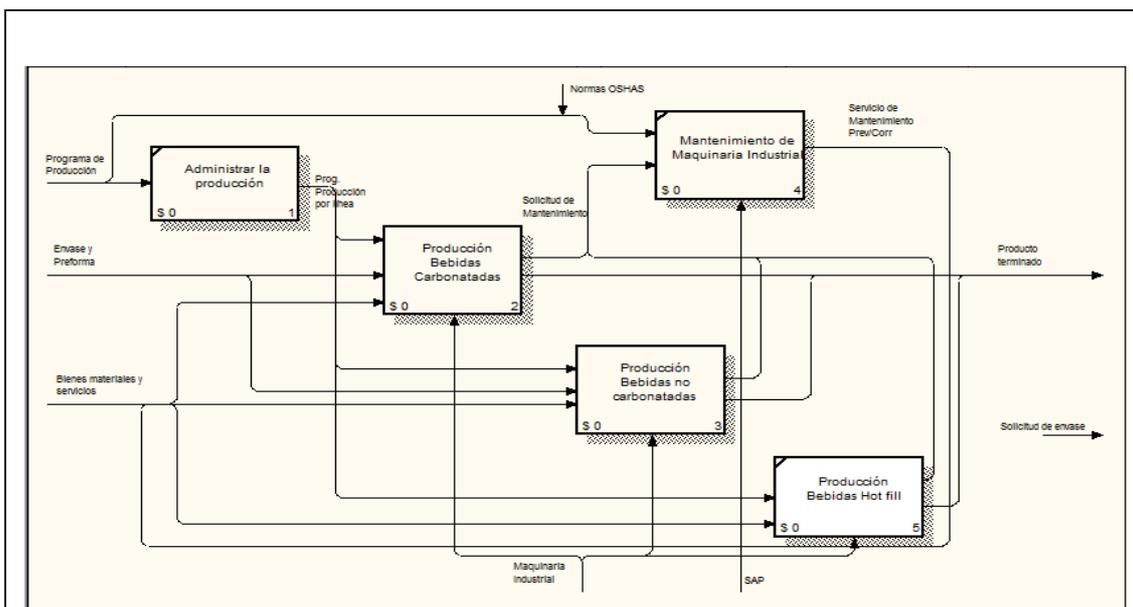


Figura 12: Proceso mantenimiento

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.3 Macro Proceso realización del producto

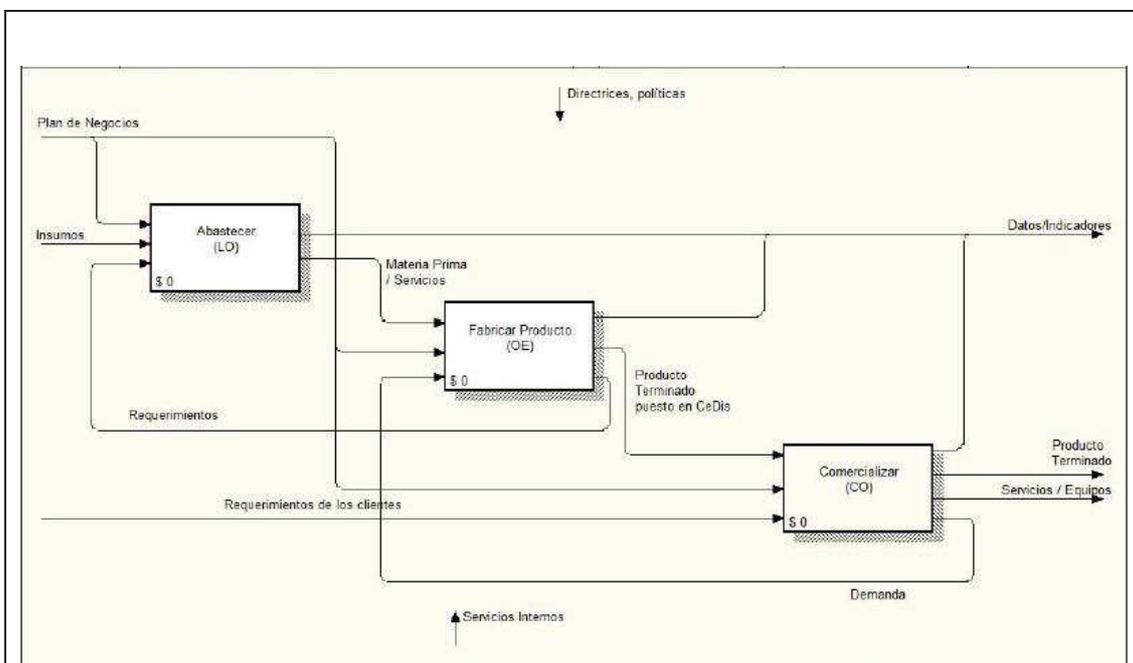


Figura 13: Macro Proceso realización del producto

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.9 Proceso abastecer

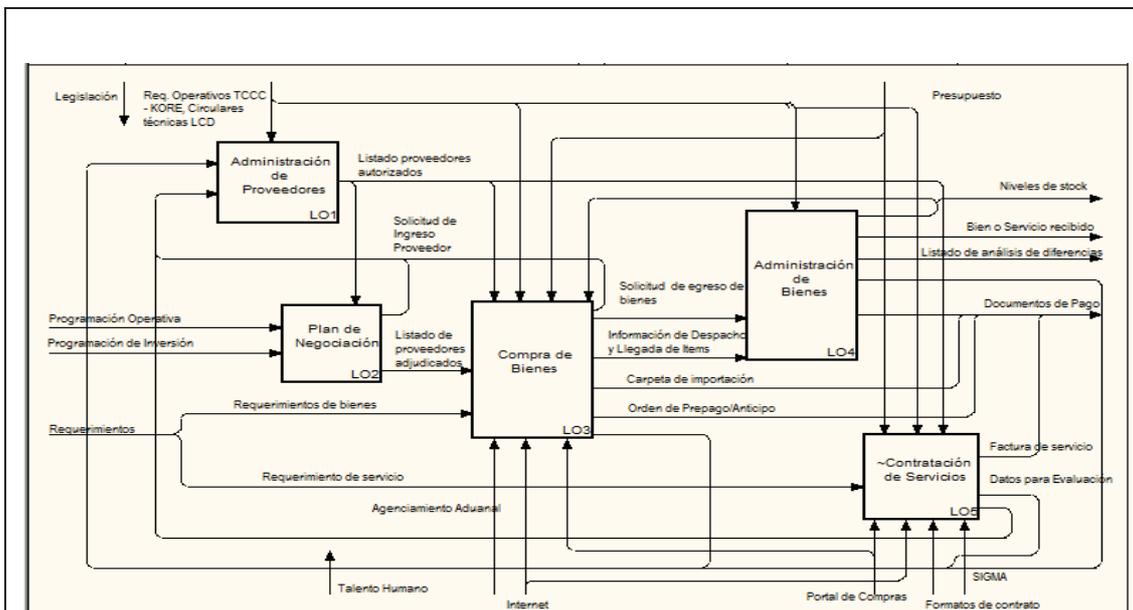


Figura 14: Proceso abastecer

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.10 Proceso fabricar producto

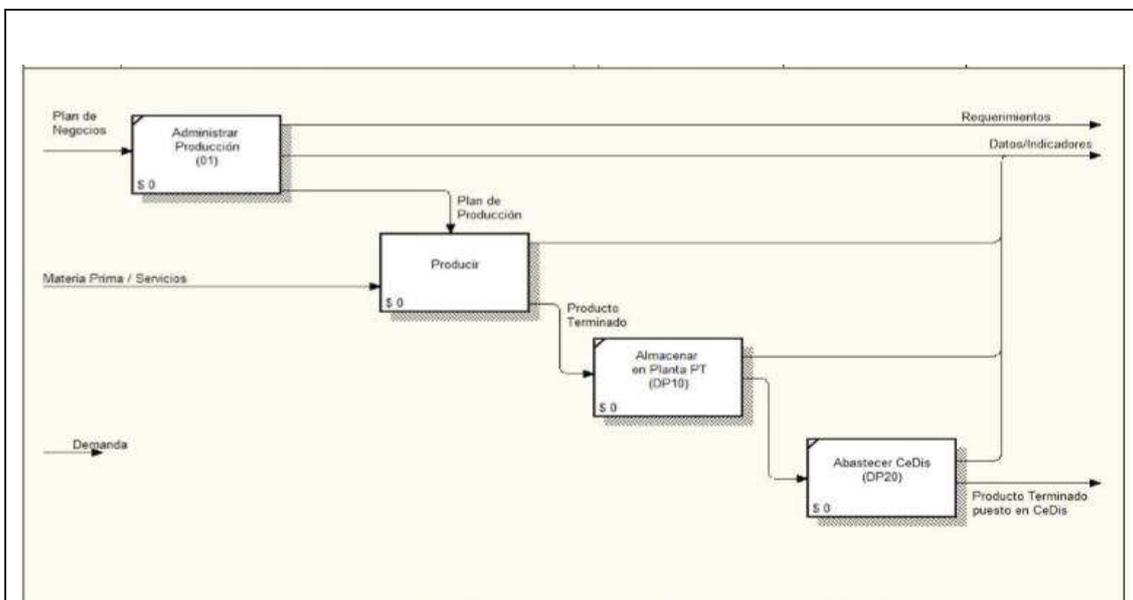


Figura 15: Proceso fabricar producto

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.10.1 Proceso producir

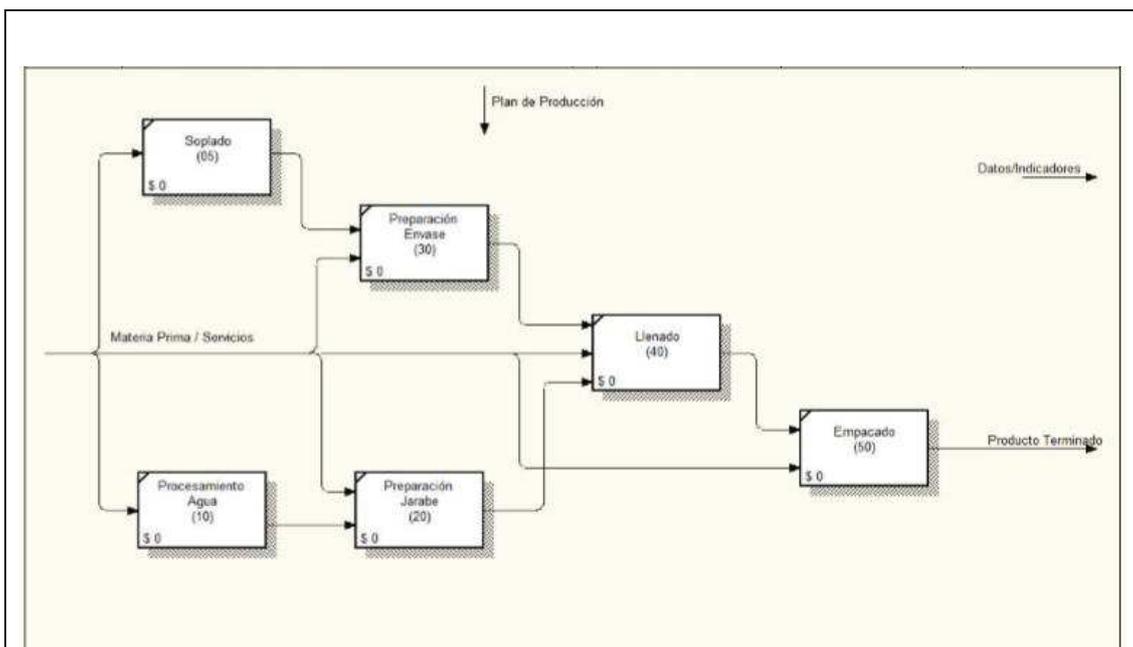


Figura 16: Proceso producir

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.1.11 Proceso comercializar

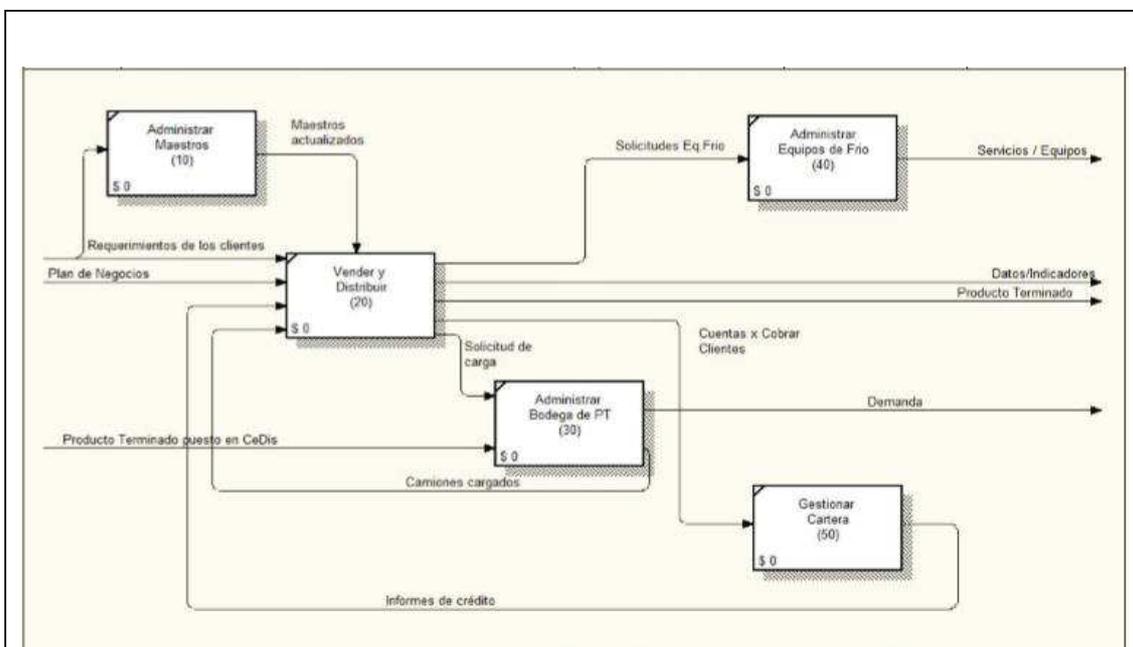


Figura 17: Proceso comercializar

Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.1.4 Macro Proceso medición, análisis y mejora

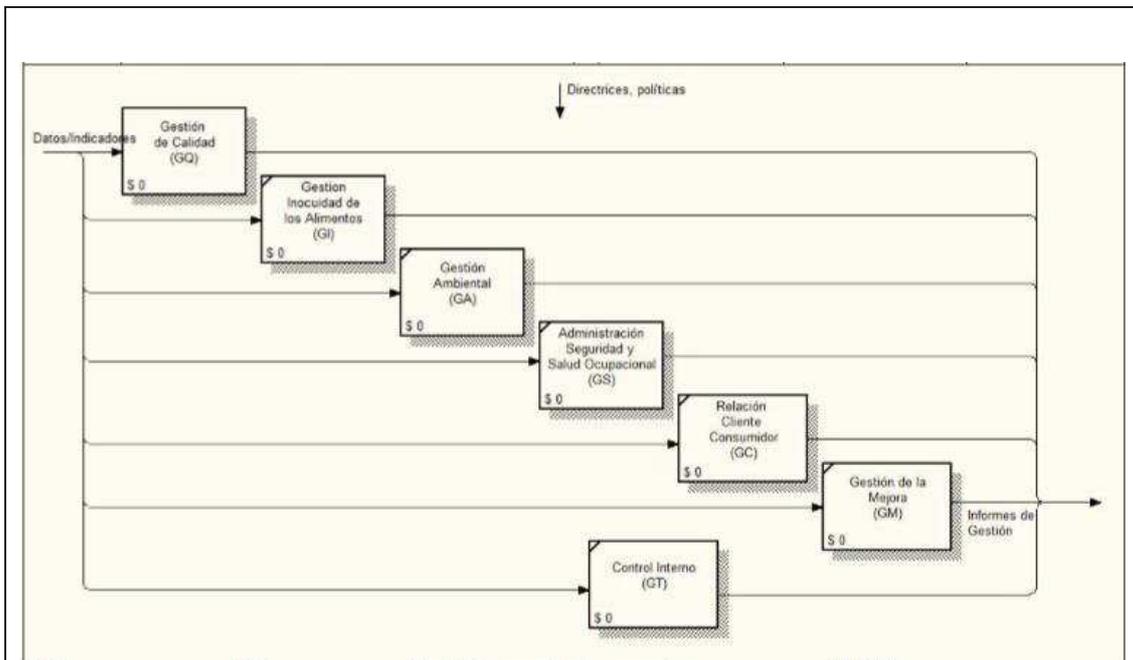


Figura 18: Macro Proceso medición, análisis y mejora

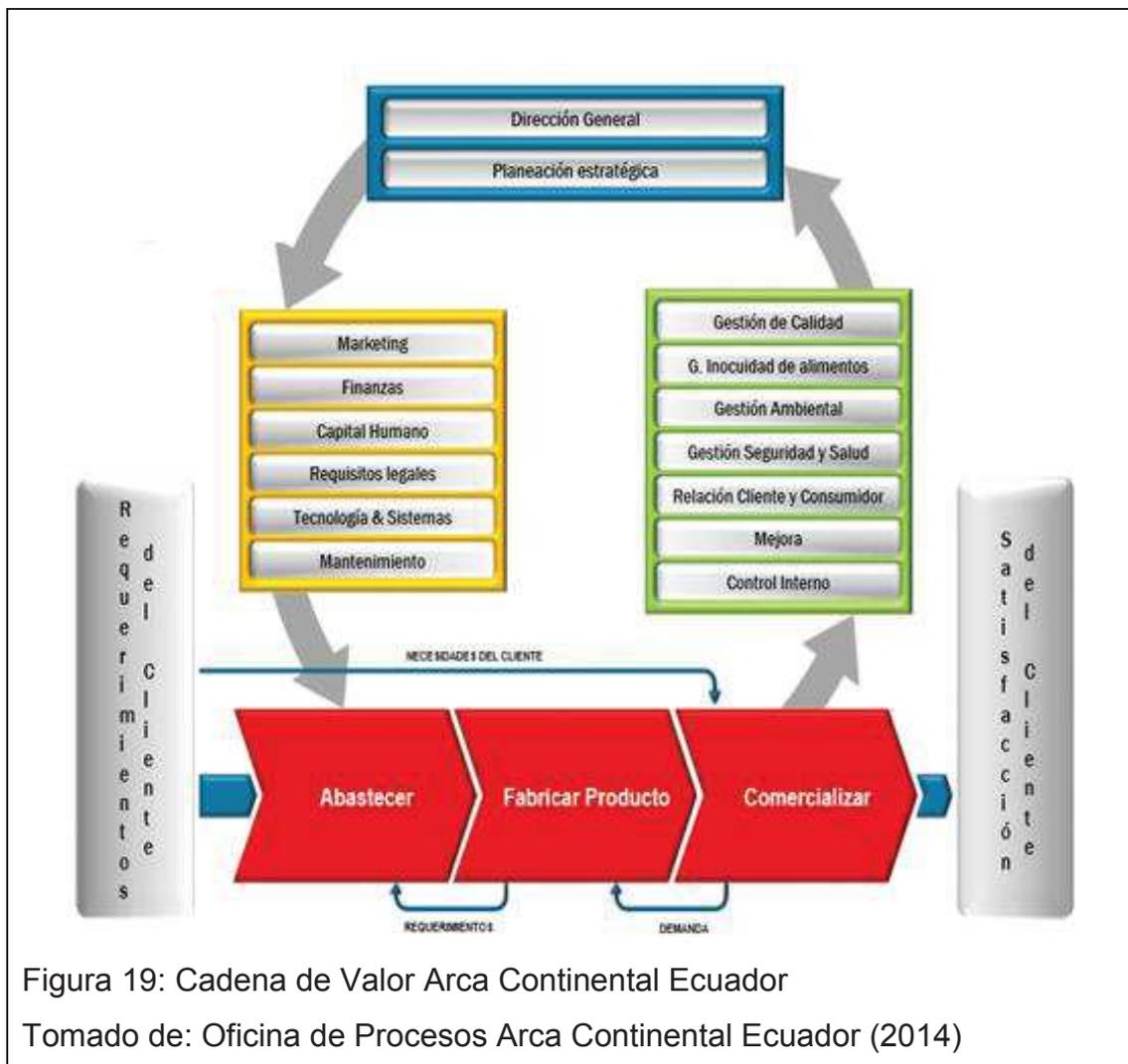
Tomado de: Oficina de Procesos Arca Continental Ecuador (2014)

2.2 Identificación de los procesos críticos y la cadena de valor

La organización es una embotelladora de bebidas en la cual sus procesos de negocio forman parte de la cadena de valor del mismo y están enfocados en el abastecimiento, fabricación y comercialización de sus productos apoyados por los procesos administrativos como son: marketing, finanzas, capital humano, requisitos legales, tecnología y sistemas, mantenimiento, gestión de calidad, gestión Inocuidad de alimentos, gestión ambiental, gestión de seguridad y salud, mejora continua, control interno, relación con el cliente y consumidor.

Por lo tanto los procesos críticos del negocio son: abastecimiento, fabricación y comercialización de las bebidas de la marca Coca Cola, estos procesos son la base para la planeación estratégica de la organización y toda iniciativa debe ir alineada a fortalecer los mismos.

A continuación se detalla un gráfico donde describe la cadena del valor del negocio y sus procesos de apoyo.



2.3 Análisis de los procesos del negocio actuales

En el macro proceso responsabilidad de la dirección se divide en dos procesos como son: Dirección general y Responsabilidad de la Dirección.

El proceso de Dirección general está enfocado en planificar y revisar los sistemas de gestión, también de definir políticas y objetivos para la organización.

El proceso de Responsabilidad de la Dirección se encarga de administrar cuatro funciones muy importantes para la organización como son: planificación de la demanda, planificación estratégica, proyectos y la continuidad del negocio.

El macro proceso Gestionar los Recursos se divide en 6 procesos como son: Marketing, Finanzas, Capital Humano, Requisitos Legales, Mantenimiento, Tecnología y Sistemas.

El proceso de Marketing es responsable de emitir información del negocio como el pronóstico de la demanda el cual definirá el lanzamiento de promociones y estrategias de mercadeo. También se encarga de investigar el mercado y sus competidores, otra función es el manejo de la publicidad y los medios de comunicación.

El proceso de Finanzas su función es administrar: la contabilidad, tesorería, cartera, tributaria, presupuestos, activos fijos y seguros de la organización.

El proceso de Capital Humano está encargado de la administración del recurso humano del negocio enfocado en: selección, reclutamiento, contratación, desarrollo del personal, nomina, salud, comunicación corporativa, bienestar social y seguridad física.

El proceso de Requisitos Legales es el encargado de asesorar y administrar los procesos legales, también de la gestión de los contratos y documentos para el funcionamiento del negocio.

El proceso de Mantenimiento es responsable de la administración de los mantenimientos: industriales, automotrices, edificios, soplado para botellas, equipos de frío.

El proceso de Tecnología y Sistemas su función es apoyar mediante el uso de las tecnologías de la información a los sistemas y servicios informáticos que se brinda a la organización, establecidos en un marco de seguridad informática.

También gestiona y administra los proyectos de tecnológicos mediante el uso de las mejores prácticas del mercado y planifica la continuidad del negocio respecto a la infraestructura informática que lo soporta.

En el macro proceso Realización del Producto, se conforma de 3 procesos muy importantes como son: Abastecer, Fabricar Producto y Comercializar.

El proceso de Abastecer su función es ejecutar los planes de negociación basados en una administración de proveedores que rija la compra de bienes y contratación de servicios y que a su vez soporte la administración de los bienes adquiridos como son las materias primas entre otros insumos.

El proceso Fabricar Producto su rol está basado en los planes de negocio y administración de la producción que está regido por un plan que al ejecutarlo producirá el producto terminado que deberá ser almacenado en las plantas para posteriormente ser trasladado y abastezca a las Cedis (sucursales, agencias) a nivel nacional.

A su vez el proceso Producir se basa en el uso de la materia prima y lo servicios que se adquieren. Este proceso conlleva el procesamiento del agua y en paralelo el soplado de las botellas que posteriormente se prepara los envases y el jarabe para el proceso de llenado y empaçado logrando como resultado el producto terminado.

El proceso de Comercializar se encarga de la administración de los maestros de clientes, la venta, distribución de los productos y gestión de la cartera vencida. También es responsable de la administración de los equipos de frio y las bodegas de producto terminado.

El macro proceso Medición, análisis y mejora mediante los indicadores e información del negocio se enfoca en la gestión de varios procesos como son: calidad, ambiental, inocuidad de alimentos, mejora continua, relación cliente consumidor, administración de seguridad y salud ocupacional. Este proceso

también se enfoca en el control interno de todos los procesos de la organización mediante el uso de la información del negocio.

2.4 Necesidades de los procesos del negocio enfocados a su automatización y del catálogo de servicios asociado

2.4.1 Macro proceso responsabilidad de la dirección

2.4.1.1 Proceso administración dirección general

Este proceso se fundamenta en los sistemas de gestión en los cuales se consolidan los indicadores por cada una de las áreas del negocio este sistema está alojado en *cloud computing*, se alimenta de la información que cada responsable maneja de los sistemas comerciales, financieros, adquisiciones, inventarios, que rigen los procesos del negocio, también de un gestor documental en donde se consolida las políticas, procedimientos, normas y formatos que rigen a la organización y son aprobados por los dueños del proceso responsable.

El negocio requiere de potenciar el uso de sus sistemas de información ya que estos están limitados en recursos y capacidades de procesamiento y almacenamiento actualmente, esto hace que en momentos en que el negocio requiera de mayor capacidad no se disponga y por ende se tenga pérdidas económicas en ventas y participación del mercado, que en este momento son solventadas por inversiones que toman tiempos altos en adquisición, implementación y puesta en marcha.

El catálogo de servicios para este proceso está enfocado en brindar disponibilidad a los usuarios del negocio sobre la infraestructura de red, servidores y servicios de soporte para los sistemas de información.

2.4.1.2 Proceso planeación estratégica

La generación de iniciativas y proyectos que estén alineados a fortalecer los pilares estratégicos del negocio forman parte de este proceso.

Mediante el uso del sistema de información ERP SAP (Sistemas o programas que permiten gestionar la información) se desarrolla la consolidación contable y financiera del negocio, mediante el sistema comercial se desarrolla la consolidación de las ventas, inventarios de producto terminado y la planificación de la demanda, todo esto se controla mediante un balance scorecard (Cuadro de mando integral, herramienta que permite visualizar estrategias) donde se validan indicadores de gestión producto de los sistemas transaccionales y que la ejecución de los proyectos se cumplan en los tiempos con los costos programados.

La ejecución del plan de continuidad del negocio se lo ejecutaría desde el centro de datos en la ciudad de Guayaquil que está en la planta embotelladora, este sitio tiene limitada capacidad de procesamiento y almacenamiento lo que hace necesario buscar soluciones que permitan brindar continuidad al negocio en caso de desastre.

El catálogo de servicios asociado tiene que ver con la disponibilidad y continuidad que requieren los usuarios a toda la infraestructura de cómputo de la organización respecto a sus sistemas de información y redes de datos (Compuesto por equipos y aplicaciones conectados por dispositivos que permiten transportar datos).

2.4.2 Macro proceso Gestionar los Recursos

2.4.2.1 Proceso de Marketing

Del sistema de *Business Intelligence* (Inteligencia de Negocios, conjunto de estrategias que facilitan la toma de decisiones) llamado *Cognos Power Play*

(Aplicación que permite analizar datos en gran volumen) en base a los cubos (Datos obtenidos de diferentes dimensiones de un negocio que se desean analizar) de información desarrollados se obtiene reportes de los pronósticos de la demanda y otros reportes que se requieran, con esta información los ejecutivos del negocio toman decisiones para definir el lanzamiento de promociones y estrategias de mercadeo.

Adicional tenemos un sistema de análisis de mercado en donde se obtiene información que ayuda a analizar el mismo.

Para el manejo de la publicidad y los medios de comunicación se requieren almacenar e interactuar con la información que este subproceso genera de forma confidencial y segura bajo las políticas de Arca Continental mediante el uso de *cloud computing* con un nivel de servicio de 7x24 (Servicio que se ofrece durante las 24 horas del día los 365 días del año).

El catálogo de servicios que utiliza este proceso está enfocado en la disponibilidad de los sistemas de información comercial e inteligencia del negocio.

2.4.2.2 Proceso de Finanzas

El ERP SAP con sus módulos FI en el cual se manejan los sub procesos: activos fijos, tesorería y el plan de cuentas, el módulo CO el cual maneja la parte de costos, FM que administra el presupuesto del negocio, PS que controla los proyectos, SD que administra las ventas de los bienes y del producto hacia la empresa comercializadora, con estos módulos se administra los subprocesos en el área financiera, los cuales están siendo controlados por todos los departamentos que la conforman.

En el proceso de facturación del producto terminado utiliza una aplicación que es propietaria *The Coca Cola Company* la cual se llama *Basis*, este sistema de información entre otros módulos se encarga del proceso de facturación de los

pedidos a nivel nacional, una de las necesidades en este proceso es implementar la facturación electrónica la cual se están validando opciones mediante *cloud computing* con un nivel de servicio de 7x24 ya que este proceso es crítico en la cadena de valor del negocio y representa parte de la imagen de la empresa con los clientes y consumidores.

El catálogo de servicios asociado a este proceso va de la mano de la disponibilidad y soporte a los sistemas de información: SAP ERP y Basis con los cuales se desarrollan estos procesos críticos para el negocio.

2.4.2.3 Proceso de Capital Humano

Es administrado de igual forma por el ERP SAP y su módulo HCM (Modulo Capital Humano en SAP), es provisto de forma centralizada, se manejan los procesos de desarrollo de personal, compensación y nómina.

Para el proceso de selección y contratación se usa una herramienta BPM llamada *MetaStorm* que maneja flujos de autorización que solicitan personal para las áreas que lo requieran.

En el proceso de seguridad física utiliza una aplicación externa para consolidar: actividades, novedades y tareas que involucra el servicio de seguridad con el uso de dispositivos móviles y que es administrada por un tercero con la supervisión del personal de la empresa.

El portafolio de servicio para este proceso tiene que ver con la disponibilidad de la aplicación que está haciendo uso de la infraestructura de servidores y la red corporativa.

2.4.2.4 Proceso de Requisitos Legales

Este proceso es soportado por las aplicaciones: *Microsoft Share Point* (Plataforma que permite guardar, organizar, compartir y acceder a información

desde un dispositivo) para la gestión de los documentos legales y el aplicativo *FielMagister* (Aplicativo registrado por Ediciones Legales) en donde se consolidan las leyes, reglamentos, normativas vigentes que son regidas por las instituciones del Estado.

El portafolio de servicios asociado tiene que ver con la disponibilidad de los servidores donde están alojados los aplicativos, la red corporativa y el internet.

2.4.2.5 Proceso de Mantenimiento

El ERP SAP tiene el módulo PM el cual se encarga de la administración de los procesos de mantenimiento, con los cuales se planifican y programan las actividades para el mantenimiento de los activos del negocio como son los equipos industriales llevando un historial de los mantenimientos y salud de los equipos.

Para el mantenimiento de los equipos de frio se usa la aplicación comercial *Basis* en su módulo de activos fijos con la cual se administran estos equipos en su ciclo de vida útil relacionados a su uso dentro de los locales del cliente.

Respecto a la calibración de equipos en el laboratorio se utiliza la herramienta *Datalyzer* con la cual se obtienen estadísticas y métricas de los procesos de producción para la fabricación del producto.

El portafolio de servicios asociado a este proceso está relacionado con la disponibilidad de los sistemas de información que se manejan en el mismo.

2.4.2.6 Proceso de Tecnología y Sistemas

Como metodología de trabajo en el área se optó por ITIL (Biblioteca de Infraestructura de Tecnologías de Información, metodología que ayuda a la organización a controlar y gestionar recursos), se tiene la aplicación Aranda la cual es una herramienta que está enfocada en ITIL y sus procesos, los cuales

son: Mesa de Ayuda, Administración de Cambios, Administración de Configuraciones, Administración de Incidentes, Administración de Seguridad y Administración de Versiones.

En la Administración de las seguridades las aplicaciones del negocio tienen sus propios módulos de seguridades como: *Basis* (Aplicación Comercial), *Bmobile* (Aplicación Móvil) mientras que otras aplicaciones como *SAP (ERP)*, *Aranda Software (ITIL Compliance* Gestiona el cumplimiento de los procesos) y *Cognos Power Play* (Inteligencia del Negocio) utilizan “single sign-one” (El usuario es autenticado una sola vez y accede a los servicios disponibles) donde la administración de estos usuarios está regida por políticas corporativas en *Windows 2008 Server* (Sistema operativo diseñado para servidores).

Para la administración de las aplicaciones para control de los enlaces de comunicación, servidores, equipos de red y perimetrales se tiene herramientas de Cisco (Empresa mundial de Tecnología Informática con sede en San José-California) y de los proveedores de telecomunicaciones Level3 (Proveedor de Telecomunicación con sede en Omaha, Nebraska que atiende en redes centrales en América del Norte, América Latina, Europa, África y Asia) y Claro (Marca de la empresa de Telecomunicaciones CONECEL que opera en Ecuador desde 1993).

También se tiene estructurada una oficina de proyectos que administra los proyectos del área, para plasmarlos en la aplicación “*Enterprise Project Management*”, la cual está regida mediante la metodología “*PMI*” (*Project Management Institute*, Organización Internacional sin fines de lucro conformada por miembros que establecen estándares y certificaciones para la gestión de proyectos) en donde se tiene formalizada toda la documentación del proyecto desde la constitución del mismo hasta la finalización, incluyendo los entregables para el negocio.

Las capacidades de procesamiento y almacenamiento están sobrepasando la capacidad actual por ello se necesita proveer de recursos informáticos que

permitan brindar al negocio lo que requiere de una manera rápida, segura y a un costo razonable.

El área por su concepción de servicio y basado en la metodología de ITIL maneja un amplio portafolio de servicios que administran todas las plataformas informáticas a nivel nacional como son: servicios de redes y telecomunicaciones, internet, computo distribuido, computo central, soporte a las aplicaciones del negocio y nuevas iniciativas que soporten los procesos del mismo.

2.4.3 Macro proceso Realización del Producto

2.4.3.1 Proceso de Abastecer

Este proceso es administrado mediante el *ERP SAP* con el módulo MM que su rol es la administración de materiales, compras y abastecimiento. Este proceso se inicia con la solicitud de los pedidos que son ejecutados por todas las áreas del negocio para la adquisición de bienes y servicios que son entregados por los proveedores que previamente han sido calificados para el efecto, después de las negociaciones efectuadas con los integrantes del área de Compras se procede a enviar la orden de compra con la cual los proveedores tienen la certeza que la solicitud es válida y requiere su intervención.

Una necesidad para este proceso es la implementación de un *CRM* para el seguimiento con los proveedores y usuarios del negocio de todo el ciclo de la compra para que se culmine con éxito la adquisición del bien o servicio requerido.

El portafolio de servicios para este proceso se relaciona con la disponibilidad del sistema *ERP SAP* y su módulo MM.

2.4.3.2 Proceso Fabricar Producto

En este proceso se crea el producto terminado mediante el uso de las líneas de producción con la ejecución también del proceso de calidad que también es administrado por el *ERP SAP* y su módulo PP en el cual se registra las tareas de producción y mantenimiento que requieren las maquinas industriales.

El catálogo de servicios asociado a este proceso está relacionado a la disponibilidad del sistema *ERP SAP* y su módulo PP con el cual se desarrollan las actividades del mismo.

2.4.3.3 Proceso de Comercializar

Este proceso es uno de los más críticos del negocio el cual es controlado mediante la aplicación *Basis* la cual está bajo la plataforma *OS400* (Creado por IBM, es un sistema operativo que permite gestionar recursos) y que fue creada por *The Coca Cola Company* para el uso de los embotelladores en el mundo, en este sistema de información los usuarios acceden a los módulos que administran: los maestros de clientes, ventas, distribución, cartera, logística y producto terminado.

Este sistema se interconecta con la aplicación *Bmobile* la cual sincroniza los dispositivos móviles llamados *hand helds* los cuales nos sirven para la toma de pedidos de los clientes, también esta aplicación puede presentar información sobre los clientes como: cartera vencida, historial de compras y otros datos que son importantes al momento de gestionar la relación con el cliente en el sitio donde se comercializa los productos de la marca.

La información recabada en el sistema *Basis* nos sirve para que el aplicativo de inteligencia de negocio *Cognos Power Play* genere los cubos y reportes con la información de ventas, producción, cartera que es requerida por los usuarios de las diferentes áreas para gestionar sus procesos de negocio.

El portafolio de servicio para este proceso tiene que ver con la disponibilidad de la infraestructura donde están alojados los sistemas de información, soportados por la red corporativa y la administración de los dispositivos móviles.

2.4.4 Macro proceso Medición, análisis y mejora

2.4.4.1 Proceso Gestión de calidad

Está fundamentado en políticas, procedimientos, normas y registros que son ejecutados mediante el control de todos los procesos de producción que son consolidados en indicadores de gestión que están sistematizados en la aplicación *Datalyzer* mediante el uso de dispositivos móviles como tabletas, esta información se consolida para posteriormente ser analizada y lograr un aseguramiento en la calidad del producto en todo el ciclo del mismo.

Se requiere que el rendimiento de la aplicación permita al usuario realizar sus actividades en el menor tiempo posible, por ende se requiere que la capacidad del servidor virtual donde está alojado esta aplicación deba aumentar.

El portafolio de servicio para este proceso tiene que ver con la disponibilidad de la aplicación *Datalyzer* y los dispositivos móviles.

2.4.4.2 Proceso Gestión ambiental

De igual forma está fundamentado en un marco regulatorio que debe cubrir todos los ámbitos para el cuidado del medio ambiente respecto a la producción del producto, insumos utilizados, desechos, lugares de trabajo, políticas y procedimientos.

La necesidad que tenemos en este proceso es el manejo de la información que se genera con los usuarios internos, proveedores y entes de control de una manera segura, confiable, confidencial y desde cualquier dispositivo, ya que los

tamaños y formatos de la misma son muy grandes, por ende un repositorio de información en *cloud computing* nos ayudaría a solventar esta necesidad.

El portafolio de servicios asociado a este proceso está relacionado con el soporte a las aplicaciones del negocio y a la disponibilidad de los equipos de cómputo que usan los usuarios para sus funciones.

2.4.4.3 Proceso inocuidad de alimentos

Se encarga de garantizar la obtención de alimentos sanos, nutritivos y libres de peligros para el consumo humano, también de asegurar la calidad en la producción y elaboración del producto que se fabrica y que no cause daño al consumidor cuando el mismo sea ingerido.

Esto se lleva a cabo mediante la consolidación de indicadores de la producción y pruebas con el producto terminado ejecutando políticas y procedimientos que soportan el proceso de fabricación.

Las necesidades de este proceso son la mejora en el rendimiento de la aplicación de gestión documental para que el acceso a las políticas, procedimientos y registros sean en el menor tiempo posible.

El portafolio de servicios asociado a este proceso está relacionado al soporte a los usuarios en la aplicación de gestión documental y otras aplicaciones del negocio, también a los equipos de cómputo que ellos utilizan.

2.4.4.4 Proceso mejora continua

Está enfocado en los cambios que debemos ejecutar en los procesos de toda la organización y que son plasmados en la documentación de los procedimientos e indicadores de la gestión realizada.

La necesidad de este proceso es rediseñar la herramienta de gestión documental para que nos permita consolidar y evidenciar las actividades que se han realizado en beneficio de la mejora de los procesos ya que los tiempos de respuesta de la misma no son los adecuados.

El portafolio de servicios asociado tiene que ver con el rediseño y disponibilidad de la aplicación de gestión documental.

2.4.4.5 Proceso relación cliente consumidor

Este proceso se fundamenta en el seguimiento a los casos reportados por el cliente respecto a novedades en el producto y la relación que debemos mantener entre las partes, para ello se usa un sistema de información por la web donde se registran estos reclamos que son escalados al personal que los atiende y se toman acciones dependiendo de los casos.

Las necesidades en este proceso son la mejora en el rendimiento de la aplicación web que administra los reclamos, también la optimización en la disponibilidad de la aplicación para que esté operando desde fuera de la red corporativa y pueda ser accedida en un ambiente seguro por cualquier dispositivo que el negocio requiera.

El portafolio de servicios asociado tiene que ver con la disponibilidad del sistema de información web.

2.4.4.6 Proceso administración de seguridad y salud ocupacional

Está enfocado en la seguridad industrial de todas las plantas productoras, también en la planificación y organización de campañas e iniciativas enfocadas a la salud ocupacional de los empleados de la organización para lograr un mejor lugar para trabajar.

Como necesidades para este proceso tenemos la creación de sistemas vía web para el manejo de la salud ocupacional con los usuarios.

El portafolio de servicios asociado tiene que ver con el soporte a las herramientas computacionales que manejen políticas de seguridad en la red. Respecto a los equipos de cómputo deben cumplir condiciones ergonómicas y de salud ocupacional para el uso de los usuarios.

2.4.4.7 Proceso control interno

Este proceso su rol es controlar mediante la verificación el cumplimiento de las políticas y procedimientos que dicta la organización mediante el uso de cuestionarios con parametrizaciones ya definidas, las preguntas están orientadas a cada uno de los procesos de la organización las cuales son ejecutadas cada año a todas las áreas del negocio con un grupo de personas que se enfocan en revisar que estos cuestionamientos se cumplan mediante la presentación de controles y evidencias que esto suceda.

Producto de esta revisión se presenta un indicador comparado con revisiones de años anteriores y se solicitan planes de acción para remediar los hallazgos encontrados.

La necesidad que tiene este proceso es la consolidación mediante una aplicación web de los cuestionarios que se ejecutan por cada una de las áreas de la empresa generando indicadores históricos y actuales de los mismos.

En este proceso el portafolio de servicios asociado tiene que ver con la entrega de información que el área de Control Interno requiere sobre los procesos del negocio que están siendo revisados como son: permisos con sus roles de usuario asignados a los empleados en las aplicaciones del negocio, reportes de información de los sistemas de información para los procesos que están siendo revisados.

A continuación se detalla una tabla 1 el resumen respecto a lo expuesto anteriormente:

Tabla 1: Necesidades y catálogo de servicios de los procesos del negocio

Macro proceso/Procesos	Necesidades	Catálogo de servicios asociado
Macro proceso responsabilidad de la dirección		
Proceso administración dirección general	Mejorar el rendimiento de los sistemas de información del negocio	Disponibilidad de la infraestructura de cómputo de la organización
Proceso planeación estratégica	Brindar alta disponibilidad a las aplicaciones del negocio	Disponibilidad y continuidad a la infraestructura respecto a sus sistemas de información y redes de datos
Macro proceso gestionar los recursos		
Proceso de Marketing	Almacenamiento e interacción con la información de forma confidencial y segura	Disponibilidad de los sistemas de información comercial e inteligencia del negocio
Proceso de Tecnología y Sistemas	Optimizar el uso de los recursos, mejorando el rendimiento de las plataformas informáticas	Disponibilidad de todas las plataformas informáticas a nivel nacional: servicios de redes y telecomunicaciones, internet, computo distribuido, computo central, soporte a las aplicaciones del negocio
Proceso Financiero	Facturación electrónica de los pedidos a nivel nacional	Disponibilidad y soporte a los sistemas de información SAP ERP y Basis
Proceso Capital Humano	Mayor rendimiento en la ejecución y consolidación del proceso de nómina con los estándares corporativos	Disponibilidad de la aplicación que está haciendo uso de la infraestructura de servidores y la red corporativa
Proceso Requisitos Legales	Mejorar el rendimiento de los sistemas de información del negocio	Disponibilidad de los servidores donde están alojados los aplicativos, la red corporativa y el internet
Proceso Mantenimiento	Mejorar el rendimiento de los sistemas de información del negocio	Disponibilidad de los sistemas de información que se manejan en el mismo
Macro proceso realización del producto		
Proceso abastecer	Implementación CRM para el seguimiento con los proveedores del ciclo de la compra	Disponibilidad del sistema ERP SAP y su módulo MM
Proceso fabricar producto	Están solventadas	Disponibilidad del sistema ERP SAP y su módulo PP
Proceso Comercializar	Facturación electrónica de los pedidos a nivel nacional	Disponibilidad de la infraestructura donde están alojados los sistemas de información: Basis, ERP SAP, Cognos y la administración de los dispositivos móviles
Macro proceso medición, análisis y mejora		
Proceso gestión de calidad	Mayor rendimiento en la ejecución y consolidación de la información en el sistema Datalyzer	Disponibilidad de la aplicación Datalyzer y las tabletas
Gestión de inocuidad de los alimentos	Mejora en el rendimiento de la aplicación de gestión documental	Soporte a aplicación de gestión documental y a la disponibilidad de los equipos de cómputo
Gestión ambiental	Manejo de la información que sea disponible en cualquier momento y desde cualquier dispositivo de forma segura y confiable	Soporte a las aplicaciones del negocio y a la disponibilidad de los equipos de cómputo
Administración de seguridad y salud ocupacional	Creación de sistemas vía web para el manejo de la salud ocupacional	Soporte a las herramientas computacionales que manejen políticas de seguridad en la red y en los equipos de cómputo deben cumplir condiciones ergonómicas y de salud ocupacional
Relación cliente consumidor	Mejorar el rendimiento de la aplicación web	Disponibilidad al sistema de información web
Gestión de la mejora	Rediseñar y mejorar en el rendimiento de la aplicación de gestión documental	Desarrollo y disponibilidad de la aplicación de gestión documental
Control interno	Consolidación mediante una aplicación web de los cuestionarios que se ejecutan por cada una de las áreas de la empresa generando indicadores históricos y actuales	Entrega de reportes con información de los sistemas de información para los procesos que están siendo revisados en cada área

Del análisis expuesto en esta tabla se deduce que la infraestructura actual de hardware está teniendo problemas de saturación en la capacidad ofrecida, lo que conlleva retrasos en los procesos de la operación del negocio en los diferentes sistemas de información, esto adicional a que al incrementar la capacidad y tenerla sobredimensionada ocasionaría sobre costos para el negocio que tendría que asumirlos o pérdidas en el caso que los sistemas no soporten las necesidades de la organización en momentos que la requiera.

También la implementación de nuevas soluciones tecnológicas involucra tiempos altos en la implementación de las mismas ya que el entorno de la infraestructura actual está enfocado a capacidades ya establecidas y que igual que en el caso anterior incrementaría los costos de la operación del negocio.

CAPITULO III. CLOUD COMPUTING

3.1 Definiciones y características

Cloud computing es el resultado de la innovación y el adelanto tecnológico desde los procesadores multinúcleo (Mejora el rendimiento y la eficacia permitiendo ejecutar varios programas al mismo tiempo repartiéndolos en cada núcleo o cerebro) con el cual el ahorro de energía y la capacidad de procesamiento en simultaneo permite que las aplicaciones puedan procesar a la vez varias tareas, logrando una optimización de su uso y mayor disponibilidad para los usuarios.

Este desarrollo tiene que ver también con los *clúster* que es un conjunto de equipos que procesan en paralelo y se compone por servidores (Aplicaciones o computadores donde se ejecuta un programa que realiza una tarea en ayuda de otra) interconectados por la red entre ellos, los usuarios lo ven como un solo recurso unificado que no necesariamente tiene las mismas características.

Uno de los paradigmas que rompió fue que los equipos de cómputo físicos sean reemplazados por máquinas virtualizadas (Programa que simula a una computadora permitiendo ejecutar aplicaciones) (Columbus, 2012) con capacidades mejoradas y dinámicas a las de un equipo físico, esto se logró mediante la implementación de una capa de *software* llamada hipervisor (Monitor de máquina virtual es una plataforma que permite visualizar varios sistemas operativos en un mismo computador) que administra y consolida los recursos físicos de los equipos de cómputo y presenta esas capacidades para que sean usadas en aplicaciones y servicios que requieran las organizaciones o usuarios.

El *cloud computing* viene de las palabras *cloud* que significa nube que la relacionamos con la infraestructura física sobre la cual se desarrolla y su medio de conexión es internet y la palabra *computing* que su significado es computación. Los usuarios que usan el *cloud computing* desconocen qué tipo

de infraestructura de *hardware* (Parte física de un dispositivo o sistema) y donde está ubicado los centros de datos que brindan estos servicios. (Torres, 2011, p. 67)

Básicamente hemos ligado este concepto del *cloud computing* a imaginar equipos computacionales que ya no están en nuestros centros de datos sino en lugares donde no los controlamos pero que nos brindan un servicio mediante el internet global, es decir estamos volviendo al pasado en donde los *mainframe* (computadora central que procesa una gran cantidad de datos) controlaban todos los procesos informáticos de forma central haciendo una analogía a nuestra realidad actual, el *cloud computing* es ese cumulo de recursos informáticos donde los usuarios concentran sus aplicaciones y servicios.

El *NIST* (Instituto Americano de Estándares y Tecnología) hizo una definición muy real del *cloud computing* en donde se indica que es un acceso bajo demanda a través del internet a un conjunto de recursos compartidos configurables como son: almacenamiento, redes, servidores, aplicaciones y servicios, también se detalla que estos servicios son entregados por parte del proveedor sin mayor esfuerzo operativo del mismo ya que se tiene la capacidad para brindarlos y quitarlos cuando se requiera sin necesidad de su intervención y solamente con la interacción del cliente que requiere estas capacidades con una plataforma que comercializa los servicios en línea (Torres, 2011, p. 68), como se muestra en la figura 20.



Figura 20: Características y modelos de servicios en cloud computing
Tomado de: (Brunette, Mogull, 2009)

A continuación detallo algunas características descritas en la figura 20:

Amplio acceso a la red

Tenemos recursos en la red con los cuales accedemos mediante el internet, estos recursos pueden ser: computadores portátiles, teléfonos móviles, tabletas como se describe en la figura 21.



Figura 21: Recursos de TI que acceden mediante cloud computing
Tomado de: (Mendez, 2010)

Elasticidad y rapidez

Poder crecer y decrecer bajo demanda en las capacidades adquiridas mediante el *cloud computing* de forma automática.

Servicio supervisado

Esta solución es administrada por los proveedores en donde mediante el monitoreo y control que es generado hace que el cliente se sienta confiado en que los servicios son llevados de forma óptima.

Autoservicio a la carta

Esto permite de forma automatizada que el cliente pueda en cualquier momento poner o quitar servicios que requiera, sea por aumento o decremento de las necesidades del negocio.

Puesta en común de recursos

Los recursos que tiene el proveedor para brindar el servicio de *cloud computing* al cliente son compartidos en la infraestructura que los soporta (NIST, 2011) ya que serán para el uso de varios clientes según sus necesidades, de esta forma la asignación de estos recursos se hace de forma dinámica, aprovechando al máximo la capacidad disponible. (NIST, 2011)

Voy a describir los modelos de servicio que se describe en la figura 22 en *cloud computing*:

Infraestructura como servicio (IaaS).- En este modelo se comercializa proveer servicios de provisión de infraestructura a los usuarios en los siguientes ámbitos: sistemas operativos (Programa o conjunto de programas que permiten transmitir datos), virtualización (Simulación de un recurso tecnológico) de servidores, capacidad de almacenamiento y red.

Este servicio se provee mediante una plataforma de virtualización en donde el cliente solo paga lo que consume. De esta forma el proveedor se encarga de proveer los recursos necesarios por el cliente.

Plataforma como servicio (PaaS).- Este servicio permite a los clientes instalar el software (Uno o varios programas que permiten realizar tareas en un sistema) desarrollado por ellos y la administración del mismo queda en manos suyas.

Mientras que el proveedor controla la infraestructura de servidores y brinda la disponibilidad pactada con el cliente.

Mediante este servicio se puede cumplir con los requerimientos de ciclo de vida del software.

Software como servicio (SaaS).- Los clientes en este servicio usan las capacidades requeridas a nivel de hardware y software para usar los sistemas de información que requiera la organización y que han sido parametrizados (Dato o datos importantes que permiten valorar una situación o recurso) previamente por el cliente. (Carrero,2014), (Aguilar, 2012)

El cliente accede a este servicio generalmente usando los navegadores (Aplicaciones que permiten acceder a información mediante una red como el internet) de internet mediante la web.

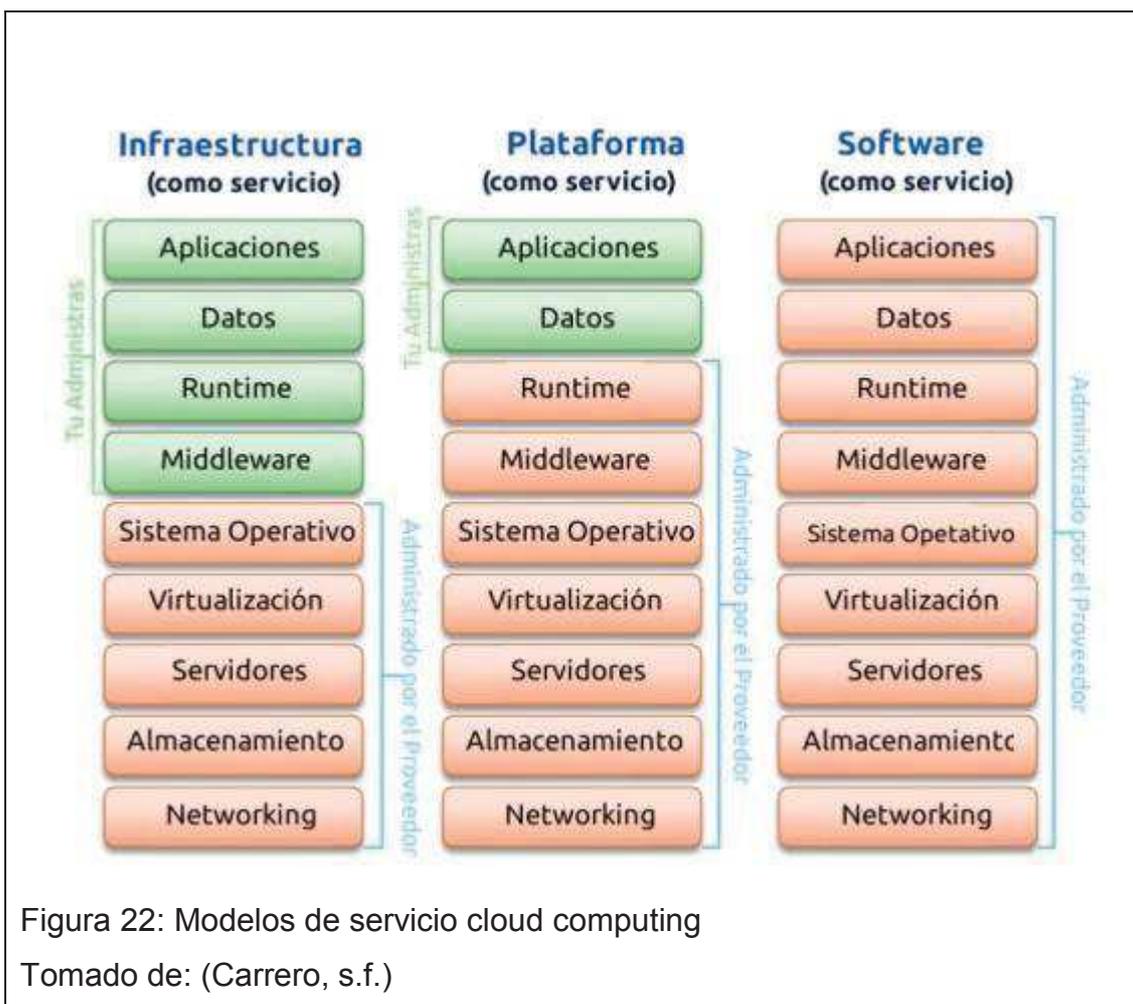
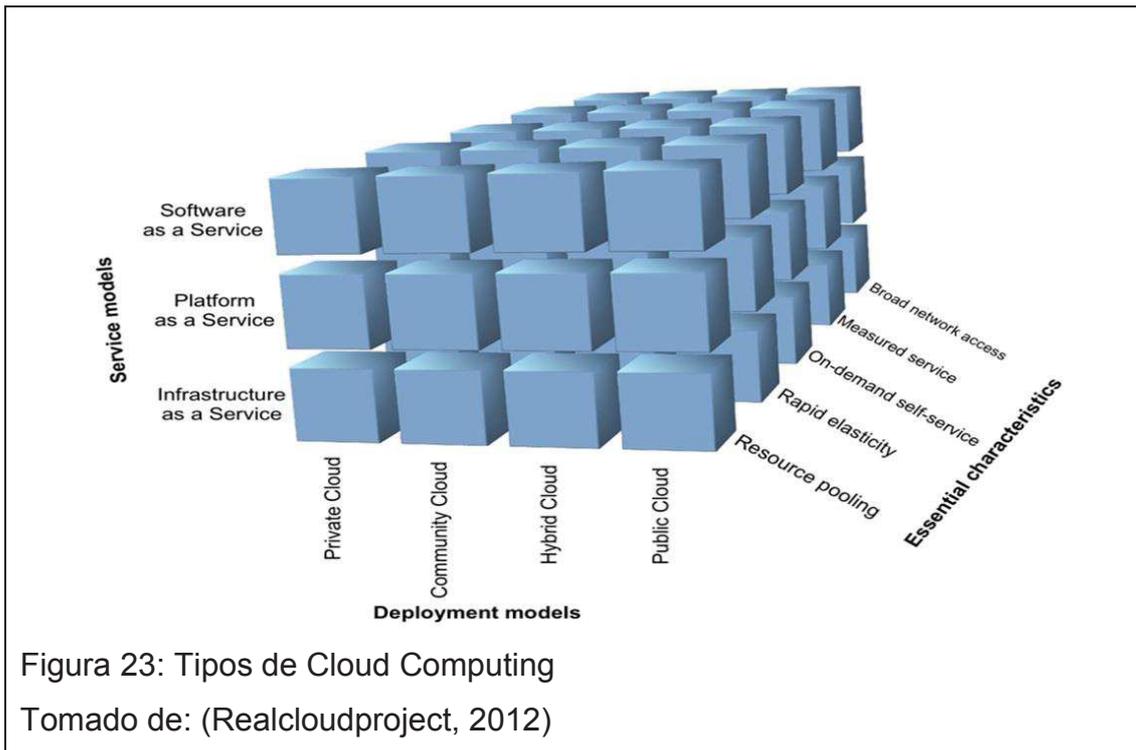


Figura 22: Modelos de servicio cloud computing

Tomado de: (Carrero, s.f.)

3.2 Tipos de *cloud computing*

El *cloud computing* se divide en cuatro tipos o modelos de implementación como son: público, privado, híbrido y comunitario que dependerán de que forman son provistos y donde están instalados, a continuación más detalle de cada uno de ellos.



3.2.1 Cloud computing público

Como su nombre lo indica el modo de acceso a este tipo de *cloud* es abierto y público, están disponibles para cualquier usuario que pueda usarlos con costo y de forma libre sin costo alguno.

Otras características del *cloud computing* público son: menor velocidad de acceso que otras soluciones de *cloud computing*, infraestructura que provee los servicios es arrendada, gobernabilidad delegada, para sistemas críticos del negocio e implementación de escritorios virtuales no es recomendable usarla.

3.2.2 Cloud computing privado

Este tipo de *cloud computing* generalmente está dentro de las instalaciones del usuario, lo que permite tener una mejor interconexión con sistemas internos de las organizaciones, se puede manejar esquemas de seguridad y niveles de servicio acordes a las políticas de la organización. (Cebrián, Bonet, Ballester, 2012)

Otras características del *cloud computing* privado son: gobernabilidad total, no está directamente dependiente del internet, implementación de escritorios virtuales, mayores capacidades de la infraestructura desplegada a nivel almacenamiento y red.

3.2.3 Cloud computing híbrido

Consiste en combinar la infraestructura local de la empresa con el *cloud computing*, de esta forma se aprovecha las capacidades de la nube pública por ejemplo respecto a almacenamiento y se mantienen las aplicaciones críticas del negocio bajo el control de la organización.

Este tipo de *cloud* es una buena estrategia para ir evaluando el paso de todas las aplicaciones del negocio al *cloud computing* privado o público.

Otras características del *cloud computing* híbrido son: mayor disponibilidad del servicio por ende menor incidencia a fallas, facilidad de acceso, integración de dos tipos de *cloud*.

3.2.4 Cloud computing comunitario

Esta creada, soportada y administrada en algunos casos por la misma organización que la patrocina, también puede tener relación con otras organizaciones.

Puede estar operando dentro o fuera de las instalaciones de las organizaciones, tiene muy claro cuál es su misión o interés dentro de la comunidad. (Cebrián, Bonet y Ballester, 2012)

3.3 Comparación del *cloud computing* frente a entornos tradicionales

El *cloud computing* revoluciono el día a día de las personas, logrando un cambio de paradigma en sus labores diarias desde en un principio utilizando su

computador para actividades como acceso a internet desde su trabajo o hogar, en donde la información estaba alojada en nuestros discos duros de los computadores mientras que ahora utilizando los dispositivos móviles (Think Big, 2012) como el *smartphone* (Teléfono móvil con funciones similares a un computador) o tabletas (Ordenador personal móvil con pantalla táctil) que nos permiten acceder desde cualquier parte del mundo a nuestros datos que están alojados en *cloud computing* y que nos han ayudado a comunicarnos en un mundo digitalizado en donde el manejo de la información es la base para el desarrollo de los negocios y la vida de las personas ya sea compartiendo imágenes o videos en *Facebook* (Es un sitio web de redes sociales que permite publicar información), *Twitter* (Servicio que permite publicar mensajes en la red), *Instagram* (Aplicación que permite publicar fotos y videos en la red) que son las aplicaciones colaborativas más conocidas en el mundo.

Facebook en el 2010 había superado los 500 millones de usuarios en el mundo que emitan e interactúan en su plataforma generando millones de comentarios y compartiendo información de su entorno. (Torres, 2011, p. 24)

En un estudio de Nokia realizado a principios del 2011 más de la mitad de españoles acceden a internet a través de su equipo móvil. (Torres, 2011, p. 24)

Estos cambios han logrado que tengamos en los actuales momentos más información digitalizada que almacenada en documentos físicos, mediante el uso de equipos computacionales que tienen bajos costos y soluciones móviles que pueden reemplazar a los antiguos ordenadores, que brindan equipos con tamaños compactos y con capacidades de procesamiento que pueden ayudarte a ejecutar en la palma de la mano actividades de tu trabajo y hogar, todo esto orquestado por una infraestructura de telecomunicaciones en donde está alojado el internet, la masificación de estos servicios y su evolución ha logrado cambios importantes que han impactado en la vida diaria de las personas y son reflejo de la globalización del mundo.

3.4 Ventajas y Desventajas de *cloud computing*

3.4.1 Ventajas de *cloud computing*

- El *cloud computing* privado permite asegurar la información del negocio y administrarla en centros de datos especializados que tengan todas las condiciones necesarias para hacerlo.
- El *cloud computing* público no requiere de inversiones costosas, mantenimientos periódicos, respaldos de información e implementaciones de servidores locales para brindar los servicios, estos temas están a cargo del proveedor que brinda los servicios, el cual debe proveerlos y planificar su capacidad disponible.
- En el *cloud computing* público el retorno de los gastos o inversiones realizadas son mucho más rápido que en otros tipos de *cloud computing*.
- Los costos del *cloud computing* público son pagados en base al uso que tiene este servicio con el cliente.
- Cuando se implementa *cloud computing* privado el hecho de manejar la información internamente permite esquemas de seguridad más controlados por la empresa.
- El *cloud computing* híbrido tiene como ventaja un bajo costo inicial de inversiones y gastos ya que estos son evaluados dependiendo de las necesidades de la organización.
- En un escenario de *cloud computing* híbrido el crecimiento de las necesidades de la organización sería bajo demanda mediante los servicios en la nube como: SaaS, PaaS o IaaS, de esta forma la empresa ahorraría recursos ya que no invertiría en el caso tradicional con equipamiento que posiblemente no lo use con frecuencia y que mediante

esta modalidad lo utilice dependiendo del requerimiento, como por ejemplo: en ventas por temporada navideña o capacidad de almacenamiento para respaldo de información.

3.4.2 Desventajas de *cloud computing*

- Son más costosos mantener los servicios en el *cloud computing* privado que en el *cloud computing* público.
- Los servicios entregados por el *cloud computing* público dependen directamente de la provisión del internet y también están expuestos a que la información pueda ser accedida o manipulada por terceras personas que interactúan con estos servicios.
- En el *cloud computing* público la integración con soluciones internas de las organizaciones puede ser un problema si no se tiene toda la información de cómo está plasmada la infraestructura pública ofrecida al cliente.
- El *cloud computing* público no debe ser usado para sistemas misión crítica del negocio.
- En el *cloud computing* público para la implementación de escritorios virtuales existe un mayor grado de dificultad para proveerlos.
- En el *cloud computing* privado existe un desembolso de recursos iniciales para adquirir la infraestructura requerida, nos permite a futuro estar limitados respecto a la escalabilidad y crecimiento del equipamiento contratado.

3.5 Seguridad en *cloud computing*

Cualquier tipo de iniciativa, control o remediación respecto a la seguridad en cualquier infraestructura informática siempre será bienvenida ya que no existe Sistema de información asegurado en un ciento por ciento de cualquier vulnerabilidad externa por fuera de la organización o interna por parte de colaboradores o socios de negocio, tomando en cuenta este antecedente, la seguridad en *cloud computing* abarca las diferentes capas que lo conforman y dependen del servicio que se está contratando al proveedor ya sea porque la administración por ejemplo del sistema de información en un escenario con IaaS es responsabilidad del cliente y en otros casos como SaaS es del proveedor por ello debemos definir muy claramente cuál es el alcance y la necesidad que requiere el negocio para una solución en *cloud computing* que nos brinde los niveles de seguridad acordes a la criticidad de la información que confiamos.

Podemos solicitar a los proveedores mejores niveles de seguridad que permitan un aislamiento de nuestra infraestructura en *cloud* lo cual conlleva equipamiento adicional que asegure a nuestros servicios y sistemas de información logrando protegerlos en mayor grado que el resto de aplicaciones de otros clientes pero a costos más altos.

La tecnología nos ha permitido separar de manera virtual las redes de comunicación, los volúmenes de almacenamiento de información, las capacidades de procesamiento; de esta forma podemos manejar confidencialidad en el acceso de los administradores, clientes y proveedores a la infraestructura de *cloud computing*.

Parte importante del manejo de la información en *cloud computing* es la integridad y confiabilidad de los datos que están alojados en los sistemas de información que son soportados mediante funcionalidades que permitan implementar algoritmos (conjunto de operaciones que permiten llegar a una solución) de encriptación (Ocultar y proteger datos de forma aleatoria), controles

de autenticación (Valida la identidad de una persona o proceso para acceder a un recurso) y monitoreo de eventos en la plataforma de *cloud computing*.

3.6 Marco de referencia de Implementaciones en *cloud computing*

Para realizar una implementación en *cloud computing* debemos basarnos en lo siguiente:

Debemos tener definido un marco de gobierno que administre el *cloud computing* en donde tengamos: marco de control, políticas, procedimientos, plan de capacitaciones.

Tiene que estar claro que tipo de solución requiere el negocio sean estas de tipo: infraestructura, plataforma, aplicaciones o mixta.

Debemos identificar claramente cuáles son los alcances y beneficios esperados por el proyecto como: incremento de productividad, reducción de gastos e inversiones, reprocesos en el manejo de la información, generación de capacidad con la celeridad que el negocio demanda, flexibilidad para el crecimiento o decrecimiento de la capacidad instalada.

Estructurar contratos que plasmen las soluciones a implementar con acuerdos de niveles de servicio acordes a las necesidades del negocio, también se debe formular: multas, pólizas y penalidades acordes a la criticidad de la información que se maneja.

Se debe hacer un análisis de riesgos exhaustivo con planes de mitigación (Ayuda a tomar medidas para reducir vulnerabilidades o riesgos) y priorización de los mismos.

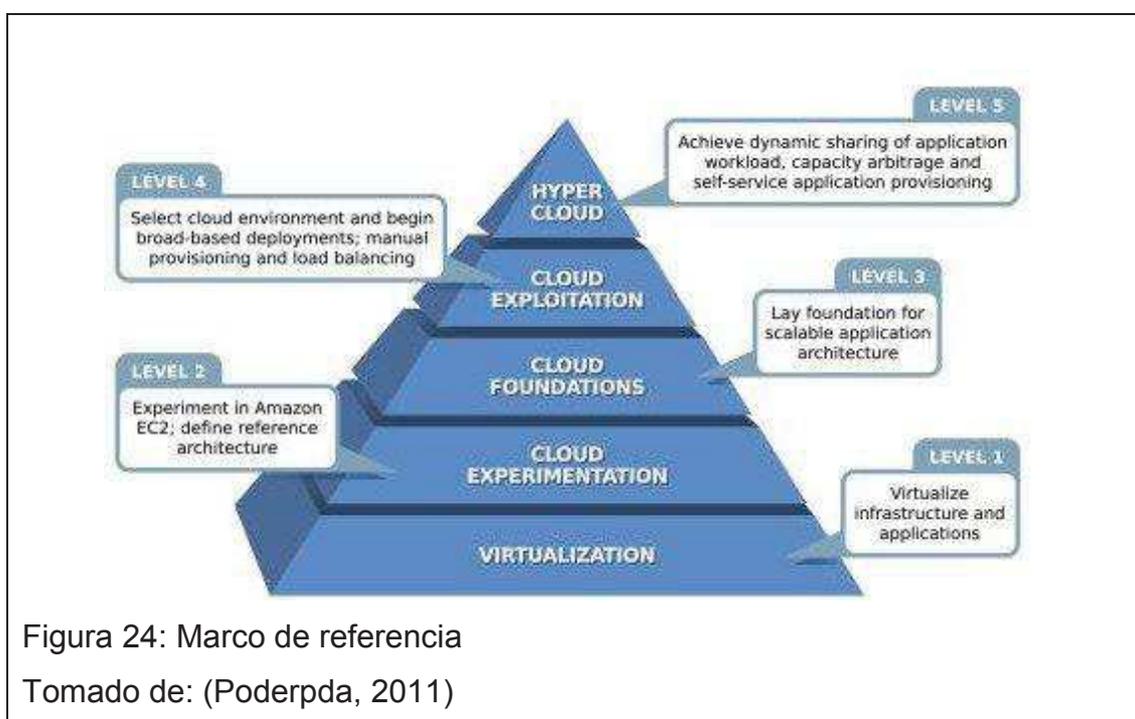
Buscar la competencia entre proveedores con formulaciones de concursos o licitaciones que permitan que los participantes manejen estándares de ética y profesionalismo en sus propuestas de valor al negocio.

Realizar un plan de migración que contribuye a los ahorros en los costos de la organización, identificando los responsables y la secuencia de migración a la solución.

Debe el área de auditoría interna estar controlando el avance del proyecto, los entregables en cada etapa, también debe evaluar los beneficios esperados y los controles que se iban a implementar en el proyecto.

Crear los indicadores de gestión para el proyecto de *cloud computing* a ejecutarse donde se formulen entre otros los siguientes indicadores:

Incremento de ingresos y reducción de costos, cumplimiento de niveles de servicio con el proveedor, costos razonables de capacidad instalada, disponibilidad de la solución, mejora en el tiempo de ejecución de los procesos del negocio. (PiCloud, s.f.)



Como se describe en la figura 24 podemos definir un marco de referencia que nos permita implementar *cloud computing* dividido en 5 niveles, los cuales son los siguientes:

- Partimos de que nuestras aplicaciones están alojadas en servidores virtuales, esto nos permitirá tener flexibilidad para migrar a cualquier entorno virtual que este en *cloud computing*.
- Podemos realizar pruebas para validar cómo se comportan nuestras aplicaciones y servicios informáticos en proveedores como: *Microsoft Azure* y *Amazon EC2*.
- Crear soluciones base en *cloud computing* que nos permitan servir como referente para implementaciones de ambientes productivos escalables.
- Seleccionar el tipo de *cloud computing* a utilizar dependiendo de las necesidades del negocio e implementar escenarios con las aplicaciones y servicios que el negocio requiera de forma de abarcar la mayoría de necesidades. Aprovisionando y equilibrando las capacidades de forma manual.
- Solicitar que el proveedor maneje aprovisionamiento dinámico de la capacidad de los recursos disponibles en los servidores, dependiendo de las necesidades de las aplicaciones del negocio y manejando auto servicio de las capacidades que se requieran. (Poderpda, 2011)

3.7 Proveedores de soluciones de *cloud computing*

Existen varios proveedores que están brindando servicios en *cloud computing* como son: *Amazon Web Services*, *Microsoft* (Multinacional estadounidense fundada por Bill Gates dedicada al sector de software y hardware), *IBM*, *Level3* y *TelcoNet* (Proveedor ecuatoriano de servicios informáticos e internet) *Telconet*. (s.f.) los cuales utilizan su infraestructura local y regional para brindar estos servicios.

Realizando un análisis de la publicación de (*Gartner*, 2014) respecto a los proveedores que comercializan la Infraestructura en la nube como servicio, a

continuación se describe en el cuadrante mágico de la figura 25 como están posicionados los proveedores en el mundo respecto a este modelo de nube:



Figura 25: Cuadrante Mágico de Infraestructura en la nube como servicio
Tomado de: (Gartner, 2014)

Como se describe en la figura 25 respecto al cuadrante mágico de IaaS, los líderes que están posicionados son: *Amazon Web Services (AWS)* y *Microsoft*.

En el cuadrante de jugadores de nicho están posicionados: *Rackspace*, *Virtustream*, *Dimension Data*, *Vmware*, *Fujitsu*, *Joyent*, *HP*, *GoGrid*. (Gartner, 2014).

En el cuadrante de jugadores de nicho están posicionados: *Rackspace*, *Virtustream*, *Dimension Data*, *Vmware*, *Fujitsu*, *Joyent*, *HP*, *GoGrid*.

A continuación vamos a analizar a los proveedores que están en el cuadrante de líderes:

- *Amazon Web Services (AWS)* es una empresa subsidiaria de *Amazon.com* este proveedor de servicios está dedicado al *cloud computing* dando soluciones automatizadas de valor agregado con infraestructura robusta y de forma flexible que se adapte a las necesidades que el cliente requiera.

Tiene centros de cómputo en diferentes regiones del mundo como: EE.UU., Irlanda, Japón, Singapur, Australia, Brasil y próximamente en China. Cuenta con servicios personalizados para el gobierno federal de EE.UU.

El soporte se proporciona en diferentes idiomas como son: inglés, japonés y portugués. También tienen personal técnico en otros idiomas como: alemán, español, hindú, coreano y mandarín.

Los servicios más importantes que ofrecen son: *Elastic Compute Cloud (EC2)* es un servicio web que brinda capacidad de procesamiento modificable y que facilita recursos informáticos escalables presentándolos en la web.

Amazon AppStream es un servicio flexible y de baja latencia que le permite transmitir aplicaciones que emplean muchos recursos.

Amazon WorkSpaces es un servicio de escritorios virtuales gestionados que permite a los clientes aprovisionar fácilmente escritorios para que los usuarios finales accedan a los documentos, aplicaciones y recursos que necesiten desde cualquier dispositivo sea este: tableta, *smartphone*, computadoras portátiles o de escritorio. (Gartner, 2014), (Amazon Web Services, s.f.)

Describo en la figura 26 como se construye la solución de *cloud computing* para la organización con Amazon:

Cálculo: instancias de Amazon EC2:

	Descripción	Instancias	Uso	Tipo	Opción de facturación	Coste mensual
[-]	Portal EPV	1	100 % utilizado/m	Windows y SQL Server Web en m3.2xlarge Optimizadas para EBS	Reservada intensa d	\$ 398.94
[-]	Web Campus	1	100 % utilizado/m	Windows en c3.2xlarge	Reservada intensa d	\$ 43.92
[-]	Web Services	1	100 % utilizado/m	Windows en m3.xlarge	Reservada intensa d	\$ 157.38
[-]	Adma	1	100 % utilizado/m	Windows y SQL Server Web en m1.large	Reservada intensa d	\$ 104.68
[-]	Aplicaciones BI	1	100 % utilizado/m	Windows en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 459.70
[-]	Planning BI	1	100 % utilizado/m	Windows y SQL Server Web en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 527.78
[-]	Bases Datos	1	100 % utilizado/m	Windows y SQL Server Std. en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 811.06
[-]	Fiel Magister	1	100 % utilizado/m	Windows en c3.large	Reservada intensa d	\$ 11.72
[-]	Archivos	1	100 % utilizado/m	Windows en m1.xlarge Optimizadas para EBS	Reservada intensa d	\$ 213.02

Figura 26: Amazon Web Services Simple Monthly Calculator
Adaptado de: (Calculator.s3.amazonaws, s.f.)

- *Microsoft* es uno de los líderes en el cuadrante mágico de *Gartner* (2014) que está por debajo de *Amazon Web Services* pero que ha tenido un cambio de estrategia de negocio enfocado al *cloud computing* ya que brindan servicios de software a través de la nube y su solución *Azure* inicialmente era PaaS, *Microsoft* lanza servicios de infraestructura *Azure* que tienen incluido provisión de máquinas virtuales con *Azure*, servicios de redes virtuales *Azure* de esa forma ingresa al modelo IaaS.

Los servicios de Infraestructura *Azure* son presentados desde varios centros de cómputo ubicados en: EE.UU., Irlanda, los Países Bajos, Hong Kong, Japón, Singapur, China y Brasil. (Gartner, 2014), (Microsoft Azure, s.f.).

El soporte al usuario se lo ejecuta en diferentes idiomas en horario de oficina en Inglés, francés, alemán, italiano, español, japonés, coreano, mandarín y portugués. Cuando los servicios son 24/7 el apoyo se ofrece en inglés y japonés.

Los servicios más importantes que ofrece son los siguientes:

Aprovisionamiento de máquinas virtuales utilizando *Hyper-V* (Aplicación de virtualización que ayuda a mejorar procesos) esto se paga por máquina virtual por minuto al mes de la infraestructura que solo se utiliza y podrá ejecutar o sacar de funcionamiento recursos cuando lo desee.

Almacenamiento en discos duros virtuales independientes de las máquinas virtuales que se tenga.

Azure Express Route este servicio maneja la conectividad de terceros es a través de la red, no tiene soporte para topologías de red complejas.

Azure Active Directory este servicio maneja mediante el *cloud computing* la administración de tus usuarios para sus aplicaciones del negocio y servicios relacionados.

Crear soluciones en *Azure* con los lenguajes de programación más conocidos en el mundo como son: *Java* (Lenguaje de programación orientado a objetos), *NET* (Plataforma que permite desarrollar aplicaciones seguras y robustas), *PHP* (Lenguaje de programación de tipo de datos dinámicos), *Node.js* (Plataforma Java Script que permite crear aplicaciones), *Python* (Diseñado para enfatizar la productividad y la legibilidad del código) o *Ruby* (Programación divertida y flexible para el programador). Las herramientas integradas de *Visual Studio* (Herramienta que permite desarrollar aplicaciones) permiten agilizar los trabajos de desarrollo, depuración e iteración de las aplicaciones. (Gartner, 2014), (Microsoft Azure, s.f.).

En la figura 27 se describe cómo se puede crear la solución en Azure para la organización con otra herramienta como es la hoja de cálculo *Microsoft Azure Pricing Calculator* que está en el Anexo 4.

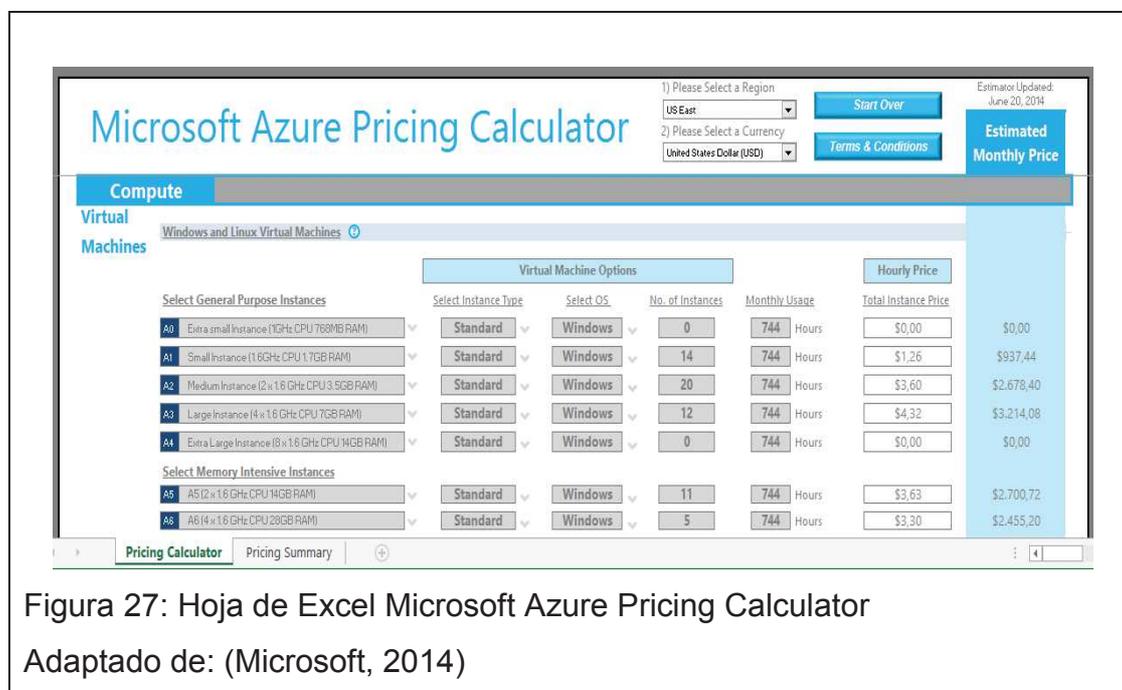


Figura 27: Hoja de Excel Microsoft Azure Pricing Calculator

Adaptado de: (Microsoft, 2014)

En el cuadrante mágico de *Gartner* respecto a la comercialización de soluciones de plataforma como servicio que se encuentra descrito en la figura 28, muestra que el líder en este ámbito es *Sales.force* y *Microsoft*.

Microsoft brindan una variedad de capacidades de infraestructura de aplicaciones para la web, con su base de datos *SQL*, servicios de bus de integración y mensajería con *Windows Azure Service Bus*, servicios de red de datos con *Windows Azure Cache*, servicios de movilidad con dispositivos móviles con *Windows Azure Mobile Services*. (Gartner, 2014), (Microsoft Azure, s.f.)

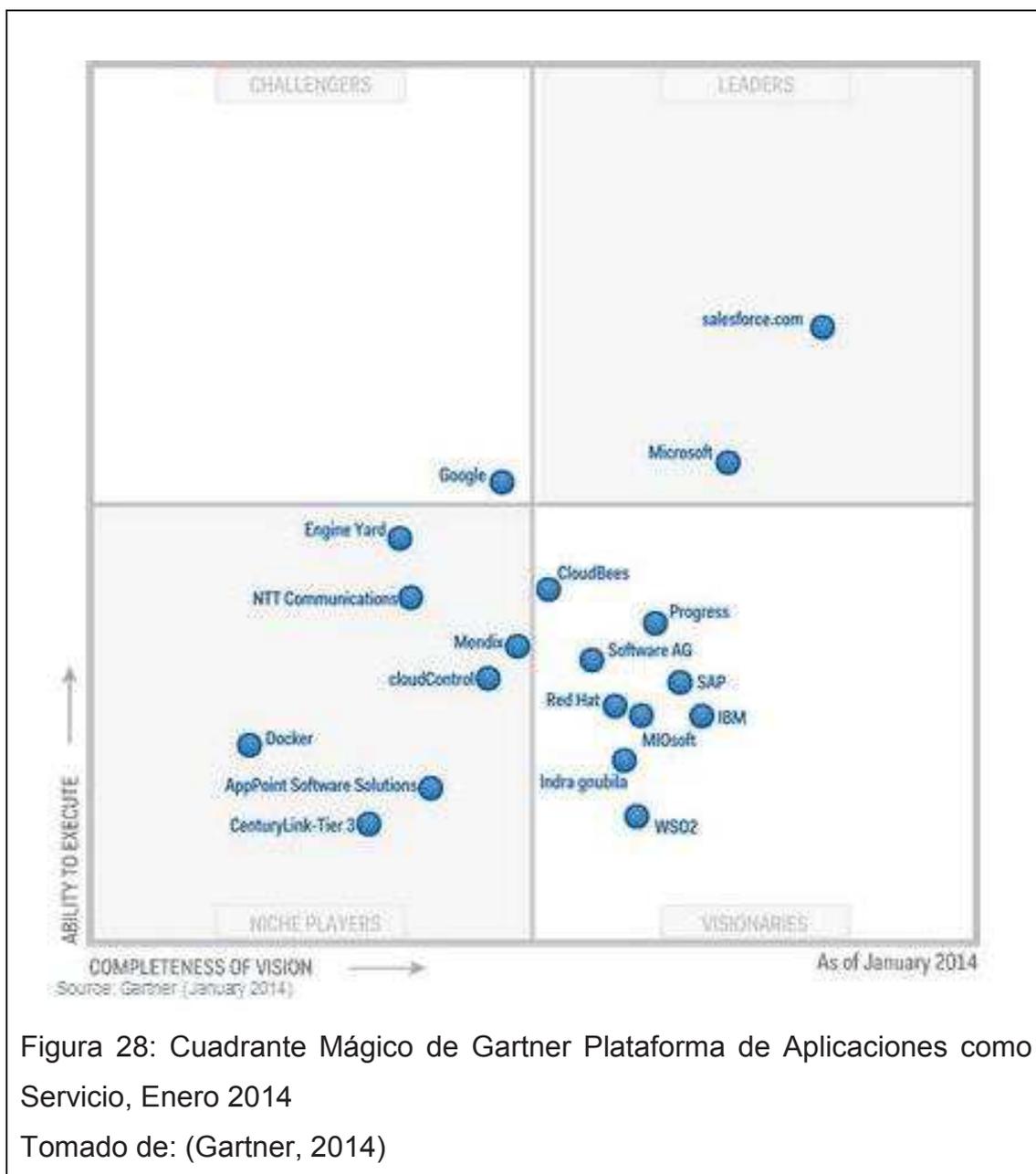
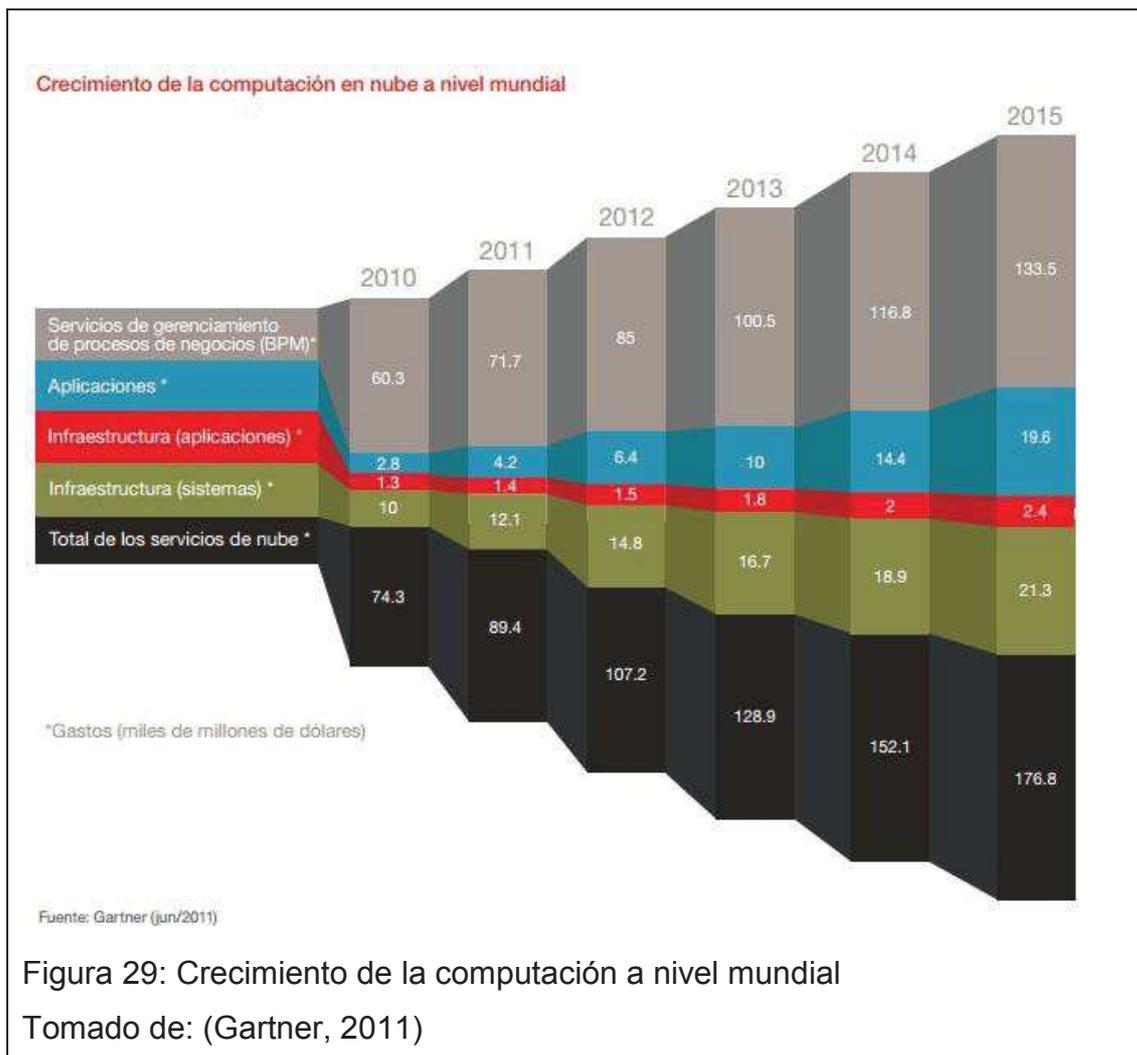


Figura 28: Cuadrante Mágico de Gartner Plataforma de Aplicaciones como Servicio, Enero 2014

Tomado de: (Gartner, 2014)

En la figura 29 se describe por parte de *Gartner* el crecimiento del *cloud computing* hasta el año 2015. Existen más proveedores cada día que brindan estos servicios en el mundo.



CAPITULO IV. Diseño de la solución

4.1 Arquitectura de la propuesta

Para crear la solución se desarrolló un análisis matemático en donde se describe la realidad actual de la empresa y sus sistemas del negocio.

Como variables que van a ser utilizadas en este análisis tenemos la cantidad de usuarios por equipo de cómputo que tiene la organización, a continuación el detalle:

Tabla 2: Cantidad Usuarios por tipo de equipo

Usuarios por tipo equipo	Cantidad Usuarios
Usuarios equipos computaciones (Escritorio y Portátiles)	800
Usuarios dispositivos móviles (Hand Helds)	600
Total de Usuarios	1400

En la tabla siguiente se describe, las aplicaciones o sistemas de información que tiene la empresa, la cantidad de usuarios de cada una de las aplicaciones, también un porcentaje del número total de usuarios versus el número máximo de usuarios con equipos de cómputo, derivado de este valor se obtiene un indicador que depende del porcentaje obtenido, en donde 57,14 es el más alto con 800 usuarios por lo cual tiene el máximo indicador es 5, en el caso del menor porcentaje tenemos valores que van desde 0,36 hasta 7,14 con lo cual su indicador es 1.

Tabla 3: Cantidad de usuarios por aplicación

Aplicación/ Sistema de información	Cantidad de Usuarios	Porcentaje	Parámetro
Aplicación FielMagister	5	0,36	1
Aplicación Análisis de Mercado	20	1,43	1
Aplicación ITIL Compliance	30	2,14	1
Aplicación BPM MetaStorm	50	3,57	1
Aplicación Proveedor Seguridad	50	3,57	1
Aplicación Datalyzer	80	5,71	1
Aplicación Servicio al Cliente	90	6,43	1
Aplicación Administración Proyectos	100	7,14	1
Aplicación Enterprise Project Management	100	7,14	1
Aplicación Inteligencia del Negocio	200	14,29	2
Aplicación Cognos Planning	200	14,29	2
Aplicación Digitalización documentos SharePoint	300	21,43	2
Archivos	400	28,57	3
Aplicación ERP SAP	430	30,71	3
Aplicación Comercial Transaccional	450	32,14	3
Aplicación Móvil Ventas	600	42,86	4
Aplicación Gestión Documental	800	57,14	5
Aplicación Correo Electrónico	800	57,14	5
Controlador de Dominio	800	57,14	5
Aplicación Antivirus	800	57,14	5
Aplicación Exchange	800	57,14	5

Se desarrolló una matriz donde se describen los macro procesos, procesos y subprocesos que se están realizando el análisis, esta matriz está conformada por las siguientes variables: servidor tipo, aplicación rol, impacto negocio, ubicación infraestructura, regulación corporativa, cantidad de usuarios. A continuación se detalla los parámetros de cada variable que conforma la matriz ordenados de menor a mayor:

- Variable Servidor Tipo

Tabla 4: Servidor Tipo

Servidor Tipo	Parámetro Servidor Tipo (PST)
Servidor Externo	2
Servidor Intel	3
Servidor Intel Granja	4
Servidor Iseries	5

En el caso del servidor Intel granja se componen de una granja de servidores virtualizados que están manejando alta disponibilidad, balanceo de carga de trabajo en el centro de datos de Triara en Monterrey.

Para el servidor Iseries su infraestructura es física, maneja un sistema operativo OS400 es un servidor Power 5 modelo 520 y está alojado en un centro de datos local.

Para los servidores intel el tipo de plataforma en la que está alojada es virtualizada con procesadores intel y sistemas operativos con Windows 2008 en versiones Estándar, Enterprise en 32 y 64 bits (Permite desplazar el doble de información que en un sistema de 32 bits).

Para el caso del servidor externo su plataforma es Windows de 32 bits con procesador Intel (Fabrica procesadores diseñados para diferentes ordenadores).

En la columna PST colocamos el indicador para el parámetro servidor tipo, este parámetro está definido del 1 al 5, el cual está dado por el grado de robustez de la plataforma.

- Variable Aplicación Rol

Tabla 5: Aplicación Rol

Aplicación Rol	Parámetro Aplicación Rol (PAR)
Aplicación Análisis de Mercado	1
Aplicación Administración Proyectos	2
Aplicación Correo Electrónico	2
Aplicación Gestión Documental	2
Archivos	2
Aplicación BPM MetaStorm	3
Aplicación Cognos Planning	3
Aplicación Datalyzer	3
Aplicación Digitalización documentos SharePoint	3
Aplicación Enterprise Project Management	3
Aplicación FielMagister	3
Aplicación ITIL Compliance	3
Aplicación Proveedor Seguridad	3
Aplicación Servicio al Cliente	3
Aplicación Antivirus	4
Aplicación Exchange	4
Aplicación Portal Ejecutivo	4
Controlador de Dominio	4
Aplicación Comercial Transaccional	5
Aplicación ERP SAP	5
Aplicación Inteligencia del Negocio	5
Aplicación Móvil Ventas	5

En la columna PAR se tiene el parámetro de aplicación rol en el cual se describe el nombre de la aplicación o para que se usa, está definido por su nivel de importancia en el negocio desde el valor 1 hasta 5.

- Variable Impacto en el negocio

Tabla 6: Impacto Negocio

Impacto Negocio	Parámetro Impacto Negocio (PIN)
Bajo	1
Medio	3
Medio alto	4
Alto	5

Esta variable se enfoca en el impacto que tiene las aplicaciones en el negocio en una escala del 1 al 5, donde se describen desde un impacto: bajo, medio, medio alto y alto.

- Variable Ubicación Infraestructura

Tabla 7: Ubicación Infraestructura

Ubicación Infraestructura	Parámetro Ubicación Infraestructura (PUI)
Remoto	1
Principal	3
Principal, Contingencia	5

En la columna ubicación infraestructura que describe el lugar donde deberían estar alojados los servidores físicamente por su criticidad para lo cual tenemos los siguientes parámetros que están descritos en la columna PUI en el caso remoto el valor es 1 ya que esta fuera de la administración de la organización en un tercero.

Para el valor 3 describimos que esa aplicación debe estar en el centro de datos principal solamente y no requiere por su criticidad manejarlo con alta disponibilidad en el centro de datos de contingencia.

Para el valor 5 se describe que esas aplicaciones deben estar en el centro de datos principal y de contingencia ya que su funcionamiento es vital para que los procesos críticos del negocio fluyan.

- Variable Regulación Corporativa

Tabla 8: Regulación Corporativa

Regulación Corporativa	Parámetro Regulación Corporativa (PRC)
Sin regulación	1
Centro Datos México	5

En la columna regulación corporativa se tiene definida estrategias de negocio para sistemas críticos que impactan en el funcionamiento del mismo, adicional a manejar estándares a nivel de plataformas, sistemas de información, entre otros.

Estas regulaciones descritas en la columna PRC son las siguientes: el valor 5 que representa el alojamiento del servidor en el centro de datos en México, el valor 1 que indica que no hay ninguna regulación al respecto.

- Variable Cantidad Usuarios

Tabla 9: Cantidad Usuarios

Cantidad Usuarios	Parámetro Cantidad Usuarios (PCU)
5	1
20	1
30	1
50	1
80	1
90	1
100	1
200	2
300	2
400	3
430	3
450	3
600	4
800	5

En las columnas cantidad de usuarios y PCU que describe el parámetro de cantidad de usuarios esto está indicado en la tabla 9 anteriormente mencionada.

En la columna Sub total se muestra la cantidad producto de la operación de multiplicación de las variables anteriormente descritas desarrolladas de la siguiente formula:

$$\text{Sub total} = \text{PST} \times \text{PAR} \times \text{PIN} \times \text{PUI} \times \text{PRC} \times \text{PCU}$$

En la columna Total se consolidan los valores de la siguiente forma: Macro proceso (suma de valores en color azul), Proceso (suma de valores en color rojo), Subproceso (suma de valores en color verde)

Posteriormente estas cantidades son normalizadas para presentar la información detallada. Se va a detallar los resultados del análisis realizado por cada macro proceso donde describimos la información al detalle:

4.1.1 Tabulación matriz para Macro proceso responsabilidad de la dirección:

Tabla 10: Matriz macro proceso responsabilidad de la dirección

Nº	Macro proceso/Procesos/Subproceso	Servidor Tipo	P S T Aplicación Rol	P A R Impacto Negocio	P I N Ubicación Infraestructura	P U I Regulación Corporativa	P R C Cantidad Usuarios	P C U Sub Total	Total
	Macro proceso responsabilidad de la dirección								40494
	Proceso administración dirección general								15315
1	Planificar los sistemas de gestión	Servidor Intel Granja	Aplicación Portal Ejecutivo 4	Medio 4	Principal, Contingencia 3	Centro Datos México 5	5	450 3	3600 3600
2	Revisar los sistemas de gestión	Servidor Iseries	Aplicación Comercial Transaccional 5	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	450 3	1875 11625
		Servidor Intel	Aplicación Móvil Ventas 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	600 4	1500
		Servidor Intel	Aplicación Inteligencia del Negocio 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	200 2	750
		Servidor Intel Granja	Aplicación ERP SAP 4	Alto 5	Principal, Contingencia 5	Centro Datos México 5	5	430 3	7500
3	Definir políticas y objetivos	Servidor Intel	Aplicación Gestión Documental 3	Bajo 2	Principal 1	Sin regulación 3	1	800 5	90 90
	Proceso planeación estratégica								25179
4	Administrar planificación de la demanda	Servidor Iseries	Aplicación Comercial Transaccional 5	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	450 3	1875 1875
5	Administración planificación estratégica	Servidor Iseries	Aplicación Comercial Transaccional 5	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	450 3	1875 11625
		Servidor Intel	Aplicación Móvil Ventas 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	600 4	1500
		Servidor Intel	Aplicación Inteligencia del Negocio 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	200 2	750
		Servidor Intel Granja	Aplicación ERP SAP 4	Alto 5	Principal, Contingencia 5	Centro Datos México 5	5	430 3	7500
6	Administración de proyectos	Servidor Intel	Aplicación Administración Proyectos 3	Medio 2	Principal 3	Sin regulación 3	1	100 1	54 54
7	Administración de la continuidad del negocio	Servidor Iseries	Aplicación Comercial Transaccional 5	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	450 3	1875 11625
		Servidor Intel	Aplicación Móvil Ventas 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	600 4	1500
		Servidor Intel	Aplicación Inteligencia del Negocio 3	Alto 5	Principal, Contingencia 5	Sin regulación 5	1	200 2	750
		Servidor Intel Granja	Aplicación ERP SAP 4	Alto 5	Principal, Contingencia 5	Centro Datos México 5	5	430 3	7500

4.1.2 Tabulación matriz para Macro proceso gestionar los recursos

Tabla 11: Matriz macro proceso gestionar los recursos

Nº	Macro proceso/Procesos/Subproceso	Servidor Tipo	P S T	Aplicación Rol	P A R	Impacto Negocio	P I N	Ubicación Infraestructura	P U I	Regulación Corporativa	P R C	Cantidad Usuarios	P C U	Sub Total	Total	
	Macro proceso gestionar los recursos															166418
	Proceso de Marketing															3927
8	Investigar mercados	Servidor Intel	3	Aplicación Análisis de Mercado	1	Medio	3	Principal	3	Sin regulación	1	20	1	27	27	
9	Publicidad y medios	Servidor Intel	3	Aplicación Correo Electrónico	2	Bajo	1	Principal, Contingencia	5	Sin regulación	1	800	5	150	150	
10	Generación del pronóstico de la demanda	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875	
11	Promociones y mercadeo	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875	
	Proceso de Tecnología y Sistemas															15852
12	Administrar seguridad informática	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	14160	
		Servidor Intel	3	Aplicación Móvil Ventas	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	600	4	1500		
		Servidor Intel	3	Aplicación Inteligencia del Negocio	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	200	2	750		
		Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500		
		Servidor Intel	3	Aplicación ITIL Compliance	3	Medio	3	Principal	3	Sin regulación	1	30	1	81		
		Servidor Intel	3	Controlador de Dominio	4	Medio alto	4	Principal, Contingencia	5	Sin regulación	1	800	5	1200		
		Servidor Intel	3	Aplicación Antivirus	4	Medio alto	4	Principal, Contingencia	5	Sin regulación	1	800	5	1200		
		Servidor Intel	3	Archivos	2	Bajo	1	Principal	3	Sin regulación	1	400	3	54		
13	Apoyo al negocio	Servidor Intel	3	Aplicación ITIL Compliance	3	Medio	3	Principal	3	Sin regulación	1	30	1	81	81	
14	Planificación de continuidad	Servidor Intel	3	Aplicación Gestión Documental	2	Bajo	1	Principal	3	Sin regulación	1	800	5	90	90	
15	Administración ambiente de TI	Servidor Intel	3	Aplicación ITIL Compliance	3	Medio	3	Principal	3	Sin regulación	1	30	1	81	81	
16	Planificación e investigación y desarrollo	Servidor Intel Granja	4	Aplicación BPM MetaStorm	3	Medio	3	Principal, Contingencia	5	Centro Datos México	5	50	1	900	900	
17	Administración de proyectos del negocio	Servidor Intel Granja	4	Aplicación Enterprise Project Management	3	Medio	3	Principal	3	Centro Datos México	5	100	1	540	540	
	Proceso Financiero															60360
18	Planificación financiera	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
19	Administrar presupuestos	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
20	Contabilidad	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
21	Administración tributaria	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
22	Administración Capex	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7860	
		Servidor Intel	3	Aplicación Cognos Planning	3	Medio alto	4	Principal, Contingencia	5	Sin regulación	1	200	2	360		
23	Administración activos fijos	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
24	Riesgos y seguros	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
25	Tesorería	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
	Proceso Capital Humano															46418
26	Gestión de la organización	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
27	Administración de selección y contratación	Servidor Intel Granja	4	Aplicación BPM MetaStorm	3	Medio	3	Principal, Contingencia	5	Centro Datos México	5	50	1	900	900	
28	Gestión del personal compensación y nómina	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
29	Desarrollo del personal	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
30	Bienestar social	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
31	Seguridad física	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7518	
		Servidor Externo	2	Aplicación Proveedor Seguridad	3	Medio	3	Remoto	1	Sin regulación	1	50	1	18		
32	Administración sistema de comunicación	Servidor Intel Granja	4	Aplicación Exchange	4	Medio alto	4	Principal, Contingencia	5	Centro Datos México	5	800	5	8000	8000	
	Proceso Requisitos Legales															405
33	Administración de procesos judiciales	Servidor Intel	3	Aplicación FielMagister	3	Medio	3	Principal	3	Sin regulación	1	5	1	81	81	
34	Gestión de documentos para funcionamiento de la empresa	Servidor Intel	3	Aplicación Digitalización documentos SharePoint	3	Medio	3	Principal	3	Sin regulación	1	300	2	162	162	
35	Gestión de contratos	Servidor Intel	3	Aplicación Digitalización documentos SharePoint	3	Medio	3	Principal	3	Sin regulación	1	300	2	162	162	
	Proceso Mantenimiento															39456
36	Gestionar mantenimiento industrial	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
37	Gestionar mantenimiento automotriz	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
38	Gestionar mantenimiento de edificios	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
39	Gestionar mantenimiento de equipos de frío	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875	
40	Gestionar mantenimiento de soplado	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	
41	Gestionar calibración de equipos	Servidor Intel	3	Aplicación Datalyzer	3	Medio	3	Principal	3	Sin regulación	1	80	1	81	81	
42	Generar servicios	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500	

4.1.3 Tabulación matriz para Macro proceso realización del producto

Tabla 12: Matriz macro proceso realización del producto

N°	Macro proceso/Procesos/Subproceso	Servidor Tipo	P S T	Aplicación Rol	P A R	Impacto Negocio	P I N	Ubicación Infraestructura	P U I	Regulación Corporativa	P R C	Cantidad Usuarios	P C U	Sub Total	Total
	Macro proceso realización del producto														66150
	Proceso abastecer														30900
43	Plan de negociación	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
44	Administración de proveedores	Servidor Intel Granja	4	Aplicación BPM MetaStorm	3	Medio	3	Principal, Contingencia	5	Centro Datos México	5	50	1	900	900
45	Compra de bienes	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
46	Administración de bienes	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
47	Contratación de servicios	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
	Proceso fabricar producto														24375
48	Administrar producción	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
49	Producir	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
50	Almacenar en planta	Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	7500
51	Abastecer cedis	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875
	Proceso Comercializar														10875
52	Administrar maestros	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875
53	Vender y distribuir	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	3375
		Servidor Intel	3	Aplicación Móvil Ventas	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	600	4	1500	
54	Administrar bodega PT	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875
55	Administrar equipos de frio	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875
56	Gestionar cartera	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	1875

4.1.4 Tabulación matriz para Macro proceso medición análisis y mejora

Tabla 13: Matriz macro proceso medición análisis y mejora

N°	Macro proceso/Procesos/Subproceso	Servidor Tipo	P S T	Aplicación Rol	P A R	Impacto Negocio	P I N	Ubicación Infraestructura	P U I	Regulación Corporativa	P R C	Cantidad Usuarios	P C U	Sub Total	Total
	Macro proceso medición, análisis y mejora														12117
	Proceso gestión de calidad														12117
57	Administración del plan de calidad	Servidor Intel	3	Aplicación Datalyzer	3	Medio	3	Principal	3	Sin regulación	1	80	1	81	81
58	Asegurar calidad de procesos	Servidor Intel	3	Aplicación Datalyzer	3	Medio	3	Principal	3	Sin regulación	1	80	1	81	81
59	Asegurar calidad en insumos	Servidor Intel	3	Aplicación Datalyzer	3	Medio	3	Principal	3	Sin regulación	1	80	1	81	81
60	Asegurar calidad de producto	Servidor Intel	3	Aplicación Datalyzer	3	Medio	3	Principal	3	Sin regulación	1	80	1	81	81
61	Administrar producto no conforme	Servidor Intel	3	Aplicación Servicio al Cliente	3	Medio	3	Principal	3	Sin regulación	1	90	1	81	81
62	Gestión de inocuidad de los alimentos	Servidor Intel	3	Aplicación Gestión Documental	2	Bajo	1	Principal	3	Sin regulación	1	800	5	90	90
63	Gestión ambiental	Servidor Intel	3	Archivos	2	Bajo	1	Principal	3	Sin regulación	1	400	3	54	54
64	Administración de seguridad y salud ocupacional														0
65	Relación cliente consumidor	Servidor Intel	3	Aplicación Servicio al Cliente	3	Medio	3	Principal	3	Sin regulación	1	90	1	81	81
66	Gestión de la mejora	Servidor Intel	3	Aplicación Servicio al Cliente	3	Medio	3	Principal	3	Sin regulación	1	90	1	81	81
67	Control interno	Servidor Iseries	5	Aplicación Comercial Transaccional	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	450	3	1875	11406
		Servidor Intel	3	Aplicación Inteligencia del Negocio	5	Alto	5	Principal, Contingencia	5	Sin regulación	1	200	2	750	
		Servidor Intel Granja	4	Aplicación ERP SAP	5	Alto	5	Principal, Contingencia	5	Centro Datos México	5	430	3	7500	
		Servidor Intel	3	Aplicación ITIL Compliance	3	Medio	3	Principal	3	Sin regulación	1	30	1	81	
		Servidor Intel	3	Controlador de Dominio	4	Medio alto	4	Principal, Contingencia	5	Sin regulación	1	800	5	1200	

El análisis realizado con esta matriz que puede ser ejecutado para otras realidades en empresas o instituciones del país tomando en cuenta las variables anteriormente expuestas. Las cuales están enfocados en los siguientes lineamientos respecto a: hardware, software, impacto y políticas del negocio, entre otras, a continuación detallamos los conceptos que se manejaron en este análisis:

- Infraestructura de servidores. (Hardware)
- Sistemas de información del negocio. (Software)
- Impacto en el negocio de las aplicaciones.
- Sitios donde estén alojadas.
- Políticas y reglas de negocio.
- Volumen de usuarios.

Del desarrollo de estas matrices se llegaron a algunos análisis como se muestra en la tabla 14, la aplicación que más se utiliza con el doble de subprocesos más que la segunda es el *ERP SAP* ya que está controlando diferentes áreas del negocio a nivel financiero, contable, impuestos, presupuestos, inventarios activos fijos, compras, mantenimiento industrial, los cuales son procesos críticos para el negocio y por regulaciones corporativas están operando desde México.

Como segunda aplicación más utilizada en los procesos del negocio tenemos al sistema comercial transaccional llamado *Basis* el cual controla los procesos que tienen que ver con la logística, venta, cartera, liquidación, inventario de producto terminado y de los equipos de frío, con lo indicado anteriormente de igual forma que en el primer caso se manejan procesos críticos de vital importancia para el negocio.

En tercer lugar tenemos a un grupo de tres aplicaciones que tienen la sexta parte de cantidad de procesos que el *ERP SAP* y la tercera parte de procesos del sistema *Basis*, los cuales no dejan de ser importantes pero su uso en los procesos del negocio es menor, las aplicaciones son: *Datalyzer* que es manejada

en el área de producción para llevar estadísticas del proceso de producción, Inteligencia del Negocio la cual utiliza la aplicación *Cognos Power Play*, la otra aplicación es la Móvil Ventas llamada *Bmobile* la cual al igual que *Basis* es una herramienta estandarizada por *The Coca Cola Company* para que los embotelladores a nivel mundial puedan utilizar estos sistemas de información y puedan cubrir la cadena de valor del negocio de la mejor forma.

Tabla 14: Cantidad de subprocesos por Aplicación

Aplicaciones	Cantidad de Subprocesos
Aplicación ERP SAP	30
Aplicación Comercial Transaccional	15
Aplicación Datalyzer	5
Aplicación Inteligencia del Negocio	5
Aplicación Móvil Ventas	5
Aplicación ITIL Compliance	4
Aplicación BPM MetaStorm	3
Aplicación Servicio al Cliente	3
Aplicación Gestión Documental	3
Controlador de Dominio	2
Aplicación Digitalización documentos SharePoint	2
Archivos	2
Aplicación Correo Electrónico	1
Aplicación Proveedor Seguridad	1
Aplicación Portal Ejecutivo	1
(en blanco)	1
Aplicación Enterprise Project Management	1
Aplicación Cognos Planning	1
Aplicación Análisis de Mercado	1
Aplicación Antivirus	1
Aplicación FielMagister	1
Aplicación Administración Proyectos	1
Aplicación Exchange	1

En la matriz de la tabla 15 se describe que el subproceso administración de seguridad informática es uno de los que más aplicaciones utilizan, ya que en este caso es el responsable de proveer los accesos a las aplicaciones del negocio. De igual forma de esta matriz deducimos que como segundo subproceso que más usa las aplicaciones del negocio está el de control interno, puesto que es

vigilante de que todos los procesos del negocio estén controlados y alineados a las estrategias corporativas que deben ser ejecutadas por los usuarios.

En tercer lugar tenemos varios subprocesos que tienen que ver con el proceso de administración de la dirección general donde se deriva: la administración de la planificación estratégica, revisión de los sistemas de gestión y administración de la continuidad del negocio.

Tabla 15: Cantidad de aplicaciones por subproceso

Subprocesos	Cantidad Aplicaciones
Administrar seguridad informática	8
Control interno	5
Administración planificación estratégica	4
Revisar los sistemas de gestión	4
Administración de la continuidad del negocio	4
Vender y distribuir	2
Administración Capex	2
Seguridad física	2
Gestionar cartera	1
Administración de proyectos	1
Planificación de continuidad	1
Administración de proyectos del negocio	1
Gestión de la mejora	1
Administración de selección y contratación	1
Gestionar mantenimiento de soplado	1
Administración del plan de calidad	1
Producir	1
Administración de bienes	1
Gestión de documentos para funcionamiento de la empresa	1
Administración sistema de comunicación	1
Gestión del personal compensación y nómina	1
Administración tributaria	1
Gestionar mantenimiento de edificios	1
Administrar bodega PT	1
Investigar mercados	1
Administración de procesos judiciales	1
Planificación financiera	1
Administración de proveedores	1
Publicidad y medios	1

Generación del pronóstico de la demanda	1
Gestión ambiental	1
Administrar equipos de frío	1
Desarrollo del personal	1
Administrar maestros	1
Generar servicios	1
Administrar planificación de la demanda	1
Gestión de contratos	1
Administrar presupuestos	1
Gestión de inocuidad de los alimentos	1
Administrar producción	1
Gestión de la organización	1
Administrar producto no conforme	1
Gestionar calibración de equipos	1
Administración activos fijos	1
Gestionar mantenimiento automotriz	1
Almacenar en planta	1
Gestionar mantenimiento de equipos de frío	1
Apoyo al negocio	1
Gestionar mantenimiento industrial	1
Asegurar calidad de procesos	1
Plan de negociación	1
Asegurar calidad de producto	1
Planificación e investigación y desarrollo	1
Asegurar calidad en insumos	1
Planificar los sistemas de gestión	1
Bienestar social	1
Promociones y mercadeo	1
Compra de bienes	1
Relación cliente consumidor	1
Contabilidad	1
Riesgos y seguros	1
Contratación de servicios	1
Tesorería	1
Abastecer cedis	1
Administración ambiente de TI	1
Definir políticas y objetivos	1
Administración de seguridad y salud ocupacional	0

Se describen en las tablas 16, 17 y 18 un resumen de los resultados de las tablas 10,11, 12, 13 donde se hizo el análisis por los parámetros anteriormente expuestos y explicados.

Nos dan como resultado en la tabla 16 que los macro proceso de gestionar los recursos tienen el mayor peso sobre otros macro procesos, ya que en este se derivan los procesos de Marketing, Financiero, Capital Humano, Mantenimiento, Tecnología y Sistemas donde esta gran parte de los procesos administrativos y financieros que controlan el negocio, esto se detalla en la tabla 17 y con mayor detalle el resumen de los subprocesos en la tabla 18.

En las tablas 16, 17, 18 en su última columna se normalizan los resultados totales obtenidos de las matrices anteriores donde esto se obtiene de la siguiente forma:

Por ejemplo de la tabla 16 ordenando los macro procesos por el valor mayor a menor, obtenemos que el Macro Proceso Gestionar los Recursos tiene el valor más alto el cual es 332836 al cual lo dividimos para el mismo valor dividido para 10 de la siguiente forma:

$$166418/10 = 16641,8$$

Para normalizar esta columna vamos a dividir todos los valores de la tabla 16 para 16641,8 por ello en el primer caso en el Macro Proceso Gestionar los Recursos el valor normalizado es de 10, para el Macro proceso Realización del Producto el valor normalizado es 3,97 y así sucesivamente con los demás campos.

Tabla 16: Resumen Macro procesos

Macro Procesos	Valor	Normalizado
Macro Proceso Gestionar los Recursos	166418	10,00
Macro Proceso Realización del Producto	66150	3,97
Macro Proceso Responsabilidad de la Dirección	40494	2,43
Macro Proceso Medición, Análisis y Mejora	12117	0,73

Tabla 17: Resumen Procesos

Procesos	Valor	Normalizado
Proceso Financiero	60360	10,00
Proceso Capital Humano	46418	7,69
Proceso Mantenimiento	39456	6,54
Proceso Abastecer	30900	5,12
Proceso Planeación Estratégica	25179	4,17
Proceso Fabricar Producto	24375	4,04
Proceso de Tecnología y Sistemas	15852	2,63
Proceso Administración Dirección General	15315	2,54
Proceso Gestión de Calidad	12117	2,01
Proceso Comercializar	10875	1,80
Proceso de Marketing	3927	0,65
Proceso Requisitos Legales	405	0,07

Tabla 18: Resumen Subprocesos

Sub Procesos	Total	Normalizado
Administrar seguridad informática	14160	10,00
Revisar los sistemas de gestión	11625	8,21
Administración planificación estratégica	11625	8,21
Administración de la continuidad del negocio	11625	8,21
Administración sistema de comunicación	8000	5,65
Administración Capex	7860	5,55
Seguridad física	7518	5,31
Planificación financiera	7500	5,30
Administrar presupuestos	7500	5,30
Contabilidad	7500	5,30
Administración tributaria	7500	5,30
Administración activos fijos	7500	5,30
Riesgos y seguros	7500	5,30
Tesorería	7500	5,30
Gestión de la organización	7500	5,30
Gestión del personal compensación y nómina	7500	5,30
Desarrollo del personal	7500	5,30
Bienestar social	7500	5,30
Gestionar mantenimiento industrial	7500	5,30
Gestionar mantenimiento automotriz	7500	5,30

Continuación de la tabla 18.

Gestionar mantenimiento de edificios	7500	5,30
Gestionar mantenimiento de soplado	7500	5,30
Generar servicios	7500	5,30
Plan de negociación	7500	5,30
Compra de bienes	7500	5,30
Administración de bienes	7500	5,30
Contratación de servicios	7500	5,30
Administrar producción	7500	5,30
Producir	7500	5,30
Almacenar en planta	7500	5,30
Planificar los sistemas de gestión	3600	2,54
Vender y distribuir	3375	2,38
Administrar planificación de la demanda	1875	1,32
Generación del pronóstico de la demanda	1875	1,32
Promociones y mercadeo	1875	1,32
Gestionar mantenimiento de equipos de frio	1875	1,32
Abastecer cedis	1875	1,32
Administrar maestros	1875	1,32
Administrar bodega PT	1875	1,32
Administrar equipos de frio	1875	1,32
Gestionar cartera	1875	1,32
Control interno	1875	1,32
Planificación e investigación y desarrollo	900	0,64
Administración de selección y contratación	900	0,64
Administración de proveedores	900	0,64
Administración de proyectos del negocio	540	0,38
Gestión de documentos para funcionamiento de la empresa	162	0,11
Gestión de contratos	162	0,11
Publicidad y medios	150	0,11
Definir políticas y objetivos	90	0,06
Planificación de continuidad	90	0,06
Gestión de inocuidad de los alimentos	90	0,06
Apoyo al negocio	81	0,06
Administración ambiente de TI	81	0,06
Administración de procesos judiciales	81	0,06

Continuación de la tabla 18.

Gestionar calibración de equipos	81	0,06
Administración del plan de calidad	81	0,06
Asegurar calidad de procesos	81	0,06
Asegurar calidad en insumos	81	0,06
Asegurar calidad de producto	81	0,06
Administrar producto no conforme	81	0,06
Relación cliente consumidor	81	0,06
Gestión de la mejora	81	0,06
Administración de proyectos	54	0,04
Gestión ambiental	54	0,04
Investigar mercados	27	0,02
Administración de seguridad y salud ocupacional	0	0,00

Se detalla en la tabla 19 el equipamiento actual en el centro de cómputo de Calderón en la ciudad de Quito para sus sistemas de información y servicios es el siguiente:

Tabla 19: Infraestructura centro de cómputo en Calderón

Aplicación	Plataforma	Tipo	Sistema Operativo	Capacidad Procesamiento (GHz)	Capacidad Memoria RAM (GB)	Capacidad Almacenamiento (GB)	Política Respaldo
Legal Field Magíster	Intel Virtual Blade	Ciente Servidor	Server 2003 Estándar	4x2.933	2	52	No se ejecuta respaldo
Archivos	Intel Virtual Blade	Archivos	Server 2008 32-bits	4x2.933	2	1640	Diario, 1.5TB, Retención 1 mensual
Servidor FTP	Intel Virtual Blade	FTP	Server 2008 32-bits	4x2.933	2	62	No se ejecuta respaldo
Control seguridad física SKNET	Intel Virtual Blade	SQL	Server 2008 32-bits	4x2.933	2	102	Diario, 50GB, Retención 1 mensual
Cisco Prime	Intel Virtual Blade	Web	Red Hat Linux 5 64-bits	4x2.933	10	205	No se ejecuta respaldo
Controlador de Dominio	Intel Virtual Blade	Directorio Activo	Server 2008 R2 64-bits	4x2.933	4	85	No se ejecuta respaldo
Antivirus	Intel Virtual Blade	Antivirus	Server 2008 R2 64-bits	4x2.933	8	160	No se ejecuta respaldo
ITIL Compliance Aranda	Intel Virtual Blade	SQL, Web	Server 2008 32-bits	8x2.933	8	188	Diario, 100GB, Retención 1 mensual
Base Datos SharePoint	Intel Virtual Blade	SQL	Server 2008 R2 64-bits	8x2.933	16	1000	Diario, 500GB, Retención 1 mensual
Digitalización ConnectKey	Intel Virtual Blade	SQL, Web	Server 2008 32-bits	8x2.933	4	54	No se ejecuta respaldo
Aplicación SharePoint	Intel Virtual Blade	Web	Server 2008 R2 64-bits	8x2.933	12	162	No se ejecuta respaldo
Auditoria Impresión Equitrac	Intel Virtual Blade	SQL, Web	Server 2008 R2 64-bits	8x2.933	8	207	No se ejecuta respaldo
Colas Impresión	Intel Virtual Blade	Impresión	Server 2008 R2 64-bits	8x2.933	4	64	No se ejecuta respaldo
Rutas de venta RoadNet	Intel Virtual Blade	SQL, Terminal Services	Server 2008 R2 64-bits	4x2.933	12	212	Diario, 200GB, Retención 1 mensual
Administración Hand Helds Mobi Control	Intel Virtual Blade	SQL, Web	Server 2008 R2 64-bits	4x2.933	5	46	No se ejecuta respaldo
Firewall TMG	Intel Virtual Blade	Proxy	Server 2008 R2 64-bits	4x2.933	5	304	No se ejecuta respaldo
Consola VMWare	Intel Físico	Ciente Servidor	Server 2003 Standard SP2	3	3	50	No se ejecuta respaldo
Respaldo Servidores	Intel Físico	Respaldo	Server 2008 Standard	2 x 2	4	50	No se ejecuta respaldo

Se detalla en la tabla 20 el equipamiento del centro de datos que está ubicado en el edificio de *IBM* en Quito:

Tabla 20: Infraestructura centro de cómputo en IBM Quito

Aplicación	Plataforma	Tipo	Sistema Operativo	Capacidad Procesamiento (GHz)	Capacidad Memoria RAM (GB)	Capacidad Almacenamiento (GB)	Política Respaldo
Portal Servidor Productivo	Intel Virtual Blade	SQL, Web	Windows Server 2008 32-bits	2x2.933	3	140	Semanal 5GB, retención una semana
Controlador de Dominio	Intel Virtual Blade	Directorio Activo	Windows Server 2008 R2 64-bits	2x2.933	4	80	No se ejecuta respaldo
Bmobile Norte Productivo	Intel Virtual Blade	DB2, Web	Windows 2003 Server Enterprise	4x 2.933	8	250	No se ejecuta respaldo
System Center IBM	Intel Virtual Blade	Monitoreo	Windows Server 2008 R2 64-bits	2x2.933	8	152	No se ejecuta respaldo
Bmobile Sur Productivo	Intel Virtual Blade	DB2, Web	Windows 2003 Server Enterprise	4x2.933	8	250	No se ejecuta respaldo
Colas Impresión	Intel Virtual Blade	Impresión	Windows Server 2008 R2 64-bits	2x2.933	4	60	No se ejecuta respaldo
Sistema de Registro	Intel Virtual Blade	SQL	Windows Server 2008 R2 64-bits	2x2.933	4	30	No se ejecuta respaldo
Web_campus	Intel Virtual Blade	SQL, Web	Windows Server 2008 32-bits	2x2.933	2	160	Semanal 5GB, retención una semana
Web Service	Intel Virtual Blade	Web	Windows Server 2008 32-bits	2x2.933	2	70	Semanal 5GB, retención una semana
ADMA	Intel Virtual Blade	SQL, Web	Windows Server 2008 R2 64-bits	4x2.933	8	210	No se ejecuta respaldo
Aplicaciones BI Productivo	Intel Físico	Web	Windows 2008 Server Enterprise	8x2.933	12	600	Semanal 400GB, retención 4 semanas
Planning Productivo	Intel Físico	SQL, Web	Windows 2008 Server Enterprise	8x2.933	14	600	Semanal 400GB, retención 4 semanas
Bases de datos Productivo	Intel Físico	SQL	Windows 2008 Server Enterprise	8x2.933	14	1300	Semanal 400GB, retención 4 semanas
VCB BrightStore	Intel Físico	Respaldo	Windows Server 2008 32-bits	3x3.16	6	350	No se ejecuta respaldo
Consola Vmware	Intel Físico	Cliente servidor	Windows 2008 Server Enterprise	2x3	2	136	No se ejecuta respaldo
Comercial BASIS Productivo	Power 6 8203-E4A	DB2	OS400 6.1	2x4.2	15	1356	Mensual 200GB, retención un año

Se detalla en la tabla 21 el equipamiento del centro de datos que está ubicado en la ciudad de Guayaquil en la planta embotelladora de la organización en esa ciudad.

Tabla 21: Infraestructura centro de cómputo en Planta Arca Continental en Guayaquil

Aplicación	Plataforma	Tipo	Sistema Operativo	Capacidad Procesamiento (GHz)	Capacidad Memoria RAM (GB)	Capacidad Almacenamiento (GB)	Política Respaldo
Comercial BASIS Contingencia/ Desarrollo	Power 6 8203-E4A	DB2	OS400 6.1	2x1.9	15	1547	Sincronización en línea
Archivos	Intel Virtual Blade	Archivos	Windows Server 2008 32-bits	2x1.86	4	800	750GB, diario, semanal
Bmobile Región Norte Contingencia	Intel Virtual Blade	DB2	Windows 2003 Server Enterprise	4x1.86	12	250	No se ejecuta respaldo
Base de datos Contingencia	Intel Físico	SQL	Windows 2008 Server Enterprise	2x1.86	16	1000	No se ejecuta respaldo
Aplicaciones BI Contingencia	Intel Físico	SQL	Windows 2008 Server Enterprise	2x1.86	16	277	No se ejecuta respaldo
Planning Contingencia	Intel Físico	SQL, Web	Windows 2008 Server Enterprise	2x1.86	16	295	No se ejecuta respaldo
Sistema de registro	Intel Virtual Blade	SQL	Windows Server 2008 32-bits	2x1.86	2	240	No se ejecuta respaldo
Portal Contingencia	Intel Virtual Blade	SQL, Web	Windows Server 2008 32-bits	4x1.86	4	383	No se ejecuta respaldo
Respaldo servidores	Intel Físico	Respaldo	Windows Server 2008 32-bits	1x2	2	100	200MB, diario, semanal.
Consola Vmware	Intel Físico	Cliente servidor	Windows Server 2008 32-bits	2x1.86	4	135	No se ejecuta respaldo
Bmobile Región Sur	Intel Virtual Blade	DB2	Windows 2003 Server Enterprise	4x1.86	12	250	No se ejecuta respaldo
Cobrix	Intel Virtual Blade	SQL	Windows 2003 Server Estándar	2x1.86	4	250	No se ejecuta respaldo
Controlador de Dominio	Intel Virtual Blade	Directorio Activo	Windows Server 2008 R2 64-bits	2x1.86	4	80	No se ejecuta respaldo
Datalyzer	Intel Virtual Blade	SQL, Web	Windows Server 2008 32-bits	2x1.86	6	260	10GB, diario, semanal
Nodo Antivirus	Intel Virtual Blade	Antivirus	Windows Server 2008 R2 64-bits	2x1.86	8	152	No se ejecuta respaldo

4.2 Costos de la solución propuesta y retorno sobre la inversión

Los costos de la solución se han desarrollado del análisis de las matrices 10,11,12,y 13 donde obtuvimos los procesos y aplicaciones que pueden ser migradas a *cloud computing* por diferentes necesidades como son: regulaciones corporativas, mejores prácticas para el desempeño de las mismas y procesos de consolidación para optimizar su uso.

Para esto se realizó un análisis con diferentes proveedores locales y del exterior como son: *Microsoft Azure, Amazon Web Services, TelcoNet y Solutions*.

Las soluciones propuestas están enfocadas a brindar disponibilidad y costos adecuados para los requerimientos de la organización.

El líder respecto a servicios en *cloud computing* de tipo Infraestructura como servicio es *Amazon Web Services* con el cual se evaluó un escenario de servicio para presentar la solución.

Se utilizó la herramienta que presenta el fabricante llamada Calculadora mensual simple con la cual se va detallando las características que se requieren configurar para lograr el diseño.

Para obtener esta solución se escogieron las instancias del servicio *Amazon EC2* que brindan soluciones de equipos virtualizados con capacidades para entornos desarrollados en *web* necesarias para las aplicaciones del negocio, basándose en la realidad actual (*Amazon Web Services, s.f.*), a continuación se detallan los parámetros a configurar:

Sistema operativo y bases de datos.- Se tienen disponibles varios sistemas operativos incluidos en algunos casos el tipo de base de datos (Conjunto de datos que son almacenados mediante una herramienta) como son los siguientes: *Linux* (Sistema operativo de software libre), *Red Hat Enterprise Linux, Suse Linux*

Enterprise Server (Software de Linux para servidores Novell), *Windows* (Sistema operativo desarrollado por *Microsoft* que permite administrar recursos), *Windows* y *SQL Server Web* (Herramienta de administración basada en Web para administrar bases de datos *SQL*), *Windows* y *SQL Server Estándar* (Ofrece más funciones para administrar los datos).

Núcleos virtualizados.- En este parámetro se escoge cuantos núcleos requiere el servidor, los cuales son virtualizados y están definidos en un rango de 1 hasta 32 núcleos.

Memoria RAM.- Aquí se debe escoger la cantidad de memoria *RAM* (Memoria de acceso aleatorio que recibe instrucciones y guarda resultados) que se requiere para el servidor como unidad de almacenamiento está definida en gigabyte, su rango está presentado desde 0,6 hasta 244.

Almacenamiento local.- Se refiere al tipo de almacenamiento sea este en discos de estado sólido o *SAS* y su tamaño descrito en gigabyte, los rangos empiezan desde 4 hasta 2048.

E/S.- Este parámetro nos indica cuán rápido puede llegar a ser la lectura y escritura de la información con los discos duros, se describe de la siguiente forma: muy baja, baja, moderada, alta, muy alta.

Opción de EBS.- Son volúmenes de almacenamiento que se replican automáticamente, de esta forma manejamos alta disponibilidad ante cualquier incidente que se produzca sobre los componentes que forman parte de la solución con rendimiento óptimo y baja latencia.

Costo por hora bajo demanda.- Este es un valor monetario en dólares respecto al costo por hora del uso bajo demanda de la infraestructura escogida.

Costo por hora efectivo de las instancias reservadas.- Este es un valor monetario en dólares por el uso de las instancias escogidas y que el cliente tendría un ahorro siempre que las reserva, tal como indica la figura 30.

Seleccionar un tipo de instancia

Sistema operativo

Linux
 Red Hat Enterprise Linux
 Suse Linux Enterprise Server
 Optimizada para EBS

Windows
 Windows y SQL Server Web
 Windows y SQL Server Std.

Seleccionar	Nombre	Núcleo(s) virtual (es)	GiB de RAM	Almacenamiento local	E/S	Opción de EBS	Coste por hora bajo demanda	Coste por hora efectivo de las instancias reservadas (porcentaje de ahorro) *
<input type="radio"/>	t1.micro	1	0.6	--	Muy baja	--	\$0.020	\$0.011 (46%)
<input type="radio"/>	t2.micro	1	1.0	--	Baja	--	\$0.018	\$0.009 (47%)
<input type="radio"/>	t2.small	1	2.0	--	Baja	--	\$0.036	\$0.017 (52%)
<input type="radio"/>	t2.medium	2	4.0	--	Baja	--	\$0.072	\$0.035 (52%)
<input type="radio"/>	m3.medium	1	3.7	SSD 1 x 4	Moderada	--	\$0.133	\$0.068 (49%)
<input type="radio"/>	m3.large	2	7.5	SSD 1 x 32	Moderada	--	\$0.266	\$0.135 (49%)
<input type="radio"/>	m3.xlarge	4	15.0	SSD 2 x 40	Alta	Yes	\$0.532	\$0.271 (49%)
<input type="radio"/>	m3.2xlarge	8	30.0	SSD 2 x 80	Alta	Yes	\$1.064	\$0.543 (49%)
<input type="radio"/>	c3.large	2	3.7	SSD 2 x 16	Moderada	--	\$0.188	\$0.115 (39%)
<input type="radio"/>	c3.xlarge	4	7.5	SSD 2 x 40	Moderada	Yes	\$0.376	\$0.233 (38%)
<input type="radio"/>	c3.2xlarge	8	15.0	SSD 2 x 80	Alta	Yes	\$0.752	\$0.465 (38%)
<input type="radio"/>	c3.4xlarge	16	30.0	SSD 2 x 160	Alta	Yes	\$1.504	\$0.929 (38%)
<input type="radio"/>	c3.8xlarge	32	60.0	SSD 2 x 320	Muy alta	--	\$3.008	\$1.856 (38%)
<input type="radio"/>	g2.2xlarge	8	15.0	SSD 1 x 60	Alta	Yes	\$0.767	\$0.417 (46%)
<input type="radio"/>	r3.large	2	15.2	SSD 1 x 32	Moderada	--	\$0.300	\$0.155 (48%)
<input type="radio"/>	r3.xlarge	4	30.5	SSD 1 x 80	Moderada	Yes	\$0.600	\$0.280 (53%)
<input type="radio"/>	r3.2xlarge	8	61.0	SSD 1 x 160	Alta	Yes	\$1.200	\$0.538 (55%)

Opciones avanzadas

* para una instancia reservada de utilización intensa a la que se da un uso del 100% (más opciones de facturación disponibles)

Figura 30: Seleccionar tipo de instancia en Amazon Web Services
Adaptado de: (Calculator.s3.amazonaws, s.f.)

Escenario con Amazon Web Services.- La solución presentada en la gráfica 31 y 32 está diseñada en el centro de datos ubicado en la ciudad de Sao Paulo en Brasil, en este momento no puede brindar el proveedor una solución total porque todos sus servicios en equipos virtuales los deben hacer con servicios que se manejan por web con Windows o red hat Enterprise Linux o base de datos SQL, por lo tanto esta solución es incompleta pero nos puede servir para comparar otras soluciones por costos y aspectos técnicos.

Cálculo: instancias de Amazon EC2:

Descripción	Instancias	Uso	Tipo	Opción de facturación	Coste mensual
Portal EPV	1	100 % utilizado/m	Windows y SQL Server Web en m3.2xlarge Optimizadas para EBS	Reservada intensa d	\$ 398.94
Web Campus	1	100 % utilizado/m	Windows en c3.2xlarge	Reservada intensa d	\$ 43.92
Web Services	1	100 % utilizado/m	Windows en m3.xlarge	Reservada intensa d	\$ 157.38
Adma	1	100 % utilizado/m	Windows y SQL Server Web en m1.large	Reservada intensa d	\$ 104.68
Aplicaciones BI	1	100 % utilizado/m	Windows en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 459.70
Planning BI	1	100 % utilizado/m	Windows y SQL Server Web en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 527.78
Bases Datos	1	100 % utilizado/m	Windows y SQL Server Std. en m2.4xlarge Optimizadas para EBS	Reservada intensa d	\$ 811.06
Fiel Magister	1	100 % utilizado/m	Windows en c3.large	Reservada intensa d	\$ 11.72
Archivos	1	100 % utilizado/m	Windows en m1.xlarge Optimizadas para EBS	Reservada intensa d	\$ 213.02
SkNet	1	100 % utilizado/m	Windows y SQL Server Web en m1.small	Reservada intensa d	\$ 37.34
Cisco Prime	1	100 % utilizado/m	Red Hat Enterprise Linux en m2.xlarge	Reservada intensa d	\$ 76.86
Aranda ITIL	1	100 % utilizado/m	Windows y SQL Server Web en m1.large	Reservada intensa d	\$ 104.68
BD SharePoint	1	100 % utilizado/m	Windows y SQL Server Std. en m1.xlarge Optimizadas para EBS	Reservada intensa d	\$ 409.19
Aplicacion SharePoint	1	100 % utilizado/m	Windows en m3.2xlarge Optimizadas para EBS	Reservada intensa d	\$ 352.10
ConnectKey	1	100 % utilizado/m	Windows y SQL Server Web en c3.xlarge	Reservada intensa d	\$ 24.89
Equitrac	1	100 % utilizado/m	Windows y SQL Server Web en m1.large	Reservada intensa d	\$ 104.68
RoadNet	1	100 % utilizado/m	Windows y SQL Server Web en m1.xlarge Optimizadas para EBS	Reservada intensa d	\$ 237.17
MobiControl	1	100 % utilizado/m	Windows y SQL Server Web en c3.xlarge	Reservada intensa d	\$ 24.89
Cobrix	1	100 % utilizado/m	Windows y SQL Server Web en m1.large	Reservada intensa d	\$ 104.68
Datalyzer	1	100 % utilizado/m	Windows y SQL Server Web en m1.xlarge	Reservada intensa d	\$ 200.57

Figura 31: Escenario con Amazon Web Services

Adaptado de: (Calculator.s3.amazonaws, s.f.)

Servicios		Estimación de la factura mensual (\$ 7160.05)	
Estimación de la factura mensual			
<input checked="" type="checkbox"/> Mostrar la factura del primer mes (incluir tarifas de pago único, si las hay)			
<p>Con AWS, pague únicamente por el uso que realice. A continuación, verá una estimación de su factura mensual. Amplie cada línea para ver el desglose del costo de cada servicio. Para guardar esta factura y los valores introducidos, haga clic en el botón "Save and Share". Para borrar un servicio de la estimación, vuelva al servicio y borre el formulario de ese servicio concreto.</p>			
Guardar y compartir			
<input type="checkbox"/>	Servicio Amazon EC2 (América del Sur)		\$ 136401.25
	Cálculo:	\$ 4405.25	
	Transferencia de datos regional:	\$ 5.00	
	Instancias reservadas (tarifa única):	\$ 131911.00	
	Transferencia saliente de datos entre regiones	\$ 80.00	
<input type="checkbox"/>	Servicio AWS Direct Connect (América del Sur)		\$ 2018.88
	Puerto(s)	\$ 878.40	
	Transferencia entrante de datos	\$ 0.00	
	Transferencia saliente de datos	\$ 1140.48	
<input type="checkbox"/>	AWS Support (Business)		\$ 8821.02
	Soporte para todos los servicios de AWS:	\$ 650.92	
	Soporte para instancias reservadas (tarifa única):	\$ 8170.10	
Pago único total:			\$ 140081.10
Pago mensual total:			\$ 7160.05

Figura 32: Estimación de la factura mensual con Amazon Web Services

Adaptado de: (Calculator.s3.amazonaws, s.f.)

Para el diseño de la solución con el proveedor *Microsoft* y su producto *Azure*, se recabo en su sitio web los costos de los diferentes servicios, aquí se detalla algunos de ellos:

The screenshot shows the Microsoft Azure portal interface for configuring a SQL Server instance. The top navigation bar includes 'MI CUENTA', 'PORTAL', and a search bar. Below the navigation, there are links for 'Características', 'Precios', 'Documentación', 'Descargas', 'Gallery', 'Comunidad', and 'Soporte técnico'. A 'VERSIÓN DE EVALUACIÓN GRATUITA' badge is visible in the top right corner.

The main content area displays 'SQL Server' with a help icon. Below it, the 'Basic' tier is selected, and the 'Standard' edition is chosen. A slider indicates the instance size, with 'Médiana' selected. The price is shown as \$148.06, and the hourly rate is \$0.199/hr. The instance is labeled '1' and 'Web'. The description below the instance is 'Máquina virtual mediana (2 CPU a 1.6 GHz, 3.5 GB de RAM)'.

Figura 33: Servidor Registro personal

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM, almacenamiento de 20 GB)

Máquinas virtuales Windows

Basic **Standard**

El nivel Estándar de las instancias de proceso ofrece un conjunto óptimo de recursos de proceso, memoria y E/S para ejecutar una amplia gama de aplicaciones. Estas instancias incluyen funcionalidad de equilibrio de carga y escalado automático.

1 \$133,92
\$0,18/hr

EXTRA PEQUEÑA PEQUEÑA **MEDIANA** GRANDE EXTRA GRANDE A5 A6 A7 A8 A9

Máquina virtual mediana (2 CPU a 1.6 GHz, 3.5 GB de RAM)

Figura 34: Servidor Web services

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE EXTRA GRANDE A5 A6 A7 A8 A9

\$0,00
\$0,00/hr

Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM, almacenamiento de 20 GB)

Máquinas virtuales Windows

Basic **Standard**

El nivel Estándar de las instancias de proceso ofrece un conjunto óptimo de recursos de proceso, memoria y E/S para ejecutar una amplia gama de aplicaciones. Estas instancias incluyen funcionalidad de equilibrio de carga y escalado automático.

1 \$535,68
\$0,72/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE **EXTRA GRANDE** A5 A6 A7 A8

Figura 35: Servidor Aplicaciones BI

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server

Basic Standard

0 \$0,00
\$0,00/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA **GRANDE** EXTRA GRANDE A5 A6 A7 A8

A9

Web

Máquina virtual grande (4 CPU a 1,6 GHz, 7 GB de RAM)

1 \$1.354,08
\$1,82/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE **EXTRA GRANDE** A5 A6 A7 A8

A9

Standard

Máquina virtual extra grande (8 CPU a 1,6 GHz, 14 GB de RAM)

0 \$0,00

Figura 36: Servidor Planning

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server

Basic Standard

0 \$0,00
\$0,00/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA **GRANDE** EXTRA GRANDE A5 A6 A7 A8

A9

Web

Máquina virtual grande (4 CPU a 1,6 GHz, 7 GB de RAM)

1 \$1.354,08
\$1,82/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE **EXTRA GRANDE** A5 A6 A7 A8

A9

Standard

Máquina virtual extra grande (8 CPU a 1,6 GHz, 14 GB de RAM)

1 \$3.660,48

Figura 37: Servidor Base de datos

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA | PORTAL | Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Máquinas virtuales Windows

Basic **Standard**

El nivel Estándar de las instancias de proceso ofrece un conjunto óptimo de recursos de proceso, memoria y E/S para ejecutar una amplia gama de aplicaciones. Estas instancias incluyen funcionalidad de equilibrio de carga y escalado automático.

1 **\$491,04**
\$0,66/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE EXTRA GRANDE A5 **A6** A7 A8 A9

Máquina virtual con uso intensivo de memoria (4 CPU a 1,6 GHz, 28 GB de RAM)

Figura 38: Servidor Archivos

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA | PORTAL | Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Máquinas virtuales Windows

Basic **Standard**

El nivel Estándar de las instancias de proceso ofrece un conjunto óptimo de recursos de proceso, memoria y E/S para ejecutar una amplia gama de aplicaciones. Estas instancias incluyen funcionalidad de equilibrio de carga y escalado automático.

1 **\$245,52**
\$0,33/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE EXTRA GRANDE **A5** A6 A7 A8 A9

Máquina virtual con uso intensivo de memoria (2 CPU a 1,6 GHz, 14 GB de RAM)

Figura 39: Servidor Cisco prime

Adaptado de: (Azure Microsoft, s.f)

The screenshot shows the Microsoft Azure portal interface. At the top, there are navigation links for 'Características', 'Precios', 'Documentación', 'Descargas', 'Gallery', 'Comunidad', and 'Soporte técnico'. The 'Precios' tab is active. Below the navigation, there are buttons for 'EXTRA PEQUEÑA', 'PEQUEÑA', 'MEDIANA', 'GRANDE', and 'EXTRA GRANDE'. The selected size is 'GRANDE'. The page title is 'SQL Server' and the selected tier is 'Basic'. The pricing table shows the following details:

Virtual Machine Size	Quantity	Hourly Price	Monthly Price
Máquina virtual grande (4 CPU a 1,6 GHz, 7 GB de RAM)	1	\$0,353/hr	\$262,64
Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)	0	\$0,00/hr	\$0,00
Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)	0	\$0,00/hr	\$0,00

Figura 40: Servidor ITIL Compliance Aranda

Adaptado de: (Azure Microsoft, s.f)

The screenshot shows the Microsoft Azure portal interface. At the top, there are navigation links for 'Características', 'Precios', 'Documentación', 'Descargas', 'Gallery', 'Comunidad', and 'Soporte técnico'. The 'Precios' tab is active. Below the navigation, there are buttons for 'EXTRA PEQUEÑA', 'PEQUEÑA', 'MEDIANA', 'GRANDE', 'EXTRA GRANDE', 'A5', 'A6', 'A7', and 'A8'. The selected size is 'EXTRA GRANDE'. The page title is 'SQL Server' and the selected tier is 'Standard'. The pricing table shows the following details:

Virtual Machine Size	Quantity	Hourly Price	Monthly Price
Máquina virtual extra grande (8 CPU a 1,6 GHz, 14 GB de RAM)	1	\$1,21/hr	\$900,24
Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)	0	\$0,00/hr	\$0,00

Figura 41: Servidor Base datos SharePoint

Adaptado de: (Azure Microsoft, s.f.)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server

Basic Standard

Size	CPU	Price	Rate
Web	1	\$262,64	\$0.353/hr
Standard	0	\$0,00	\$0.00/hr
Enterprise	0	\$0,00	\$0.00/hr

Máquina virtual grande (4 CPU a 1,6 GHz, 7 GB de RAM)

Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)

Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)

Figura 42: Servidor Connectkey

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Máquinas virtuales Windows

Basic Standard

El nivel Estándar de las instancias de proceso ofrece un conjunto óptimo de recursos de proceso, memoria y E/S para ejecutar una amplia gama de aplicaciones. Estas instancias incluyen funcionalidad de equilibrio de carga y escalado automático.

Size	CPU	Price	Rate
EXTRA GRANDE	8	\$535,68	\$0.72/hr

Máquina virtual extra grande (8 CPU a 1,6 GHz, 14 GB de RAM)

Figura 43: Servidor Aplicación Share Point

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server ?

Basic Standard

Size	Role	Count	Total Price	Unit Price
EXTRA PEQUEÑA	Web	1	\$262,64	\$0,353/hr
PEQUEÑA	Web			
MEDIANA	Web			
GRANDE	Web			
EXTRA GRANDE	Web			
Máquina virtual grande (4 CPU a 1,6 GHz, 7 GB de RAM)				
EXTRA PEQUEÑA	Standard	0	\$0,00	\$0,00/hr
PEQUEÑA	Standard			
MEDIANA	Standard			
GRANDE	Standard			
EXTRA GRANDE	Standard			
Máquina virtual extra pequeña (CPU a 1 GHz, 768 MB de RAM)				

Figura 44: Servidor Equitrac

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server ?

Basic Standard

Size	Role	Count	Total Price	Unit Price
EXTRA PEQUEÑA	Web	1	\$525,27	\$0,706/hr
PEQUEÑA	Web			
MEDIANA	Web			
GRANDE	Web			
EXTRA GRANDE	Web			
Máquina virtual extra grande (8 CPU a 1,6 GHz, 14 GB de RAM)				

Figura 45: Servidor RoadNet

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

SQL Server

Basic Standard

1 \$262,64
\$0.353/hr

EXTRA PEQUEÑA PEQUEÑA MEDIANA GRANDE EXTRA GRANDE Web

Máquina virtual grande (4 CPU a 1.6 GHz, 7 GB de RAM)

Figura 46: Servidor Mobicontrol y Datalyzer

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA PORTAL Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Ancho de banda

Salida de Estados Unidos y Europa	500GB	\$59,40
Salida de otras ubicaciones	500GB	\$94,05

Figura 47: Servicio Ancho de banda

Adaptado de: (Azure Microsoft, s.f)

Microsoft Azure

MI CUENTA | PORTAL | Buscar

Características Precios Documentación Descargas Gallery Comunidad Soporte técnico

VERSIÓN DE EVALUACIÓN GRATUITA

Active Directory Gratis

Directory (gratis hasta 500.000 objetos), mejoras en la aplicación (vista previa) y Access Control

Traffic Manager 100Millón \$75,00

Consultas DNS

Figura 48: Servicio Consultas DNS
Adaptado de: (Azure Microsoft, s.f)

Con la información presentada en las figuras anteriores se realizó la tabla 22 en donde se hace un comparativo de las dos soluciones de Amazon y Microsoft sumado al proveedor local IBM para el sistema comercial porque Amazon y Microsoft no pueden brindar ese servicio con servidores Iseries ver figura 49.

Tipo/Modelo	Nombre Comercial	Cantidad	Sistema Operativo	Ubicación
3573-L2U	System Storage TS3100	1		IBM Quito
7042-CR8	HMC	1		IBM Quito
8202-E4D	iSeries Power7+	1	OS/400	IBM Quito

Figura 49: Equipos para solución de IaaS para sistema comercial con proveedor IBM del Ecuador
Tomado de: (IBM del Ecuador, 2014)

Los costos de esta solución son un pago único de \$ 60.000 más el impuesto del valor agregado y cuotas mensuales por 36 meses de \$ 7.770 más el impuesto del valor agregado, de igual forma que la solución en cloud computing sea con Amazon o Microsoft el tiempo de duración del servicio será de 3 años.

Detallamos la tabla 22 donde realizamos un comparativo de las soluciones presentadas analizándolo como gasto o inversión, de esta forma tendremos un costo total de propiedad comparado de 1 a 5 años, asumiendo que los costos del servicio se mantendría en este lapso de tiempo.

Tabla 22: TCO comparado de 1 a 5 años

Aplicación	Solución	Costo Microsoft (Gasto)	Costo Amazon (Gasto)	Costo IBM del Ecuador (Gasto)	Costo Solutions e IBM (Inversión)	Costo Solución Propuesta
Comercial BASIS Contingencia/ Desarrollo	Local Interno	-	-	-		
Archivos	Amazon y Microsoft - Consolidado	491,04	176,42	-		176,42
Bmobile Región Norte Contingencia	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Base de datos Contingencia	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Aplicaciones BI Contingencia	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Planning Contingencia	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Sistema de registro	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Portal Contingencia	Amazon y Microsoft - Alta Disponibilidad entre sitios	-	-	-		
Respaldo servidores	Sale de operación	-	-	-		
Consola Vmware	Sale de operación	-	-	-		
Bmobile Región Sur Contingencia	Amazon y Microsoft - Consolidación Eliminado	-	-	-		
Controlador de Dominio	Local interno	-	-	-		
Nodo Antivirus	Local interno	-	-	-		
Cobrix	Amazon y Microsoft	262,64	104,68	-		104,68
Datalyzer	Amazon y Microsoft	262,64	200,57	-		200,57
Portal Servidor Productivo	Amazon y Microsoft	148,06	362,34	-		148,06
Controlador de Dominio	Local interno - Consolidación	-	-	-		
Bmobile Norte Productivo	Microsoft - Consolidado	535,68	-	-		535,68
Antivirus Nodo	Microsoft - Consolidado	491,04	-	-		491,04
Bmobile Sur Productivo	Amazon y Microsoft - Consolidación Eliminado	-	-	-		
Colas Impresión	Microsoft - Consolidado	245,52	-	-		245,52
Sistema de Registro	Amazon y Microsoft	148,06	180,81	-		148,06
Web_campus	Amazon y Microsoft	148,06	43,92	-		43,92
Web Service	Amazon y Microsoft	133,92	157,38	-		133,92
ADMA	Amazon y Microsoft	262,64	104,68	-		104,68
Aplicaciones BI Productivo	Amazon y Microsoft	535,98	423,10	-		423,10
Planning Productivo	Amazon y Microsoft	1.354,08	491,18	-		491,18
Bases de datos Productivo	Amazon y Microsoft	3.660,48	774,46	-		774,46
Respaldo servidores	Sale de operación	-	-	-		
Consola Vmware	Sale de operación	-	-	-		
Comercial BASIS Productivo	IaaS con IBM	-	-	7.770,00		7.770,00
Legal Field Magíster	Microsoft	148,06	11,72	-		11,72
Archivos	Amazon y Microsoft	491,04	176,42	-		176,42
Servidor FTP	Sale de operación	-	-	-		
Control seguridad física SKNET	Amazon y Microsoft	148,06	37,34	-		37,34
Cisco Prime	Amazon y Microsoft	245,52	76,86	-		76,86
Controlador de Dominio	Local interno - Consolidación	-	-	-		

Continuación de la tabla 22.

Antivirus Nodo	Local interno - Consolidación	-	-	-		
ITIL Compliance Aranda	Amazon y Microsoft	262,64	104,68	-		104,68
Base Datos SharePoint	Amazon y Microsoft	900,24	372,59	-		372,59
Digitalización ConnectKey	Amazon y Microsoft	262,64	24,89	-		24,89
Aplicación SharePoint	Amazon y Microsoft	535,68	315,50	-		315,50
Auditoría Impresión Equitrac	Amazon y Microsoft	262,64	104,68	-		104,68
Colas Impresión	Amazon y Microsoft - Consolidación Eliminado	-	-	-		
Rutas de venta RoadNet	Amazon y Microsoft	525,27	200,57	-		200,57
Administración Hand Held Mobi Control	Amazon y Microsoft	262,64	24,89	-		24,89
Firewall TMG	Local interno	-	-	-		
Consola VMWare	Sale de operación	-	-	-		
RespalDOS Servidores	Sale de operación	-	-	-		
	Servicio Contingencia máquinas virtuales	432,00		-		432,00
	Servicio Capacidad información con redundancia geográfica	435,78		-		435,78
	Servicio DNS	75,00	22,00	-		97,00
	Servicio Ancho de banda	153,45	2.018,00	-		2.171,45
	Servicio Soporte técnico	1.000,00	650,92	-		1.650,92
	Adquisición de servidores, storage, expansiones, discos y unidad de respaldo para los centros de cómputo con garantía extendida a 3 años 24x7				756.170,00	
	Costo mensual personal para manos remotas, monitoreo, soporte				5.000,00	
	Costo mensual mantenimiento centros de cómputo (UPS, AA, Sist. Incendio, Swiching, Energía Eléctrica) de Arca Continental en Quito y Guayaquil				4.000,00	
	Costo inicial servicio con IBM (pago único)			60.000,00		60.000,00
	Total Costo mensual	14.820,50	7.160,60	7.770,00	9.000,00	18.028,58
	TCO Primer año	177.846,00	85.927,20	153.240,00	864.170,00	276.342,96
	TCO Segundo año	355.692,00	171.854,40	246.480,00	972.170,00	492.685,92
	TCO Tercer año	533.538,00	257.781,60	339.720,00	1.080.170,00	709.028,88
	Costo de Mantenimiento servidores para el Cuarto año				151.234,00	
	TCO Cuarto año	711.384,00	343.708,80	432.960,00	1.339.404,00	925.371,84
	Costo de Mantenimiento servidores para el Quinto año				151.234,00	
	TCO Quinto año	889.230,00	429.636,00	432.960,00	1.447.404,00	1.141.714,80

Después de analizar lo expuesto en la tabla 22 obtenemos que la mejor opción que cubre todas las necesidades actuales de la empresa es una combinación entre la solución como servicio: IaaS, SaaS, con los proveedores: Microsoft, Amazon e IBM con un costo de \$ 18.028,58 mensuales, el valor por tres años de este servicio es de \$ 709.028,88 y a cinco años es de \$ 1.141.714,80.

Los costos que involucra una inversión de la infraestructura sumado a la garantía extendida por 3 años con un nivel de servicio de 24x7, adicionando los servicios del personal para: manos remotas, monitoreo, soporte, incluyendo también los costos del mantenimiento para los centros de datos en Arca Continental donde se debería implementar esta solución respecto a: UPS, equipos de red, sistemas de incendio, aires acondicionados el valor total en el mismo período del tiempo es de \$ 1.080.170,00 por lo tanto se tiene un ahorro de \$ 371.141,12.

En el caso para 5 años la diferencia entre el servicio respecto a la inversión con los costos totales de mantenimiento y servicios de personal es de \$ 305.689,20 que se tendría de ahorro.

Plan de Implementación

El plan de implementación de la solución abarca 4 etapas que están divididas de la siguiente forma: análisis de las aplicaciones actuales, pruebas de la solución, implementación de la solución (transición), producción.

- Inicialmente se va realizar un análisis de la estrategia de ejecución de la migración de los servidores y aplicaciones. Manejando los de menor impacto inicialmente y posteriormente los otros.
- Se debe realizar pruebas de estrés de las aplicaciones en los ambientes de *cloud computing*, estas aplicaciones no son las críticas del negocio en una etapa inicial, se debe gradualmente ir migrando a otras aplicaciones que requieran mayores prestaciones y tengan un uso importante por los usuarios.

- Habiendo realizando varios escenarios de pruebas se planifica la ejecución de la migración en las aplicaciones del negocio desde las menos críticas a las más críticas, tomando en cuenta que tendremos el ambiente antiguo como contingencia a cualquier problema que se suscite con la implementación en esta etapa de transición.
- En esta etapa pasamos de un estado de transición a producción de las aplicaciones del negocio.

Se detalla el cronograma a seguir en la tabla 23 para el plan de implementación:

Tabla 23: Cronograma de implementación

<u>Etapas</u>	<u>Mes</u> <u>1</u>	<u>Mes</u> <u>2</u>	<u>Mes</u> <u>3</u>	<u>Mes</u> <u>4</u>	<u>Mes</u> <u>5</u>	<u>Mes</u> <u>6</u>	<u>Mes 7 a</u> <u>36</u>
Análisis de las aplicaciones actuales							
Pruebas de la solución							
Implementación de la solución (transición)							
Producción							

Microsoft Azure tiene un portafolio de políticas y procedimientos respecto a temas de seguridad y confidencialidad de la información, lo cual esta adjunto en el Anexo 2.

De igual forma Amazon Web Services tiene un amplio detalle sobre que políticas y procedimientos de seguridad se manejan internamente dentro de su organización, esto se detalla en el Anexo 3.

Retorno sobre la inversión

Este cálculo es realizado con una proyección de los ingresos y egresos actuales de la empresa tomada del año 2013, restados con los valores del costo de la solución propuesta.

Tabla 24: Calculo Retorno sobre la inversión

AÑO	Años	Ingresos totales	Egresos Totales	EGRESOS	EGRESOS PROYECTO	FLUJO DE CAJA
		-	60.000,00	60.000,00		(60.000,00)
Primer Año	1	474.000.000,00	444.216.342,96	444.000.000,00	216.342,96	29.783.657,04
Segundo Año	2	474.000.000,00	444.216.342,96	444.000.000,00	216.342,96	29.783.657,04
Tercer Año	3	474.000.000,00	444.216.342,96	444.000.000,00	216.342,96	29.783.657,04
Cuarto año	4	474.000.000,00	444.216.342,96	444.000.000,00	216.342,96	29.783.657,04
Quinto año	5	474.000.000,00	444.216.342,96	444.000.000,00	216.342,96	29.783.657,04
TIR 3 años			49639%			
TIR 5 años			49639%			

4.3 Análisis de Impacto en el negocio de la solución propuesta.

Realizando una revisión del plan de continuidad del negocio en donde se describe que los sistemas y servicios críticos para la operación del mismo como el caso del sistema comercial Basis si sufriera una caída de este se requiere que máximo en una hora se levanten los servicios, por ello se manejan sistemas de replicación entre los lseries que estarán alojados en los centros de datos de IBM del Ecuador y de Arca Continental en la planta Guayaquil.

Para los otros sistemas de información y soluciones planteadas con el proveedor Microsoft tenemos servicios contratados para recuperación de servidores virtualizados en Azure y el servicio de capacidad de almacenamiento de información con redundancia geográfica definido en la figura 50 y 51 respectivamente, de esta manera logramos que los sistemas del negocio optimicen su disponibilidad y en caso de desastre puedan estar disponibles de inmediato, cumpliendo con los requerimientos actuales y futuros de la organización.



4.4 Comparación de la solución con aprovisionamiento de infraestructura interna.

Se realizó una evaluación de costos con el proveedor Solutions para cotizar la renovación de todos los equipos de cómputo que se encuentran alojados en los tres centros de datos: Calderon, Guayaquil e IBM, para manejarlo con plataformas estandarizadas y acordes a las necesidades del negocio que la infraestructura actualmente en operación ya no abastece por motivos de capacidad de procesamiento y almacenamiento.

Detalle las capacidades de los servidores y del almacenamiento con las cuales se realizó el diseño de la solución, descritos en la tabla 19:

Tabla 25: Infraestructura actual Julio 2014

ID	Localidad	Marca	Modelo	# CPUs	Sistema Operativo	Aplicaciones	# VCores por CPU	Vel. Core (Hz)	Vel. NIC (Mbps)	Disco 1 (C:) (GB)
1	IBM	IBM	HS22	1	Vcenter Vmware ESXi	Servidores Virtuales	4	2933	100	2750
2	IBM	IBM	HS22	1	Vcenter Vmware ESXi		4	2933	100	
3	IBM	IBM	HS22	1	Vcenter Vmware ESXi		4	2933	100	
4	IBM	IBM	HS22	1	WIN 2008 Server Enterprise Sp2	Servidor base de datos BI	4	2933	100	1750
5	IBM	IBM	HS22	1	WIN 2008 Server Enterprise Sp2	Servidor de Contributor	4	2933	100	600
6	IBM	IBM	HS22	1	WIN 2008 Server Enterprise Sp2	Servidor de Aplicaciones BI	4	2933	100	600
7	IBM	IBM	Xseries	1	WIN 2008 Server Standard Sp2	Servidor respaldos de cintas	3	3160	100	350
8	IBM	IBM	Xseries	1	WIN 2008 Server Enterprise Sp2	Servidor de administración de máquinas virtuales	2	3000	100	140
9	Guayaquil	IBM	HS21	1	WIN 2008 Server Enterprise Sp2	Planning Fin-Com. Contingencia	4	3000	100	250
10	Guayaquil	IBM	HS21	1	WIN 2008 Server Enterprise Sp2	Aplicativo BI-SQLContingencia	4	3000	100	250
11	Guayaquil	IBM	HS21	1	WIN 2008 Server Enterprise Sp2	Datamart Contingencia BD	4	3000	100	1143
12	Guayaquil	IBM	HS21	1	Vcenter Vmware ESXi	Servidores Virtuales	4	3000	100	1718
13	Guayaquil	IBM	HS21	1	WIN 2003 Server Sp2	Bmobile Rnorte Contingencia	4	3000	100	250
14	Guayaquil	IBM	HS21	1	Vcenter Vmware ESXi	Servidores Virtuales	4	3000	100	1613
15	Guayaquil	IBM	Xseries	1	WIN 2008 Server Enterprise Sp2	Servidor ARC backup	4	2000	100	120
16	Guayaquil	IBM	Xseries	1	WIN 2003 Server Sp2	Administrador VMWare y Cisco	4	3000	100	120
17	Calderon	IBM	Xseries	1	Server 2003 Standard SP2	VMWARE	4	3000	100	50
18	Calderon	IBM	Xseries	2	Server 2008 Standard	ARCServer	4	4000	100	50
19	Calderon	IBM	HS22	1	Vcenter Vmware ESXi	Servidores Virtuales	4	2933	100	9300
20	Calderon	IBM	HS22	1	Vcenter Vmware ESXi		4	2933	100	
21	Calderon	IBM	HS22	1	Vcenter Vmware ESXi		4	2933	100	
TOTAL				22			81	62557	2100	21054

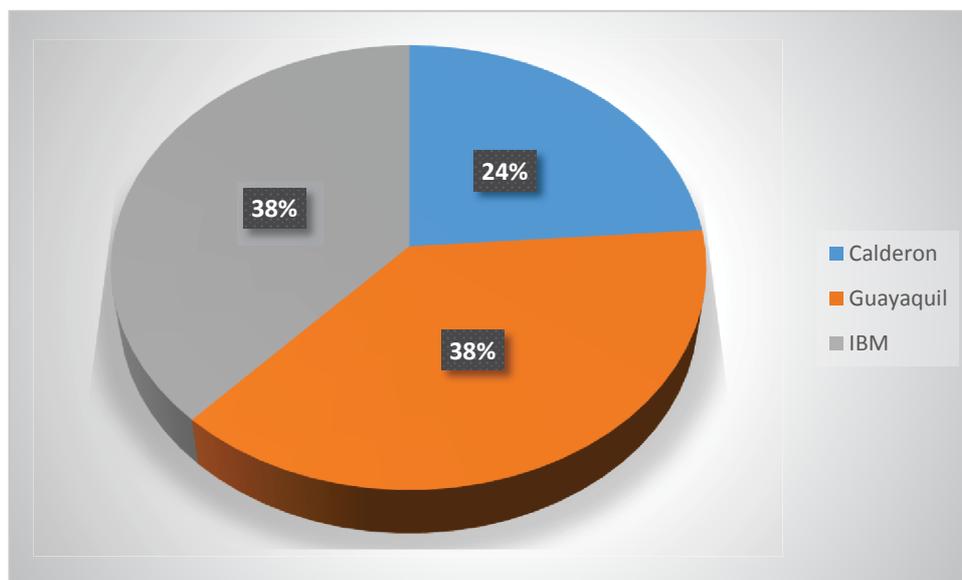


Figura 52: Cantidad de equipos por Centro de Cómputo

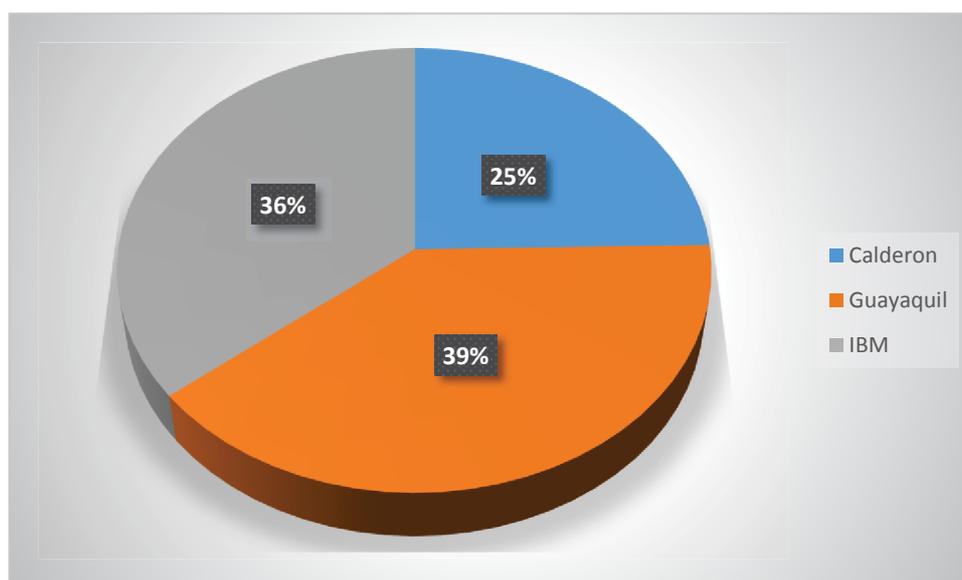


Figura 53: Procesamiento Virtual por Centro de Cómputo

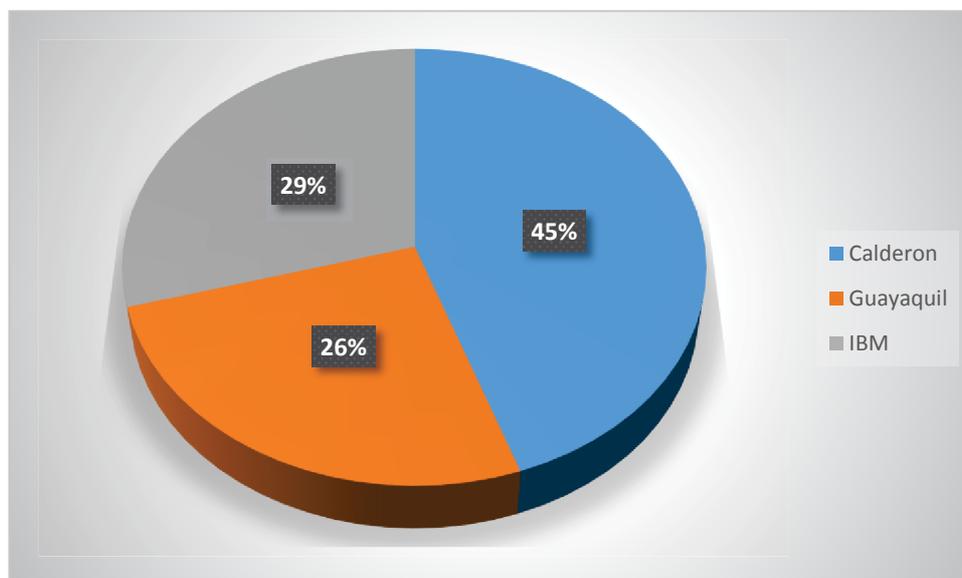


Figura 54: Capacidad de almacenamiento en los Centros de Cómputo

Los costos por parte del proveedor Solutions que se obtuvieron renovando toda la infraestructura de servidores Intel son los indicados en la tabla 26 como primera parte de la cotización tenemos el equipamiento para el centro de datos de Guayaquil.

Tabla 26: Costos inversión para centro de datos en Planta Guayaquil

SITE 1					
1,1 Chasis IBM Flex System					
8721A1U	IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable	1			
43W9049	IBM Flex System Enterprise Chassis 2500W Power Module	4			
69Y1930	IBM Flex System FC3171 8Gb SAN Switch	2			
1,2 Nodos Físicos Tipo 1					
8721A1U	IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable	1			
43W9049	IBM Flex System Enterprise Chassis 2500W Power Module	4			
69Y1930	IBM Flex System FC3171 8Gb SAN Switch	2			
95Y3309	IBM Flex System Fabric EN4093R 10Gb Scalable Switch	4			
68Y7030	IBM Flex System Chassis Management Module	1			
44X1964	IBM 8 Gb SFP+ SW Optic Transceiver	12			
46C3447	IBM SFP+ SR Transceiver	10			
00FE333	IBM RJ45 1Gbps Transceiver	10			
43W9078	IBM Flex System Enterprise Chassis 80mm Fan Module Pair	2			
			67.986,10		67.986,10
1,3 Nodos Físicos Tipo 2					
873724U	IBM Flex System x240 Compute Node, Xeon 6C E5-2620v2 80W 2.1GHz/1600MHz/15MB, 8GB, O/Bay 2.5in SAS 16GB (1x16GB, 2Rx4, 1.5V) PC3-14900 CL13 ECC DDR3 1866MHz LP RDIMM	1			
00D5048		5			
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	1			
			6.496,10		6.496,10
1,4 Nodos Físicos Tipo 3					
873724U	IBM Flex System x240 Compute Node, Xeon 6C E5-2620v2 80W 2.1GHz/1600MHz/15MB, 8GB, O/Bay 2.5in SAS 16GB (1x16GB, 2Rx4, 1.5V) PC3-14900 CL13 ECC DDR3 1866MHz LP RDIMM	3			
00D5048		9			
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	3			
			17.592,90		17.592,90
1,5 Nodos Físicos Tipo 4					
873724U	IBM Flex System x240 Compute Node, Xeon 6C E5-2620v2 80W 2.1GHz/1600MHz/15MB, 8GB, O/Bay 2.5in SAS Intel Xeon 6C Processor Model E5-2620v2 80W 2.1GHz/1600MHz/15MB	1			
00Y2852		1			
00D5048	16GB (1x16GB, 2Rx4, 1.5V) PC3-14900 CL13 ECC DDR3 1866MHz LP RDIMM	3			
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	1			
			7.246,20		7.246,20
1,6 Site 1 - Storage					
207252C	IBM Storwize V3700 SFF Dual Control Enclosure	1			
00Y2479	4GB to 8GB Cache Upgrade	2			
00Y2499	300GB 2.5in 15K rpm 6Gb SAS HDD	17			
00Y2511	1TB 2.5in 7.2K rpm 6Gb SAS NL HDD	11			
00Y2491	8Gb FC 4 Port Host Interface Card	2			
20725EU	IBM Storwize V3700 SFF Expansion Enclosure	1			
00Y2520	400GB 6Gb SAS 2.5in SSD	2			
00Y2469	3m SAS Cable (mSAS HD to mSAS HD)	2			
00Y2487	Easy Tier	1			
00Y2481	Turbo Performance	1			
00Y2523	8Gb FC SW SFP Transceivers (Pair)	2			
00AR088	5m Fiber Cable (LC)	8			
			37.572,60		37.572,60
1,7 Site 1 - Rack					
93634CX	IBM PureFlex System 42U Rack	1			
39Y8951	DPI Universal Rack PDU with Nema L5-20P and L6-20P (US line)	2			
39Y8948	IBM DPI C19 Enterprise PDU w/o Line Cord	2			
40K9614	IBM DPI 30a Cord (NEMA L5-30P)	2			
			9.081,80		9.081,80
TOTAL SITE 1					159.836,30

Tomado de: (Cotización Solutions 2014)

Los costos para la unificación de los centros de datos que están ubicados en Quito en las ubicaciones actuales de IBM y Calderon. También se incluye los servicios de instalación, configuración de los equipos en los dos sitios y están descritos en la tabla 27.

Tabla 27: Costos de la inversión y servicios de instalación para los equipos de los centros de datos de Calderón e IBM

SITE 2				
2 Chasis 1 IBM Flex System				
8721A1U	IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable	1	67.986,10	67.986,10
43W9049	IBM Flex System Enterprise Chassis 2500W Power Module	4		
69Y1930	IBM Flex System FC3171 8Gb SAN Switch	2		
95Y3309	IBM Flex System Fabric EN4093R 10Gb Scalable Switch	2		
68Y7030	IBM Flex System Chassis Management Module	1		
44X1964	IBM 8 Gb SFP+ SW Optic Transceiver	12		
46C3447	IBM SFP+ SR Transceiver	10		
00FE333	IBM RJ45 1Gbps Transceiver	10		
43W9078	IBM Flex System Enterprise Chassis 80mm Fan Module Pair	2		
2,1 Chasis 2 IBM Flex System				
8721A1U	IBM Flex System Enterprise Chassis with 2x2500W PSU, Rackable	1	67.986,10	52.297,00
43W9049	IBM Flex System Enterprise Chassis 2500W Power Module	4		
69Y1930	IBM Flex System FC3171 8Gb SAN Switch	2		
95Y3309	IBM Flex System Fabric EN4093R 10Gb Scalable Switch	2		
68Y7030	IBM Flex System Chassis Management Module	1		
44X1964	IBM 8 Gb SFP+ SW Optic Transceiver	12		
46C3447	IBM SFP+ SR Transceiver	10		
00FE333	IBM RJ45 1Gbps Transceiver	10		
43W9078	IBM Flex System Enterprise Chassis 80mm Fan Module Pair	2		
2,3 Nodos Físicos Tipo 1				
873714U	IBM Flex System x240 Compute Node, Xeon 4C E5-2609v2 80W 2.5GHz/1333MHz/10MB, 8GB, O/Bay 2.5in SAS	7	34.188,70	34.188,70
00D5036	8GB (1x8GB, 1Rx4, 1.35V) PC3L-12800 CL11 ECC DDR3 1600MHz LP RDIMM	14		
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	7		
2,4 Nodos Físicos Tipo 2				
873714U	IBM Flex System x240 Compute Node, Xeon 4C E5-2609v2 80W 2.5GHz/1333MHz/10MB, 8GB, O/Bay 2.5in SAS	3	13.536,90	13.536,90
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	3		
2,5 Nodos Físicos Tipo 3				
873724U	IBM Flex System x240 Compute Node, Xeon 6C E5-2620v2 80W 2.1GHz/1600MHz/15MB, 8GB, O/Bay 2.5in SAS	3	15.865,20	15.865,20
00D5036	8GB (1x8GB, 1Rx4, 1.35V) PC3L-12800 CL11 ECC DDR3 1600MHz LP RDIMM	6		
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	3		
2,6 Nodos Virtuales Tipo 1				
8737R2U	IBM Flex System x240 Compute Node, Xeon 8C E5-2690 135W 2.9GHz/1600MHz/20MB, 2x4GB, O/Bay 2.5in SAS	3	80.406,30	61.851,00
49Y8116	Intel Xeon 8C Processor Model E5-2690 135W 2.9GHz/1600MHz/20MB	3		
49Y8119	IBM Flex System x240 USB Enablement Kit	3		
69Y1938	IBM Flex System FC3172 2-port 8Gb FC Adapter	3		
41Y8307	IBM USB Memory Key for VMware ESXi 5.0 Update1	3		
49Y1567	16GB (1x16GB, 4Rx4, 1.35V) PC3L-10600 CL9 ECC DDR3 1333MHz LP LRDIMM	27		

Continuación de la tabla 27.

42D0637	IBM 300GB 2.5in SFF Slim-HS 10K 6Gbps SAS HDD	6		
2,7	Storage			
207252C	IBM Storwize V3700 SFF Dual Control Enclosure	1		
00Y2479	4GB to 8GB Cache Upgrade	2		
00AR259	800GB 2.5in 6Gb SAS SSD	2		
00Y2505	900GB 2.5In 10K rom 6Gb SAS HDD	16		
00Y2491	8Gb FC 4 Port Host Interface Card	2	32.930,30	25.331,00
00Y2487	Easy Tier	1		

ITEM	DESCRIPCION	CANT.	PRECIO UNITARIO	PRECIO TOTAL
00Y2481	Turbo Performance	1		
00Y2523	8Gb FC SW SFP Transceivers (Pair)	2		
00AR088	5m Fiber Cable (LC)	8		
2,8	Rack			
93634CX	IBM PureFlex System 42U Rack	1		
39Y8951	DPI Universal Rack PDU with Nema L5-20P and L6-20P (US line)	2	9.081,80	9.081,80
39Y8948	IBM DPI C19 Enterprise PDU w/o Line Cord	2		
40K9614	IBM DPI 30a Cord (NEMA L6-30P)	2		
	Subtotal:			280.137,70
Servicios Profesionales				
11	Instalación y Configuración Equipos Site 1 en Guayaquil	1	23.400,00	23.400,00
11	Instalación y Configuración Equipos Site 2 en Quito	1	24.700,00	24.700,00
	Subtotal:			24.700,00
TOTAL SITE UNO CON INSTALACION, CONFIGURACIÓN Y PUESTA EN MARCHA				183.236,30
TOTAL SITE DOS CON INSTALACION, CONFIGURACIÓN Y PUESTA EN MARCHA				304.837,70

Tomado de: (Cotización Solutions, 2014)

Los costos para la inversión del servidor Iseries para el centro de datos en IBM sería el descrito en la tabla 28.

Tabla 28: Costos para la adquisición de servidor Iseries en centro de datos IBM

ITEM	DESCRIPCION	CANT.	PRECIO UNITARIO	PRECIO TOTAL
Nuevo Equipo Power S814: 6 cores de 3.02 GHz Power 8 activos 6, 32 GB RAM, 14 Discos de 283GB 15K SAS y 4 Discos de 387GB SSD				
1	Server 1:8286 Model 41A IBM i 7.1 Cuatro discos de 387GB SFF-3 SSD for IBM i Catorce Discos de 283GB 15K RPM SAS SFF Disk Drive (IBM i) Seis PowerVM Standard Edition Dos - 8 Gigabit PCI Express Dual Port Fibre Channel Adapter SATA Slimline DVD-RAM Drive Dos - PCIe2 4-port 1GbE Adapter Dos - AC Power Supply - 1400W 2 DIMMs de 16 GB DDR3 Memory 6-core 3.02 GHz POWER8 Processor Card, activados 6 WebSphere Express for i IBM Rational Application Management Tool Set for i Application Runtime Expert for i Web Enablement for i5/OS IBM Application Runtime Expert for i IBM Web Query for System i Standard IBM Web Query for System i Registration IBM Backup Recovery and Media Services for i IBM Performance Tools for i IBM DB2 Query Manager and SQL Development Kit for i IBM Rational Development Studio for i IBM Query for i Garantía 3 años 24 x 7	1	247,388.32	247,388.32
HMC 1:7042-CR7 Rack-mounted				
8	7042-CR7 HMC 1:7042-CR7 Rack-mounted Hardw.Mgmt.Console Garantía 3 años 24 x 7	1	11,125.71	11,125.71
Librería TS3100 con 2 Drives LTO5 FC para Quito				
9	TS3100 Tape Library Model L2U Driveless Dos LTO Ultrium 5 Half High Fibre Drive Sled 3573 Rack Mount Kit Dos - Ultrium 5 Data Cartridge (5-pack) Dos Ultrium Cleaning Cartridge 13.0 m LC/LC Fibre Cable Garantía 3 años 24 x 7	1	9,582.16	9,582.16

Tomado de: Cotización Solutions (2014)

En el caso del servidor de contingencia que estaría alojado en el centro de datos de Guayaquil su capacidad de procesamiento y almacenamiento se mantiene ya que es adecuada para usarlo en caso de ser necesario.

El resumen de las cotizaciones realizadas se obtuvo los siguientes valores de la tabla 29 que denotan que el costo del equipamiento al ser renovado representa una inversión para la organización de gran cantidad de dinero que a mediano plazo podría no ser suficiente para las necesidades del día a día y requiera de inversiones posteriores y gastos de mantenimiento constantes.

Tabla 29: Resumen cotización inversión para centros de datos

Descripción infraestructura a renovar	Costos
Servidor iSeries Producción Basis	\$ 268.096
Servidores Intel centro de datos planta Guayaquil	\$ 183.236
Servidores intel centro de datos Quito e IBM	\$ 304.838
Total inversiones	\$ 756.170

Tomado de: Cotizaciones de IBM y Solutions (2014)

CONCLUSIONES

Conclusiones de la realidad actual de la organización y hallazgos encontrados:

- La infraestructura actual de hardware que tienen los centros de datos y servidores no es suficiente para las necesidades del negocio ya que está sufriendo saturación en la capacidad ofrecida. Esto ha ocasionado inconvenientes y pérdidas en los procesos que operan el negocio enfocados a los sistemas de información que no podrían soportar crecimientos en el procesamiento cuando se requiera.
- El aprovisionamiento e incremento de capacidad de cómputo podría ocasionar sobredimensionamiento de la misma, lo cual perjudica a la organización ya que sus costos operativos se incrementarían, no permitiendo ser competitivos en el mercado.
- La implementación de nuevas soluciones tecnológicas involucra tiempos altos en la implementación de las mismas de forma tradicional, adquiriendo equipamiento con tiempos altos de importación, instalación, configuración, puesta en marcha e incremento de costos en la operación del negocio, ya que en el entorno actual está limitado a capacidades establecidas que no permitan su crecimiento.
- Mediante el análisis realizado se obtiene que la organización requiere de soluciones tecnológicas que permitan brindar disponibilidad y escalabilidad acorde a las necesidades del negocio, por ello un ambiente en *cloud computing* permitirá enfocar al área de tecnologías de información a lograr este objetivo mediante servicios de aprovisionamiento de infraestructura con los proveedores: *Microsoft Azure, Amazon Web Services e IBM*.

Conclusiones de lo que ofrece el *cloud computing*:

- Las necesidades de proveer nuevas soluciones tecnológicas al negocio de forma más rápida y escalable solamente se puede lograr con servicios en *cloud computing* ya que tenemos todas las ventajas de la infraestructura presentada de esta forma y sin activos que causan a largo plazo gastos de mantenimiento y obsolescencia, mientras que en *cloud computing* son gestionados en entornos de alta disponibilidad, sincronizando entre sitios alternos y con las mejores prácticas tecnológicas del mercado.
- De las investigaciones y consultas realizadas las soluciones en *cloud computing* se van innovando e implementando nuevos servicios para las organizaciones con infraestructura y servicios para cualquier tipo de necesidad con precios sumamente convenientes y niveles de servicio acordes a cualquier requerimiento.
- Los proveedores ofrecen mejores niveles de seguridad que permiten un aislamiento de la infraestructura en *cloud* lo cual conlleva equipamiento adicional que asegure a nuestros servicios y sistemas de información logrando protegerlos en mayor grado que el resto de aplicaciones de otros clientes pero a costos más altos.
- La innovación de nuevas tecnologías en infraestructura para procesamiento y almacenamiento en un entorno de *cloud computing* permiten que la organización se beneficie de las mismas sin necesidad de invertir ingentes cantidades de dinero en este tipo de equipamiento.
- Los proveedores de servicios de *cloud computing* están enfocados en brindar servicios de la más alta calidad que apalanquen economías de escala y les permita brindar muchos más servicios a sus clientes con costos operativos adecuados para las partes.

Conclusiones del diseño propuesta:

- Los costos de renovar la infraestructura de los centros de datos actuales representan inversiones costosas para el negocio que no garantizan que a mediano plazo tenga resuelto sus necesidades informáticas, esto a comparación de ejecutar pagos mensuales de los servicios a costos muy convenientes de fácil crecimiento y ajustados a la demanda que el negocio requiera.
- El entorno de seguridad acorde a los lineamientos y requerimientos de la organización debe tener un balance que depende de la criticidad de las aplicaciones que estarán alojadas en los diferentes servicios en *cloud computing* que se han diseñado, tomando en cuenta que para cada solución podemos tener consideraciones como equipamiento dedicado para la organización y no con terceros, en otros tipos de servicios se fijara equipamiento compartido de esta forma optimizamos los costos de operación y seguimos brindando seguridad a los sistemas de información más importantes.
- Con el diseño presentado se evidencia que tendremos ahorros financieros para la organización versus los costos que involucraría implementar una solución local, la cual tiene muchos costos de servicios directos e indirectos que pueden surgir en el tiempo de operación y que deberán ser cubiertos por la organización para seguir funcionando sin contratiempos.
- Del análisis realizado se obtuvo un diseño para la migración de las aplicaciones a *cloud computing* basado en diferentes necesidades y regulaciones del negocio como son: sistemas de información centralizados en centros de datos fuera del país, aumento de capacidad para los servidores que alojan los sistemas de información actuales, mejores prácticas para el desempeño de los sistemas de información, procesos de consolidación de servidores para optimizar su uso.

- El proveedor Amazon Web Services no puede brindar una solución total porque todos sus servicios en equipos virtuales los deben ejecutar mediante sitios web con Windows o red hat Enterprise Linux y bases de datos SQL, por lo tanto esta solución es incompleta pero nos ha servido para comparar otras opciones por costos y aspectos técnicos.
- El proveedor *Microsoft Azure* brinda soluciones en SaaS e IaaS con bases de datos en SQL, Oracle lo cual permite tener flexibilidad en el tipo de motor de base de datos a usar y también en optar por una solución completa si fuera el caso en donde ellos se encarguen de todo el servicio incluido el software.
- Del análisis comparativo realizado a las soluciones de *cloud computing* para los proveedores: Amazon, Microsoft se investigó que estos proveedores no pueden brindar el servicio para servidores Iseries con lo cual se optó por una solución como IaaS con el proveedor IBM para únicamente el sistema comercial que requiere esta plataforma.
- El resultado del análisis realizado se obtuvo que la mejor opción que cubre todas las necesidades actuales de la empresa es una combinación entre la solución de *cloud computing* como servicio: IaaS, SaaS, con los proveedores: Microsoft, Amazon e IBM con un costo de \$ 18.028,58 mensuales.

Se realizó un análisis de los costos que involucraría el diseño de la solución con inversión de la infraestructura, sumado a la garantía extendida de los equipos con un nivel de servicio de 24x7, adicionando los servicios del personal para tareas operativas como: manos remotas, monitoreo, soporte e incluyendo también los costos del mantenimiento para los centros de datos en Arca Continental donde se debería implementar esta solución respecto a: ups, equipos de red, sistemas de incendio, aires acondicionados el valor total en un período de 3 años es de \$ 1.080.170,00 por lo tanto se tiene un ahorro de \$ 371.141,12 en

comparación a la solución anteriormente propuesta con un valor mensual de \$ 18.028,58.

RECOMENDACIONES

- Se recomienda hacer un piloto de pruebas antes de migrar a la solución en *cloud computing* con sistemas de desarrollo, contingencia que sean de bajo impacto para la organización y posteriormente en algún entorno crítico para encausar y afinar los procesos del negocio a esta nueva modalidad de servicio.
- Comunicar activamente y lograr el apoyo de los altos directivos y responsables de cada una de las áreas del negocio para concientizar e informar de las ventajas y desventajas de estas soluciones tecnológicas que están rompiendo paradigmas y cambiando la realidad actual de muchas organizaciones en el mundo haciéndolas más competitivas.
- Involucrar en todas las etapas del proyecto a todas las áreas del negocio y sus responsables para que estén al tanto y participen con sus colaboradores activamente en los pilotos de pruebas y posteriores pasos a seguir hasta culminar con el proyecto.
- Lograr acuerdos corporativos contractuales con el proveedor que brinde el servicio que sean beneficios para ambas partes, logrando niveles de servicio acordes a las necesidades del negocio.
- Estar en constante búsqueda y análisis de soluciones en la nube que permitan exigir a los proveedores actuales a mejorar los niveles de servicio implementados, logrando ventajas en la disponibilidad, seguridad y escalabilidad de las soluciones en *cloud computing*.

REFERENCIAS

- Aguilar, L. (2012). *Computación en la Nube*. Estrategias de Cloud Computing en las Empresas. México D.F., México: Alfaomega.
- Azure Microsoft. (s.f.). *Microsoft Azure Pricing Calculator*. Recuperado el 24 de Febrero 2014 de <http://azure.microsoft.com/en-us/pricing/calculator/?scenario=full>
- Amazon Web Services (s.f.). AWS. Recuperado el 25 de Enero de 2014 de <https://aws.amazon.com/es/>
- Brunette, G. y Mogull, R. (2009). *Security Guidance for critical areas of focus in Cloud Computing V2.1*. CSA (Cloud Security Alliance), USA. Recuperado el 16 Febrero de 2015 de <http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>
- Calculator.s3.amazonaws. (s.f.). *Amazon web services simple monthly calculator*. Recuperado el 30 de Enero 2014 de <http://calculator.s3.amazonaws.com/index.html>
- Carrero, A. (2014). *IaaS, PaaS y SaaS, cuáles son sus diferencias*. Recuperado el 28 Abril de 2014 de <http://acloudhosting.es/page/2/>
- Cebrián, C., Bonet, S. y Ballester, J. (2012). *Modelos de Despliegue de Cloud Computing (taxonomía del NIST)*. Recuperado el 16 de Abril de 2014 de <http://www.realcloudproject.com/modelos-de-despliegue-de-cloudcomputing-taxonomia-del-nist/>
- Columbus, L. (2012). *Hype Cycle for Cloud Computing Shows Enterprises Finding Value in Big Data, Virtualization*. Recuperado el 18 de Enero de 2014 de <http://www.forbes.com/sites/louiscolombus/2012/08/04/hype-cycle-for-cloud-computing-shows-enterprises-finding-value-in-big-data-virtualization/>
- Gartner Inc. (2011). *Crecimiento de la Computación a nivel mundial*. Recuperado el 16 de Febrero de 2014 de <http://telecomunicaciones-cali.blogspot.com/p/articulos.html>
- Gartner Inc. (2014). *Magic Quadrant for Cloud Infrastructure as a Service*. Recuperado el 20 de Junio 2014

de <http://www.gartner.com/technology/reprints.do?id=1-1UKQQA6&ct=140528&st=sb>

Level 3 (s.f.). *Cloud and IT Services by Level 3*: Quito, Ecuador: Recuperado el 23 de Enero de 2014 de <http://www.level3.com/en/products-and-services/cloud-and-it/>

Mendez, F. (2010). *Cloud Computing. La computación en nube un modelo económico, eficiente y polémico*. Recuperado el 12 de Febrero de 2014 de <http://tic-tac.teleco.uvigo.es/profiles/blogs/cloud-computing-la-computacion>

Microsoft Azure. (s.f.). *Azure*. Recuperado el 10 de Febrero 2014 de <http://azure.microsoft.com/es-es/>

Molina, M. (2011). *Qué es Cloud computing*. Recuperado el 12 de Abril 2014 de <http://www.poderpda.com/editorial/%C2%BFque-es-cloud-computing/>

NIST. (2011). *The NIST Definition of Cloud Computing*. Recuperado el 15 de Enero 2015 de <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>

PiCloud. (s.f.). *San Francisco, EU*: Recuperado el 22 de Enero 2014 de <http://www.picloud.com/>

SAP. (s.f.). *Cloud Computing | Cloud Solutions | SAP. EU*: Recuperado el 29 Enero 2014 de <http://www.sap.com/pc/tech/cloud.html>

TelcoNet. (s.f.). *La fibra del Ecuador - Centro de Datos Guayaquil, Ecuador*. Recuperado el 20 de Enero 2014 de <http://www.telconet.net/servicios/datacenter>

Torres, J. (2011). *Empresas en la nube: Ventajas y retos del cloud computing*. Barcelona, España: Libros de Cabecera.

Think Big. (2012). *Gartner apuesta por cloud, social, movilidad y big data para 2013 Think Big*. EU: Recuperado el 4 Febrero 2014 de <http://blogthinkbig.com/gartner-tendencias-tecnologicas-2013/>

ANEXOS

ANEXO 1: GLOSARIO DE TÉRMINOS

- **.NET.-** Plataforma que permite desarrollar aplicaciones seguras y robustas.
- **64 bits.-** Permite desplazar el doble de información que en un sistema de 32 bits
- **Algoritmos.-** conjunto de operaciones que permiten llegar a una solución
- **Autenticación.-** Validar la identidad de una persona o proceso para acceder a un recurso.
- **Balance scorecard.-** Cuadro de mando integral, herramienta que permite visualizar estrategias.
- **Base de datos.-** Conjunto de datos que son almacenados mediante una herramienta.
- **BPM.-** Sistemas informáticos para administración por procesos del negocio.
- **Business Intelligence.-** Inteligencia de Negocios, conjunto de estrategias que facilitan la toma de decisiones
- **Cedis.-** Sucursales, agencias.
- **Cisco.-** Empresa mundial de Tecnología Informática con sede en San José-California.
- **Claro.-** Es la marca de la empresa de Telecomunicaciones CONECEL que opera en Ecuador desde 1993.
- **Cognos Power Play.-** Aplicación que permite analizar datos en gran volumen.
- **CRM.-** Sistemas informáticos para la administración de la relación con los clientes.
- **Cubos.-** Datos obtenidos de diferentes dimensiones de un negocio que se desean analizar.
- **Encriptación.-** Ocultar y proteger datos de forma aleatoria.
- **EPM.-** Sistemas informáticos para la administración de proyectos empresariales.

- **ERP.-** Sistemas informáticos destinados a la administración de recursos en una organización.
- **Escalabilidad.-** Mejorar recursos sin perder calidad de servicio.
- **Facebook.-** Es un sitio web de redes sociales que permite publicar información.
- **FielMagister.-** Aplicativo registrado por Ediciones Legales.
- **Flexibilidad.-** Amplitud del recurso para intercambiar información.
- **Hardware.-** Es la parte física de un dispositivo o sistema
- **HCM.-** Modulo Capital Humano en SAP
- **Hipervisor.-** Monitor de máquina virtual es una plataforma que permite visualizar varios sistemas operativos en un mismo computador.
- **Hyper-V.-** Es una aplicación de virtualización de Microsoft que ayuda a mejorar procesos.
- **IBM.-** International Business Machine, empresa multinacional estadounidense que fabrica y comercializa hardware y software con filiales en varios países.
- **Instagram.-** Aplicación que permite publicar fotos y videos en la red.
- **Intel.-** Fabrica procesadores diseñados para diferentes ordenadores.
- **ITIL Compliance.-** Gestiona el cumplimiento de los procesos.
- **ITIL.-** Biblioteca de Infraestructura de Tecnologías de Información, metodología que ayuda a la organización a controlar y gestionar recursos.
- **Java.-** Lenguaje de programación orientado a objetos
- **Level3.-** Proveedor de Telecomunicación con sede en Omaha, Nebraska que atiende en redes centrales en América del Norte, América Latina, Europa, África y Asia.
- **Linux.-** Sistema operativo de software libre
- **Mainframe.-** Computadora central que procesa una gran cantidad de datos
- **Máquinas virtualizadas.-** Es un programa que simula a una computadora permitiendo ejecutar aplicaciones.
- **Microsoft SharePoint.-** Plataforma que permite guardar, organizar, compartir y acceder a información desde un dispositivo.

- **Microsoft.-** Multinacional estadounidense fundada por Bill Gates dedicada al sector de software y hardware.
- **Mitigación.-** Ayuda a tomar medidas para reducir vulnerabilidades o riesgos
- **Navegadores.-** Aplicaciones que permiten acceder a información mediante una red como el internet.
- **Node.js.-** Es una plataforma JavaScript que permite crear aplicaciones.
- **OS400.-** Creado por IBM, es un sistema operativo que permite gestionar recursos.
- **Parametrizados.-** Dato o datos importantes que permiten valorar una situación o recurso
- **PHP.-** Lenguaje de programación de tipo de datos dinámicos
- **Plataformas robustas.-** Sistema que permite al usuario recuperar la información con facilidad.
- **PMI Project Management Institute.-** Organización internacional sin fines de lucro conformada por miembros que establecen estándares y certificaciones para la gestión de proyectos.
- **Procesadores Multinúcleo.-** Mejora el rendimiento y la eficacia permitiendo ejecutar varios programas al mismo tiempo repartiéndolos en cada núcleo o cerebro.
- **Python.-** Diseñado para enfatizar la productividad y la legibilidad del código
- **RAM.-** Memoria de acceso aleatorio que recibe instrucciones y guarda resultados.
- **Redes de datos.-** Compuesto por equipos y aplicaciones conectados por dispositivos que permiten transportar datos.
- **Ruby.-** Programación divertida y flexible para el programador.
- **SAP.-** Sistemas o programas que permiten gestionar la información.
- **Servicio de 7x24.-** Servicio que se ofrece durante las 24 horas del día los 365 días del año.
- **Servidor.-** Es una aplicación o un computador donde se ejecuta un programa que realiza una tarea en ayuda de otra.

- **Single sign-one.-** El usuario es autenticado una sola vez y accede a los servicios disponibles.
- **Sistemas de información.-** Compuesto por elementos que permiten al usuario obtener y administrar datos de acuerdo a su perfil.
- **Sistemas operativos.-** Programa o conjunto de programas que permiten transmitir datos
- **Smartphone.-** Teléfono móvil con funciones similares a un computador.
- **Software.-** Es uno o varios programas que permiten realizar tareas en un sistema.
- **SQL Server Estándar.-** Ofrece más funciones para administrar los datos.
- **SQL Server Web.-** Herramienta de administración basada en Web para administrar bases de datos SQL.
- **Suse Linux Enterprise Server.-** Software de Linux para servidores Novell.
- **Tabletas.-** Ordenador personal móvil con pantalla táctil.
- **TelcoNet.-** Proveedor ecuatoriano de servicios informáticos, telecomunicaciones e internet.
- **The Coca Cola Company.-** Corporación multinacional dedicada a la elaboración de bebidas.
- **Twitter.-** Servicio que permite publicar mensajes en la red.
- **Virtualización.-** Simulación de un recurso tecnológico
- **Visual Studio.-** Herramienta que permite desarrollar aplicaciones.
- **Web.-** Significa red o malla que puede ser una página, un sitio o un servidor.
- **Windows 2008 Server.-** Sistema operativo diseñado para servidores.
- **Windows.-** Sistema operativo desarrollado por Microsoft que permite administrar recursos.

ANEXO 2: SEGURIDAD, PRIVACIDAD, CUMPLIMIENTO, RECURSOS EN MICROSOFT AZURE

Microsoft Azure Centro de confianza

Como cliente de Azure, que ha confiado Microsoft para ayudar a proteger sus datos. Microsoft valora esta confianza, y la privacidad y seguridad de sus datos es una de nuestras principales preocupaciones. Microsoft se esfuerza por tomar un papel de liderazgo en lo que respecta a las prácticas de seguridad, privacidad y cumplimiento.

Independientemente verificado

Cumplimiento de las normas de la industria de clase mundial verificadas por terceros

Microsoft se asocia con los clientes para ayudarlos a abordar una amplia gama de requisitos regulatorios internacionales, nacionales y específicos de la industria. Al proporcionar a los clientes con servicios en la nube, verificados de forma independiente compatibles, Microsoft hace que sea más fácil para los clientes a lograr el cumplimiento de la infraestructura y las aplicaciones que se ejecutan en Azure.

Implacable en la seguridad

Excelencia en la reducción de las prácticas de seguridad de borde

A través de las prácticas de seguridad de vanguardia y experiencia inigualable correr algunos de los mayores servicios en línea de todo el mundo, Microsoft ofrece la empresa de servicios cloud clientes pueden confiar.

Para informar sobre problemas de seguridad de contactos de 24X7 Microsoft Online Services Incidentes de Seguridad y reportes de abuso

Diseño y Seguridad Operacional

Microsoft ha desarrollado las mejores prácticas de la industria líder en el diseño y gestión de los servicios en línea, incluyendo:

- Centros de Excelencia de Seguridad. La Unidad de Crímenes Digitales Microsoft, Microsoft Ciberdelincuencia Center y Microsoft Malware Protection Center dar una idea de la evolución de las amenazas a la seguridad mundial.
- . Security Development Lifecycle (SDL) Desde 2004, todos los productos y servicios de Microsoft se han diseñado y construido desde cero utilizando su Ciclo de Vida de Desarrollo de Seguridad - un enfoque integral para escribir código más seguro, confiable y privacidad mejorada.
- Operational Security Assurance (OSA). El programa Microsoft OSA proporciona una línea de base de seguridad operacional en todos los principales servicios en la nube, ayudando a asegurar los riesgos clave son mitigados de forma coherente.
- Supongamos Incumplimiento. Los equipos especializados de ingenieros de seguridad de Microsoft utilizan prácticas de seguridad pioneras y operan con una 'asumir incumplimiento' mentalidad de identificar posibles vulnerabilidades y proactivamente eliminar las amenazas antes de que se conviertan en riesgos para los clientes.
- Respuesta a Incidentes. Microsoft opera un evento 24x7 y el equipo de respuesta a incidentes mundial para ayudar a mitigar las amenazas de ataques y actividades maliciosas.

Controles de seguridad y Capacidades

Azure proporciona una base confiable de que los clientes pueden diseñar, construir y gestionar sus propias aplicaciones en la nube seguras e infraestructura.

- 24 horas supervisa la seguridad física. Los centros de datos se construyen físicamente, administrado y controlado a los datos y servicios de albergue de accesos no autorizados, así como las amenazas ambientales.
- El seguimiento y la explotación forestal. La seguridad se controla con la ayuda de sistemas de vigilancia, de correlación y análisis centralizados que gestionan la gran cantidad de información generada por los dispositivos dentro del entorno y proporcionar alertas oportunas. Además, múltiples niveles de supervisión, registro y presentación de informes están disponibles para proporcionar visibilidad a los clientes.
- Parches. Sistemas de despliegue integrados gestionar la distribución e instalación de parches de seguridad. Los clientes pueden aplicar procesos de gestión de parches similares para máquinas virtuales desplegadas en Azure.
- Antivirus / Antimalware protección. Microsoft Antimalware está integrado en servicios en la nube y se puede habilitar para máquinas virtuales para ayudar a identificar y eliminar virus, spyware y otro software malicioso y proporciona protección en tiempo real. Los clientes también pueden ejecutar soluciones antimalware de los socios en sus máquinas virtuales.
- Sistemas de detección y prevención de intrusiones de detección de intrusiones y ataques DDoS., La negación de la prevención del ataque del servicio, pruebas de penetración regular, y herramientas forenses ayudan a identificar y mitigar las amenazas de dentro y fuera de Azure.
- Cero privilegios permanentes. El acceso a los datos de los clientes por operaciones de Microsoft y personal de apoyo se le niega por defecto. Cuando se otorga el acceso se gestiona y registra cuidadosamente. El acceso del centro de datos a los sistemas que almacenan datos de los clientes es controlado estrictamente por medio de procesos de la caja de bloqueo.
- Aislamiento. Azure utiliza aislamiento de la red para evitar que las comunicaciones no deseadas entre las implementaciones, y los controles de

acceso bloquear usuarios no autorizados. Máquinas virtuales no reciben tráfico entrante de Internet a menos que los clientes les configuren para hacerlo.

- Redes virtuales Azure. Los clientes pueden optar por asignar múltiples despliegues a una red virtual aislada y permitir que esos despliegues se comuniquen entre sí a través de direcciones IP privadas.
- Las comunicaciones cifradas. Built-in SSL y TLS criptografía permite a los clientes para cifrar las comunicaciones dentro y entre los despliegues, desde Azure para centros de datos de correo locales, y de Azure para administradores y usuarios.
- Conexión privada. Los clientes pueden utilizar ExpressRoute para establecer una conexión privada a los centros de datos de Azure, manteniendo su tráfico de Internet.
- Cifrado de datos. Azure ofrece una amplia gama de capacidades de cifrado hasta AES-256, dando a los clientes la flexibilidad para implementar los métodos que mejor se adapte a sus necesidades.
- Identidad y acceso. Azure Active Directory permite a los clientes administrar el acceso a Azure, Office 365 y un mundo de otras aplicaciones de la nube. Multi-Factor oferta monitoreo de autenticación y acceso mejorado la seguridad.

Descargue el Azure Seguridad, Privacidad y Cumplimiento whitepaper para aprender más.

Pruebas de Penetración

Microsoft lleva a cabo pruebas de penetración regular para mejorar los controles de seguridad Azure y procesos. Entendemos que la evaluación de seguridad es también una parte importante del desarrollo de aplicaciones de nuestros clientes y la implementación. Por lo tanto, hemos establecido una política para los clientes para llevar a cabo pruebas de penetración autorizado en sus aplicaciones alojadas en Azure. Debido a que estas pruebas puede ser indistinguible de un ataque real, es fundamental que los clientes lleven a cabo pruebas de penetración sólo después de obtener la aprobación previa de Azure de asistencia al cliente. Las pruebas de penetración deben llevarse a cabo de acuerdo con nuestros términos y condiciones. Las solicitudes de pruebas de penetración deben presentarse con un mínimo de 7 días de aviso por adelantado.

Para obtener más información sobre las pruebas de penetración, consulte la prueba de penetración general, y para iniciar las pruebas de penetración, por favor complete el Formulario de Aprobación pruebas de penetración.

Tu privacidad importa

Última actualización: septiembre 2014

La privacidad es uno de los fundamentos de la informática de confianza de Microsoft. Microsoft tiene una larga trayectoria de compromiso con la privacidad, que es una parte integral de nuestro producto y servicio del ciclo de vida. Trabajamos para ser transparentes en nuestras prácticas de privacidad, ofrecer a los clientes opciones de privacidad significativas, y gestionar de forma responsable los datos que almacenamos.

Los Principios de Privacidad de Microsoft, nuestras declaraciones de privacidad específicas y nuestros estándares de privacidad internos guían cómo recopilamos, utilizamos y protegemos los datos del cliente. Información general

sobre la nube privacidad está disponible en la privacidad Microsoft sitio Web. También publicamos un libro blanco de privacidad en la nube para explicar cómo Microsoft está abordando la vida privada en el ámbito de la computación en nube.

La Declaración de Privacidad Azure describe la política y las prácticas que rigen el uso de los clientes de Azure de privacidad específica.

Localización de datos de clientes

Microsoft opera actualmente Azure en los centros de datos de todo el mundo. En esta sección, nos dirigimos a consultas de los clientes comunes sobre el acceso y la ubicación de los datos del cliente.

- Los clientes pueden especificar el área (s) geográfica “geos y “regiones “de los centros de datos de Microsoft en el que se almacenarán los datos del cliente Geos y regiones disponibles se muestran a continuación Por favor, consulte la disponibilidad del servicio por región

Geo

Región

(Anteriormente subregión)

Estados Unidos Este de Estados Unidos (Virginia)

Este de Estados Unidos 2 (Virginia)

Central de Estados Unidos (Iowa)

Oeste de Estados Unidos (California)

Norte de Estados Unidos (Illinois)

Sur de Estados Unidos (Texas)

Europa Norte de Europa (Irlanda)

West Europe (Países Bajos)

Asia y el Pacífico Sudeste de Asia (Singapur)

Este de Asia (Hong Kong)

Japón Oriental (prefectura de Saitama)

Japón West (Prefectura de Osaka)

Brasil Brasil Sur (Sao Paulo)

Replicación unidireccional a US South Central (Texas)

Australia Australia Oriental (Nueva Gales del Sur)

Australia Sudeste (Victoria)

Los Australia Regiones sólo están disponibles para los clientes con direcciones de facturación en Australia y Nueva Zelanda.

- Microsoft puede transferir datos de clientes dentro de un geo (por ejemplo, dentro de Europa) para la redundancia de datos u otros fines. Por ejemplo, Azure se replica Blob y Tabla de datos entre dos regiones de un mismo geo para una mayor durabilidad de datos en caso de un desastre mayor centro de datos.
- Microsoft no transferirá datos de clientes fuera de los geo (s) específica del cliente (por ejemplo, de Europa a los Estados Unidos o desde los Estados Unidos a Asia) excepto cuando sea necesario para que Microsoft proporciona soporte al cliente, solucionar problemas del servicio, o el cumplimiento de los requisitos legales; o donde el cliente configura la cuenta para permitir dicha transferencia de datos de clientes, incluso mediante el uso de:
 - Características que no permiten la selección geo como Content Delivery Network (CDN), que proporciona un servicio de almacenamiento en caché a nivel mundial;
 - Roles Web y trabajador, que los paquetes de despliegue de software de copia de seguridad a los Estados Unidos, independientemente de geo despliegue;
 - Vista previa, beta, u otras características de pre-lanzamiento que puede almacenar o transferir los datos de los clientes a los Estados Unidos, independientemente de geo despliegue;
 - Azure Active Directory (excepto Access Control), que puede almacenar datos de Active Directory en todo el mundo a excepción de los Estados Unidos (donde

los datos de Active Directory se mantiene en los Estados Unidos) y Europa (donde Active Directory de datos se encuentra en Europa y los Estados Unidos);

- Azure Multi-Factor de autenticación, que almacena datos de autenticación en los Estados Unidos;
- Azure RemoteApp, que puede almacenar nombres de usuario final y las direcciones IP del dispositivo a nivel mundial, según el lugar donde el usuario final accede al servicio.
- Microsoft no controla ni limita los geos de la cual los clientes o los usuarios finales pueden acceder a los datos del cliente.

Vea la sección de la Directiva sobre protección de datos de abajo para obtener información sobre el marco normativo bajo el cual transfiere datos de Microsoft.

Directiva de protección de datos de la UE

La Directiva de la UE de protección de datos (95/46 / CE) contiene requisitos estrictos para el tratamiento de los datos personales en la Unión Europea. Bajo la ley europea, nuestro cliente es el responsable del tratamiento de los datos de sus clientes y Microsoft es el procesador de datos. Para permitir el flujo de la información requerida por los negocios internacionales (incluida la transferencia transfronteriza de datos personales), Microsoft se adhiere al Marco de Puerto Seguro entre Estados Unidos y la UE desarrollado por el Departamento de Comercio en coordinación con la Comisión Europea. La certificación de puerto seguro permite la transferencia legal de los datos personales de la UE fuera de la UE a Microsoft para su procesamiento.

Microsoft también ofrece a los clientes estándar de la UE cláusulas contractuales que proporcionan garantías contractuales adicionales alrededor de las transferencias de datos de carácter personal para los servicios comprendidos en el estudio. La implementación de Microsoft de las cláusulas modelo de la UE ha sido validado por las autoridades de protección de datos de la Unión Europea

como en consonancia con las normas de privacidad estrictas que regulan las transferencias internacionales de datos de las empresas que operan en sus países miembros. Microsoft es la primera empresa en recibir la aprobación conjunta del artículo de la UE 29 Grupo de Trabajo por sus fuertes compromisos contractuales para cumplir con las leyes de privacidad de la UE, sin importar dónde se encuentran los datos.

Es importante tener en cuenta que Microsoft va a transferir datos de clientes de la UE fuera de la UE, sólo en circunstancias muy limitadas. Ver la ubicación de la sección de datos para obtener más detalles.

Los datos de clientes y otros tipos de datos

- Datos del cliente son todos los datos, incluyendo todos los archivos de texto, sonido, software o imágenes que usted proporciona, o se proporcionan en su nombre, a nosotros a través de su uso de los Servicios. Por ejemplo, los datos del cliente incluye datos que usted carga para el almacenamiento o transformación en los servicios y aplicaciones que usted o sus usuarios finales subas por haber acogido en los Servicios. No incluye la configuración o ajustes técnicos y la información.
- Data Administrator es la información acerca de los administradores (incluyendo la cuenta de contacto y administradores de suscripción) proporcionada durante el registro, compra, o la administración de los servicios, tales como nombre, dirección, número de teléfono y dirección de correo electrónico.
- Los metadatos incluyen configuración y los ajustes técnicos y la información. Por ejemplo, incluye los ajustes de configuración de disco para una Máquina Virtual Azure o el diseño de base de datos para una base de datos SQL Azure.
- Los datos de control de acceso se utiliza para gestionar el acceso a otros tipos de datos o funciones dentro de Azure. Incluye contraseñas, certificados de seguridad, y otros datos relacionados con la autenticación.

Respetamos la privacidad de sus datos

La privacidad es uno de los fundamentos de la informática de confianza de Microsoft. Microsoft tiene una larga trayectoria de compromiso con la privacidad, que es una parte integral de nuestro producto y servicio del ciclo de vida.

Responsabilidad compartida

Nuestros clientes de todo el mundo están sujetos a muchas leyes y reglamentos diferentes. Los requisitos legales de un país o la industria pueden ser incompatibles con los requisitos legales aplicables en otros lugares. Como proveedor de servicios en la nube globales, debemos ejecutar nuestros servicios con las prácticas operacionales comunes y funciones a través de múltiples geografías y jurisdicciones. Para ayudar a nuestros clientes a cumplir con sus propias necesidades, construimos nuestros servicios con requisitos comunes de seguridad y privacidad en mente. Es en última instancia a nuestros clientes, sin embargo, para evaluar nuestra oferta con sus propios requisitos, para que puedan determinar si nuestros servicios satisfacen sus necesidades regulatorias. Estamos comprometidos a proporcionar a nuestros clientes información detallada sobre nuestros servicios en la nube para ayudarles a hacer sus propias evaluaciones reglamentarias.

También es importante señalar que una plataforma en la nube como Azure exige una responsabilidad compartida entre el cliente y Microsoft. Microsoft es responsable de la plataforma, y busca ofrecer un servicio de nube que puede satisfacer las de seguridad, privacidad y las necesidades de cumplimiento de nuestros clientes. Los clientes son responsables de su entorno una vez que el servicio se ha aprovisionado, incluyendo sus aplicaciones, el contenido de datos, máquinas virtuales, las credenciales de acceso, y el cumplimiento de los requisitos normativos aplicables a su industria en particular y la configuración regional.

Actualizaciones

La información presentada en el Centro de confianza Azure es la vigente en la "última actualización" en la parte superior, pero está sujeta a cambios sin previo

aviso. Le animamos a que revise el Centro de confianza periódicamente para estar informado de los nuevos desarrollos de seguridad, privacidad y cumplimiento.

ANEXO 3: AMAZON WEB SERVICES, INFORMACIÓN GENERAL ACERCA DE LOS PROCESOS DE SEGURIDAD

Amazon Web Services (AWS) ofrece una plataforma de informática en nube escalable, con alta disponibilidad y fiabilidad, además de la flexibilidad necesaria para permitir a sus clientes crear una amplia gama de aplicaciones. Además de mantener la confianza de nuestros clientes, para AWS es de suma importancia ayudar a proteger la confidencialidad, integridad y disponibilidad de los sistemas y los datos de los clientes. Con el presente documento se pretende responder a preguntas del tipo "¿Cómo puede ayudarme AWS a proteger mis datos?". En particular, se describen los procesos de seguridad física y operativa de AWS para infraestructuras de red y de servidor administradas con AWS, así como las implementaciones de seguridad específicas del servicio. En este documento se ofrece información general de seguridad en relación con los siguientes ámbitos relevantes para AWS:

Entorno de responsabilidad compartida

Resumen del entorno de control

Principios sobre el diseño seguro

Copia de seguridad

Supervisión

Información y comunicación

Permanencia del empleado

Seguridad física

Medidas para la protección del medio ambiente

Gestión de la configuración

Gestión de la continuidad del negocio

Copias de seguridad

Aislamiento de errores

Características de seguridad de la cuenta de Amazon

Seguridad de la red

Seguridad específica del servicio de AWS

Seguridad de Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Virtual Private Cloud (Amazon VPC)
Seguridad de Amazon Simple Storage Service (Amazon S3)
Seguridad de Amazon SimpleDB
Seguridad de Amazon Relational Database Service (Amazon RDS)
Seguridad de Amazon Simple Queue Service (Amazon SQS)
Seguridad de Amazon Simple Notification Service (SNS)
Seguridad de Amazon CloudWatch
Seguridad de Auto Scaling
Seguridad de Amazon CloudFront
Seguridad de Amazon Elastic MapReduce

Entorno de responsabilidad compartida

Al transferir la infraestructura de TI a AWS, se crea un modelo de responsabilidad compartida entre AWS y su cliente. Este modelo compartido puede aliviar la carga operativa del cliente, ya que AWS opera, gestiona y controla los componentes del sistema operativo host y la capa de virtualización a fin de ofrecer seguridad física en las instalaciones en las que operan los servicios. Por otra parte, el cliente asume la responsabilidad y la gestión, entre otros elementos, del sistema operativo invitado (incluidas las actualizaciones y las revisiones de seguridad), de cualquier otro software de aplicaciones asociadas y de la configuración del firewall del grupo de seguridad que ofrece AWS. Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de los mismos en su entorno de TI y de la legislación y los reglamentos aplicables. Los clientes pueden mejorar la seguridad o cumplir requisitos de conformidad más estrictos gracias a la utilización de aplicaciones tecnológicas como firewalls basados en host, prevención y detección de intrusiones basadas en host, cifrado y gestión de claves. La naturaleza de esta responsabilidad compartida también ofrece flexibilidad y la posibilidad de que el cliente pueda controlar la implementación de soluciones que satisfagan los requisitos de certificación específicos del sector.

Resumen del entorno de control

AWS gestiona un entorno de control completo que incluye las políticas, los procesos y las actividades de control necesarios para prestar todos los servicios web que ofrece. El entorno de control colectivo abarca las personas, los procesos y la tecnología necesarios para mantener un entorno que admita la eficacia de controles específicos y de marcos de control para los que AWS dispone de certificación o para los que cumple los requisitos pertinentes.

AWS dispone de varias certificaciones y de acreditaciones de terceros. Entre ellas se incluyen:

- SAS 70 Tipo II. Este informe incluye controles detallados que AWS aplica junto con declaraciones de auditoría independientes acerca de la utilización eficaz de dichos controles.
- PCI DSS Nivel 1. AWS ha obtenido una validación independiente por la que se certifica que cumple con el estándar de seguridad de datos del sector de la tarjeta de pago (Payment Card Industry, PCI) como un proveedor de servicios de host.
- ISO 27001. AWS ha obtenido la certificación ISO 27001 del sistema de gestión de la seguridad de la información (SGSI) que abarca la infraestructura, los centros de datos y los servicios.
- FISMA. AWS permite a los clientes de organismos gubernamentales conseguir y mantener el cumplimiento de la ley estadounidense Federal Information Security Management Act (FISMA) relativa a la gestión de la seguridad de la información. AWS ha obtenido una aprobación para operar en el nivel FISMA-Low. También ha completado la implementación de control y ha pasado satisfactoriamente las pruebas de seguridad independiente y la evaluación necesarias para operar en el nivel FISMA-Moderate. AWS está tratando de que los organismos gubernamentales le concedan la aprobación para poder operar en el nivel FISMA-Moderate.

Además, los clientes han creado en AWS aplicaciones sanitarias que cumplen con las normas de seguridad y privacidad HIPAA.

Puede encontrar información adicional acerca de estas certificaciones y de las acreditaciones de terceros en el documento técnico sobre riesgos y conformidad legal que se encuentra disponible en el sitio.

Principios sobre el diseño seguro

El proceso de desarrollo de AWS aplica las mejores prácticas seguras de desarrollo de software, que incluyen las revisiones formales de diseño de AWS Security Team, el modelado de amenazas y la realización de una evaluación de riesgos. Las herramientas de análisis de código estático se ejecutan como parte de un proceso de compilación estándar y todo el software implementado se somete a pruebas de penetración recurrentes realizadas por expertos de la industria.

Seleccionados de forma minuciosa. Las revisiones de la evaluación de riesgos de seguridad que realizamos empiezan en la fase de diseño y el compromiso se extiende desde el lanzamiento hasta las operaciones en curso.

Supervisión

AWS utiliza sistemas automáticos de supervisión para ofrecer un alto nivel de rendimiento y disponibilidad de los servicios. La supervisión proactiva se encuentra disponible a través de una serie de herramientas en línea destinadas tanto para uso interno como externo. Los sistemas de AWS disponen de una gran variedad de recursos para poder supervisar las principales métricas operativas. Las alarmas se configuran para notificar al personal de operaciones y gestión cuándo las métricas operativas clave superan los umbrales de advertencias anticipadas. Se utiliza un programa de asistencia de guardia a fin de que este personal esté siempre disponible para solucionar los problemas de funcionamiento. Incluye además un sistema de localización de personas a fin de que las alarmas se comuniquen al personal de operaciones de forma rápida y fiable.

La documentación también se mantiene actualizada para ayudar e informar al personal de operaciones en la gestión de incidentes o problemas. En caso de que se precise de colaboración para solucionar algún problema, se utiliza un sistema de videoconferencia que incorpora funcionalidades de comunicación y registro. Los coordinadores cualificados de la llamada facilitan la comunicación y el progreso durante la gestión de los problemas operativos que precisan de colaboración. Se solicita un análisis de los resultados después de cualquier problema operativo importante, independientemente del impacto externo y, además, se elaboran documentos de la causa del error (COE) a fin de detectar la causa principal y de adoptar medidas preventivas en el futuro. Se organizan reuniones operativas semanales para realizar un seguimiento en ellas de la aplicación de medidas preventivas.

Información y comunicación

AWS ha implementado varios métodos de comunicación interna a escala mundial para ayudar a que los empleados conozcan las funciones y las responsabilidades individuales y para comunicar eventos importantes de manera puntual. Estos métodos incluyen programas de orientación y capacitación para empleados recién contratados, reuniones periódicas de gestión con motivo de las actualizaciones en materia de rendimiento empresarial y de otras cuestiones, y recursos electrónicos como las videoconferencias, los mensajes de correo electrónico y la publicación de información a través de la intranet de Amazon.

AWS también ha implementado varios métodos de comunicación externa para prestar asistencia a su cartera de clientes y a la comunidad. El equipo de atención al cliente dispone de mecanismos para recibir notificaciones sobre problemas operativos que afecten a la experiencia de los clientes. El equipo de atención al cliente realiza el mantenimiento del panel en el que se indica el estado del servicio "Service Health Dashboard" para que se encuentre disponible a fin de advertir al cliente de cualquier problema que pueda tener un gran impacto. También se encuentra disponible un "Security and Compliance Center" para ofrecer a los clientes una única ubicación donde puedan obtener

información acerca de las prestaciones de seguridad y conformidad legal propias de AWS.

Los clientes también pueden suscribirse a un nivel de asistencia Premium Support que incluye comunicación directa con el equipo de atención al cliente y la recepción de alertas proactivas relacionadas con todos los problemas que afecten a los clientes.

Permanencia del empleado

AWS ha establecido políticas y procedimientos formales para definir normas mínimas de acceso lógico a los hosts de la plataforma y la infraestructura de AWS. AWS exige que el personal con posibilidad de acceso a los datos de los clientes se someta a una comprobación exhaustiva de sus antecedentes (de conformidad con la legislación vigente) en consonancia con su cargo y nivel de acceso a los datos. Las políticas también identifican responsabilidades funcionales para la administración de la seguridad y del acceso lógico.

Aprovisionamiento de cuentas

El departamento de recursos humanos (RR. HH.), el de operaciones corporativas y los propietarios de servicios comparten la responsabilidad de la concesión de acceso a empleados y contratistas.

Cuando un jefe de recursos humanos da su aprobación, se crea una cuenta estándar de empleado o contratista con los privilegios mínimos, pero esta se ofrece desactivada. La cuenta se activa automáticamente cuando el historial del empleado se activa en el sistema de recursos humanos de Amazon.

El propietario o gestor pertinente debe aprobar de forma explícita el acceso a otros recursos, entre los que destacan los grupos de servicios, de dispositivos de red, de Windows y de UNIX, en el sistema de gestión de permisos de propietarios de Amazon. Todos los cambios realizados en la herramienta de gestión de permisos se identifican en una auditoría. Cuando se produce un cambio en la función de un empleado, ha de aprobarse de forma explícita el

acceso continuado al recurso o, de lo contrario, dicho acceso se revocará automáticamente.

Revisión de cuentas

Todas las concesiones de acceso se revisan cada 90 días; después de la revisión se precisará de una nueva aprobación explícita o, de lo contrario, se revocará el acceso al recurso automáticamente.

Revocación de acceso

El acceso se revoca automáticamente cuando se anula el historial de un empleado en el sistema de recursos humanos de Amazon. Se deshabilitan las cuentas de Windows y UNIX y el sistema de gestión de permisos de Amazon elimina al usuario de todos los sistemas.

Política de contraseñas

El acceso y la administración de seguridad lógica de Amazon se basa en ID de usuarios, contraseñas y Kerberos para autenticar a los usuarios a fin de que puedan acceder a servicios, recursos y dispositivos, así como para autorizar el nivel adecuado de acceso del usuario. AWS Security ha establecido una política de contraseñas con las configuraciones y los intervalos de caducidad necesarios.

Seguridad física

Amazon tiene muchos años de experiencia en el diseño, la construcción y el manejo de centros de datos operativos a gran escala. Esta experiencia se ha aplicado a la infraestructura y plataforma de AWS. Los centros de datos de AWS se alojan en instalaciones sin identificación externa. El acceso físico está estrictamente controlado en el perímetro y en los puntos de acceso del edificio por personal de seguridad profesional mediante video vigilancia, sistema de detección de intrusiones y otros recursos electrónicos. El personal autorizado debe confirmar dos veces como mínimo una autenticación de dos factores para acceder a los pisos del centro de datos. Todos los visitantes y contratistas han de presentar su identificación y deberán firmar e ir acompañados en todo momento de personal autorizado.

AWS solo ofrece acceso al centro de datos y solo facilita información a los empleados y contratistas que tengan necesidad empresarial legítima de tales privilegios. Cuando un empleado deja de tener necesidad empresarial de tales privilegios, su acceso se revoca de inmediato, incluso aunque siga siendo empleado de Amazon o de Amazon Web Services. El acceso físico a los centros de datos de los empleados de AWS está sujeto a registros y auditorías rutinarios.

Medidas para la protección del medio ambiente

Los centros de datos de Amazon son vanguardistas, ya que utilizan enfoques innovadores en materia de arquitectura e ingeniería.

Detección y extinción de incendios

Se ha instalado un equipo automático de detección y extinción de incendios para reducir los riesgos. El sistema de detección de incendios utiliza sensores de detección de humo en todos los entornos del centro de datos, en los espacios mecánicos y eléctricos de la infraestructura, en las salas del refrigerador y en las salas del equipo del generador. Estas zonas están protegidas por sistemas de acción preventiva de tubos húmedos interconectados o por sistemas de rocío de gases.

Energía

Los sistemas de alimentación eléctrica del centro de datos están diseñados para que puedan redundarse y mantenerse por completo sin que ello repercuta en las operaciones, con un ciclo de 24 horas al día durante los 7 días de la semana. Los sistemas de alimentación ininterrumpida (SAI) ofrecen alimentación de seguridad en casos de cortes eléctricos a fin de poder realizar cargas importantes y esenciales en la instalación. Los centros de datos utilizan generadores para ofrecer una alimentación de seguridad para toda la instalación.

Condiciones climáticas y temperatura

Se precisa de control climático para mantener una temperatura de funcionamiento constante en los servidores y en otro hardware, lo que impide el sobrecalentamiento y reduce la posibilidad de que se produzcan interrupciones

del servicio. Los centros de datos se acondicionan para mantener las condiciones atmosféricas en niveles óptimos. El personal y los sistemas supervisan y controlan la temperatura y la humedad a fin de mantenerlas en niveles adecuados.

Gestión

AWS controla los sistemas eléctricos, mecánicos y de asistencia de la vida útil, además del equipo, a fin de poder identificar de inmediato todos los problemas que puedan surgir. Se llevan a cabo tareas de mantenimiento preventivo a fin de que el equipo pueda funcionar sin interrupciones.

Gestión de la configuración

Los cambios de emergencia, no rutinarios y de cualquier otro parámetro de configuración en la infraestructura existente de AWS están sujetos a autorización, registros, pruebas, aprobaciones y documentación de conformidad con las normas del sector establecidas para sistemas similares. Se realizan actualizaciones en la infraestructura de AWS para minimizar cualquier impacto en el cliente y en el uso que este hace de los servicios. AWS se comunicará con los clientes, ya sea por correo electrónico o a través del panel que indica el estado del servicio "AWS Service Health Dashboard" (<http://status.aws.amazon.com/>) cuando quepa la posibilidad de que el servicio pueda verse afectado negativamente.

Software

AWS aplica un enfoque sistemático para gestionar los cambios, a fin de revisar minuciosamente, probar, aprobar y comunicar según proceda los cambios introducidos en los servicios que repercutan en los clientes.

El proceso de gestión de cambios de AWS pretende evitar interrupciones no intencionadas del servicio y ofrecer al cliente la integridad del servicio. Los cambios introducidos en los entornos de producción son:

- Revisado: revisiones de homólogos de los aspectos técnicos de algún cambio
- Probado: al aplicarse se comportará según lo previsto sin repercutir negativamente en el rendimiento
- Aprobado: para ofrecer previsiones e información adecuadas sobre el impacto empresarial

Los cambios suelen introducirse en la fase de producción con una implementación gradual, empezando por áreas de impacto mínimo. Las implementaciones se prueban en un único sistema y se supervisan minuciosamente a fin de poder evaluar el impacto. Los propietarios del servicio cuentan con métricas configurables que permiten medir el estado de las dependencias ascendentes del servicio. Estas métricas se controlan de forma minuciosa con la disponibilidad de umbrales y alarmas. Los procedimientos de reversión se documentan en una etiqueta de gestión de cambios (CM).

Cuando es posible, los cambios se programan durante periodos de tiempo regulares. Los cambios de emergencia en los sistemas de producción que requieren desviaciones de los procedimientos estándar de gestión de cambios se asocian con un incidente y se registran y aprueban según proceda.

De forma periódica, AWS realiza auditorías automáticas de los cambios introducidos en los servicios principales para controlar la calidad, mantener altos estándares y facilitar la mejora constante del proceso de gestión de cambios. Todas las excepciones se analizan para determinar la causa raíz y se aplican las acciones adecuadas para realizar los cambios oportunos en materia de conformidad o para revertir el cambio en caso de que proceda. A continuación, se adoptan las medidas oportunas para solucionar y remediar el proceso o el problema del usuario.

Infraestructura

El equipo de aplicaciones corporativas de Amazon desarrolla y gestiona el software para automatizar los procesos de TI para los hosts de UNIX/Linux en los ámbitos de entrega de software de terceros, de software desarrollado

internamente y de gestión de la configuración. El equipo de infraestructuras mantiene y opera un marco de gestión de configuración de UNIX/Linux para gestionar la escalabilidad, disponibilidad, auditoría y gestión de seguridad en relación con el hardware. Gracias a una gestión centralizada de los hosts mediante la utilización de procesos automatizados que gestionan los cambios, la empresa puede conseguir sus objetivos en términos de alta disponibilidad, repetibilidad, escalabilidad, alta seguridad y recuperación ante desastres. Los ingenieros de sistemas y redes controlan el estado de estas herramientas automatizadas con carácter diario, además de revisar informes para responder a los host que fallan a fin de obtener o actualizar su configuración y el software. Cuando se incorpora nuevo hardware, se instala un software de gestión de configuración cuyo desarrollo se realiza internamente. Estas herramientas se ejecutan en todos los hosts de UNIX para validar si están configurados y que el software está instalado de conformidad con las normas determinadas por la función asignada al host. Este software de gestión de configuración también permite actualizar con regularidad los paquetes que ya están instalados en el host. Solo el personal autorizado a través del servicio de permisos puede acceder a los servidores de gestión de la configuración central.

Gestión de la continuidad del negocio

La infraestructura de Amazon presenta un alto nivel de disponibilidad y ofrece a los clientes las prestaciones necesarias para implementar una arquitectura resistente de TI. AWS ha diseñado sus sistemas para que toleren fallos del sistema o del hardware con un impacto mínimo en los clientes. La gestión de la continuidad del negocio del centro de datos de AWS es competencia de la dirección del grupo de infraestructuras de Amazon.

Disponibilidad

Los centros de datos están compilados en clústeres en varias regiones del mundo. Todos los centros de datos están en línea y a disposición de los clientes, por lo que ninguno está "inactivo". En caso de fallo, los procesos automatizados

desvían el tráfico de datos del cliente de la zona afectada. Las aplicaciones principales se implementan en una configuración N+1, de forma que en el caso de que se produzca un fallo en el centro de datos, haya capacidad suficiente para permitir equilibrar la carga del tráfico entre los demás sitios.

AWS ofrece a los clientes la flexibilidad necesaria para colocar las instancias y almacenar datos en varias regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. Cada zona de disponibilidad está diseñada como una zona de fallo independiente. Esto significa que las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana habitual y se encuentran en llanuras poco propensas a inundaciones (las categorías específicas de zonas propensas a inundaciones varían según la región). Además de las instalaciones de sistemas de alimentación ininterrumpida (SAI) discretos y de generación de copias de seguridad in situ, se alimentan a través de diferentes redes a partir de utilidades independientes para reducir aún más cada uno de los puntos de fallos. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1.

Los clientes han de planificar el uso que realizan de AWS para poder utilizar varias regiones y zonas de disponibilidad. La distribución de aplicaciones por varias zonas de disponibilidad ofrece la posibilidad de mantener la resistencia ante la mayoría de los modos de fallo, incluidos los desastres naturales o los fallos del sistema.

Respuesta ante incidentes

El equipo de gestión de incidentes de Amazon utiliza procedimientos de diagnóstico propios del sector para gestionar las soluciones durante los eventos que repercuten en el negocio. El personal ofrece un servicio de 24 horas al día durante los 365 días de año para poder detectar incidentes y gestionar el impacto y su resolución.

Revisión ejecutiva de toda la empresa

El grupo de auditoría interno de Amazon ha revisado recientemente los planes de resistencia de los servicios de AWS, que también revisan periódicamente los miembros del equipo senior de gestión ejecutiva y del Comité de auditoría de la Junta directiva.

Cabe considerar que el 21 de abril de 2011, EC2 sufrió una interrupción del servicio que afectó a los clientes en la región Este de los Estados Unidos. Puede encontrar los detalles de la interrupción del servicio en la página “Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region” (Amazon Web Services, s.f.)

Copias de seguridad

Los datos almacenados en Amazon S3, Amazon SimpleDB o Amazon Elastic Block Store (EBS) se almacenan de forma redundante en varias ubicaciones físicas como parte del funcionamiento normal de dichos servicios y sin ningún cargo adicional. Amazon S3 y Amazon SimpleDB ofrecen durabilidad de objetos mediante el almacenamiento de los objetos varias veces en varias zonas de disponibilidad la primera vez que se graban y, posteriormente, realizan replicaciones adicionales de forma activa en el caso de que el dispositivo no esté disponible o si se detecta una degradación de los datos. La replicación de Amazon EBS se almacena en la misma zona de disponibilidad, no en varias zonas y, por tanto, es muy recomendable que los clientes realicen instantáneas periódicas de Amazon S3 a fin de ofrecer una durabilidad de los datos a largo plazo. En caso de que se trate de clientes que han creado bases de datos transaccionales complejas con EBS, se recomienda que las copias de seguridad de Amazon S3 se realicen a través de un sistema de gestión de bases de datos, a fin de que puedan determinarse las transacciones distribuidas y los registros. AWS no realiza copias de seguridad de los datos que se almacenan en discos virtuales conectados a instancias en ejecución en Amazon EC2.

Retirada de dispositivos de almacenamiento

Cuando un dispositivo de almacenamiento alcanza el final de su vida útil, los procedimientos de AWS incluyen un proceso de retirada diseñado para prevenir

que los datos de los clientes queden expuestos al acceso de personas no autorizadas. AWS utiliza técnicas detalladas en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para la desinfección de soportes") para destruir datos como parte del proceso de retirada. En caso de que no se pueda retirar un dispositivo de hardware con estos procedimientos, el dispositivo se desmagnetizará o destruirá físicamente de conformidad con las prácticas estándar del sector.

Aislamiento de errores

AWS ofrece a los clientes la flexibilidad necesaria para colocar instancias y almacenar datos en varias regiones geográficas. Cada región es un conjunto independiente de recursos de AWS en una geografía determinada. AWS admite actualmente cinco regiones: EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Norte de California), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio). La región estándar de los Estados Unidos de Amazon S3 incluye las instalaciones del Este de los Estados Unidos del Norte de Virginia y las instalaciones del Estado occidental de Washington.

La selección de una región dentro de una jurisdicción geográfica aceptable para el cliente ofrece un fundamento sólido para cumplir los requisitos de conformidad y privacidad en función de la ubicación, como la Directiva europea relativa a la privacidad de los datos. Los datos no se replican entre las regiones a menos que el cliente así lo haga de forma proactiva, de forma que se permite a los clientes con estos tipos de ubicación de datos y de requisitos de privacidad tener la opción de definir entornos de conformidad. Cabe destacar que todas las comunicaciones entre las regiones se realizan a través de la infraestructura pública de Internet. Han de utilizarse métodos de cifrado apropiados para proteger los datos sensibles.

Dentro de una región determinada, Amazon EC2, Amazon EBS y Amazon Relational Database Service (RDS) permiten a los clientes colocar instancias y almacenar datos en varias zonas de disponibilidad. Consulte la sección "Gestión

de la continuidad del negocio" para obtener información adicional acerca de la disponibilidad.

Amazon S3, Amazon SimpleDB, Amazon Simple Notification Service (SNS) y Amazon Simple Queue Service (SQS) no exponen a los clientes el concepto de las zonas de disponibilidad. Con estos servicios, los datos se almacenan automáticamente en varios dispositivos distribuidos entre varias instalaciones dentro de una misma región.

En el diagrama siguiente se indican las regiones y las zonas de disponibilidad dentro de cada región para Amazon EC2, Amazon EBS y Amazon RDS.

Características de seguridad de la cuenta de Amazon

AWS ofrece a los clientes distintas formas de identificación personal y para acceder de forma segura a la cuenta de AWS. Puede obtener una lista completa de las credenciales admitidas por AWS en la página Credenciales de seguridad a la que puede acceder tras registrarse en su cuenta. AWS también ofrece opciones de seguridad adicionales que permiten a los clientes proteger más su cuenta de AWS y controlar el acceso: AWS Identity and Access Management (AWS IAM), Multi-Factor Authentication (MFA) y Key Rotation.

AWS Identity and Access Management (AWS IAM)

AWS Identity and Access Management (IAM) permite que un cliente cree múltiples usuarios y gestione los permisos para cada uno de estos usuarios dentro de su cuenta de AWS. Un usuario es una identidad (dentro de su cuenta de AWS) con credenciales de seguridad únicas que pueden usarse para acceder a los servicios de AWS. Con IAM no tiene que compartir contraseñas o claves de acceso y hace que resulte verdaderamente sencillo habilitar o deshabilitar el acceso de un usuario, según proceda.

AWS IAM permite a los clientes implementar las mejores prácticas de seguridad, como los privilegios mínimos, mediante la concesión de credenciales exclusivas a cada usuario dentro de su cuenta de AWS y concediendo permisos exclusivos

para acceder a los servicios y recursos de AWS necesarios para que los usuarios puedan desarrollar su trabajo. AWS IAM es un servicio seguro de forma predeterminada; los usuarios nuevos no tendrán acceso a AWS hasta que se concedan de forma explícita los permisos.

Región UE (IRE)

Zona de disponibilidad A

Zona de disponibilidad B

Región Este de EE. UU. (Norte de Virginia)

Zona de disponibilidad A

Zona de disponibilidad C

Zona de disponibilidad B

Región APAC

(Tokio)

Zona de disponibilidad A

Zona de disponibilidad B

Región Oeste de EE. UU.

(Norte de California)

Zona de disponibilidad A

Zona de disponibilidad B

Región APAC

(Singapur)

Zona de disponibilidad B

Zona de disponibilidad A

AWS IAM permite a los clientes minimizar el uso de sus credenciales de la cuenta de AWS. En su lugar, todas las interacciones con los servicios y los recursos de AWS deben realizarse con las credenciales de seguridad de usuario de AWS IAM. Puede encontrar información adicional acerca de AWS Identity and Access Management (AWS IAM) en el sitio web de AWS: (Amazon Web Services, s.f.)

AWS Multi-Factor Authentication (AWS MFA)

AWS Multi-Factor Authentication (AWS MFA) es una capa de seguridad adicional que ofrece un mayor control de los ajustes de la cuenta de AWS y de la gestión de los recursos y servicios de AWS a los que está suscrita su cuenta. Cuando los usuarios activan esta función opcional, tendrán que facilitar un código de uso exclusivo compuesto de 6 dígitos, además de sus credenciales estándar correspondientes con el nombre de usuario y la contraseña, antes de que se les conceda acceso a la configuración de su cuenta de AWS o a los servicios y recursos de AWS. Los clientes obtienen este código de uso exclusivo de un dispositivo de autenticación que es propiedad física del usuario. Esto recibe el nombre de autenticación multifactor porque se comprueban dos factores antes de conceder acceso: el cliente ha de facilitar el nombre de usuario (el correo electrónico de Amazon para la cuenta de AWS) y la contraseña (el primer "factor": algo que conoce) y el código preciso del dispositivo de autenticación (el segundo "factor": algo que posee). Los clientes pueden habilitar dispositivos MFA para su cuenta de AWS, así como para los usuarios que hayan creado con AWS IAM para dicha cuenta de AWS.

Resulta sencillo obtener un dispositivo de autenticación de un proveedor externo participante y configurarlo para utilizarlo a través del sitio web de AWS. Puede encontrar información adicional acerca de la autenticación multifactor en el sitio web de AWS: (Amazon Web Services, s.f.)

Key Rotation

Por los mismos motivos que es importante cambiar la contraseña con frecuencia, AWS recomienda que los clientes roten las claves de acceso y los certificados de manera regular. Para que los clientes puedan hacerlo sin que se vea afectada la disponibilidad de la aplicación, AWS admite varias claves de acceso y certificados simultáneos. Con esta característica, los clientes pueden rotar el funcionamiento de las claves y los certificados de forma regular, sin que la aplicación sufra períodos de inactividad. Esto ayuda a mitigar los riesgos de pérdida o de que peligren los certificados o las claves de acceso. Las API de AWS IAM permiten que un cliente rote las claves de acceso de su cuenta de

AWS, así como las de los usuarios que haya creado en su cuenta de AWS mediante la utilización de AWS IAM.

Seguridad de la red

La red de AWS ofrece protección de alto nivel frente a los problemas tradicionales de seguridad de la red y el cliente puede implementar medidas adicionales de protección. A continuación, exponemos algunos ejemplos:

Ataques de denegación de servicio distribuido (DDoS)

Los puntos finales de la interfaz de programación de aplicaciones (API) de AWS están alojados en una infraestructura grande de primera clase y a escala de Internet que se beneficia de la misma experiencia de ingeniería que ha posicionado a Amazon como el proveedor en línea más importante del mundo. Se utilizan técnicas patentadas de mitigación de DDoS. Además, las redes de AWS tienen hosts múltiples entre una serie de proveedores a fin de conseguir diversidad de acceso a Internet.

Ataques tipo "Man In the Middle" (MITM)

Todas las API de AWS se encuentran disponibles a través de puntos finales protegidos por SSL que ofrecen autenticación del servidor. Las AMI de Amazon EC2 generan nuevos certificados host SSH automáticamente la primera vez que se inician y se registran en la consola de la instancia. Posteriormente, los clientes pueden utilizar las API seguras para llamar a la consola y acceder a los certificados host antes de acceder a la instancia por primera vez. Se insta a los clientes a utilizar el protocolo SSL para todas las interacciones con AWS.

Suplantación de IP

Las instancias de Amazon EC2 no pueden enviar tráfico de red suplantado. La infraestructura del firewall basada en host y controlada por AWS no permitirá que una instancia envíe tráfico con una dirección IP o MAC de origen distinto de las que posee.

Escaneo de puertos

Los escaneos no autorizados de puertos realizados por los clientes de Amazon EC2 suponen una vulneración de la política de uso aceptable de AWS. Las infracciones de la política de uso aceptable de AWS se consideran graves y, por tanto, se investigará cualquier vulneración detectada. Los clientes pueden notificar un supuesto abuso a través de los contactos disponibles en nuestro sitio web en: <http://aws.amazon.com/contact-us/report-abuse/> Cuando se detecta un escaneo no autorizado de puerto, este se detiene y se bloquea. Los escaneos de puertos de las instancias de Amazon EC2, por lo general, resultan ineficaces porque, de forma predeterminada, todos los puertos de entrada de las instancias de Amazon EC2 se cierran y, en consecuencia, solo pueden abrirlas los clientes. Además, los clientes pueden realizar una gestión estricta de los grupos de seguridad para poder mitigar la amenaza de los escaneos de puertos con mayor eficacia. Si el cliente configura el grupo de seguridad para que permita el tráfico procedente de un origen a un puerto específico, entonces dicho puerto específico será vulnerable a los escaneos de puertos. En estos casos, el cliente ha de aplicar las medidas adecuadas de seguridad para proteger los servicios de escucha que puedan resultar esenciales para su aplicación a fin de que no pueda detectarlos un escaneo no autorizado de puerto. Por ejemplo, un servidor web debe tener el puerto 80 (HTTP) claramente abierto para todo el mundo y el administrador de este servidor es responsable de la seguridad del software del servidor HTTP, como Apache. Los clientes pueden solicitar permisos para realizar escaneos de vulnerabilidades según sea necesario para satisfacer los requisitos específicos de cumplimiento. Estos escaneos pueden limitarse a las instancias del cliente y no deben infringir la política de uso aceptable de AWS. La aprobación avanzada para estos tipos de escaneos se puede iniciar presentando una solicitud a través del sitio web, en: (Amazon Web Services, s.f.)

Análisis de paquetes por parte de otros arrendatarios

No es posible que una instancia virtual que se ejecute en modo promiscuo reciba o "examine" tráfico previsto para una instancia virtual diferente. Aunque los clientes pueden activar el modo promiscuo para sus interfaces, el hipervisor no

les entregará tráfico que no vaya dirigido a ellos. Dos instancias que pertenezcan al mismo cliente y que estén ubicadas en el mismo host físico tampoco pueden escuchar su tráfico entre sí. Los ataques del tipo "poisoning" de la memoria caché ARP no repercuten en Amazon EC2 y Amazon VPC. Aunque Amazon EC2 ofrece una protección alta frente a los intentos inadvertidos o malintencionados de los clientes de visualizar datos de otros, como práctica general, los clientes deben encriptar el tráfico sensible.

Seguridad de Amazon Elastic Compute Cloud (Amazon EC2)

La seguridad dentro de Amazon EC2 se ofrece en diferentes niveles: el sistema operativo (SO) del sistema host, el sistema operativo de la instancia virtual o el SO invitado, un firewall y las llamadas firmadas de las API. Cada uno de estos elementos se basa en las capacidades de los otros. El objetivo consiste en ofrecer protección frente al acceso de sistemas o usuarios no autorizados a los datos almacenados en Amazon EC2, así como ofrecer a las instancias de Amazon EC2 la máxima protección posible sin que ello repercuta en la flexibilidad de la configuración que los clientes demandan.

Varios niveles de seguridad

Sistema operativo host: los administradores que tengan necesidades empresariales de acceder a los planes de gestión han de utilizar la autenticación multifactor para poder acceder a hosts de administración en función del propósito. Estos hosts de administración son sistemas específicamente diseñados, compilados, configurados y con seguridad extra para proteger el plano de gestión de la nube. Todo este acceso está sujeto a registros y auditorías. Cuando algún empleado deja de tener la necesidad empresarial de acceder al plano de gestión, se revocan los privilegios y el acceso en relación con estos hosts y con los sistemas pertinentes.

Sistema operativo invitado: las instancias virtuales están totalmente controladas por el cliente. Los clientes tienen acceso total a la raíz o control administrativo sobre las cuentas, los servicios y las aplicaciones. AWS no tiene ningún derecho de acceso sobre las instancias de los clientes y no pueden acceder al SO

invitado. AWS recomienda un conjunto base de mejores prácticas de seguridad para incluir la desactivación del acceso de solo contraseña a sus hosts y a través de la utilización de la autenticación multifactor para obtener acceso a sus instancias (o un acceso mínimo a la versión 2 de SSH basado en certificación). Además, los clientes deben utilizar un mecanismo de escalado mediante privilegios basado en un registro por cada usuario. Por ejemplo, si el sistema operativo invitado es Linux, después de proteger su instancia, deben utilizar la versión 2 de SSH basada en certificados para acceder a la instancia virtual, desactivar el acceso remoto a la raíz, utilizar el registro de línea de comandos y utilizar "sudo" para el escalado de privilegios. Los clientes deben generar sus propios pares de claves a fin de garantizar que sean exclusivas y que no coincidan con las de otros clientes ni con las de AWS.

Firewall: Amazon EC2 ofrece una solución completa de firewall; este firewall de entrada obligatorio está configurado con un modo de denegación total predeterminado y los clientes de Amazon EC2 deben abrir de forma explícita todos los puertos necesarios para admitir el tráfico entrante. El tráfico ha de restringirse por protocolo, por puerto de servicio, así como por dirección IP de origen (IP individual o por bloque de enrutamiento entre dominios sin clases (CIDR)).

El firewall puede configurarse por grupos que permitan que las diferentes clases de instancias tengan diferentes normas. Pensemos, por ejemplo, en el caso de una aplicación web tradicional de tres niveles. El grupo de servidores web tendría el puerto 80 (HTTP) o el puerto 443 (HTTPS) abierto para Internet. El grupo de servidores de aplicaciones tendría el puerto 8000 (específico de la aplicación) abierto solo para el grupo de servidores web. El grupo de servidores de bases de datos tendría el puerto 3306 (MySQL) abierto solo para el grupo de servidores de aplicaciones. Los tres grupos permitirían el acceso administrativo a través del puerto 22 (SSH), pero solo desde la red corporativa del cliente. Las aplicaciones con un alto nivel de seguridad pueden implementarse utilizando este mecanismo expresivo. Consulte el diagrama siguiente:

El firewall no se controla a través del SO invitado; en su lugar, precisa del certificado y la clave X.509 del cliente para autorizar cambios, además de tener que añadir una capa adicional de seguridad. AWS admite la posibilidad de conceder acceso pormenorizado a las diferentes funciones administrativas sobre las instancias y el firewall, permitiendo así al cliente implementar la seguridad adicional mediante la separación de obligaciones. El nivel de seguridad que ofrece el firewall constituye una función por la que los clientes son los que han de abrir los puertos, en función de una duración y un propósito determinados. El estado predeterminado consiste en denegar todo el tráfico entrante, y los clientes deben planificar detenidamente qué abrirán a la hora de compilar y proteger sus aplicaciones. Aún se precisa de un diseño de seguridad y una gestión del tráfico bien informada por cada instancia. AWS insta además a los clientes a que apliquen filtros adicionales por cada instancia con firewalls basados en host como IPtables o el firewall de Windows y las VPN. Esto puede restringir el tráfico entrante y saliente en cada instancia. La API llama para iniciar y terminar instancias, cambiar los parámetros del firewall y realizar otras funciones firmadas por la clave de acceso secreta de Amazon del cliente, que puede ser la clave de acceso secreto de las cuentas de Amazon o la clave de acceso secreta de un usuario creado con AWS IAM. Sin el acceso a la clave de acceso secreta del cliente, no se pueden realizar llamadas de la API de Amazon EC2 en su nombre. Además, las llamadas de la API pueden cifrarse con SSL para mantener la confidencialidad. Amazon recomienda utilizar siempre puntos finales de las API protegidos con el protocolo SSL. AWS IAM también permite que un cliente pueda controlar aún más qué API creadas por un usuario con AWS IAM tiene permisos para llamar.

El hipervisor

Amazon EC2 utiliza actualmente una versión muy personalizada del hipervisor Xen, beneficiándose de la para virtualización (en el caso de los invitados de Linux). Habida cuenta de que los invitados paravirtualizados dependen del hipervisor para ofrecer soporte para las operaciones que normalmente requieren acceso privilegiado, el SO invitado no tiene acceso elevado a la CPU. La CPU ofrece cuatro modos de privilegios independientes: 0-3, denominados anillos. El

anillo 0 se corresponde con el nivel de máximos privilegios y el 3 con el de menos. El SO host se ejecuta en el anillo 0. Sin embargo, en lugar de ejecutarse en el anillo 0, como lo hacen la mayoría de los sistemas operativos, el SO invitado se ejecuta en el anillo 1, que tiene menos privilegios, y las aplicaciones en el anillo 3, es decir, en el que menos privilegios ofrece. Esta virtualización explícita de los recursos físicos se traduce en una separación clara entre el invitado y el hipervisor, que resulta en una separación de seguridad adicional entre ambos.

Aislamiento de instancias

Las diferentes instancias ejecutadas en el mismo equipo físico se separan entre sí a través del hipervisor Xen. Amazon está activo en la comunidad Xen, que ofrece sensibilización acerca de los últimos desarrollos. Además, el firewall de AWS se aloja en la capa del hipervisor, entre la interfaz de la red física y la interfaz virtual de la instancia. Todos los paquetes deben pasar por esta capa, por lo que los vecinos de una instancia dejan de tener acceso a dicha instancia en relación que cualquier otro host de Internet y se pueden tratar como si estuvieran en host físicos independientes. La RAM física se separa usando mecanismos similares.

Las instancias de los clientes no tienen acceso a los dispositivos del disco sin procesar, sino que, en su lugar, se presentan con discos virtualizados. La capa de virtualización del disco propietario de AWS restablece automáticamente cualquier bloque de almacenamiento utilizado por el cliente, de forma que los datos de un cliente no se vean expuestos de forma no intencionada a otros usuarios. AWS recomienda que los clientes adopten medidas adicionales para proteger sus datos mediante los recursos apropiados. Una solución común consiste en ejecutar un sistema de archivos cifrados sobre el dispositivo del disco virtualizado.

Seguridad de Elastic Block Storage (Amazon EBS)

El acceso al volumen de Amazon EBS está restringido a la cuenta de AWS que ha creado el volumen, así como a los usuarios creados para la cuenta de AWS con AWS IAM en caso de que al usuario se le haya concedido el acceso a las

operaciones de EBS, de forma que se deniega el permiso a todas las cuentas y a todos los usuarios de AWS para que puedan visualizar el volumen o acceder a él. No obstante, un cliente puede crear instantáneas de Amazon A3 para su volumen de Amazon EBS y dar a otras cuentas de AWS la capacidad de utilizar la instantánea compartida como la base para crear sus propios volúmenes. Los clientes también tienen la posibilidad de crear instantáneas del volumen de Amazon EBS de forma que estas estén públicamente disponibles para todas las cuentas de AWS. El hecho de compartir las instantáneas del volumen de Amazon EBS no concede el permiso a las demás cuentas de AWS para que puedan alterar o eliminar la instantánea original, ya que dicho privilegio está reservado de forma explícita para la cuenta de AWS que creó el volumen. Una instantánea de EBS se corresponde con una vista de nivel de bloque de un volumen completo de EBS. Los datos que no puedan visualizarse a través del sistema de archivos del volumen, como los archivos que se han suprimido, pueden encontrarse en la instantánea de EBS. Los clientes que deseen crear instantáneas compartidas han de hacerlo cuidadosamente. Se puede crear un nuevo volumen de EBS en caso de que un volumen haya contenido datos sensibles o si se han eliminado archivos del mismo. Los datos que vaya a contener la instantánea compartida deben copiarse en un nuevo volumen, y la instantánea ha de crearse a partir del nuevo volumen.

Los volúmenes de Amazon EBS se presentan al cliente como dispositivos de bloques sin formato y sin procesar, que se borran antes de habilitarse para su uso. Los clientes que tengan procedimientos que requieran que todos los datos se borren con un método específico, como los que se detallan en DoD 5220.22-M ("Manual de operaciones del programa de seguridad industrial nacional") o NIST 800-88 ("Directrices para la desinfección de soportes"), pueden aplicarlos en Amazon EBS. Los clientes han de realizar un procedimiento de borrado especializado antes de eliminar el volumen a fin de cumplir con los requisitos establecidos. El cifrado de datos sensibles normalmente es una buena práctica de seguridad, y AWS insta a los usuarios a que cifren sus datos sensibles a través de un algoritmo coherente con la política de seguridad establecida.

Seguridad de Amazon Virtual Private Cloud (Amazon VPC)

La seguridad en Amazon Virtual Private Cloud parte del concepto de una VPC y se amplía para incluir los grupos de seguridad, las listas de control de acceso a la red (ACL), el enrutamiento y las puertas de enlace externas. Cada uno de estos elementos es complementario para ofrecer una red aislada y segura que pueda ampliarse a través de una habilitación selectiva de acceso directo a Internet o de la conexión privada a otra red. A continuación, describimos los distintos niveles de seguridad en Amazon VPC. A esto le sigue un diagrama en el que se representa la forma en que se relacionan los componentes de Amazon VPC.

Varios niveles de seguridad

Virtual Private Cloud: cada VPC constituye una red distinta e independiente dentro de la nube. En el momento de la creación, el cliente selecciona un rango de dirección IP para cada VPC. El tráfico de red dentro de cada VPC es independiente de todas las demás VPC; por tanto, varias VPC pueden utilizar rangos de direcciones IP que se solapan (incluso idénticos) sin necesidad de que se pierda este aislamiento. De forma predeterminada, las VPC no disponen de conexión externa. Los clientes pueden crear y conectar una puerta de enlace de Internet, una puerta de enlace de VPN o ambas para establecer la conexión externa, de conformidad con los siguientes controles.

API: llama para crear y eliminar VPC, cambiar el enrutamiento, el grupo de seguridad y los parámetros de ACL de la red y para realizar otras funciones firmadas por la clave de acceso secreta de Amazon del cliente, que puede ser la clave de acceso secreto de las cuentas de Amazon o la clave de acceso secreta de un usuario creado con AWS IAM. Sin el acceso a la clave de acceso secreta del cliente, no se pueden realizar llamadas de la API de Amazon VPC en nombre del cliente. Además, las llamadas de la API pueden cifrarse con SSL para mantener la confidencialidad. Amazon recomienda utilizar siempre puntos finales de las API protegidos con el protocolo SSL. AWS IAM también permite que un

cliente pueda controlar aún más para qué API tiene permiso de llamada un usuario recién creado.

Subredes: los clientes crean una o varias subredes dentro de cada VPC; cada instancia iniciada en la VPC está conectada a una subred. Se bloquean los ataques de seguridad de la capa 2 tradicionales, incluida la suplantación de MAC y ARP.

Tablas de enrutamiento y enrutamientos: cada subred de una VPC está asociada con una tabla de enrutamiento, y todo el tráfico de red que parte de una subred se procesa mediante la tabla de enrutamiento para determinar el destino.

Puerta de enlace de VPN: una puerta de enlace de VPN permite la conectividad privada entre la VPC y otra red. El tráfico de red dentro de cada puerta de enlace de VPN está aislado del tráfico de red de otras puertas de enlace de VPN. Los clientes deben establecer conexiones VPN con la puerta de enlace de VPN a partir de los dispositivos de puerta de enlace que se encuentran en las instalaciones del cliente. Cada conexión se protege mediante una clave compartida previamente y con una dirección IP del dispositivo de la puerta de enlace del cliente.

Puerta de enlace a Internet: una puerta de enlace a Internet puede enlazarse a una VPC para permitir la conectividad directa a Amazon S3, a otros servicios de AWS y a Internet. Cada instancia que precise de este acceso debe tener una IP elástica asignada o dirigir el tráfico a través de una instancia de NAT. Además, los enrutamientos de red se configuran (véase la información anterior) para dirigir el tráfico hacia la puerta de enlace a Internet. AWS ofrece AMI de NAT de referencia que los clientes pueden ampliar para realizar registros de red, inspecciones exhaustivas de paquetes, filtros de capas de aplicaciones u otros controles de seguridad.

Este acceso solo puede modificarse a través de la invocación de las API de Amazon VPC. AWS admite la posibilidad de conceder acceso pormenorizado a

las diferentes funciones administrativas sobre las instancias y la puerta de enlace a Internet, permitiendo así al cliente implementar la seguridad adicional mediante la separación de obligaciones.

Instancias de Amazon EC2: las instancias de Amazon EC2 que se ejecutan con una VPC de Amazon contienen todas las ventajas descritas anteriormente que están relacionadas con el sistema operativo host, el sistema operativo invitado, el hipervisor, el aislamiento de instancias y la protección frente al análisis de paquetes.

Propiedad: VPC permite a los clientes lanzar instancias de Amazon EC2 que estén físicamente aisladas a nivel del hardware host; se ejecutarán en un único hardware propietario. Una VPC se puede crear con una propiedad "dedicada", en cuyo caso todas las instancias lanzadas en la VPC utilizarán esta función. De forma alternativa, una VPC puede crearse con una propiedad "predeterminada", pero los clientes pueden especificar la propiedad "dedicada" para instancias particulares lanzadas dentro de la VPC.

Firewall (grupos de seguridad): al igual que Amazon EC2, Amazon VPC admite una solución completa de firewall que permite filtrar la entrada y salida del tráfico de una instancia. El grupo predeterminado permite la comunicación de entrada de otros miembros del mismo grupo y la comunicación de salida a otro destino. El tráfico ha de restringirse por cualquier protocolo IP, por puerto de servicio, así como por dirección IP de origen/destino (IP individual o por bloque de enrutamiento entre dominios sin clases (CIDR)).

El firewall no se controla a través del sistema operativo invitado; en su lugar, puede modificarse solo a través de la invocación de las API de Amazon VPC. AWS admite la posibilidad de conceder acceso pormenorizado a las diferentes funciones administrativas sobre las instancias y el firewall, permitiendo así al cliente implementar la seguridad adicional mediante la separación de obligaciones. El nivel de seguridad que ofrece el firewall constituye una función por la que los clientes son los que han de abrir los puertos, en función de una duración y un propósito determinados. Aún se precisa de un diseño de seguridad

y una gestión del tráfico bien informada por cada instancia. AWS insta además a los clientes a que apliquen filtros adicionales por cada instancia con firewalls basados en host como IPtables o el firewall de Windows.

Listas de control de acceso a la red: para añadir una capa adicional de seguridad en Amazon VPC, los clientes pueden configurar las listas de control de acceso a la red (ACL). Son filtros de tráfico sin estado que se aplican a todo el tráfico entrante y saliente procedente de una subred dentro de la VPC. Estas ACL pueden contener normas solicitadas para permitir o denegar el tráfico basado en el protocolo IP, por el puerto de servicio, así como basado en la dirección IP de origen/destino.

Como en el caso de los grupos de seguridad, las ACL de red se gestionan a través de las API de Amazon VPC, añadiendo una capa adicional de protección y activando un nivel adicional de seguridad a través de la separación de obligaciones.

Resumen sobre la seguridad de red

En el diagrama siguiente se muestra cómo se interrelacionan los controles de seguridad para habilitar las topologías de redes flexibles al mismo tiempo que se ofrece un control total de los flujos del tráfico de red.

Seguridad de Amazon Simple Storage Service (Amazon S3)

Con todos los sistemas de almacenamiento compartido, la cuestión de seguridad más común es si los usuarios no autorizados pueden acceder a la información de forma intencionada o por error. De esta forma, los clientes tienen la flexibilidad de determinar cómo, cuándo y a quién desean exponer la información que almacenan en AWS, las API de Amazon S3 ofrecen controles de acceso de nivel de depósito y de nivel de objeto, con valores predeterminados que solo permiten el acceso autenticado del creador del depósito o del objeto. Salvo que un cliente conceda acceso anónimo a sus datos, el primer paso antes de que un usuario de la cuenta de AWS o creado con AWS IAM pueda acceder a los datos consiste en autenticarlo con una firma HMAC-SHA1 de la solicitud usando la clave privada

del usuario. Un usuario autenticado puede leer un objeto solo si al usuario se le han concedido permisos de lectura en una lista de control de acceso (ACL) a nivel de objeto. Un usuario autenticado puede enumerar las claves o sobrescribir objetos en un depósito solo si al usuario se le han concedido permisos de lectura y escritura en una ACL a nivel de depósito o a través de los permisos que se le hayan concedido con AWS IAM. Las ACL de nivel de depósito y de nivel de objeto son independientes; un objeto no hereda las ACL de su depósito. Los permisos para leer o modificar las ACL del depósito o del objeto se controlan mediante las ACL que de forma predeterminada solo conceden acceso al creador. Por tanto, el cliente sigue teniendo el control total sobre los usuarios que tienen acceso a sus datos. Los clientes pueden conceder acceso a los datos de Amazon S3 de las cuentas de AWS mediante el ID o el correo electrónico de la cuenta de AWS o con el ID del producto DevPAy. Los clientes también pueden conceder acceso a los datos de Amazon S3 de todas las cuentas de AWS o a todos en general (mediante la activación del acceso anónimo).

Gestión de datos

A fin de obtener el máximo nivel de seguridad, se puede acceder a Amazon S3 a través de los puntos finales de SSL. Es posible acceder a los puntos finales cifrados desde Internet o desde Amazon EC2, de forma que los datos se transfieran de manera segura dentro de AWS, así como desde y hacia todos los orígenes que no fuera de AWS.

La protección de datos en reposo implica seguridad física y cifrado de datos. Tal como se ha descrito de forma detallada en "Seguridad física", Amazon utiliza varias capas de medidas de seguridad física para proteger los datos de los clientes en reposo. Por ejemplo, el acceso físico a los centros de datos de Amazon está limitado a una lista auditada del personal de Amazon. El cifrado de datos sensibles, por lo general, es una buena práctica de seguridad, y AWS insta a los usuarios a que cifren sus datos sensibles antes de cargarlos en Amazon S3.

Cuando se suprime un objeto de Amazon S3, se inicia inmediatamente la eliminación de la asignación del nombre público al objeto, y normalmente se procesa a través del sistema distribuido en cuestión de segundos. Después de que se elimina la asignación, no hay acceso remoto al objeto eliminado. Posteriormente, el sistema reclama el área de almacenamiento subyacente para su uso.

Amazon S3 está diseñado para ofrecer una durabilidad del 99,999999999% y una disponibilidad de los objetos del 99,99% durante un año concreto. Los objetos se almacenan de forma redundante en varios dispositivos de diversas instalaciones dentro de una Región de Amazon S3. Para ayudarle a ofrecer durabilidad, las operaciones PUT y COPY de Amazon S3 almacenan de forma sincrónica sus datos en varias instalaciones antes de devolver SUCCESS. Una vez almacenados, Amazon S3 ayuda a mantener la durabilidad de sus objetos detectando y reparando rápidamente cualquier pérdida de redundancia. Del mismo modo, Amazon S3 comprueba de forma regular la integridad de los datos almacenados mediante sumas de comprobación. Si se detecta algún tipo de daño en los objetos, se reparan utilizando los datos redundantes. Además, Amazon S3 calcula las sumas de comprobación de todo el tráfico de la red para detectar paquetes de datos con daños durante el almacenamiento o la recuperación de los datos.

Amazon S3 ofrece una protección aún mayor mediante el control de versiones. Podrá utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de todos los objetos almacenados en su depósito de Amazon S3. Gracias al control de versiones, puede recuperarse fácilmente de acciones no deseadas del usuario y de fallos de la aplicación. De forma predeterminada, las solicitudes recuperarán la versión escrita más recientemente. Las versiones más antiguas de un objeto podrán recuperarse especificando una versión en la solicitud. Puede ofrecer más protección a sus versiones si utiliza la función de eliminación de MFA del control de versiones de Amazon S3; después de activarla para un depósito de S3, cada solicitud de eliminación de versiones debe incluir

un código de 6 dígitos y un número de serie del dispositivo de autenticación multifactor.

Registro de acceso

Se puede configurar un depósito de Amazon S3 para registrar el acceso al depósito y a los objetos incluidos en él. El registro de acceso contiene los detalles acerca de cada solicitud de acceso, entre otros, el tipo de solicitud, el recurso solicitado, la IP del solicitante y la hora y la fecha de la solicitud. Cuando el registro está activado para un depósito, los registros se añaden de forma periódica a los archivos de registro y se entregan al depósito específico de Amazon S3.

Seguridad de Amazon Simple Data Base (SimpleDB)

Las API de Amazon SimpleDB ofrecen controles de nivel de dominio que solo permiten el acceso autenticado del creador del dominio; por tanto, el cliente mantiene el pleno control de los usuarios que tienen acceso a sus datos.

El acceso de Amazon SimpleDB se puede conceder mediante una ID de la cuenta de AWS. Tras la autenticación, una cuenta de AWS tiene acceso total a todas las operaciones. El acceso a cada uno de los dominios lo controla una lista de control de acceso independiente que asigna usuarios autenticados a los dominios que poseen. Un usuario creado con AWS IAM solo tiene acceso a las operaciones y los dominios para los que se le haya concedido permiso en virtud de alguna política.

Se puede acceder a Amazon SimpleDB a través de los puntos finales cifrados por SSL. A los puntos finales cifrados se puede acceder desde Internet y desde Amazon EC2. AWS cifra los datos almacenados en Amazon SimpleDB; no obstante, el cliente puede cifrar los datos antes de cargarlos en Amazon SimpleDB. Estos atributos cifrados podrían recuperarse como parte del parámetro Get operation only. No se podrían utilizar como parte de una condición de filtrado de consultas. El cifrado de los datos antes de enviarlos a Amazon

SimpleDB ayuda a ofrecer protección frente al acceso no autorizado a datos sensibles del cliente, incluso por parte de AWS.

Gestión de datos de Amazon SimpleDB

Cuando se elimina un dominio de Amazon SimpleDB, se inicia de inmediato la eliminación de la asignación de dicho dominio, y suele procesarse a través del sistema distribuido en cuestión de segundos. Después de que se elimina la asignación, no hay acceso remoto al dominio eliminado.

Cuando se elimina un elemento y los datos de atributo de un dominio, se inicia de inmediato la asignación dentro del dominio, y también suele completarse en cuestión de segundos. Después de que se elimina la asignación, no hay acceso remoto a los datos eliminados. A continuación, el área de almacenamiento se encuentra disponible exclusivamente para tareas de escritura y los datos se sobrescriben con los datos nuevos que se hayan almacenado.

Seguridad de Amazon Relational Database Service (Amazon RDS)

Amazon RDS le permite crear rápidamente una instancia de base de datos relacional y escala de forma flexible los recursos informáticos asociados y la capacidad de almacenamiento para satisfacer la demanda de la aplicación. Amazon RDS gestiona la instancia de base de datos en su nombre mediante la realización de copias de seguridad, la gestión de conmutaciones por error y el mantenimiento del software de base de datos.

El cliente controla el acceso a la instancia de base de datos de Amazon RDS a través de grupos de seguridad de base de datos similares a los grupos de seguridad de Amazon EC2, pero no son intercambiables. El valor predeterminado de los grupos de seguridad de base de datos es un modo de acceso "denegar todo" y los clientes pueden autorizar específicamente el acceso a la red. Hay dos formas de hacerlo: autorizar un rango de IP de red o autorizar un grupo de seguridad existente de Amazon EC2. Los grupos de seguridad de

base de datos solo permiten acceder al puerto del servidor de la base de datos (todos los demás están bloqueados) y se pueden actualizar sin reiniciar la instancia de base de datos de Amazon RDS, lo que permite al cliente ejercer un control directo del acceso de la base de datos.

Con AWS IAM, un cliente puede controlar aún más el acceso a sus instancias de base de datos de RDS. AWS IAM permite que un cliente controle qué operaciones de RDS puede llamar cada uno de los usuarios de AWS IAM con permisos para ello.

Amazon RDS genera un certificado de SSL para cada instancia de base de datos, permitiendo a los clientes cifrar las conexiones de la instancia de base de datos para aumentar la seguridad.

Cuando se ejecuta la API de eliminación de la instancia de base de datos de Amazon RDS (`DeleteDBInstance`), dicha instancia se marca para su eliminación y se identifica su eliminación cuando en la instancia deja de mostrarse el estado "Eliminando". En este punto, la instancia deja de estar accesible y, a menos que se haya solicitado una copia de la instantánea final, no podrá restablecerse y no se mostrará para ninguna de las herramientas ni para las API.

Seguridad de Amazon Simple Queue Service (Amazon SQS)

Amazon SQS es un servicio de cola de mensajes escalable y de alta fiabilidad que permite la comunicación asíncrona de los mensajes entre los componentes distribuidos de una aplicación. Los componentes pueden ser ordenadores o instancias de Amazon EC2 o una combinación de ambos. Con Amazon SQS, puede enviar una serie de mensajes a una cola de Amazon SQS en cualquier momento desde cualquier componente. Los mensajes pueden recuperarse desde el mismo componente o desde otro distinto de forma inmediata o en un momento posterior (en un período de 4 días). Los mensajes son muy duraderos; cada mensaje se almacena de forma permanente en colas de alta disponibilidad y fiabilidad. En una cola de Amazon SQS se pueden leer o grabar varios procesos al mismo tiempo sin que interfieran entre sí.

El acceso a Amazon SQS se concede por cuenta de AWS o por usuario creado con AWS IAM. Tras la autenticación, una cuenta de AWS tiene acceso total a todas las operaciones de los usuarios. No obstante, un usuario de AWS IAM solo tiene acceso a las operaciones y colas para las que se le haya concedido acceso de conformidad con alguna política. De forma predeterminada, el acceso a cada una de las colas se restringe a la cuenta de AWS que la haya creado. Sin embargo, un cliente puede permitir otro acceso a una cola, usando una política generada por SQS o una política escrita por el usuario.

Se puede acceder a Amazon SQS a través de los puntos finales cifrados por SSL. A los puntos finales cifrados se puede acceder desde Internet y desde Amazon EC2. AWS no cifra los datos almacenados en Amazon SQS; no obstante, el usuario puede cifrar datos antes de cargarlos en Amazon SQS, siempre que la aplicación que utiliza la cola tenga recursos para descifrar el mensaje cuando se recupera. El cifrado de los mensajes antes de enviarlos a Amazon SQS ayuda a ofrecer protección frente al acceso no autorizado a datos sensibles del cliente, incluso por parte de AWS.

Seguridad de Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Notification Service (Amazon SNS) es un servicio web que facilita las tareas de configuración, utilización y envío de notificaciones desde la nube. Ofrece a los desarrolladores capacidad altamente escalable, flexible y rentable para publicar mensajes desde una aplicación y entregarlos inmediatamente a suscriptores o a otras aplicaciones.

Amazon SNS ofrece una sencilla interfaz de servicios web que puede utilizarse para crear temas de los que los clientes desean informar a las aplicaciones (o a personas), para suscribir a clientes a estos temas, para publicar mensajes, y para que estos mensajes se entreguen a través del protocolo que elija el cliente (como, por ejemplo, HTTP, correo electrónico, etc.). Amazon SNS entrega las notificaciones a los clientes utilizando un mecanismo de "inserción" que elimina la necesidad de comprobar o "sondear" de forma periódica en busca de nueva información y actualizaciones. Amazon SNS puede utilizarse para crear flujos de

trabajo y aplicaciones de mensajería de alta fiabilidad gestionadas mediante eventos, sin necesidad de complejo middleware ni gestión de la aplicación. Entre los usos potenciales de Amazon SNS se incluyen las aplicaciones de supervisión, sistemas de flujo de trabajo, actualizaciones de información en las que el tiempo es un aspecto a tener en cuenta, aplicaciones móviles y muchos otros. De la misma forma que con Amazon Web Services, no se requiere ningún tipo de inversión inicial, únicamente tendrá que pagar los recursos que utilice.

Amazon SNS proporciona mecanismos de control de acceso diseñados para garantizar que los temas y los mensajes están protegidos frente a acceso no autorizado. Los propietarios de los temas podrán definir políticas de un tema que restringirán quién puede publicar o suscribirse a un tema. Además, los propietarios de los temas podrán cifrar las notificaciones especificando que el mecanismo de entrega debe ser HTTPS.

El acceso a Amazon SNS se concede por cuenta de AWS o por usuario creado con AWS IAM. Tras la autenticación, una cuenta de AWS tiene acceso total a todas las operaciones de los usuarios. No obstante, un usuario de AWS IAM solo tiene acceso a las operaciones y temas para los que se le haya concedido acceso de conformidad con alguna política. De forma predeterminada, el acceso a cada uno de los temas se restringe a la cuenta de AWS que lo haya creado. Sin embargo, un cliente puede permitir otro acceso a una cola, usando una política generada por SNS o una política escrita por el usuario.

Seguridad de Amazon CloudWatch

Amazon CloudWatch es un servicio web que proporciona supervisión para los recursos en nube de AWS, empezando por Amazon EC2. Proporciona a los clientes datos sobre la utilización de recursos, el rendimiento operativo y los patrones globales de demanda, incluidos indicadores como la utilización de la CPU, las lecturas y escrituras de disco y el tráfico de red.

Amazon CloudWatch requiere, como todos los servicios de AWS, que cada solicitud realizada a su API de control se autentique para que solo los usuarios

autenticados puedan acceder a CloudWatch y gestionar este servicio. Las solicitudes se firman con una firma MAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario. Además, a la API de control de Amazon CloudWatch solo se puede acceder a través de los puntos finales cifrados de SSL.

Un cliente puede controlar aún más el acceso a Amazon CloudWatch mediante la creación de usuarios en su cuenta de AWS usando AWS IAM, y controlando para qué operaciones de CloudWatch tienen permisos para llamar los usuarios.

Seguridad de Auto Scaling

Auto Scaling permite a los clientes aumentar o disminuir su capacidad de Amazon EC2 en función de las condiciones que definen, de forma que el número de instancias de Amazon EC2 que utilizan aumenten sin ningún problema durante los picos de demanda para mantener el rendimiento y se reduzcan automáticamente durante los estancamientos de la demanda a fin de minimizar los costes.

Auto Scaling requiere, como todos los servicios de AWS, que cada solicitud realizada a su API de control se autentique para que solo los usuarios autenticados puedan acceder a Auto Scaling y gestionar este servicio. Las solicitudes se firman con una firma MAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario.

Un cliente puede controlar aún más el acceso a Auto Scaling mediante la creación de usuarios en su cuenta de AWS usando AWS IAM, y controlando para qué operaciones de Auto Scaling tienen permisos para llamar los usuarios.

Seguridad de Amazon CloudFront

Amazon CloudFront requiere que todas las solicitudes realizadas a su API de control se autentiquen para que solo los usuarios autenticados puedan crear, modificar o eliminar sus propias distribuciones de Amazon CloudFront. Las solicitudes se firman con una firma MAC-SHA1 calculada a partir de una solicitud

y la clave privada del usuario. Además, a la API de control de Amazon CloudFront solo se puede acceder a través de los puntos finales cifrados de SSL.

No se garantiza la durabilidad de los datos almacenados en las ubicaciones de extremos de Amazon CloudFront. En algunas ocasiones, el servicio puede eliminar los objetos de las ubicaciones de los extremos si dichos objetos no se solicitan con frecuencia. La durabilidad la ofrece Amazon S3, que funciona como el servidor de origen de Amazon CloudFront que aloja las copias originales y definitivas de los objetos que ofrece Amazon CloudFront.

Si quiere tener el control de quién puede descargar el contenido de Amazon CloudFront, puede activar la función del contenido privado del servicio. Esta función tiene dos componentes: el primero controla la forma en que las ubicaciones de extremo de Amazon CloudFront acceden a los objetos en Amazon S3. El segundo controla la forma en que las ubicaciones de extremos de Amazon CloudFront ofrecen el contenido a los usuarios de Internet.

Para controlar el acceso a las copias originales de los objetos de Amazon S3, Amazon CloudFront le permite crear una o varias "Identidades de acceso al origen" y asociarlas con las distribuciones. Cuando se asocia una identidad de acceso al origen con una distribución de Amazon CloudFront, la distribución utiliza dicha identidad para recuperar los objetos de Amazon S3. Por tanto, puede utilizar la función de ACL de Amazon S3, que limita el acceso a dicha identidad de acceso al origen a fin de que la copia original del objeto no pueda leerse de forma pública.

Para controlar quién puede descargar los objetos desde las ubicaciones de extremo de Amazon CloudFront, el servicio utiliza un sistema de verificación firmado mediante URL. Para utilizar este sistema, primero debe crear una parte de clave pública-privada, y cargar la clave pública en la cuenta a través del sitio web de Amazon Web Services. En segundo lugar, debe configurar la distribución de Amazon CloudFront para indicar qué cuentas autorizaría para firmar solicitudes (puede indicar hasta cinco cuentas de AWS en las que confíe para

firmar las solicitudes). En tercer lugar, a medida que reciba solicitudes, podrá crear documentos sobre políticas en los que se indiquen las condiciones en función de las cuales desee que Amazon CloudFront muestre el contenido. Estos documentos sobre políticas pueden especificar el nombre del objeto solicitado, la fecha y la hora de la solicitud, y la IP de origen (o el rango de CIDR) del cliente que realiza la solicitud. Posteriormente puede calcular la codificación RSA-SHA1 del documento de la política y firmarlo con la clave privada. En cuarto lugar, puede incluir el documento de política codificado y la firma como parámetros de cadena de consulta al hacer referencia a sus objetos. Cuando Amazon CloudFront recibe una solicitud, descodificará la firma con la clave pública. Amazon CloudFront solo atenderá las solicitudes que tengan un documento de política válido y firmas coincidentes.

Tenga en cuenta que el contenido privado es una función opcional que debe estar activada cuando configure la distribución de CloudFront. El contenido entregado sin esta función activada lo podrán leer todos los usuarios, ya que será público.

Amazon Cloudfront también ofrece la posibilidad de transferir contenido a través de una conexión cifrada (HTTPS) para autenticar el contenido que se entrega a los usuarios. De forma predeterminada, Amazon Cloudfront aceptará las solicitudes enviadas a través de los protocolos HTTP y HTTPS.

Si lo prefiere, también puede configurar Amazon Cloudfront para que requiera HTTPS para todas las solicitudes y para que rechace todas las solicitudes HTTP. Para las solicitudes de HTTPS, Amazon Cloudfront también utilizará HTTPS para recuperar el objeto de Amazon S3, para que su objeto se cifre cuando se transmita.

Los registros de acceso de Amazon CloudFront contienen un conjunto completo de información acerca de las solicitudes de contenido, incluido el objeto solicitado, la fecha y la hora de la solicitud, la ubicación de extremo que aloja la solicitud, la dirección IP del cliente, el referente y el agente del usuario. Para permitir el acceso, los registros solo especifican el nombre del depósito de

Amazon S3 para almacenar los registros al configurar la distribución de Amazon CloudFront.

Seguridad de Amazon Elastic MapReduce (Amazon EMR)

Amazon Elastic MapReduce requiere que se autenticquen todas las solicitudes que realizan a sus API para que solo los usuarios autenticados puedan crear, buscar o terminar sus flujos de trabajo. Las solicitudes se firman con una firma MAC-SHA1 calculada a partir de una solicitud y la clave privada del usuario. Amazon Elastic MapReduce ofrece puntos finales de SSL para acceder a la consola y a las API del servicio web.

Para iniciar flujos de trabajo en nombre de un cliente, Amazon Elastic MapReduce configura un grupo de seguridad de Amazon EC2 del nodo principal para permitir solo el acceso externo a través de SSH. El servicio crea un grupo de seguridad independiente de los elementos subordinados que no permite el acceso externo. Para proteger los conjuntos de datos de entrada y salida, Amazon Elastic MapReduce transfiere datos a y desde S3 usando SSL.

- Adición de AWS Identity and Access Management (AWS IAM)
- Adición de Seguridad de Amazon Simple Notification Service (SNS)
- Adición de Seguridad de Amazon CloudWatch
- Adición de Seguridad de Auto Scaling
- Actualización de Amazon Virtual Private Cloud (Amazon VPC)
- Actualización del Entorno de control
- Eliminación de la gestión de riesgos porque se ha ampliado en un documento técnico independiente
- Cambios desde la última versión (noviembre de 2009):
- Revisión importante
- Cambios desde la última versión (junio de 2009):
- Cambios introducidos en la sección Certificaciones y acreditaciones para incluir la certificación SAS70
- Adición de Amazon Virtual Private Cloud (Amazon VPC)

- Adición de la sección Credenciales de seguridad para destacar AWS Multi-Factor Authentication y Key Rotation
- Adición de Seguridad de Amazon Relational Database Service (Amazon RDS)
- Cambios desde la última versión (septiembre de 2008):
- Adición de principios de diseño de seguridad
- Actualización de la información sobre seguridad física e inclusión de las comprobaciones de antecedentes
- Sección de copias de seguridad actualizada para incluir aclaraciones sobre Amazon EBS
- Actualización de la sección Seguridad de Amazon EC2 para incluir:
- SSHv2 basado en certificados
- Diagrama y detalles del grupo de seguridad multicapa
- Descripción del hipervisor y diagrama de aislamiento de instancias
- Aislamiento de errores
- Adición de Gestión de la configuración
- Actualización de la sección Amazon S3 para incluir detalles y aclaraciones
- Adición de Retirada de dispositivos de almacenamiento
- Adición de Seguridad de Amazon SQS
- Adición de Seguridad de Amazon CloudFront
- Adición de Seguridad de Amazon Elastic MapReduce

Avisos

© 2010-2011 Amazon.com, Inc. o sus afiliados. Este documento se ofrece solo con fines informativos. Representa la oferta de productos actual de AWS en la fecha de publicación de este documento, que está sujeto a cambios sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece "tal cual", sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, representación, compromiso contractual, condición ni garantías de AWS, sus filiales, proveedores ni licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS, y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Anexo 4: Microsoft Azure Pricing Calculator

Microsoft Azure Pricing Calculator

1) Please Select a Region: **Brazil** Start Over Estimated Updated: June 20, 2014

2) Please Select a Currency: **United States Dollar (USD)** Terms & Conditions Estimated Monthly Price

Express Route Price: **Not Available**

Data Transfers

Zone 1: **0** Zone 2: **0**

Outbound Data Transfers: **500** GB Outbound Data Transfers: **500** GB

Zone 1 Price: \$59,40
Zone 2 Price: \$94,05
Data Transfers Price: **\$153,45**

Virtual Networks

Connection Hours: **0** Hours

VPN Price: **\$0,00**

Traffic Manager

Traffic Manager: **0**

DNS Queries Per Month: **100** Million DNS Queries DNS Queries: **\$75,00**

Pricing Calculator | Pricing Summary

Microsoft Azure Pricing Calculator

1) Please Select a Region: **Brazil** Start Over Estimated Updated: June 20, 2014

2) Please Select a Currency: **United States Dollar (USD)** Terms & Conditions Estimated Monthly Price

Outbound Data Transfers: **500** GB Outbound Data Transfers: **500** GB

Zone 1 Price: \$59,40
Zone 2 Price: \$94,05
Data Transfers Price: **\$153,45**

Virtual Networks

Connection Hours: **0** Hours

VPN Price: **\$0,00**

Traffic Manager

Traffic Manager: **0**

DNS Queries Per Month: **100** Million DNS Queries DNS Queries: **\$75,00**

Health Checks Per Month (Azure): **0** Service Endpoints Health Checks (Azure): **\$0,00**

Health Checks Per Month (External): **0** Service Endpoints Health Checks (External): **\$0,00**

Traffic Manager Price: **\$75,00**

Pricing Calculator | Pricing Summary

Microsoft Azure Pricing Calculator

1) Please Select a Region: **Brazil** Start Over Estimated Updated: June 20, 2014

2) Please Select a Currency: **United States Dollar (USD)** Terms & Conditions Estimated Monthly Price

Total Visual Studio Online Price: **Not Available**

Support

Select Support Level: **Professional Direct** Support Price: **\$1.000,00**

Options

MOSP Options: **Pay-As-You-Go** Estimated Discount: **0,00%**

Select MOSP Plan Options and Commitment Spending: **N/A**

Payment Options

Total **Estimated Monthly Price** **Estimated Annual Price** Show Prices In: **United States Dollar (USD)**

Pricing Calculator | Pricing Summary