Plan de negocio de un servicio virtual en nube publica para la administración de farmacias mediante un Producto Mínimo Viable (MVP)

Trabajo De Grado Presentado Para Obtener El Título De

Ingeniero En Telecomunicaciones

Universidad Militar Nueva Granada

Director

Ing. Luis Fernando González de la Calle

Paula Alejandra Garzón Sánchez, David Leonardo Leaño Arcila

Octubre 2016, Bogotá D.C

Resumen

Se presenta el plan de servicio mediante cloud computing utilizando el proveedor Microsoft Azure, para así adoptar los diferentes tipos de servicios integrados con los que cuenta y comparar el funcionamiento y la implementación de dos de los modelos de nube, PaaS (Platform as a Service) e IaaS (Infrastructure as a Service).

Implementando el servicio en Microsoft Azure, se tendrá una herramienta que permitirá lograr una competitividad mayor en el mercado. Ya que aumentará la funcionalidad y productividad en la forma de cómo administran los procesos internos y externos de su negocio, además podrá contar con una serie de análisis o predicciones que les brindará una ventaja frente a otras farmacias, beneficios que serán mencionados a lo largo de este documento.

1. Administración de farmacias en cloud computing

La evolución de la tecnología ha permitido grandes avances en la gestión y administración de varios sectores empresariales, por esta razón se evidencio como cloud computing brinda una posibilidad más óptima y productiva de implementación, desarrollo y operación. [1]

Cuando se habla de brindar un servicio óptimo, se hace referencia a que existe un déficit en la administración y control de los procesos internos de muchas empresas, que en este caso se centra dicho análisis en las farmacias. En donde en repetidas ocasiones tanto dueños como clientes se ven afectados, lo que ocasiona pérdidas en dinero y tiempo para dichas partes.

Una de las mejores alternativas para llevar a cabo este proceso es por medio de la utilización de cloud computing de Microsoft Azure, el cual permite realizar mejoras y satisfacer las necesidades esenciales. [2]

1.1. Objetivos

El propósito de este documento consiste en un plan de negocio para un inversionista ángel del servicio virtual en nube pública para la administración de Farmacias mediante un Producto Mínimo Viable (MVP). [3]

El servicio presenta diversas fluctuaciones desde su primera versión, requiriendo así su segunda versión para la adopción y mejora de su funcionalidad y operación como lo expone el ciclo de sobreexposición de Gartner. [4]

Cuenta con servicios modernos que en la actualidad se encuentran en auge, además brinda metodologías de administración, consultores de tecnología, al igual el servicio requiere cumplir con estándares de industria como los emitidos por ISO. En este caso se utilizó la norma ISO/IEC 27001/27002:2013, también se utilizó la metodología PMBOK que, al ser un instituto de proyectos, [5] brinda un modelo de referencia para la metodología de desarrollo y dirección de proyectos, el eTOM al ser un marco de referencia que describe los procesos empresariales, ayudo a crear y mejorar la administración de empresas de TI. [6]

Además, se condiciono que se debía cumplir con seguridad para los clientes en el momento de realizar sus transacciones y sus controles de accesos seguro. Por lo cual se implementó el estándar de seguridad de datos para la industria de tarjetas de pago PCI (Payment Card Industry). [7]

1.1.1. Objetivos específicos

- ✓ La Industria de Tarjetas de Pago - PCI (Payment Card Industry) requiere que las transacciones bancarias se efectúen de manera segura y se encuentren protegidas, razón por la cual este estándar fue aplicado en los modelos PaaS (Platform as a Service) e IaaS (Infrastructure as a Service) del servicio ***Aliviese-Pronto ®.*** [7]

- ✓ Los estándares de seguridad ISO/IEC 27001/27002:2013 e ISO/IEC 27018:2014 permiten un modelo para el establecimiento, operación, seguimiento, revisión y mejora de un sistema de gestión de la seguridad de la información, los cuales se implementaron en el servicio ***Aliviese-Pronto ®.*** [8][9]

- ✓ El Instituto Nacional de Estándares y Tecnología - NIST (National Institute of Standard and Technology) definió los modelos de servicios de cloud computing en PaaS (Platform as a Service) e IaaS (Infrastructure as a Service), y SaaS (Software as a Service). El servicio ***Aliviese-Pronto ®*** evaluó los despliegues PaaS (Platform as a Service) e IaaS (Infrastructure as a Service), realizando una comparación del consumo de recursos tanto en tiempo como en dinero.[10]

- ✓ Con el propósito de dar a conocer la importancia y viabilidad del proyecto se realizó un modelo del plan de negocio para un inversionista ángel, basándose en herramientas como Mapa de Operaciones - eTOM, Ciclo de Sobreexposición Gartner y Metodologías de Proyectos - PMBOK en Ms Project.

- ✓ Con el fin de implementar y diseñar el MVP con una estructura jerárquica que involucré la gestión y el proceso de cómo interactúan los clientes, suministradores y los diferentes recursos en la prestación del servicio dentro de las farmacias, y con ello garantizar las operaciones y la continuidad del servicio ***"Aliviese-Pronto ®"*** se implementó el eTOM.

1.2. Estándares, normas y un poco más de ti en el servicio *"Aliviese-Pronto ®"*

La implementación del Producto Mínimo Viable - MVP permite la aproximación de un servicio casi-real a un servicio comercial real, como un modelo conceptual para validar el uso hacia clientes y costo hacia los dueños. El MVP tendrá algunos aspectos y estándares como PCI, normas internacionales de seguridad ISO, la implementación del ciclo de sobreexposición de Gartner, eTOM y PMBOK.

Para llevar a cabo el desarrollo del producto mínimo viable se hizo uso de uno de los servicios con mayor auge en la actualidad cloud computing, "*el cual es un modelo que permite el acceso a la red de manera ubicua, con el fin de tener un conjunto de recursos compartidos; teniendo características esenciales como: demanda bajo servicio, amplio acceso a la red, recursos en común, rápida elasticidad, medición de servicio."* [10]

En varias ocasiones a la hora de desarrollar proyectos de TI, es común preguntarse qué tecnología, plataforma o solución de los diversos fabricantes existentes en la industria están marcando liderazgo en cuanto a características tales como facilidades de operación, seguridad, costo, tendencias tecnológicas o simplemente posicionamiento.

Ya que el fin del servicio es prestar un servicio de la más alta calidad, era necesario conocer cuáles eran los líderes en cloud computing. Es por esto que nos referimos al cuadrante mágico de Gartner, el cual es desarrollado por Gartner Inc., Gartner Inc. Es una empresa de consultoría dedicada de manera exclusiva a investigar la industria de las TI, analizar las tendencias del mercado y elaborar el ranking de soluciones tecnológicas para facilitar la selección de soluciones y productos, basados en una metodología de trabajo propia y un equipo de trabajo con una vasta experiencia y distribuido en todo el planeta. Gartner, nos presenta los rankings de fabricantes de tecnologías en algo que denominó los cuadrantes mágicos. [4]

Según el cuadrante mágico de Gartner publicado en mayo de 2015 existen dos proveedores líderes de cloud computing, los cuales son Microsoft Azure y Amazon Web Service. [4]

Teniendo como referencia el cuadrante mágico de Gartner mencionado anteriormente, para llevar a cabo el MVP (Producto Mínimo Viable) se eligió el proveedor Microsoft Azure, el cual es la plataforma de Microsoft cloud computing, debido a que fue el que ofreció tres pases cada uno con un monto de 600 dólares para llevar a cabo el MVP, además de esto ofrece ISO 27000, la implementación de PCI y las características esenciales de cloud computing. (Microsoft Azure , 2016)[11]

El servicio ofrecido al estar dirigido al área de la salud, requiere ciertos parámetros, controles, reglamentaciones u organizaciones competentes que se encargan de verificar el correcto funcionamiento y prestación del servicio. Es importante garantizar la confidencialidad y seguridad de la información de los pacientes, es por esto que para brindar un servicio con las mejores características y un alto nivel capaz de competir y cumplir con las normativas a nivel internacional se tuvo en cuenta para el desarrollo del servicio la ley

federal *HIPAA (Health Insurance Portability and Accountability Act of 1996),* que es la ley federal para la contabilidad y portabilidad del aseguramiento de la salud de 1996. El objetivo principal de la ley es facilitar a las personas para tener un seguro médico, proteger su confidencialidad y seguridad de la información relacionada con la salud y ayudar a la industria de la salud a controlar los costos administrativos. HIPAA se divide en diferentes títulos o secciones que se ocupan de un aspecto único de la reforma del seguro de salud; sus dos secciones principales son Título I con portabilidad y el Título II que se centra en la simplificación administrativa. [12]

Para que el producto mínimo viable sea atractivo se debe garantizar que haya una continuidad del negocio y que la norma ISO/IEC 27001/27002:2013 se cumpla, la cual nos va a permitir garantizar la protección y privacidad de los datos de cada uno de los usuarios, brindando así la fiabilidad del negocio que los clientes necesitan.

Con el fin de cumplir dichos requerimientos se recurrió a la organización internacional de estandarización (International Organization for Standarization - ISO) específicamente a las normas ISO/IEC 27001/27002:2013.

ISO/IEC 27001/27002:2013 es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa que puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. [8][9]

Por otro lado, para garantizar a los clientes otro factor vital en cuanto al tema de la seguridad de la información y garantizar así lo referente a transacciones o pagos electrónicos y de igual forma que el ingreso al servicio, se decide adoptar e implementar la norma de seguridad de datos para la industria de tarjetas de pago más conocido como PCI, con el fin de poder llegar a realizar la facturación por el servicio implementado.

PCI DSS (Payment Card Industry Data Security Standard) versión 3.2 publicada en abril de 2016 el cual *"consiste en una serie de estándares de seguridad que incluyen:* Requerimientos para administrar la seguridad, las políticas, procedimientos, la arquitectura de redes, el diseño de software y otras medidas críticas de protección de la información." [7]

Todas las normas PCI son avaladas y desarrolladas por el consejo de estándares de seguridad de la industria de tarjetas de pago (Payment Card Industry Security Standards Council) PCI SSC y se encuentra conformado por Visa Internacional, mastercard Worldwide, American Express, JCB, Discover Financial Services. [7]

Con el propósito de mostrar un plan de negocio para inversionista ángel es necesario evidenciar los avances y el ciclo de la evolución que tendría el servicio a lo largo del tiempo, razón por la cual se fundamentó el estudio en el ciclo de sobreexposición de Gartner, que es una herramienta gráfica desarrollada y utilizada para la representación de la madurez, adopción y aplicación comercial/social de una tecnología particular, según un ciclo de vida, y la forma en que esta es potencialmente relevante para la resolución de problemas reales de negocio y para explotar nuevas oportunidades. Esta metodología da una visión de cómo una tecnología o aplicación puede evolucionar con el tiempo, proporcionando así una fuente para

gestionar su implementación en el contexto específico de cada negocio y así aprovechar mejor las oportunidades venideras. [4]

Para mantener una relación entre el flujo por el cual se va a desenvolver el proceso administrativo interno y externo de las farmacias es necesario tener un marco de referencia para modelar los diferentes procesos del servicio y de su aprovisionamiento en las farmacias. Por este motivo, se incluyó la implementación del eTOM (Mapa de operaciones de telecomunicación mejorado) en el desarrollo y planeación del servicio para garantizar las operaciones y la continuidad del servicio ***Aliviese-Pronto ®.*** [6]

El eTOM, fue desarrollado por el Foro de gestión de las telecomunicaciones, describe los procesos empresariales que necesita un proveedor de servicios y los analiza con distintos niveles de detalle de acuerdo con su significado y prioridad para el negocio. Este enfoque, orientado a los procesos de negocio, se basa en los conceptos de servicios y funciones de gestión y permite desarrollar un marco para clasificar todas las actividades de negocio. [6]

1.3. Actualidad e importancia de cloud computing en las farmacias

A pesar de que cloud computing es un tema que no es conocido en la mayor parte de la sociedad, existen en la actualidad algunas organizaciones y/o empresas que ya están adoptando este tipo de tecnología en su negocio. A continuación, se mencionan algunas de dichas empresas y temas que abarcan la tecnología cloud computing en los servicios de farmacia.

La organización mundial de la salud (WHO - World Health Organization) no contaba con un sistema eficaz que le permitiera recolectar información en poblaciones numerosas, debido a esta situación recurría a organizaciones como Wikipedia para que les suministrarán información acerca de las enfermedades más consultadas y de esta forma comenzar a actuar en dicha población. Sin embargo, ya que esta información por tratarse de una fuente no confiable, no se puede tomar como un punto de referencia totalmente verídico. Razón por la cual se vieron en la obligación y necesidad de buscar un sistema que satisfaga sus necesidades, es así como las empresas de tecnología comienzan a darse cuenta de la importancia de desarrollar y brindar servicios en el sector médico y de allí surgen servicios como Microsoft Health y AWS Service Health. [13]

Con el fin de regular y proteger los derechos de los pacientes se crea en 1996 la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA - Health Insurance Portability and Accountability Act) HIPAA y HITECH (Health Information Technology for Economic and Clinical Health Act in 2009) establecieron un conjunto de normas federales que se encargan de proteger la seguridad y privacidad de la PHI (Protect Health Information). De acuerdo a esto se imponen nuevos requisitos relacionados con el uso y divulgación de PHI, manteniendo la protección de dato, derechos individuales y las diferentes responsabilidades administrativas. [12] [14] [15]

Además de los temas y organizaciones que utilizan cloud computing, se presenta como punto de referencia a nivel internacional la cadena de farmacias CVS que adopta y administra su operación de servicio en cloud computing.

CVS pharmacy, es una de las cadenas farmacéuticas más grandes del mundo cuenta con más de 7800 sedes en Estados Unidos fue fundada en 1953, posee virtualizados todos sus sistemas desde la parte administrativa de la empresa hasta el reporte de sus ventas generales y por usuario vale la pena aclarar que el historial del usuario es confidencial y es solo el quien tiene acceso a esto. Sin embargo, con el reporte de ventas generales se pretende mejorar sus servicios y generar predicciones respecto a algunas enfermedades. [16]

Además de contar con sistemas virtualizados, CVS cuenta con una aplicación móvil la cual abarca características como: Visualización de fórmulas médicas, acceso al respectivo historial de medicamentos recetados, encontrar información de puntos de atención y el horario de apertura/cierre, ofertas semanales y crear una lista de compras, ver las imágenes del pedido, entre otras. [17]

Otros usos dentro del área de la salud que implementa y apoya su operación en cloud computing son la multinacional General Electric Healthcare e IMS health.

GE Healthcare con sede en Inglaterra y oficinas en todo el mundo cuenta con una base de clientes global que se basa en sus productos. La empresa requiere una plataforma flexible y altamente escalable que puede entregar una amplia gama de soluciones y servicios para ayudar a imaginar nuevas formas de diagnosticar y tratar el cáncer, enfermedades del corazón, enfermedades neurológicas y otras condiciones anteriores, de forma más rentable y más eficiente. [18]

GE Healthcare cuenta con un ecosistema de socios en la nube y decidió aprovechar la plataforma Microsoft Azure con su oferta de infraestructura como servicio (IaaS). Trasladarse a la nube podría ofrecer múltiples beneficios, incluyendo una distribución más fácil, más centralizada de software y gestión, y una mejor escalabilidad. La compañía también se señaló a la disposición del entorno de Microsoft Azure para ayudar a los clientes a cumplir con sus requisitos de cumplimiento en la industria de la salud. Además de las salvaguardas técnicas, Azure ofrece un Contrato de Asociación HIPAA Negocios (BAA) en el que Microsoft se compromete a cumplir con ciertas disposiciones de seguridad y privacidad establecidas en la Ley de alta tecnología y HIPAA. [18]

IMS Health es una empresa fundada en 1954, su sede principal se encuentra en Danbury, Connecticut, Estados Unidos en donde se encargan de la recolección y análisis de información médica, cuenta con sedes alrededor del mundo, llego a Colombia en 1972, sin embargo se dieron cuenta que recolectar esta información puede llegar a ser complicado y aún más si se hace manualmente, además el margen de error es bastante alto. En 2010 comienza a utilizar los servicios de AWS para almacenar y procesar la información que recolecta, actualmente cuenta en Colombia recibe la información de más de 25 mil puntos de venta. [19] [20]

2. Implementación de PCI en el servicio *Aliviese-Pronto* ®

PCI es el estándar de seguridad de datos para la industria de tarjeta de pago PCI DSS (Payment Card Industry Data Security) consiste en una serie de requerimientos para administrar la seguridad, las políticas, procedimientos, la arquitectura de redes, el diseño de software y otras medidas críticas de protección de la información a nivel mundial.
Fue desarrollado por el comité formado por las empresas de tarjetas más importantes como lo son Visa, Diners Club, Mastercard y American Express entre otros. [6] [21]

La Industria de Tarjetas de Pago - PCI (Payment Card Industry) requiere que las transacciones bancarias se efectúen de manera segura y se encuentren protegidas, razón por la cual este estándar fue aplicado en los modelos PaaS e IaaS del servicio "Alíviese Pronto".

El propósito de esta organización es estandarizar y proteger la seguridad de las tarjetas de pago y reducir los fraudes a nivel mundial, por eso PCI DSS aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD). [22]

PCI ofrece múltiples beneficios a las entidades tales como: [21]

1. Promover la integridad del comercio y aumentar la confianza de los consumidores en el negocio.
2. Incrementar las ventas como consecuencia del aumento en la confianza de los consumidores.
3. Proteger al comercio de posibles pérdidas de ingresos, investigaciones no deseadas y costos legales.
4. Reducir el riesgo de atención no deseada de la prensa como resultado de un compromiso o fuga de información de clientes.
5. Proyectar mayor conciencia de los controles y medidas preventivas de seguridad disponibles para el comercio.
6. Reducir las disputas de Tarjetahabientes y costos asociados a transacciones fraudulentas resultantes de un compromiso de información.
7. Prevenir el robo masivo de información de clientes.
8. Facilitar la adopción de estándares de seguridad válidos a nivel global.
9. Generar una herramienta que establece las posibles vulnerabilidades que tiene el sistema de información.

Actualmente PCI se en cuenta en la versión 3.2 la cual fue publicada en abril de 2016 cuenta con 12 requerimientos los cuales se encuentran organizados en 6 objetivos de control tal como se muestra a continuación:

Desarrollar y Mantener una Red Segura	Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
	Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
Proteger los Datos de los propietarios de tarjetas	Requisito 3: Proteger los datos almacenados de los propietarios de tarjetas
	Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
Mantener un Programa de Gestión de Vulnerabilidades	Requisito 5: Usar y actualizar regularmente un software antivirus.
	Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.
Implementar Medidas sólidas de control de acceso	Requisito 7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
	Requisito 8: Asignar una identificación única a cada persona que tenga acceso a un computador.
	Requisito 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.
Monitorizar y probar regularmente las redes	Requisito 10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
	Requisito 11: Probar regularmente los sistemas y procesos de seguridad.
Mantener una Política de Seguridad de la Información	Requisito 12: Mantener una política que contemple la seguridad de la información

Tabla. 1 Requerimientos PCI v 3.2

Cada uno de los requisitos anteriormente nombrados se encuentran detallados en el **anexo a** en donde se puede observar cuales fueron los ítems implementados.

3. Implementación de la norma ISO/EIC 27001/27002:2013 e ISO/EIC 27018:2014 en el servicio *Aliviese-Pronto* ®

La protección de datos en la plataforma ***Aliviese-Pronto*** **®** son fundamentales ya que se manejan información sensible como lo es la información de las tarjetas de crédito inscritas e información médica, [23] uno de los métodos utilizados para garantizar la protección de datos fue implementación de las normas ISO/EIC 27001/27002:2013 e ISO/EICE 27018:2014.

Se realizó la elección de estas dos normas ya que Microsoft Azure se encuentra totalmente certificado en estas, [24] [25] la norma ISO/EIC 27001/27002:2013 la cual brinda los requisitos para garantizar la seguridad de los datos, sin embargo esta norma no toma en cuenta varios aspectos de cloud computing es por esto que se vieron en la necesidad de crear otra norma que para tratar todo el tema de cloud computing es así como en 2014 publican la norma ISO/EIC 27018 y se encarga de "*establecer los requisitos destinados a garantizar que los proveedores de servicios en cloud computing puedan ofrecer controles adecuados de seguridad de la información"* [26]

3.1. Implementación de la norma ISO/EIC 27001/27002:2013 en el servicio *Aliviese-Pronto* ®

La norma ISO/EIC 27001/27002:2013 es una norma internacional que suministra requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo y brindad confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se difunda de acuerdo con las necesidades de la organización.

Se evaluaron los ítems de la norma y se seleccionaron acorde a las necesidades del servicio ***Aliviese-Pronto*** **®** los cuales se pueden observar en el **anexo b.**

3.2. Implementación de la norma ISO/EIC 27018:2014 en el servicio *Aliviese-Pronto* ®

La norma ISO / IEC 27018: 2014 se puede considerar relativamente nueva, ya que fue publicada en el mes de agosto de 2014 y proporciona una orientación destinada a los proveedores de nube para que puedan ofrecer controles adecuados de seguridad de la información con el objetivo de proteger la privacidad de los clientes, estableciendo así directrices con relación a medidas de protección de información de identificación personal (PII).

La norma pretende ser "una referencia para la selección de los controles de protección de información de carácter personal en el proceso de implementación de un sistema de gestión de seguridad de información basado en la norma ISO / IEC 27001 para un sistema cloud"

El estándar ISO 27018 será sin duda un instrumento útil que puede contribuir a proporcionar confianza en el mercado respecto a la capacidad el cumplimiento normativo de los proveedores de servicios en entornos de almacenamiento en la nube.

Se evaluaron los ítems de la norma y se seleccionaron acorde a las necesidades del servicio ***Aliviese-Pronto*** **®** los cuales se pueden observar en el **anexo c.**

4. Diseño en Infrastructure as a Service (IaaS) y Platform as a Service (PaaS) para la administración farmacias utilizando Microsoft Azure

A continuación, se muestra la metodología empleada para la elaboración del producto mínimo viable en los dos modelos de servicios elegidos Infrastructure as a Service (IaaS) y Platform as a Service (PaaS), profundizando en los procesos utilizados para las arquitecturas propuestas con el fin de obtener resultados favorables con los requerimientos encontrados.

4.1. Descripción General del Servicio

El servicio ***Aliviese-Pronto*** **®** es una plataforma con administración y procesamiento remoto en Cloud diseñado para los procesos que se realizan en las farmacias colombianas, donde los clientes ingresan con fórmulas médicas o desean realizar la compra de medicamentos de venta libre con el fin de atacar la enfermedad que este presentando en ese momento.

Adicionalmente, ***Aliviese-Pronto*** **®** cuenta con la seguridad apropiada para almacenar las formulas medicas de cada usuario, las cuales son visualizadas por el cliente, el farmaceuta por tiempo limitado y el médico tratante cumpliendo con estándares de manejo de datos médicos como HIPAA, EHR y estándares de protección de datos como lo son ISO 27001 e ISO 27018. Por otra parte, la plataforma permite administrar los productos de las

farmacias llevando un riguroso control del inventario de este, lo cual permite identificar alertas cuando existan pocos productos.

Además, cuenta con la implantación del estándar PCI lo cual permite brindar seguridad tanto a los clientes como a las farmacias a la hora de realizar transacciones a través de la plataforma.

El proceso realizado por cada una de las farmacias según eTOM se encuentra explícito en el **anexo d.**

4.2. Descripción de roles en el sistema

Con el fin de integrar los diferentes actores del proceso de negocio de las farmacias y su administración la plataforma ***Aliviese-Pronto*** **®** cuenta con cinco roles los cuales se explican a continuación:

Médico: Realiza la creación de la formula médica y se la asigna al usuario que se encuentre en consulta, es capaz de visualizar la formula médica, el proceso paso a paso que realiza este rol se encuentra detallado en el **anexo e**.

Usuario: Cliente de las farmacias, quien realiza su registro en la plataforma, realiza el pedido de su fórmula médica, efectúa el pago los medicamentos solicitados y es capaz de visualizar su fórmula médica, el proceso paso a paso que realiza este rol se encuentra detallado en el **anexo f**.

Farmaceuta: Funcionario la farmacia se encarga de recibir las fórmulas de los usuarios, despacha el pedido, valida que el usuario obtenga los productos solicitados.

Administrador: Usuario encargado de crear usuarios en los diferentes roles, administra el inventario de la farmacia, actualiza el precio de los productos, realiza el aprovisionamiento de los productos, el proceso paso a paso que realiza este rol se encuentra detallado en el **anexo g**.

Gerente: Realiza la contratación del personal idóneo para las actividades a realizar, evalúa el desempeño de los empleados, genera y analiza los reportes mensualmente, planea la cantidad de medicamentos que necesita la farmacia, el proceso paso a paso que realiza este rol se encuentra detallado en el **anexo h**.

4.3. Pre-Requisitos y Especificaciones del Sistema

Según la ley federal “Health Insurance Portability and Accountability Act of 1996” (HIPAA), la cual permite la contabilidad y portabilidad de los datos de la salud, facilitando a las personas tener seguridad de sus datos, fueron implementados procedimientos y se establecieron directivas técnicas para la plataforma AliviesePronto, con el fin de mantener datos de la salud protegidos electrónicamente para permitir el acceso sólo a las personas a quienes se han otorgado derechos de acceso:

1. Según las cargas de datos y operaciones, fueron identificadas las necesidades de acceso de todos los usuarios, integrando sus procesos ante las farmacias y la información que estos manejan.
2. Fueron establecidos mecanismos de identificación de usuarios por medio de su usuario y una contraseña asignada por ellos mismos para el acceso a la parte de los datos correspondiente a sus procesos establecidos.
3. Con ayuda del marco de procesos de las telecomunicaciones eTOM, fue diseñado un mapa para cada uno de los roles diferentes del sistema, donde se delimita el alcance de acceso a la información para cada usuario y se exponen posibles reglas que se pueden establecer al interior de cada laboratorio médico.

4. La implementación del control de acceso se realiza por medio de una base de datos albergada en una máquina virtual diferente que realiza la interacción con el usuario, a la cual tiene acceso único el propietario del producto, quien se encargará de gestionar los accesos de un usuario administrativo, el cual se encarga de gestionar el acceso de los demás usuarios del sistema.

5. Cada usuario será capaz de actualizar su información personal en cuanto a identificación, datos de contacto y de método de pago. En caso de contar con un incremento en la población de usuarios funcionarios del laboratorio médico, el usuario administrador cuenta con el privilegio de otorgar acceso a los nuevos integrantes o denegar a los antiguos.

6. En cuanto a seguridad de los datos, se aplica el protocolo IPSec dentro de una red privada virtual entre las instancias del sistema para el transporte de los datos entre máquinas virtuales, con el fin de proteger la información que no puede ser descargada de la plataforma AliviesePronto. Además de esto, se cuenta con el mecanismo de desconexión automática del sistema después de que se detectan más de 5 minutos de inactividad por parte del usuario, con el fin de evitar accesos indeseados mientras se deja sin atender una estación de acceso, se ha implementado un firewall en cada máquina virtual con el fin de evitar que exista cualquier tipo de virus o ataque a las máquinas virtuales donde se almacena la información.

7. Cuando el usuario ha terminado su proceso en la plataforma AliviesePronto, se permite cerrar la sesión en el momento deseado con el fin de evitar realizar actividades indeseadas dentro del sistema y que personal no autorizado haga uso de ella.

Para la elaboración del sistema y brindar su completa funcionalidad se deben establecer ciertos criterios y condiciones brindando un desempeño optimo al servicio, por lo que es indispensable el análisis de unos requisitos para tener claro que funcionalidades se pueden aprovechar de los diferentes servicios de Microsoft Azure, llevando a cabo un estudio a partir de los recursos disponibles y brindados por lo suministradores Cloud.

Uno de los principales objetivos del proyecto es dar un énfasis y demostración del uso de servicios mediante el uso de Cloud Computing, llevando todo alojamiento de sistemas a este medio demostrando ventajas y desventajas que se pueden llegar a considerar con esta solución. De igual manera, es necesario saber y entender cómo funcionan los servicios de IaaS y PaaS en Microsoft Azure

En paralelo, se estudiaron casos de uso para las diferentes categorías nativas de Cloud lo que significa que también se hizo un estudio del sistema para un desarrollo y ejecución respectiva por parte del desarrollo PaaS.

Marketplace Azure (PaaS): Es la opción más sencilla y de poco costo a nivel de recursos que ofrecen ambos proveedores, sin embargo, por preferencia se hicieron las pruebas necesarias mediante un solo servidor como lo fue Microsoft Azure. Este es un servicio PaaS que como bien se sabe es el punto en el que se genera cierta parte del desarrollo creando aplicaciones que se mantienen en ejecución en la misma nube. Lo único que se hace dentro de esta plataforma es escoger las respectivas herramientas ya existentes como servicios y empezar a darles el despliegue que se considere necesario, dejando la responsabilidad de temas como escalabilidad y disponibilidad por parte del mismo proveedor.

Virtual Machines (IaaS): Es la alternativa más compleja respecto a PaaS, pero completa a su vez, es la única opción que permite un control robusto y su debida gestión sea completa que el mismo servicio PaaS, ya que desde este punto se hace énfasis en la asignación de recursos e infraestructura en la que se planea desarrollar. Primordialmente contamos con Microsoft Azure que garantizan una serie de servicios como Máquinas Virtuales y por medio de estas un almacenamiento adecuado y garantizado. Las instancias están a disposición de las necesidades requeridas haciendo que todo lo que corresponda a nivel de hardware sea totalmente transparente para los usuarios finales, permitiendo que su control y gestión se encuentre de manera virtual en todo momento.

Para la realización del diseño de la plataforma ***Aliviese-Pronto*** **®** se evaluaron tres grandes aspectos que fueron almacenamiento, procesamiento y conectividad cuando uno de estos agrupa diferentes características vitales para el correcto funcionamiento de la plataforma a continuación se realizara un análisis profundo acerca de cada uno de los ítems anteriormente nombrados.

Con el fin de realizar una valoración objetiva se le ha asignado un porcentaje a cada característica de cada grupo, dicha característica será evaluada en los dos servicios que se evaluaron IaaS (Infrastructure as a Service) y PaaS (Platform as a Service) para ello se asigna una calificación de 1 a 4 donde 1 es la peor calificación y 4 la mejor calificación en donde cumple con los requisitos y expectativas esperadas, dicha calificación tiene un nota final de acuerdo al porcentaje asignado y al final se obtiene una calificación total del Marketplace (PaaS) y otra de las máquinas virtuales (IaaS) en cada ítem mencionado anteriormente (almacenamiento, conectividad y procesamiento).

4.4. Almacenamiento

El almacenamiento es una parte fundamental en la creación de la plataforma la cual permite guardar la información de privada, publica y semiprivada para esto se hace uso de diferentes herramientas que admiten y facilitan la organización y visualización de dicha información.

1. ***Creación de base de datos:*** la creación de las bases de datos permitirá almacenar la información de todos los usuarios registrados en la plataforma en cualquiera de los roles definidos además creará un historial para las fórmulas de cada usuario. [27]

   El Market place crea una base de datos por defecto que viene incluida cuando se crea elige el plan de servicios, adicionalmente crea las tablas por defecto las cuales almacenan la información deseada de acuerdo los pluggins establecidos.
   En las máquinas virtuales se tiene la opción de elegir como se desea almacenar la información, en qué tipo de leguaje y definir instancias concretas lo que aumenta la seguridad.

2. ***Back up:*** El back up permite tener una copia de la información deseada en caso de que se cometa algún error humano o por fallas del sistema este podrá ser recuperado en una fecha y hora deseada. [28]

   El Market place ofrece un back up incluido en el plan de servicios el cual se realiza semanalmente de la base de datos creada por defecto en dicho servicio, adicionalmente ofrece una capacidad de recuperacion lenta.

   En cuanto las máquinas virtuales ofrecen un servicio de back up diario de la base de datos creadas y la red interna a un precio moderado y cuenta con capacidad de recuperación prácticamente inmediatas.

3. ***Gestión de bases de datos:*** resulta ser la característica mas importante en el ítem almacenamiento ya que la información que se va a tratar en la plataforma es delicada y necesita de seguridad y protección, además es necesario definir tablas específicas para el desarrollo de las actividades de cada rol definido. [29]

   El Market place no permite una gestión efectiva de las bases de datos, ya que al crearla por defecto dificulta el manejo de este y no permite desarrollas las actividades asignadas a cada rol con normalidad.
   En cuanto a las máquinas virtuales admiten qué se gestionen de todas las formas deseadas cuenta con un sin fin de posibles soluciones, pero al tener tantas opciones es necesario informarse y evaluar cuál es la más adecuada para el servicio es por esto qué se incrementa la curva de aprendiza sin embargo cumple con las expectativas y objetivos propuestos.

   A continuación, se muestra la calificación en cada una de las características evaluadas en los servicios IaaS y PaaS del ítem almacenamiento.

ALMACENAMIENTO					
Características	**Porcentaje**	**PaaS**		**IaaS**	
Creación BD	25	3	0,75	4	1
Back up	20	2	0,4	4	0,8
Gestión de BD	35	2	0,7	4	1,4
Directorio activo	20	3	0,6	4	0,8
TOTAL	**100**		**2,45**		**4**

Tabla. 2 Evaluación de almacenamiento PaaS vs IaaS

4.5. Conectividad

La conectividad es la herramienta que va a permitir al usuario ingresar a la plataforma de acuerdo a los permisos que tenga dependiendo el rol que vaya a ejecutar, con esto se tendrá conexión con la base de datos, permitiendo también realizar la autenticación con el directorio activo facilitando evidenciar quien realiza cada acción con el fin de buscar los responsables de estas.

Este ítem cuenta con varias características ya que para poder llegar a todos los usuarios es necesario hacer uso de múltiples herramientas es por esto que los porcentajes asignados a las características son similares porque todas las herramientas tienen gran importancia.

1. ***Dirección IP:*** la dirección IP es una dirección publica la cual identifica la plataforma y le permite obtener conexión a internet haciendo ubicua la plataforma ***Aliviese-Pronto ®***.[30]

   Tanto el Market place como las máquinas virtuales asignan una dirección IP publica que identifica el servicio y permite tener una correcta conexión con internet.

2. ***Grupo de red:*** El grupo de seguridad de red (NSG) contiene una lista de reglas de la lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a sus instancias de VM en una red virtual.[31]

   El Market place no permite crear un grupo de red debido a que la base de datos y el directorio activo se crean por defecto y no permite agruparlas en una red LAN diferente ya que estos vienen agrupados desde el plan de servicios.

   A diferencia de las máquinas virtuales que permiten la creación y agrupación de las máquinas virtuales en la LAN deseada configurada con las instancias deseadas.

3. ***Directorio Activo:*** El directorio activo, aunque cumple funciones de almacenamiento como se observó anteriormente también cumple en su mayoría funciones de conectividad ya que cada vez que el usuario va a ingresar a la plataforma se realiza la autenticación de clave y contraseña en este. [32]

Esta herramienta la brinda tanto el Market place como las máquinas virtuales, sin embargo, el Market place no permite gestionar fácilmente ya que se crea por defecto de acuerdo al plan de servicios que se elija, a diferencia de las máquinas virtuales que permite elegir y gestionar todos los aspectos deseados en el directorio activo

4. ***Seguridad de grupos*:** la seguridad de grupos permite agrupar las herramientas deseadas para identificarlas con mayor facilidad, administrarlas y gestionarlas con mayor facilidad.[33]

   El Market place al igual que las máquinas virtuales permiten crear la seguridad de grupos y configurar las instancias deseadas aumentando la seguridad de la plataforma.

5. ***Escalabilidad:*** la escalabilidad es la herramienta que permite aumentar la capacidad del servicio dependiendo la cantidad de usuarios que se conecten simultáneamente a la plataforma, el Market place y las máquinas virtuales ofrecen este servicio y el costo varía de acuerdo a los servicios que se deseen utilizar. [34]

6. ***Disponibilidad:*** en general la plataforma Microsoft Azure cuenta con 99.95% de disponibilidad para cualquiera de los servicios que ofrece sin embargo esta disponibilidad no puede ser la misma que ofrece el servicio ***Aliviese-Pronto ®*** debido a que no se tienen en cuenta factores externos como las fallas eléctricas es por esto que si se tomaran las fallas eléctricas que se presentan en Colombia se tendría una disponibilidad aproximada de 95% en el año tanto en el Market place como en las máquinas virtuales. [35]

7. ***DNS:*** el DNS es el nombre que se le asigna a la IP publica que Microsoft Azure brindo al servicio, este nombre es elegido desde que se crea de la plataforma y facilita al nos usuario el acceso a la plataforma ya que esté termina siendo la URL de la aplicación, dicho URL puede ser totalmente personalizado el cual tiene un costo mensual o se puede utilizar el formato estándar el cual no tiene ningún costo. [36]

A continuación, se muestra la calificación en cada una de las características evaluadas en los servicios IaaS y PaaS del ítem Conectividad.

CONECTIVIDAD					
Características	**Porcentaje**	**PaaS**		**IaaS**	
Dirección ip	15	4	0,6	4	0,6
Tarjeta de red	10	2	0,2	4	0,4
Vnet	15	1	0,15	4	0,6
Directorio activo	15	3	0,45	4	0,6
Seguridad de grupos	15	2	0,3	4	0,6
VPN	10	4	0,4	4	0,4
Escalabilidad	5	4	0,2	4	0,2
Disponibilidad	5	4	0,2	4	0,2
DNS	10	4	0,4	4	0,4
TOTAL	**100**		**2,9**		**4**

Tabla. 3 Evaluación de almacenamiento PaaS vs IaaS

4.6. Procesamiento

Procesamiento es el conjunto de herramientas donde se realiza el análisis de datos, incluye la velocidad de las máquinas y la velocidad con la que se pueden generar los informes, además de la rapidez con la que se puede ingresar a la plataforma.

1. ***Disco de datos:*** Un disco de datos es un disco duro virtual que se adjunta a una máquina virtual para almacenar los datos de la aplicación u otros datos que necesita mantener. Los discos de datos se registran como unidades SCSI y se etiquetan con una letra. [37]

   Aunque el servicio de PaaS maneja disco de datos esto se hace transparente al usuario ya que no es posible realizar alguna gestión sobre este, se crea con el plan de servicios y adicionalmente la información brinda es poca.

   Sin embargo, en el modelo de servicio IaaS si se tiene control sobre este a la hora de crear la máquina virtual y varia su precio de acuerdo a la cantidad de discos y capacidad que se deseen.

2. ***Núcleos CPU:*** Los núcleos de la CPU permite procesar la información de las maquinas virtuales tiene ayuda a que ese procesamiento sea más lento o más rápido. [38]

   Aunque el servicio de PaaS maneja núcleos de CPU esto se hace transparente al usuario ya que no es posible realizar alguna gestión sobre este, se crea con el plan de servicios y adicionalmente la información brinda es poca.

   Sin embargo, en el modelo de servicio IaaS si se tiene control sobre este a la hora de crear la máquina virtual y varia su precio de acuerdo a la cantidad de núcleos de CPU capacidad que se deseen.

3. ***Ancho de banda:*** Calcular el uso del ancho de banda por usuario es muy complejo y requiere la ejecución de varias aplicaciones simultáneamente en escenarios multitarea donde las aplicaciones podrían influir en el rendimiento de la otra basándose en la demanda del ancho de banda de red. Incluso el tipo de cliente de escritorio remoto (por ejemplo, un cliente de Mac frente a un cliente de HTML5) puede provocar resultados diferentes de ancho de banda. [39]

4. ***RAM:*** Tipo de memoria a la que se accede aleatoriamente, se puede acceder a cualquier byte de memoria sin acceder a los bytes precedentes. La memoria RAM es el tipo de memoria más común en ordenadores y otros dispositivos como impresoras.

   Aunque el servicio de PaaS maneja memoria RAM esto se hace transparente al usuario ya que no es posible realizar alguna gestión sobre este, se crea con el plan de servicios y adicionalmente la información brinda es poca.

   Sin embargo, en el modelo de servicio IaaS si se tiene control sobre este a la hora de crear la máquina virtual y varia su precio de acuerdo a la cantidad de memoria RAM y capacidad que se deseen.

A continuación, se muestra la calificación en cada una de las características evaluadas en los servicios IaaS y PaaS del ítem almacenamiento

PROCESAMIENTO					
Características	**Porcentaje**	**PaaS**		**IaaS**	
Disco de datos	20	1	0,2	4	0,8
Núcleos de CPU	15	2	0,3	3	0,45
Memoria	20	2	0,4	3	0,6
Ancho de banda	20	3	0,6	4	0,8
RAM	15	3	0,45	4	0,6
TOTAL	90		1,95		3,25

Tabla. 4 Evaluación de desempeño en procesamiento IaaS vs PaaS

4.7. Arquitecturas Planteadas Para el Desarrollo del Sistema

Microsoft Azure (PaaS): Para la elaboración del sistema y completar su desarrollo mediante las especificaciones anteriormente nombradas se tienen en cuenta todos los conceptos requeridos y a su vez se plantean los esquemas pertinentes al funcionamiento que se desea dar al sistema, empleando los servicios que sean necesarios por parte de ambos proveedores y de esta manera establecer cuales cumplen con los alcances que se desean.

Por lo tanto, se evaluarán los posibles métodos por los cuales se realizará el producto; en primera instancia se cuenta con una alternativa rápida y sencilla con un servicio a nivel PaaS el cual fue realizado con el fin de tener en cuenta en alcance que este puede tener, haciendo análisis en cuanto a las posibilidades que este genera con su gran variedad de ventajas y eficacia al realizarse sin embargo cuenta con un gran fallo.

Este medio no es del todo controlable ni gestionable por el administrador en su totalidad puesto que cuenta con varios servicios limitados, uno de estos fue el control de almacenamiento, lo que quiere decir que las bases de datos no pueden ser manipuladas, sino que se restringen las posibilidades a las que esta plataforma proporciona. De modo que es un servicio útil si las necesidades fueran diferentes o el ambiente de ejecución tuviera otras condiciones menos exigentes, por lo cual este esquema que se muestra a continuación fue planeado según lo que se aproxima a lo que se desarrollara.

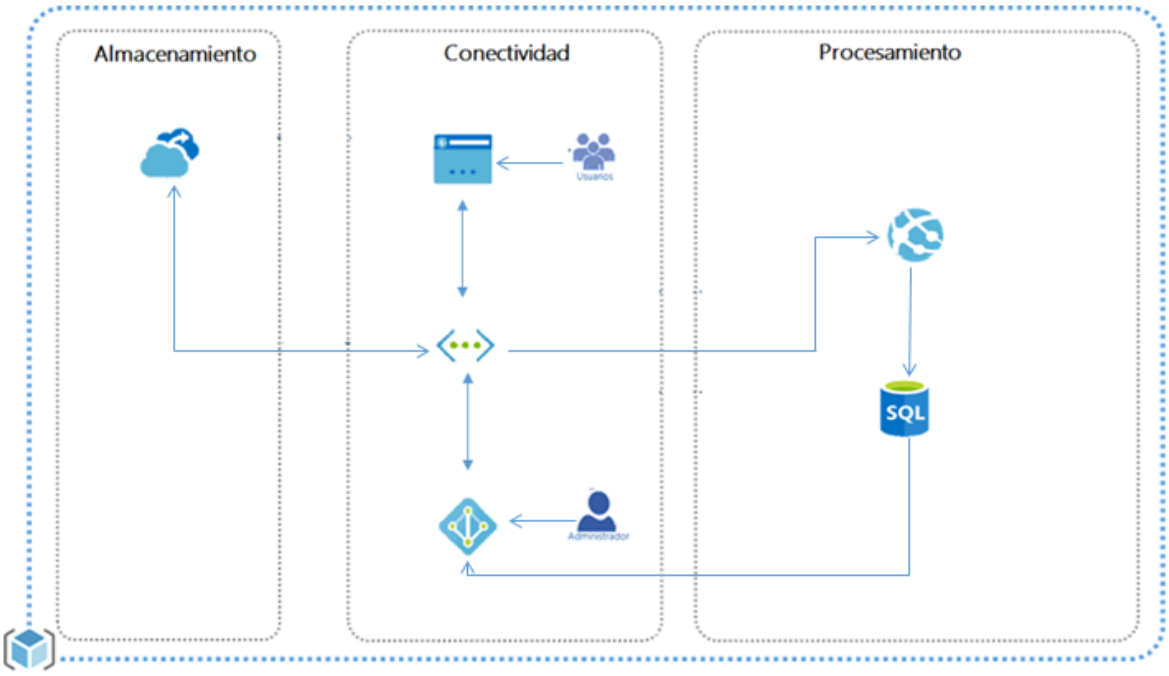


Figura 1. Esquema Marketplace Azure, creación servicio PaaS.

Máquinas Virtuales Microsoft Azure (IaaS): En la planeación del Sistema de laboratorios médicos, se hace el esquema pertinente a nivel de IaaS lo que permite un desarrollo personalizado el cual es lo que sería lo correcto para la ejecución de este.

De esta manera se plantean hacer la adquisición de servicio propios de este proveedor como lo es Microsoft Azure haciendo el uso de Máquinas Virtuales con el fin de emplearlas como servidores, manteniendo aisladas ambas instancias por seguridad y haciendo independiente cada uno de los servicios a incorporar dentro de ellas.

Se busca que estas instancias compartan el uso de una red privada el cual identifique los servicios para las conexiones que sean necesarias, haciendo que para una instancia exista su servicio correspondiente como es el de almacenamiento y consultas mediante servicios de

Bases de Datos; por otra parte, el servidor WEB que le dará toda la ejecución y soporte para que la disponibilidad del sistema siempre permanezca. A continuación, se hace la distribución de elementos necesarios para el desarrollo del servicio.

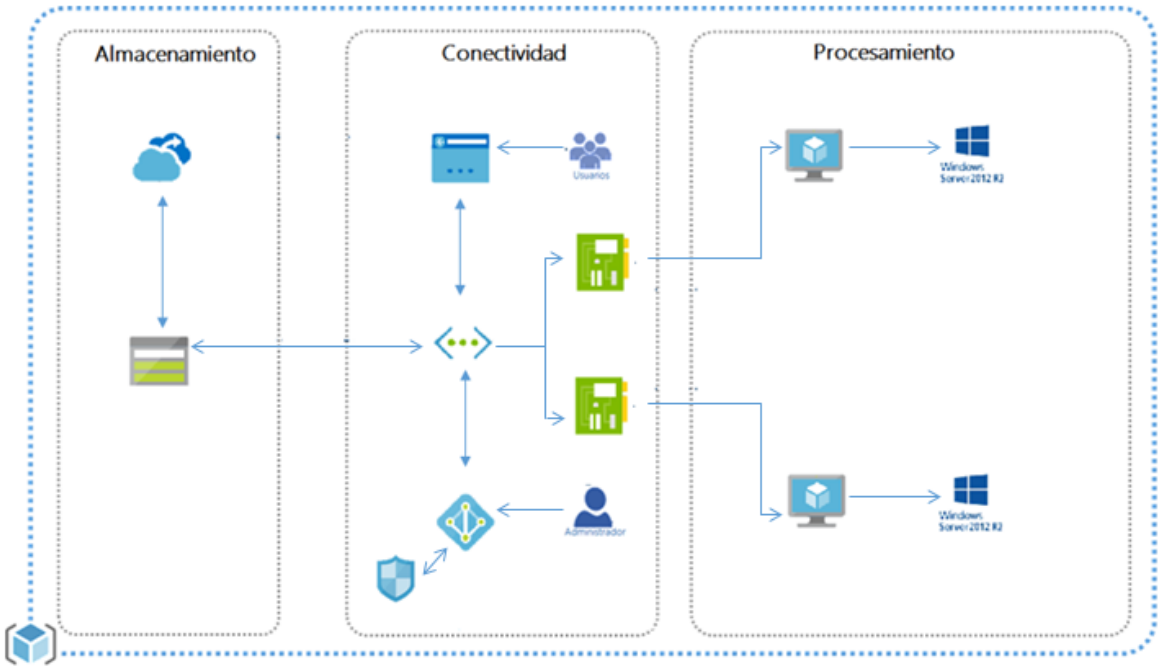


Figura 2. Esquema Máquinas Virtuales en Windows Azure, creación servicio IaaS.

4.8. Evaluación y Conclusiones a Metodologías a Implementar

De acuerdo a las planeaciones elaboradas anteriormente, cada esquema fue evaluado con el fin de entender qué servicio era el más apropiado para el desarrollo del sistema haciendo énfasis en su funcionalidad y sin olvidar que se espera prestar el servicio con la mayor disponibilidad presente a cada uno de sus usuarios, ya sean clientes o administrativos.

Por ello se revisaron las dos posibilidades mencionadas anteriormente teniendo en cuenta las especificaciones del sistema, obteniendo por conclusión que unos de los dos esquemas presentan un mejor despliegue y mayor cobertura a la prestación del servicio que uno en especial. Dicho esto se hará todo el desarrollo y proceso mediante el uso de Infrastructure as a Service (IaaS), ya que al hacer el análisis respectivo por parte de la elaboración del sistema mediante Platform as a Service (PaaS) sus funcionalidades estarían estrictamente restringidas por el alcance de la plataforma y esto sería un incidente a futuro, puesto que si se desea tener una gestión y control completa del servicio se espera hacer mención a lo que son sistemas operativos, Bases de Datos, manipulación de contenido, disponibilidad, asignación de roles y permisos, entre otros, por lo tanto el entorno de desarrollo será el más apropiado para la solución de los objetivos y alcance del proyecto.

Desarrollo y ejecución planteada para el Producto Mínimo Viable en solución de un servicio de administración de farmacias, bajo modelo de servicio IaaS y PaaS.

El Producto Mínimo Viable que se hace presente obtuvo dentro de su despliegue una serie de pasos para su funcionamiento, puesto que al hacer uso de las plataformas Cloud se deben tener en cuenta ciertas características y aspectos que estos ofrecen, haciendo el servicio eficaz y funcional para lo que se esperaba realizar, por lo tanto, se describirán todas las pautas necesarias para la plataforma ***Aliviese-Pronto*** ®.

4.9. Creación y Configuración de los Servicios a Utilizar

Para la creación de los servicios expuestos como proyecto, se da iniciación al proceso mediante la creación y respectiva configuración de los servicios pertinentes a los proveedores a utilizar, haciendo uso de las máquinas virtuales como tal, para dar creación al servicio IaaS que se pretende desarrollar.

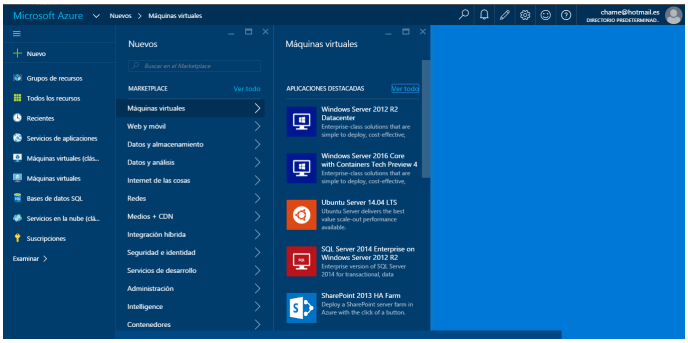


Figura 3. Creación de las máquinas virtuales.

Creamos las estancias necesarias para los servicios, permitiendo que cumplan con las condiciones deseadas, por lo que damos origen de las máquinas virtuales de la siguiente manera:

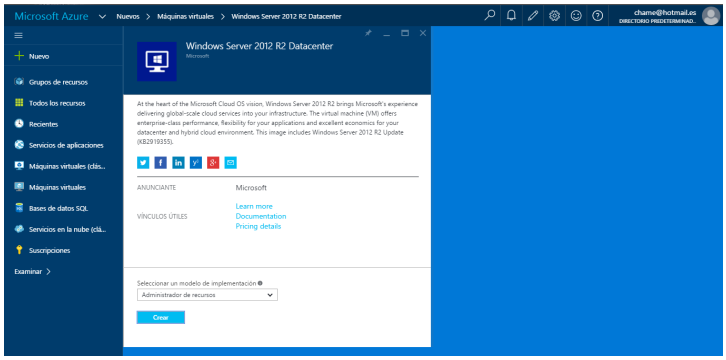


Figura 4. Selección de las instancias y Aprovisionamiento.

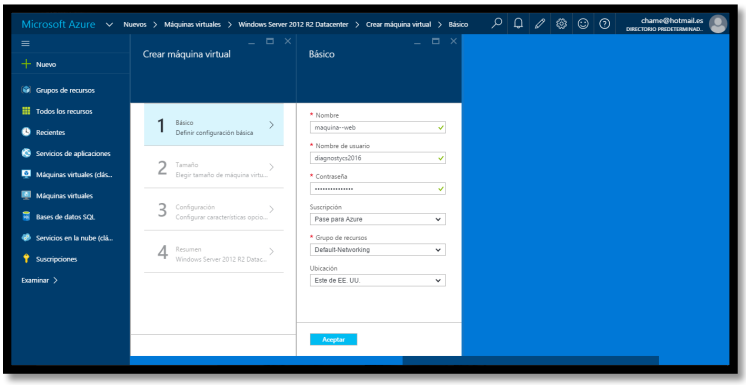


Figura 5. Elección de características Principales en Máquinas Virtuales.

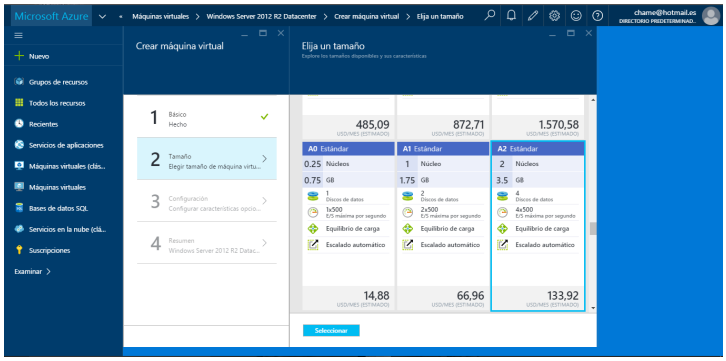


Figura 6. Selección de Características Físicas de las Máquinas Virtuales.

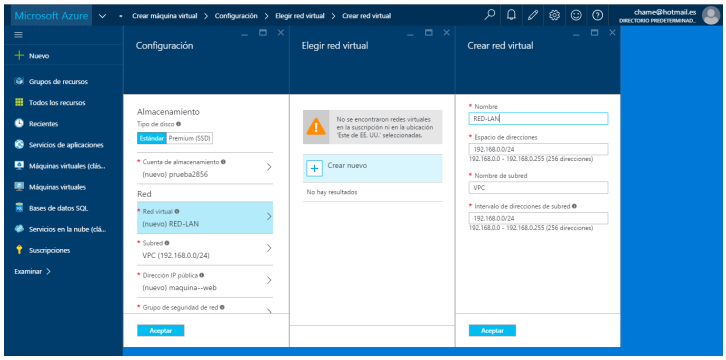


Figura 7. Creación de Grupo de Red

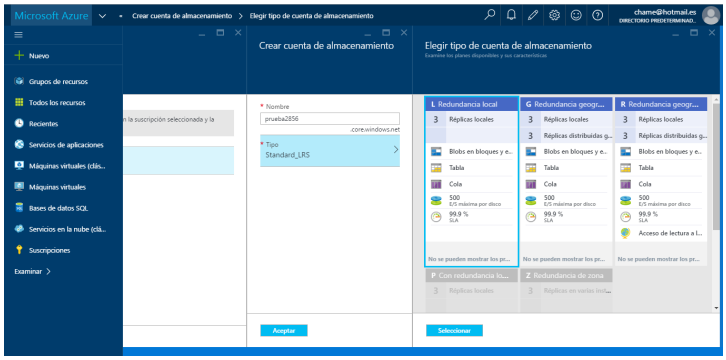


Figura 8. Configuración elemental de Almacenamiento en Servidores SQL.

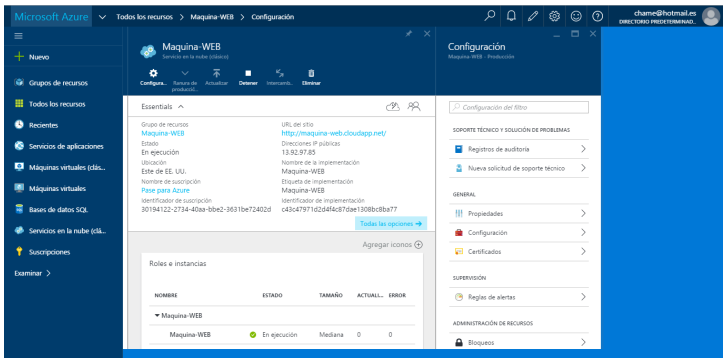


Figura 9. Visualización de ejecución de las instancias.

Teniendo en cuenta las especificaciones requeridas se hará el uso de un sistema operativo de Windows Server 2012 R2, de acuerdo a sus características y debido a ser uno de los más recientes sistemas operativos de Windows. Esta elección también corresponde al criterio en que los usuarios convencionales están acostumbrados a manipular servicios Windows por lo que otro sistema operativo seria desconocido para aquellos que al final pretendan manipular el servicio.

Teniendo presente las funcionalidades que se le asignaran a las máquinas virtuales, se necesitan condiciones como el tamaño de procesador y disco duro de cada máquina, debido a que el trabajo que se les va a establecer a correr debe tener un rendimiento y una disponibilidad dedicada no pueden ser una de las instancias más económicas, sin embargo no significa que se haga elección de una instancia con mayor rendimiento al que realmente se necesita, por estas condiciones se escogió una maquina media entre los rangos de elección. En paralelo a estos criterios fue necesaria la creación de un grupo de red (VPC), con el fin de mantener la conectividad entre las instancias creadas haciendo más fácil el proceso de conexión entre estos de acuerdo a los servicios que se ejecutaran, puesto que los servicios se mantienen independientes uno de otro por medidas de seguridad y así mismo de respaldo permitiendo que ningún fallo en ellos intervenga en el servicio de otras instancias.

Dicho esto, se prosigue a configurar uno de los pasos más importantes para la implementación del servicio y es contar con un espacio de almacenamiento dedicado, el cual cuente con una capacidad considerable para el tipo de archivos que se desean almacenar. Por esta razón se hace la creación de un Disco Duro (SSD), el cual permanezca fijo en la máquina para tener el acceso necesario a este componente y dar el uso adecuado, con un tamaño de 1TB aproximadamente para realizar todas las pruebas necesarias.

Por último y el paso más importante de esta creación y configuración, son las reglas a establecer a las instancias, lo que quiere decir que es necesario dar permisos a cada máquina con el fin de poder tener control en cuanto conexiones, conectividad y relación a las demás instancias, puesto que al tratar el tema de lo que son servicios WEB y Bases de Datos siempre existirán procesos de comunicación lo cual se conceden dando permisos a diferentes puertos.

Se concluye todo este proceso con la visualización de las instancias creadas con sus respectivas características y todo lo implementado se encuentra en detalle para cada servicio.

De tal manera se tendrían listas las instancias para ejecutarse y dar inicio a la creación de los servicios que se esperan realizar por cada máquina.

4.10. Instalación de Servidor de Aplicaciones

Al tener las máquinas virtuales ya en completas condiciones se procede a dar servicio en cada una de ellas, por lo que se tendría que en una de estas se implementara un servidor WEB que permita el despliegue del servicio IaaS de manera gráfica o visual para los respectivos usuarios. A partir de esto, se cuenta con la inicialización de esta instancia el cual permita un control completo de los servicios.

Al encontrarse dentro de la instancia, se hará uso de un aplicativo hecho por terceros llamado GlassFish el cual es un software que permite la implementación de tecnologías definidas por lenguaje Java haciendo que dichos servicios se ejecuten por medio de este según las especificaciones, por lo tanto, se tendrá la instalación de este servidor de aplicaciones para mayor beneficio en los servicios que se realizaran. La instalación se lleva manual desde el mismo sistema haciendo las descargas pertinentes y las configuraciones guiadas por el mismo software.

4.11. Configuración de Servidor de Aplicaciones

Seguido a estos parámetros de administración, para tener y desplegar un mejor servicio de control de este servidor de aplicaciones, se hace una debida configuración de cliente de uso, el cual permita un acceso remoto de este servicio, permitiendo en cualquier momento que se desee brindar servicios se pueda tanto iniciar como detener las instancias con el contenido definido a presentar por medio de publicaciones web.

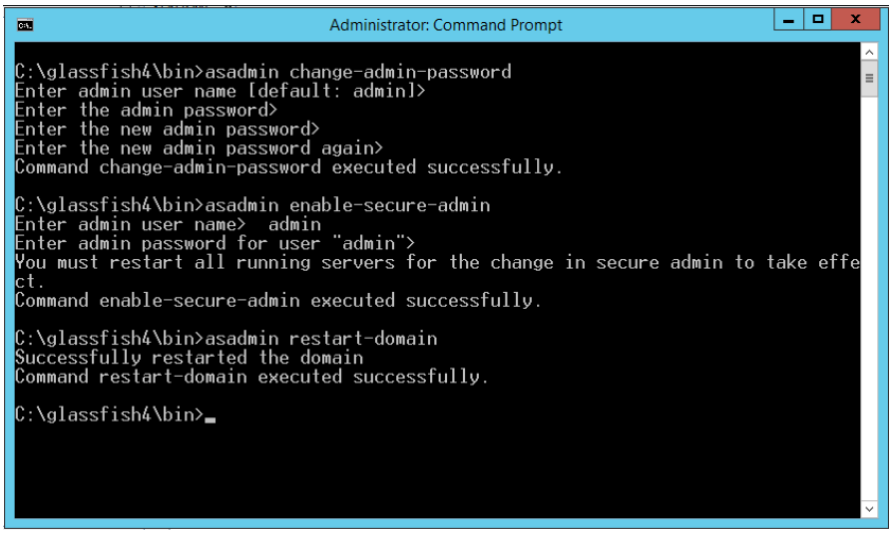


Figura 11. Creación de perfil administrativo en servidor de aplicaciones GlassFish.

Como se observa en la imagen presentada, se visualiza la creación de un usuario el cual tenga acceso y a su vez control sobre este, por lo que se le hace la debida asignación de un perfil tanto con usuario como contraseña para proteger su acceso remoto. Luego de esto

se hace evidencia de la seguridad que contiene este nuevo usuario de manera que el dominio creado mediante este servidor de aplicaciones le corresponda el completo acceso y único acceso a dicho usuario con debida seguridad. Por último, se hace el reinicio del servicio para comprobar con éxito la existencia del administrador, para que a futuros cambios ya no es necesario ingresar por completo al sistema, sino que conociendo el dominio o dirección del servidor se pueda tener un ingreso automático.

4.12. Configuración del Servidor de Bases de Datos (SQL Server)

Como segunda instancia se implementará para el correcto funcionamiento del servicio, un servidor SQL debido a que en medio de lo que se espera realizar como servicio para laboratorio médico, es necesario el almacenamiento en masa de información personal, registros, consultas, datos, dirección de rutas y la prestación del servicio completo.

Para ello se hace énfasis en la instancia creada para estos datos SQL-Server el que se inicia mediante la depuración de la máquina virtual creada ya previamente en los primeros pasos, siguiente a esto es necesario crear un perfil de administrador de manera similar a la configuración del servidor de aplicaciones GlassFish, con el fin de tener un usuario que se pueda autenticar para la gestión pertinente de la información que se espera almacenar.

Se hace la respectiva creación de usuario administrador, con el fin de mantener las bases de datos creadas dentro de este, permitiendo que el contenido y su gestión se administre de manera correcta y resolviendo la necesidad de realizar conexiones con servicios futuros el cual garanticen una conexión exitosa a la base de datos mediante dicho usuario. Dentro de esta instancia se hará la creación de campos necesarios a medida que vayan surgiendo necesidades para la plataforma a implementar, campos validos como para formatos, formularios, registros, entre otros.

Teniendo en cuenta los registros que se esperan almacenar, es relevante hacer la aplicación de cada uno de los campos requeridos para el buen funcionamiento del servicio, de manera que se tiene la creación de los respectivos roles para el servicio, haciendo énfasis en las aplicaciones de cada uno de estos y la relación que se crea entre ellos para llevar en correcto orden el almacenamiento deseado. Dicho esto, se prosigue a iniciar sesión mediante el perfil creado y a dar inicio y ejecución a las tablas con sus respectivos campos que sean necesarios para todo el despliegue de la aplicación. A continuación, se hace evidencia de las tablas que son importantes entender para darles la relación entre ellas de manera correcta, con el fin de hacer un almacenamiento correcto y organizado para cada uno de los roles involucrados en el proceso.

Al hacer énfasis en todos los campos y tablas necesarias a crear, se puede ver el despliegue que se quiere dar por medio del servicio de Bases de Datos, en donde se evidencian las tablas que serán utilizadas en relación a los roles, situación, personas y momentos necesarios de almacenamiento; debido a que se trata de un servicio de laboratorios médicos, se hace inclusión a cada uno de los servicios que se pueden llevar a cabo con cada una de las personas involucradas con el sistema, teniendo siempre en cuenta el debido archivador de cada datos por mínimo que se llegue a considerar.

4.13. Modelo Entidad-Relación para Funcionamiento de Bases de Datos

En búsqueda del funcionamiento deseado mediante la conexión SQL al servicio WEB que se implementara, en primera instancia, es pertinente dar una organización adecuada y al mismo tiempo establecer un esquema basado en cuanto Entidad-Relación para darle función a las tablas que se quieren utilizar, por lo que a través de este modelo se hará entender de manera clara y certera la relación que existe entre los diferentes elementos a utilizar en el servicio.

Dicho esto, se hace énfasis en las tablas ya previamente involucradas y en el servicio que se quiere establecer y junto a eso un mapa de lo que generaría el servicio con los datos implementados, de tal forma que por cada ítem exista una relación definida, dándole el valor y función que se esperaría tener.

Este modelo se hace con las especificaciones aginadas a en las tablas del servidor SQL de forma que, al hacer cada campo dentro de cada elemento, se tiene una asociación entre ellos, esto permite que, al tener la relación deseada y vital del funcionamiento del sistema, se genere un código de consulta ‘Query’. Este código establece de manera lógica las mismas relaciones que se entienden visualmente, es decir, este mismo modelo se plantea de manera escrita automáticamente por cada vez que se establecen conexiones.

Para la realización del diagrama se usó como software Visual Studio 2010 ya que permite una mejor lógica y de fácil manejo permitiendo que las relaciones si se asignen como se plantean. Al ejecutarse tal cual como viene del Visual Studio se crean automáticamente las relaciones a aplicar al servicio, por ende, no es necesario especificar las entidades por cada elemento mencionado, simplemente establecer bien la nueva consulta esperando que ejecute de manera correcta.

Figura 12. Modelo entidad relación

4.14. Ejecución del Ambiente de Desarrollo para Servidor WEB

Al dejar el servidor SQL ya previamente configurado, lo último que se necesita de este servicio, es la dirección a conectar a futuro el servicio WEB con el servidor SQL, de manera que al hacer presente ambos servicios no exista dificultad con la debida conexión, y así mismo con el almacenamiento y procesos que conlleva todo el servicio. Los primeros pasos

para llevar el desarrollo y despliegue del servicio WEB cuentan con el servidor de aplicaciones GlassFish como ya anteriormente se mencionó.

Evidentemente este no cumple con toda la funcionalidad requerida para el proceso deseado, por lo que se hace necesario obtener herramientas que se acoplen a este lenguaje y tengan mejor conexión con otros servicios, mencionado esto se hace la instalación de un nuevo software dentro de esta instancia llamado NetBeans 8.1, se hace preferencia por esta aplicación debido a que son creaciones de un mismo proveedor tanto GlassFish como NetBeans por lo que permite una mejor conexión para el desarrollo de la aplicación WEB permitiendo mejores desarrollos y resultados satisfactorios para lo que se espera realizar.

Para la creación de cada uno de los módulos requeridos para el despliegue de la aplicación, se debe tener en cuenta primero el desarrollo creado por parte del servidor SQL, de modo que la conexión siempre permanezca haciendo que el servicio cuente con la implementación de las Bases de Datos y todo almacenamiento se ponga a prueba a partir de los que se desarrolle por medio de esta instancia.

Para conseguir dicha conexión, es necesaria la implementación de una red LAN entre las máquinas virtuales la cual permitirá que exista conectividad entre las instancias y así evitar problemas futuros de conexión, teniendo ambos enlaces unidos a una misma red privada que proporcionan los mismos proveedores; esta red se crea con el fin de hacer pruebas y de la misma manera permitir una conexión entre los servicios, asignando direcciones IP a cada máquina debido a la conexión que se necesita.

Se realiza una conexión nueva en el Software NetBeans directamente con la dirección IP del servidor SQL, puesto que en el entorno de desarrollo es muy importante dar valores a cada parámetro siempre y cuando se tenga conectada la Base de Datos; luego de generar todo el desarrollo pertinente no se tendrá en cuenta más la conexión por este medio sino que será remplazado el enlace directo mediante el servidor de aplicación que se empleó, haciendo el papel de controlador entre los servicios para que se ejecuten de manera correcta y simultánea.

Lo siguiente a tener la conexión entre los servicios ejecutándose de manera correcta, lo pertinente a realizar a continuación es la creación de cada uno de los módulos del aplicativo, empezando el desarrollo mediante la implementación de lenguaje Java para el funcionamiento y procesos internos de este y por otra parte el ambiente mediante desarrollo en HTML que permitirá dar presentación gráfica y visual al servicio mientras se va dando desarrollo y funcionalidad al servicio.

Para este ambiente se implementa el uso de lenguajes vitales del entorno de desarrollo tal como lo fue Java, debido a que la conexión con el servidor de aplicaciones era eficaz por este medio y permitía un enlace directo y de igual manera con la conexión de bases de datos ejerciendo un enlace menos complejo de terminar. Por otra parte, el desarrollo web se completó con esquemas básicos de estilos y diseños médiate implementación de CSS y HTML el cual permitieron mayor organización en cuanto a la definición de contenidos y datos a emplear en la ejecución del servicio.

4.15. Encapsulación del Aplicativo WEB

Para obtener la publicación y ejecución del sistema luego de haber creado todo el contenido con sus respectivas actualizaciones y servicios en correcto funcionamiento, es pertinente la encapsulación de los servicios al mismo servidor, lo que quiere decir que al tener las instancias de manera independiente estas se conectan mediante el servidor de aplicaciones GlassFish, de manera que el aplicativo Web creado mediante el software NetBeans establece la conexión al servidor SQL y de la misma manera se hace ese proceso con la conexión al servidor web el cual se realiza mediante el uso de GlassFish, permitiendo a este servidor de aplicaciones hacer el enlace requerido para el sostenimiento del sistema, creando la unificación por parte de ambos servicios para que quede el complemento por parte de ambos.

De esta manera el servicio ya está en completo funcionamiento puesto que ambas instancias quedan integradas al servidor de aplicaciones y corren de manera correcta y su ejecución es la ideal. Por último, se debe aclarar que el servicio que se encuentra ubicado en el software NetBeans y todo lo que corresponde al entorno de desarrollo del sistema fue hecho en una maquina privada con la seguridad y el respaldo que permite el alojamiento de mantener el sistema en estas condiciones, ya que el ideal es a partir de una maquina propia ejecutar todas las actualizaciones y cambios necesarios al servicio sin alterar su funcionamiento, lo que permite que todas las pruebas sean realizadas de manera local sin intervenir su publicación ni contenido de lo que se ubica en la nube.

Por lo tanto, fue necesario hacer la conexión del servidor de aplicaciones con la instancia ubicada localmente, lo que daba lugar a que toda actualización que fuera debida realizar para el buen funcionamiento del servicio, primero se ejecutara en un Local Host permitiendo analizar cualquier tipo de fallo o error que se encontrara en plena ejecución del sistema y de esta manera solucionarlo antes de tiempo. Luego de atender a todas las demandas pertinentes se proseguía a dar este tipo de cambios a los servidores alojados en la nube, por medio de la conexión que ya se habían establecido desde un principio por parte de las creaciones de cada instancia

Una de las razones fundamentales de mantener el servicio aislado de manera local, es permitir que este solo sea diseñado e implementado por sus creadores y no dar su comercialización en cuanto al contenido, parte funcional y lógica que esta lleva a cabo.

4.16. Comparación de costos, rendimiento e implementación del Producto Mínimo Viable

Uno de los parámetros fundamentales en el desarrollo del proyecto fue el análisis de producción y de costos, tema en el cual se llega a tener un mayor énfasis a la hora de promocionar y ofrecer el producto final tanto para el inversionista Ángel como para las farmacias.

Por lo tanto, es importante mencionar y especificar en detalle los recursos necesarios que se tuvieron en cuenta para el desarrollo de la plataforma Aliviese-Pronto, y con ello resaltar los costos en dólares de cada uno de los elementos que componen el Producto Mínimo Viable, con el fin de brindar un presupuesto muy aproximado de los gastos por uso

de los servicios que provee Microsoft Azure. Inicialmente en la figura xx se pueden observar dichos servicios provenientes de Microsoft Azure para el desarrollo de la plataforma en el modelo de nube IaaS.

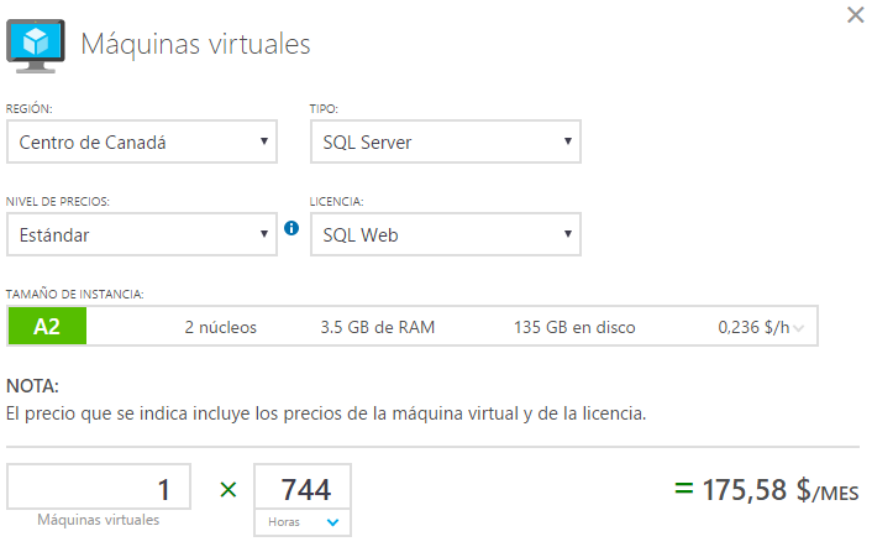


Figura 13. Costo máquina virtual

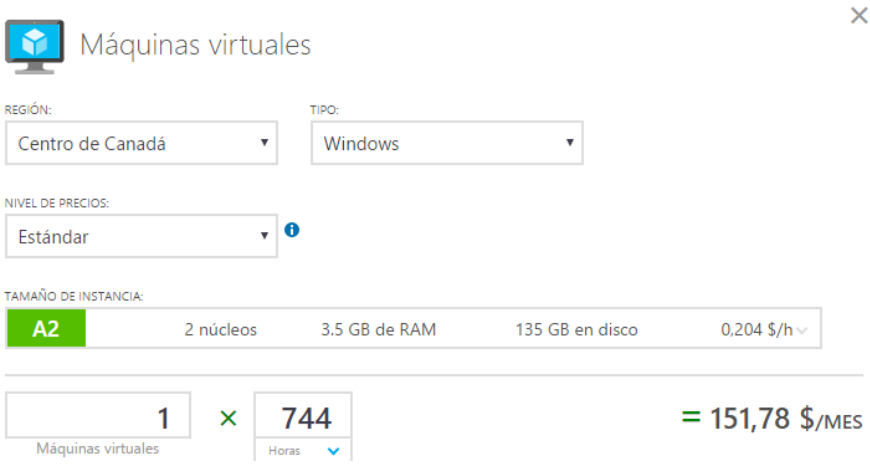


Figura 14. Costo máquina virtual

Para evidenciar un consumo más amplio de los recursos de la plataforma Aliviese-Pronto, se realizó una prueba estudio en este modelo durante 9 días aproximadamente para poder observar el consumo real de los recursos instalados que provee Microsoft Azure.

Costes de recursos

NOMBRE	TIPO	GASTO ACTUAL (USD)
AliviesseProntoD	Máquina virtual	32,19
AliviesseProntoW	Máquina virtual	9,20
alivieseprontо	Cuenta de almacenamiento	0,62
AliviesseProntoD-ip	Dirección IP pública	0,23
AliviesseProntoW-ip	Dirección IP pública	0,23
dscExtension	Máquina virtual	0,00
SqlIaasExtension	Máquina virtual	0,00
alivieseprontod526	Interfaz de red	0,00
alivieseprontow338	Interfaz de red	0,00
AliviesseProntо	Grupo de seguridad de red	0,00
AliviesseProntо-vnet	Red virtual	0,00

Figura 14. Costo elementos de trabajo

Luego de observar los costos de creación y sostenimiento de la plataforma Aliviese Pronto en el modelo IaaS, queda por resaltar los gastos del otro modelo PaaS. Ver tabla 5.

TAMAÑO DE INSTANCIA	NIVEL DE PRECIOS	NUCLEOS	GB de RAM	GB STORAGE	COSTO / HORA	
S1	Estándar	1	1.75	50	0.102 $ / h	74.40 $ / MES

Tabla. 5 Costo máquina virtual

Las características por las cuales se paga este tipo de recurso son principalmente porque cuenta con las características básicas para la creación y el funcionamiento de las dimensiones de Aliviese-Pronto. Ya que a parte de las características descritas en la tabla xx también ofrece un escalado automático, administrador de tráfico, backup, y otras características que hacen que sea un servicio funcional.

El análisis comparativo de costos y rendimiento de la plataforma Alíviese Pronto brinda una visión más acertada de lo que se puede lograr con cada uno de los modelos de nube en el que se implementó el Producto Mínimo Viable. Ya que, por un lado, ofrece unos costos supremamente bajos, pero con unas limitaciones considerables en el rendimiento y la funcionalidad, mientras que por otro lado se encuentra el modelo IaaS que es la clara evidencia de “Pay as you Go”, es decir, pagar por lo que vas utilizando. Razón por la cual como se evidencio en las figuras xx es más costosa, pero con unas ventajas considerables como lo son el control absoluto de los recursos implementados y una gestión administrativa mucho más amplia.

Por lo que se llega a la conclusión que, para poder brindar un Producto Mínimo Viable capaz de competir en el mercado de las grandes industrias, es necesario adoptar el modelo de negocio IaaS, invirtiendo así un poco más en cuanto a costos y tiempo se refiere.

Para evidenciar un consumo más amplio de los recursos de la plataforma Aliviese-Pronto, se realizó una prueba estudio en este modelo durante 9 días aproximadamente para poder observar el consumo real de los recursos instalados que provee Microsoft Azure.

Costes de recursos

NOMBRE	TIPO	GASTO ACTUAL (USD)
AliviesepProntoD	Máquina virtual	32,19
AliviesepProntoW	Máquina virtual	9,20
aliviesepronto	Cuenta de almacenamiento	0,62
AliviesepProntoD-ip	Dirección IP pública	0,23
AliviesepProntoW-ip	Dirección IP pública	0,23
dscExtension	Máquina virtual	0,00
SqlIaasExtension	Máquina virtual	0,00
aliviesepprontod526	Interfaz de red	0,00
aliviesepprontow338	Interfaz de red	0,00
AliviesePronto	Grupo de seguridad de red	0,00
AliviesePronto-vnet	Red virtual	0,00

Figura 15. Costos elementos de trabajo.

Microsoft Azure muestra el consumo en horas de proceso con un total de 119,85 horas del servicio disponible y funcionando, por un cobro de 19,18 dólares por los componentes utilizados; este consumo refleja un total de $0,16 dólares por cada hora en que este se encuentra disponible la plataforma Aliviese-Pronto. Consumiendo aproximadamente 5.85 dólares / día. Ver figura 16.

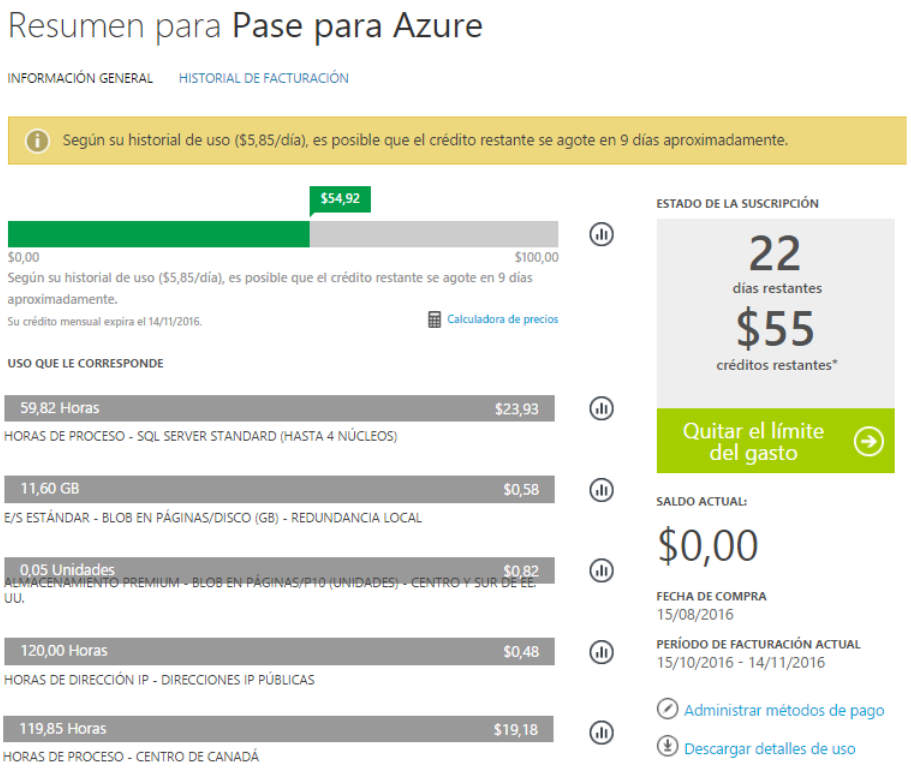


Figura 15. Resumen de costos de los elementos de trabajo en semana.

5. Viabilidad de *Aliviese-Pronto* ® para un inversionista ángel.

5.1. Implementación de ciclo de sobre exposición de Gartner

1. ***I&D – Investigación y Desarrollo:***

   Se inicia con la investigación de uno de los proveedores líderes de computación en la nube según el cuadrante mágico de Gartner, para implementar así el desarrollo de la plataforma de administración de farmacias "*Alíviese Pronto"*, con el fin de optimizar los procesos del manejo de inventario, incluyendo la reducción de costos y prestar un servicio estable tanto para los administradores de las farmacias, los vendedores en cada uno de los puntos y los clientes.

2. ***Lanzamiento, primera financiación de capital de riesgo:***

   Contando con el desarrollo del producto mínimo viable es necesario obtener la primera inversión de capital de riesgo, por lo cual se da a conocer este producto mínimo viable a los inversionistas Ángel, con el fin de obtener capital que permita continuar con un mejor modelo de operación y servicio para la plataforma de administración de las farmacias.

3. ***Servicio Droguería alíviese pronto 1.0:***

   Sale al mercado la primera generación de nuestro servicio para aquellas farmacias que adquieran esta plataforma, el costo de este es alto ya que es un producto innovador y las fallas son inevitables.

4. ***Adaptación de investigaciones:***

   Se realizan estudios, tanto en cuentas como en estadísticas para observar cuales son las fallas que está presentando nuestro servicio, para así satisfacer todas las necesidades del cliente; se inicia una nueva etapa de investigación y desarrollo en la que se corrigen y adaptan las sugerencias y reclamos del cliente.

5. ***Publicidad:***

   Teniendo satisfechos a nuestros primeros clientes que adoptaron la implementación de nuestro servicio, se realizara un plan de mercadotecnia para así poder difundir nuestra plataforma en los medios de comunicación, resaltando la importancia y los beneficios que conlleva adoptar este servicio en sus negocios para tener un nivel de competitividad mayor.

6. ***Punto de máxima adaptación:***

   Ya que el servicio funciona correctamente y la publicidad fue efectiva, nuestro servicio se comienza a vender en masa, y los consumidores aumentan día a día al

igual que las operaciones, por lo cual se comienzan a observar las utilidades netas del servicio.

De la misma manera al contar con un gran crecimiento de nuevos clientes se percibirán nuevas necesidades y por ende mejoras que se tendrán que desarrollar e implementar en la plataforma ***Aliviese-Pronto ®***

7. ***Comienzo periodo negativo:***

   Ya que la mayoría de nuestros potenciales clientes han adquirido nuestro servicio y se han adaptado a él, y con los nuevos requerimientos o necesidades de los clientes, se presenta la disminución de interés en el servicio, comienzan a bajar las ventas en nuestra compañía.

8. ***Consolidación y fracaso de suministradores:***

   Las tecnologías entran en el abismo de desilusión porque no se cumplen las expectativas. Por lo cual se realiza una investigación de los posibles suministradores para consolidar el mejor servicio de calidad con precios competitivos en el mercado de las farmacias.

9. ***Segunda inversión de capital de riesgo:***

   Es necesaria una segunda inversión de capital de riesgo de nuestro inversionista Ángel, ya que es necesario realizar modificaciones al servicio, contemplar las nuevas necesidades de los clientes, e innovar nuevamente en la plataforma para llamar la atención de nuevos clientes y proveer un mayor valor agregado.

10. ***Menos del 5% de la audiencia potencial ha adoptado completamente:***

    Después de contemplar las modificaciones pertinentes al servicio y las nuevas reestructuraciones a la plataforma *"Aliviese Pronto"*, es necesario retomar la idea de realizar un lanzamiento publicitario de la nueva versión con el fin de obtener clientes fieles que adopten nuestro servicio plenamente, dichos clientes ofrecerán cierta estabilidad a la compañía.

11. ***Servicio Droguería alíviese pronto 2.0:***

    Se realiza el desarrollo de las nuevas funcionalidades y herramientas de "Aliviese Pronto", para brindarle a las farmacias las nuevas mejoras implementadas y los nuevos valores agregados con los que podrán contar adoptando esta nueva versión del servicio.

12. ***Desarrollo de las mejores prácticas y metodologías:***

    Con la experiencia ya adquirida y vivida con las versiones iniciales de la plataforma, se estudian posibilidades y variables para lograr la implementación de nuevas

metodologías con el fin obtener mayor impacto en los nuevos clientes potenciales adoptando así un crecimiento en las ventas del servicio e ir plantando una mejor experiencia y buenas prácticas de desarrollo.

13. Servicio Droguería alíviese pronto 3.0:

Finalmente se tienen corregidas todas las falencias, la adopción de las nuevas metodologías estudiadas y por ende el servicio se ha divulgado nuevamente en su nueva versión. “Aliviese Pronto” esta igual que siempre disponible a nuevas peticiones de mejoras o cambios en el servicio y por supuesto a la innovación de su funcionamiento.

14. Fase de alta adopción:

Los clientes comienzan a aumentar gradualmente con relación a las versiones anteriores, aceptan y adoptan nuestra plataforma, con lo cual el servicio inicia un periodo de estabilidad y productividad.

Figura 16. Ciclo de sobre exposición de garnert

5.2. Plan de negocio de la plataforma *Aliviese-Pronto* ® en MS Project

Con el propósito de dar a conocer la viabilidad e importancia del Producto Mínimo Viable, se realizó un modelo del plan de negocio para un inversionista Ángel, con el fin de presentar las tareas necesarias para llevar a cabo la implementación real de la plataforma Aliviese-Pronto y con ello estipulando o delimitando costos, duración del proyecto, es decir, asignando duración para cada una de las tareas a realizar y pactando el inicio y fin del plan de negocio, también realizando la asignación de trabajo para cumplir con cada una de las tareas programadas.

Id	Mo de tare	EDT	Nombre de tarea	Prioric	Duración	Costo	Trabajo
1		1	Plataforma para la administración de Farmacias - Aliviese-Pronto	500	90 días	$18.717	837,02 horas
2		1.1	Planificación de servicios y productos de la plataforma Aliviese-Pronto	500	24 días	$3.177	208,02 horas
13		1.2	Estrategia y planificación de la cadena de suministro de la plataforma Aliviese-Pronto	500	15,25 días	$3.712	113 horas
25		1.3	Estrategia y planificación de recurso de las bases de datos de la plataforma Aliviese-Pronto	500	6,75 días	$810	54 horas
43		1.4	Estrategia y planificación de recursos para las interfaces de usuarios de la plataforma Aliviese-Pronto	500	45,5 días	$8.198	274 horas
81		1.5	Estrategia y planificación de servicios de la plataforma Aliviese-Pronto	500	51,5 días	$1.320	88 horas
109		1.6	Capacidad de entrega de los productos y ofertas de la plataforma Aliviese-Pronto	700	20 días	$1.500	100 horas
128		2	Actividades de mercadeo	900	26,25 días	$12.020	94 horas
137		3	Operaciones	500	570 días	-$133.472	3.864 horas
138		3.1	Costos de operación	600	520,25 días	$19.968	24 horas
289		3.2	Costos de Ventas	600	509,25 días	$86.560	3.840 horas
325		3.3	Ventas	1000	480 días	-$240.000	0 horas

Figura 17. Plan de negocio elaborado para ***Aliviese-Pronto*** ®

Aliviese-Pronto ® cuenta con una inversión total de $137.265.000 en el segundo trimestre de haber iniciado el proyecto. Después de este periodo se empiezan a obtener ganancias, pero solo hasta el séptimo trimestre de haber iniciado el proyecto se alcanza el punto de equilibrio y de ahí en adelante se comienza a ver las ganancias netas del proyecto, es decir, que según la gráfica xx el retorno de la inversión se logra al cabo de, pero con un retorno de la inversión al cabo de 15 meses y los periodos de inversión de implementación del proyecto.

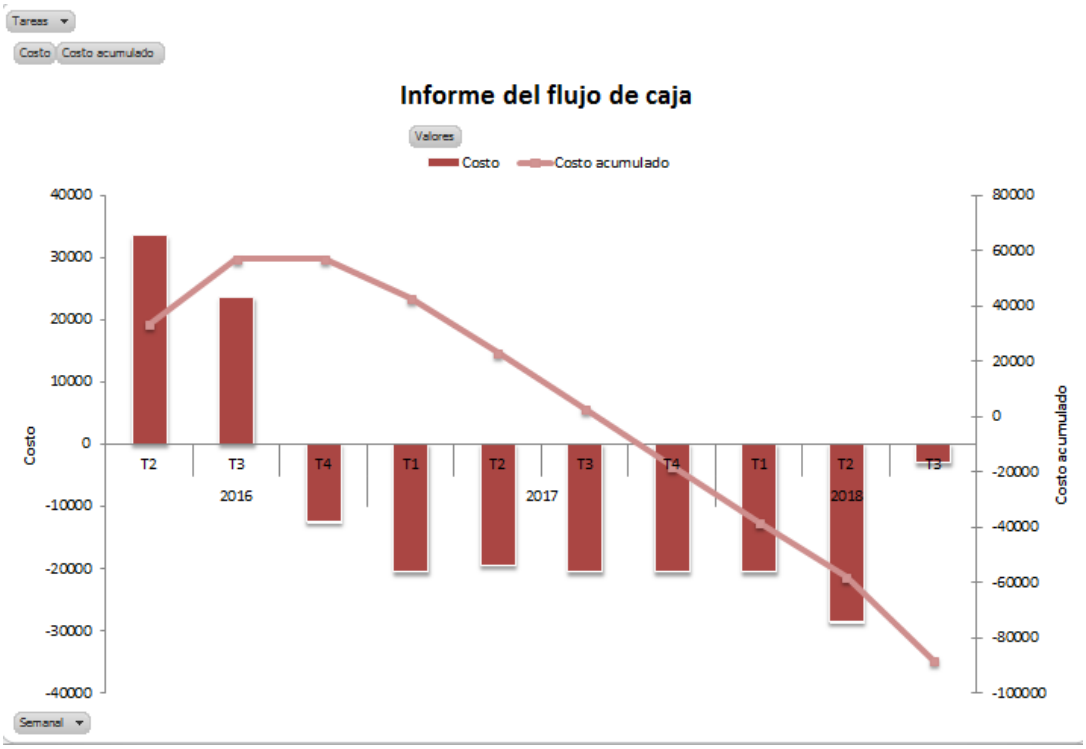


Figura 18. Flujo de Caja para la implementación de ***Aliviese-Pronto*** ®.

Figura 19. Informe de costos para la implementación de ***Aliviese-Pronto*** ®

Con el plan de negocio de ***Aliviese-Pronto*** ® y como se evidencia en la figura 19, informa que es necesario una inversión aproximada del 29% del capital en material, donde clasifican los recursos de procesamiento, conectividad y almacenamiento que ofrece Microsoft Azure, un porcentaje aproximado del 34% del capital invertido en trabajo de las diferentes actividades y recursos de capital humano se necesitan para la preparación de esta plataforma, y finalmente el 37% será invertido en costos extras como por ejemplo dentro de las actividades estipuladas se cuenta con la publicidad, el desplazamiento de los integrantes del equipo de trabajo en actividades del proyecto, y el pago por agentes externos.

6. Conclusiones

Para continuar con el modelo de negocio y el plan de implementación y desarrollo del servicio del Producto Mínimo Viable se presentara una nueva versión que cumplirá con las siguientes características y objetivos.

- ✓ La Industria de Tarjetas de Pago - PCI (Payment Card Industry) requiere que las transacciones bancarias se efectúen de manera segura y se encuentren protegidas, razón por la cual este estándar fue aplicado al modelo IaaS (Infrastructure as a Service) haciendo uso de la plataforma Share Point.

- ✓ Los estándares de seguridad ISO/IEC 27001/27002:2013 permiten un modelo para el establecimiento, operación, seguimiento, revisión y mejora de un sistema de gestión de la seguridad de la información, los cuales se implementaran en el servicio.

- ✓ El Instituto Nacional de Estándares y Tecnología - NIST (National Institute of Standard and Technology) definió el modelo de servicios de cloud computing IaaS (Infrastructure as a Service). Por lo cual se realizara el despliegue de IaaS (Infrastructure as a Service) en la plataforma de colaboración empresarial de Microsoft Azure – Share Point.

- ✓ Con el propósito de dar a conocer la importancia y viabilidad del proyecto se realizó un modelo del plan de negocio para un inversionista ángel, basándose en herramientas como Mapa de Operaciones - eTOM, Ciclo de Sobreexposición Gartner y Metodologías de Proyectos - PMBOK en Ms Project.

- ✓ Con el fin de implementar y diseñar el MVP con una estructura jerárquica que involucré la gestión y el proceso de cómo interactúan los clientes, suministradores y los diferentes recursos en la prestación del servicio, para con ello garantizar las operaciones y la continuidad del servicio.

ANEXO A

A continuación de describen cada uno de los requisitos, se muestra quien es el responsable de este y los lineamientos para la implementación

Desarrollar y Mantener una Red Segura

Los firewalls son dispositivos que controlan el tráfico computarizado entre las redes (internas) y las redes no confiables (externas) de una entidad, así como el tráfico de entrada y salida a áreas más sensibles dentro de las redes internas confidenciales de una entidad. El entorno de datos de los titulares de tarjetas es un ejemplo de un área más confidencial dentro de la red confiable de una entidad.

El firewall examina todo el tráfico de la red y bloquea las transmisiones que no cumplen con los criterios de seguridad especificados.

Todos los sistemas deben estar protegidos contra el acceso no autorizado desde redes no confiables, ya sea que ingresen al sistema a través de Internet como comercio electrónico, del acceso a Internet desde las computadoras de mesa de los empleados, del acceso al correo electrónico de los empleados, de conexiones dedicadas como conexiones entre negocios mediante redes inalámbricas o a través de otras fuentes. Con frecuencia, algunas vías de conexión hacia y desde redes no confiables aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los firewalls son un mecanismo de protección esencial para cualquier red de computadoras.

1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.

Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.

1. Establezca e implemente normas de configuración para firewalls y routers que incluyan lo siguiente:

Requisitos de PCI	Responsabilidad	Implementación	Valoración
Un proceso formal para aprobar y probar todos los cambios y las conexiones de red en la configuración de los firewalls y los routers	Cliente	1. Se debe realizar la solicitud diligenciando el formato control de cambio. 2. El formato debe contar con las firmas de los responsables según sea el caso.	4

		3. Se entregará el formato al recepcionista, quien debe colocar firma y sello en el recibido con fecha y hora. 4. El recepcionista guardará el formato en la carpeta correspondiente y enviará el requerimiento al líder del área vía correo electrónico. 5. El líder del área cuenta con máximo 24 horas para realizar la solicitud. 6. El líder debe notificar al solicitante mediante correo electrónico el estado de su solicitud.	
Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica.	Cliente	El cliente es responsable de configurar y mantener actualizado el diagrama de red, que se haya implementado.	4
Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.	Cliente	El cliente se encarga de establecer y definir las funciones de los usuarios necesarios sus servicios. ***Roles*** 1. Administrador de red 2. Administrador de la seguridad y firewall 3. Líder de infraestructura 4. Administrador de bases de datos	3
Requisito de la revisión de las	Cliente	El administrador de red junto al administrador de	4

normas de firewalls y routers, al menos, cada seis meses.		firewall y seguridad deberán generar un informe cada seis meses con el fin de validar que las normas y configuraciones realizadas se encuentren actualizadas de acuerdo a los cambios, para esto pueden usar como guía los controles de cambio efectuados.	

2. Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables y cualquier componente del sistema en el entorno de los datos de titulares de tarjetas.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
Asegure y sincronice los archivos de configuración de routers.	Microsoft Azure	Todos los servicios utilizados en Microsoft Azure se encuentran sincronizados.	4
Instale firewalls de perímetro entre las redes inalámbricas y el entorno de datos del titular de la tarjeta y configure estos firewalls para negar o, si el tráfico es necesario para fines comerciales, permitir solo el tráfico autorizado entre el entorno inalámbrico y el entorno de datos del titular de la tarjeta.	Conjunta	En el servicio no se utilizan redes inalámbricas sin embargo cada uno de los servidores cuenta con firewall habilitado. El firewall se configura en la opción general de la máquina virtual deseada allí se establecen los puertos y direcciones IP a las cuales se debe tener acceso	3

3. Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
Implementar medidas anti suplantación para	Microsoft Azure	Implementa un filtro de red para evitar el tráfico falsificado y restringir el tráfico entrante y	4

detectar y bloquear direcciones IP manipuladas a fin de que no ingresen en la red.		saliente de componentes de la plataforma.	
No permita que el tráfico saliente no autorizado proveniente del entorno de datos del titular de la tarjeta ingrese en Internet.	Cliente	Cuando se digitan los datos del titular de la tarjeta esta se almacena en el servidor de bases de datos el cual por configuración del firewall cuenta únicamente con conexión al servidor web interno. Todo esto gracias a la configuración del firewall	3
Solo permita conexiones "establecidas" en la red.	Microsoft Azure	La red Azure es segregada para separar el tráfico de los clientes del tráfico de administración.	4
Coloque los componentes del sistema que almacenan datos del titular de la tarjeta (como una base de datos) en una zona de red interna segregada desde una DMZ (zona desmilitarizada) y otras redes no confiables.	Conjunta	Azure utiliza redes segregadas y NAT para separar el tráfico de los clientes del tráfico de administración. El cliente es responsable de configurar instancias definidas en las bases de datos.	3
No divulgue direcciones IP privadas ni información de enrutamiento a partes no autorizadas.	Cliente	Únicamente los administradores de cada servicio tienen acceso a las direcciones IP de cada servidor, adicionalmente se hace firmar un acuerdo de confidencialidad en donde en uno de sus puntos se indica que no está permitido en ninguna circunstancia divulgar por ningún medio las direcciones IP de los servidores/dispositivos utilizados en el servicio.	3

4. Asegúrese de que las políticas de seguridad y los procedimientos se encuentren documentados.

Requisitos de PCI	Responsabilidad	Implementación	Valoración
Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Se encuentra un manual de configuración del firewall, adicionalmente se cuenta con una bitácora donde se encuentran los cambios realizados, junto al número de formulario para así identificar para que se realizó dicho cambio y quien autorizo ejecutarlo	3

2. No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

Las personas malintencionadas (externas e internas a una entidad), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para comprometer los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se establecen fácilmente por medio de información pública.

1. Desarrolle normas de configuración para todos los componentes de sistemas. Asegúrese de que estas normas contemplen todas las vulnerabilidades de seguridad conocidas y que concuerden con las normas de alta seguridad de sistema aceptadas en la industria.

Requisitos de PCI	Responsabilidad	Implementación	Valoración
Implemente sólo una función principal por servidor a fin de evitar que coexistan funciones que requieren diferentes niveles de seguridad en el mismo servidor	Cliente	Cada servidor cumple una única y exclusiva función esto con el fin de mitigar errores.	4
Habilite solo los servicios, protocolos y daremos, etc., necesarios, según lo	Conjunta	Las configuraciones de software y hardware de Microsoft Azure son revisados al menos cada	4

requiera la función del sistema.		tres meses para identificar y eliminar las funciones innecesarias, puertos, protocolos y servicios. Se han habilitado solo los servicios necesarios al igual que los protocolos, en cada servidor.	
Configure los parámetros de seguridad del sistema para evitar el uso indebido.	Microsoft Azure	Restringe el acceso a la configuración de seguridad de la plataforma, únicamente acceden personas autorizas y requieren una justificación de negocio.	**4**
Elimine todas las funcionalidades innecesarias, como secuencias de comandos, drivers, funciones, subsistemas, sistemas de archivos y servidores web innecesarios.	Cliente	Se encuentran solamente los servicios necesarios, adicionalmente no se entregan drivers, ni funciones adicionales a las necesarias.	4

2. Cifre todo el acceso administrativo que no sea de consola.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
Cifre todo el acceso administrativo que no sea de consola.	Cliente	Todos los accesos cuentan con su usuario y contraseña debidamente cifrada.	4

Proteger los Datos de los propietarios de tarjetas.

3. Proteja los datos del titular de la tarjeta que fueron almacenados

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos. También se deberían considerar otros métodos eficaces para proteger los datos almacenados oportunidades para mitigar posibles riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario; truncar los datos del

titular de la tarjeta si no se necesita el PAN (número de cuenta principal) completo y no enviar el PAN (número de cuenta principal) utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea.

1. Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.	Cliente	En cuanto los datos del titular de la tarjeta se guardan únicamente el número de la tarjeta de crédito digitado a la hora del registro, esto con el fin de facilitar al usuario el proceso de compra, NUNCA se almacena código de seguridad, ni clave de la tarjeta.	4

2. No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
No almacene contenido completo de ninguna pista (de la banda magnética ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo)	Cliente	Únicamente se almacena el número de tarjeta digitado por el usuario a la hora del registro	4
No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización.	Cliente	Este código de seguridad SIEMPRE debe ser digitado por el usuario cada vez que desee realizar una compra.	4

3.3. Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

Requisitos de PCI	Responsabilidad	Implementación	Valoración
Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Todas las políticas de seguridad se entregan al personal cuando firman contrato con la entidad.	4

4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

La información confidencial se debe cifrar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación siguen siendo los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.

1. Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).

Requisitos de PCI	Responsabilidad	Implementación	Valoración
Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.	Cliente	Se utiliza el antimalware de Microsoft Azure en todos los servicios.	3
Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que pueden aparecer a fin de determinar si es necesario o	Cliente	Cada mes se debe realizar un scanero de los servidores para validar el diagnostico que es generado de cada dispositivo, máquina virtual.	3

no implementar un software antivirus en dichos sistemas.			
Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: Estén actualizados. Ejecuten análisis periódicos.	Microsoft Azure	Se encarga de mantener actualizados los antivirus instalados, genera reportes periódicamente y envía alertas según lo configurado	3
Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Todas las políticas de seguridad y procedimientos operativos se entregan al personal cuando firman contrato con la entidad.	4

Mantener un Programa de Gestión de Vulnerabilidades

5. Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.

El software malicioso, llamado "malware", incluidos los virus, los gusanos (worm) y los troyanos (Trojan), ingresa a la red durante muchas actividades de negocio aprobadas incluidos los correos electrónicos de los trabajadores y la utilización de Internet, de computadoras portátiles y de dispositivos de almacenamiento y explota las vulnerabilidades del sistema. El software antivirus deberá utilizarse en todos los sistemas que el malware, por lo general, afecta para proteger los sistemas contra las amenazas de software maliciosos actuales o que eventualmente se desarrollen. Se puede considerar la opción de incluir otras soluciones antimalware como complemento del software antivirus; no obstante, estas soluciones adicionales no reemplazan la implementación del software antivirus.

1. Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).

Requisitos PCI	Responsabilidad	Implementación	Valoración
Implemente un software antivirus en todos los sistemas que,	Microsoft Azure	***Opción 1.*** Cuando se cree la máquina virtual se habilita la opción de Microsoft antimalware	4

generalmente, se ven afectados por software malicioso		en las extensiones de seguridad. ***Opción 2*** Habilitarlo mediante comandos en la consola administradora de powershell	
Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.	Microsoft Azure	Azure envía actualizaciones periódicamente para actualizar el antimalware que se encuentra protegiendo las máquinas virtuales.	4
Asegúrese de que los mecanismos de antivirus, estén actualizados y ejecuten análisis periódicos.	Microsoft Azure	Siempre que se desee se puede descargar el historial que ha registrado el antimalware instalado	4

6. Desarrollar y mantener sistemas y aplicaciones seguros

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas deben contar con los parches de software correctos para evitar que personas malintencionadas o software maliciosos usen, de manera indebida, o pongan en riesgo los datos del titular de la tarjeta.

1. Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.

Requisitos de PCI	**Responsabilidad**	**Implementación**	**Valoración**
Defina las necesidades de acceso de cada función	Cliente	Cada rol tiene funciones específicas de acuerdo a ellas se definieron los permisos necesarios para	4

		cumplir con toda su actividad.	
Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo	Cliente	Se brindarán los permisos necesarios dependiendo el perfil solicitado, vía correo electrónico en donde se debe justificar el motivo de la solicitud de cada permiso, para brindar dichos permisos se debe contar con el aval de los lideres	4
Asigne el acceso según la tarea, la clasificación y la función del personal.	Cliente	Cada rol tiene funciones específicas de acuerdo a ellas se definieron los permisos necesarios para cumplir con todas sus actividades.	4
Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.	Cliente	Para esto se utiliza el correo electrónico en donde se especifican y justifican los privilegios de cada usuario.	4
Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Cada perfil cuenta con políticas definidas y restricciones que se entregan al personal cuando firman el contrato, adicionalmente en las capacitaciones anuales se refuerzan dichas políticas	4

Implementar Medidas sólidas de control de acceso

7. Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información

A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo.

"La necesidad de saber" es la situación en que se otorgan derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea.

7.1 Limitar el acceso a los componentes del sistema y los datos de los titulares de aquellos individuos cuyas tareas necesitan de ese acceso.

Requisitos PCI	Responsabilidad	Implementación	Valoración
Limite el acceso de usuarios con ID privilegiadas a la menor cantidad de privilegios necesarios para llevar a cabo las responsabilidades del trabajo	Microsoft Azure - Cliente	Se brindan los permisos necesarios dependiendo el perfil, creando un administrador encargado de brindar dichos permisos. Notificando los permisos realizados.	4
Asignar privilegios de acceso según la tarea, la clasificación y la función del personal.	Microsoft Azure - Cliente	Cada rol tiene funciones específicas de acuerdo a ellas se definieron restricciones de acceso en bases de datos a los ID de usuario con privilegios mínimos, necesarios para cumplir con todas las responsabilidades.	4
Solicite la aprobación documentada de las partes autorizadas en la que se especifiquen los privilegios necesarios.	Microsoft Azure - Cliente	Se exige que todas las políticas de seguridad y procedimientos en relación a los accesos restringidos deben ser documentados y notificados a las partes implicadas.	4

Implementación de un sistema de control de acceso automatizado.	Microsoft Azure - Cliente	Generación mediante bases de datos usuarios y contraseñas para cada uno de los roles requeridos.	4

8. Asignar una identificación única a cada persona que tenga acceso a un computador.

Al asignar una ID (identificación) exclusiva a cada persona que tenga acceso garantiza que cada una se hará responsable de sus actos. Cuando se ejerce dicha responsabilidad, las

medidas implementadas en datos y sistemas críticos están a cargo de procesos y usuarios conocidos y autorizados y, además, se puede realizar un seguimiento.

La eficacia de una contraseña se determina, en gran medida, por el diseño y la implementación del sistema de autenticación, especialmente, la frecuencia con la que el atacante intenta obtener la contraseña y los métodos de seguridad para proteger las contraseñas de usuarios en los puntos de acceso durante la transmisión y el almacenamiento.

8.1 Asignar un único ID para cada acceso del personal

Requisitos PCI	**Responsabilidad**	**Implementación**	**Valoración**
Hacer ilegibles todas las contraseñas durante la transmisión y almacenamiento de todos los componentes del sistema, utilizando criptografía fuerte.	Microsoft Azure - Cliente	La contraseña de los usuarios debe contener caracteres, mayúsculas y números.	3

8.2 Asegurar la identificación de usuario y manejo apropiado de autenticación para los consumidores y administradores en todos los componentes del sistema de la siguiente manera:

Requisitos PCI	**Responsabilidad**	**Implementación**	**Valoración**
Aumentar control, eliminando y modificando el ID de usuario, credenciales y otros objetos de identificación.	Microsoft Azure - Cliente	Dentro de los lineamientos se encuentran recomendaciones como no revelar por ningún motivo la contraseña, cambiarla periódicamente, no escribirla en documentos que estén al alcance de todos entre otros	3
Verificar la identidad del usuario antes de restablecer contraseñas.	Microsoft Azure	Dese el administrador de la cuenta de Azure que cuente con los permisos, se pueden generar modificaciones requeridas en las contraseñas de los usuarios.	3

Establecer contraseñas para usarlo por primera vez y se restablece a un valor único para cada usuario y cambiar inmediatamente después de la primera utilización.	Cliente	Se crea el control de acceso seguro para cada usuario, brindando un usuario único con una contraseña genérica de primer acceso.	3
Eliminar o desactivar las cuentas de usuarios inactivos al menos cada 90 días.	Microsoft Azure	Con el informe de usuarios por parte del cliente, en el perfil de administrador de Azure se actualizan las cuentas, permisos y accesos de cada usuario.	3
Revocar inmediatamente el acceso de cualquier usuario terminado	Cliente	El cliente es responsable de documentar y definir la aprobación de acceso de los usuarios y verificar si los usuarios se deben encontrar activos o inactivos.	3
Comunicar los procedimientos y políticas de autenticación a todos los usuarios que tienen acceso a los datos de titulares de tarjetas.	Cliente	Se realiza una capacitación a todo el personal con el fin de actualizar e informar al personal los cambios. Y así mismo se distribuye junto a los contratos las políticas y procedimientos de seguridad.	3
Cambiar las contraseñas de usuario al menos cada 90 días.	Cliente	Se recomienda al cliente actualizar por políticas de seguridad el acceso a las plataformas, modificando periódicamente sus contraseñas.	3

No utilice grupo, compartido o cuentas genéricas y contraseñas, u otros métodos de autenticación.	Cliente	Cada usuario debe contar con un usuario que lo identifique dicho usuario es personal e intransferible. Solamente se crearán usuarios genéricos en el ambiente de pruebas.	3
Requerir una longitud mínima de contraseña de al menos siete caracteres.	Cliente	En las capacitaciones entregadas a los usuarios y por recomendaciones de estándares de seguridad, se establecen parámetros a seguir en el control de acceso.	3
Límite de repeticiones en los intentos de acceso para el bloqueo del ID de usuario.	Cliente	Por políticas de seguridad se le informa a cada usuario que cuenta con un número de no más de seis intentos para poder acceder a sus servicios.	2
Establecer la duración del bloqueo.	Cliente	Se establece un mínimo de 30 minutos o hasta que el administrador permite la identificación del usuario.	2
Si una sesión ha estado inactiva durante más de 15 minutos, requiere que el usuario vuelva a introducir la contraseña para volver a activar el terminal.	Cliente	Basado en los requerimientos PCI DSS, se realiza una verificación de uso activo de la plataforma.	2

Mantener una política de seguridad de información

Requisito 12: Mantener una política que aborde la seguridad de la información de todo el personal

Una política de seguridad solida establece el grado de seguridad para toda la entidad e informa al personal lo que se espera de ellos. Todo el personal debe estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos. A los fines del Requisito 12, él termino “personal” hace referencia a los empleados de tiempo completo y parcial, a los empleados temporales, a los contratistas y consultores que “residen” en las instalaciones de la entidad o que tienen acceso al entorno de datos del titular de la tarjeta.

12.1 Establecer, publicar, mantener y difundir una política de seguridad.

Requisitos PCI	Responsabilidad	Implementación	Valoración
Incluye un proceso anual para identificar amenazas y vulnerabilidades, y da como resultado una evaluación formal de riesgos.	Cliente	Cada vez que se realiza una modificación en un ambiente se evalúa el impacto que este va a tener en la operación.	2
Revise la política de seguridad, al menos, una vez al año y actualícela cuando se realicen cambios en el entorno	Cliente	Anualmente se realizará una capacitación a todo el personal con el fin de actualizar e informar al personal los cambios.	2
Establecer contraseñas para usarlo por primera vez y se restablece a un valor único para cada usuario y cambiar inmediatamente después de la primera utilización.	Cliente	Se crea el control de acceso seguro para cada usuario, brindando un usuario único con una contraseña genérica de primer acceso.	3

12.2 Desarrollar políticas de utilización para tecnologías críticas y definir el uso adecuado de estas tecnologías.

Requisitos PCI	Responsabilidad	Implementación	Valoración
Autenticación para el uso de la tecnología	Cliente	Cada vez que se vaya a acceder a un servicio es necesario autenticarse con el usuario creado.	3
Una lista de todos los dispositivos y personal con acceso.	Cliente	Documentar todos los accesos de cada uno de los usuarios.	2

ANEXO B

1. Contexto de la organización

1.1. Conocimiento de la organización y de su contexto

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.	***Aliviese-Pronto*** **®**	La organización ***Aliviese-Pronto*** **®** define y limita cual es él propósito de la empresa y como la gestión de la seguridad de la información permite cumplirlo.	3

1.2. Comprensión de las necesidades expectativas de las partes interesadas.

La organización debe determinar:

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
Las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información	***Aliviese-Pronto*** **®,** Cliente	Se entrega al cliente la descripción del servicio en donde se delimita el alcance de la plataforma el cliente evalúala si los requerimientos resuelven sus necesidades o en caso de necesitar otro requerimiento especial se realiza un acuerdo para satisfacer dicha necesidad	3
Los requisitos de estas partes interesadas pertinentes a seguridad de la información	***Aliviese-Pronto*** **®,** Cliente	Se entrega al cliente la descripción del servicio en donde se muestra cómo se va a proteger la información de la plataforma, el cliente evalúala si los requerimientos resuelven sus necesidades o en caso de necesitar otro requerimiento especial se	3

		realiza un acuerdo para satisfacer dicha necesidad	

1.3. Determinación del alcance del sistema de gestión de la seguridad de la información.

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
La organización debe establecer implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma	***Aliviese-Pronto ®***	Se debe estar en contacto permanente con el cliente validando como se encuentra funcionando la plataforma, tomando en cuenta los problemas que hayan presentado y validando como realizar la mejora continua de este.	3

2. Liderazgo

2.1. Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Asegurando que se establezca la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la información	***Aliviese-Pronto*** **®**	Las politicas de seguridad de la información siempre deben ejecutarse en paralelo con la dirección estratégica de la información, es por esto que el existe un rol en la empresa que audita el avance de estos dos	2
Asegurando la integración de los requisitos del sistema de la información en los procesos de la organización	***Aliviese-Pronto*** **®**	Se realiza una evaluación trimestral de la ejecución e integración de los requisitos del sistema de la información en los procesos de la organización	3
Asegurando que él resultado necesario para él sistema de gestión de la seguridad de la información esté disponible	***Aliviese-Pronto*** **®**	Todos los análisis realizados siempre estarán disponibles para que nuestros clientes observen la evolución en la plataforma	4
Comunicando la importancia de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información	***Aliviese-Pronto*** **®**	Se envían constantemente informando y recordando la importancia de la seguridad de la información ya que la información tratada es muy sensible.	3
Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**

Asegurando que él sistema de gestión de la seguridad de la información los resultados previstos	***Aliviese-Pronto ®***	De acuerdo a los análisis realizados se inician los procesos de mejora	2
Dirigiendoy apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información	***Aliviese-Pronto ®***	Junto a los comunicados enviados se adjuntan recomendaciones indicando como pueden contribuir a la eficacia del sistema de gestión de la seguridad de la información	3
Promoviendo la mejora continua	***Aliviese-Pronto ®***	Se realizan comités trimestrales en donde socializan las actividades de mejora y el avance de estas	3

2.2. Política

La alta dirección debe establecer una política de la seguridad de la información:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Sea adecuada al propósito de la organización	***Aliviese-Pronto ®***	El propósito de la organización va de la mano con el propósito de la empresa, adicionalmente es revisado por el comité de la empresa y los clientes	3

La política de seguridad de la información debe:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Estar disponible como información documentada	***Aliviese-Pronto ®***	Se documenta la política a la cual tienen acceso todos los funcionarios de la compañía	3

Comunicarse dentro de la organización	***Aliviese-Pronto ®***	Se informa a los empleados donde pueden encontrar la información y las modificaciones que se le realiza a esta	3
Estar disponible para las partes interesadas, según sea apropiado	***Aliviese-Pronto ®***	De acuerdo al plan que adquiera el cliente se muestra información relacionada con su cuenta.	3

2.3. Roles, responsabilidades y autoridades en la organización

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta norma	***Aliviese-Pronto ®***	Se realiza revisiones con personal certificado en esta norma con el fin de cumplir con todos los requerimientos nombrados.	2
Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información	***Aliviese-Pronto ®***	Se realizan comités trimestrales informando el avances y estado de este	3

3. Planificación

3.1. Acciones para tratar riesgos y oportunidades.

3.1.1. Generalidades

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos	***Aliviese-Pronto ®***	Se realiza un estricto control en la ejecución del sistema de gestión de la seguridad de la información	2

Prevenir o reducir efectos indeseados	***Aliviese-Pronto ®***	Se hace mapa de riesgos con el fin de mitigarlos	2
Lograr la mejora continua	***Aliviese-Pronto ®***	Seguimiento continuo de las actividades de mejora	3

3.1.2. Valoración de riesgos de la seguridad de la información

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Establezca y mantenga criterios de riesgo de la seguridad de la información	***Aliviese-Pronto ®***	Se realiza informe de los posibles riesgos que puede correr la plataforma	2
Asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables	***Aliviese-Pronto ®***	Se tiene un historial de los riesgos encontrados con el fin de mitigarlos	2
Identifique los riesgos de la información	***Aliviese-Pronto ®***	Se hace mapa de riesgos con el fin de mitigarlos	3

3.1.3. Tratamiento de riesgos de la seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la valoración de riesgos	***Aliviese-Pronto ®***	Al evaluar y analizar cada uno de los posibles riesgos se le otorga una valoración de acuerdo que tanto afecte la operación	3

Determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información	***Aliviese-Pronto ®***	El rol encargado de realizar el seguimiento al plan debe hacerse responsable de realizar los controles necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información	3
Formular un plan de tratamiento de riegos de la seguridad de la información	***Aliviese-Pronto ®***	Con el historial de riesgos de la empresa se realiza el plan de tratamiento de los posibles riesgos	2

3.2. Objetivos de seguridad de la información y planes para lograrlos

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Ser coherentes con la política de seguridad de la información	***Aliviese-Pronto ®***	Los objetivos se generan a partir de la política de seguridad de la información	3
Ser comunicados	***Aliviese-Pronto ®***	Se socializan con todos los empleados de la compañía	3

La organización debe conservar información documentada sobre los objetivos de la seguridad de la información.

Cuando se hace la planificación para lograr sus objetivos de la seguridad se la información, la organización debe determinar:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Lo que se va a hacer	***Aliviese-Pronto*** **®**	Se realiza un Project de las actividades necesarias, recursos a utilizar, responsable de cada actividad y tiempo de cada actividad	3
Que recursos se requerirán	***Aliviese-Pronto*** **®**	Se realiza un Project de las actividades necesarias, recursos a utilizar, responsable de cada actividad y tiempo de cada actividad	3
Quien será el responsable	***Aliviese-Pronto*** **®**	Se realiza un Project de las actividades necesarias, recursos a utilizar, responsable de cada actividad y tiempo de cada actividad	3
Cuando finalizara	***Aliviese-Pronto*** **®**	Se realiza un Project de las actividades necesarias, recursos a utilizar, responsable de cada actividad y tiempo de cada actividad	3
Como se evaluarán los resultados	***Aliviese-Pronto*** **®**	La evaluación se realiza de 1 a 4 donde 1 es la peor calificación y 4 la mejor.	2

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información	***Aliviese-Pronto ®***	Al iniciar el proyecto se realiza un listado de los recursos necesarios para realiza el presupuesto designado para este proyecto, dichos recursos pueden ser de software, materiales o humanos	3

4. Soporte

4.1. Recursos

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información	***Aliviese-Pronto ®***	Al iniciar el proyecto se realiza un listado de los recursos necesarios para realiza el presupuesto designado para este proyecto, dichos recursos pueden ser de software, materiales o humanos	3

4.2. Competencia

Requerimiento ISO 27001	Responsabilidad	Implementación	Valoración
Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información	***Aliviese-Pronto ®***	Se definen las competencias necesarias definidas por cada rol	3

Asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencias adecuadas.	***Aliviese-Pronto ®***	Se realiza la verificación de la información presentada ante la compañía por cada aspirante y elegir quien cumpla con los requerimientos solicitados.	3
Conservar la información documentada apropiada, como evidencia de la competencia	***Aliviese-Pronto ®***	Se debe almacenar los documentos que acrediten la experiencia, logros académicos y perfil de cada empleado	3

5. Evaluación de desempeño

5.1. Seguimiento, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y eficacia del sistema de gestión de la seguridad de la información

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
A que es necesario hacer seguimiento y que es necesario medir	***Aliviese-Pronto ®***	Se determinan que los puntos más vulnerables son los necesarios medir y hacer seguimiento	3
Cuando se deben llevar a cabo el seguimiento y la medición	***Aliviese-Pronto ®***	El seguimiento se debe realizar a diarios	3
Quien debe llevar a cabo el seguimiento y la medición	***Aliviese-Pronto ®***	Se asigna la tarea en la definición de roles	3
Cuando se deben analizar y evaluar los resultados del seguimiento y la medición	***Aliviese-Pronto ®***	Se entrega un informa mensual	3

6. Mejora

6.1. No conformidades y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

Requerimiento ISO 27001	**Responsabilidad**	**Implementación**	**Valoración**
Reaccionar ante la no conformidad	***Aliviese-Pronto*** **®**	Tomar acciones para controlar y corregir la no conformidad	3
Evaluar la necesidad de acciones para eliminar las causas de la no conformidad	***Aliviese-Pronto*** **®**	Revisar detalladamente y determinar las causas de la no conformidad	3
Implementar cualquier acción necesaria	***Aliviese-Pronto*** **®**	Actuar lo más pronto posible para mitigar la no conformidad	3
Revisas la eficacia de las acciones correctivas tomadas	***Aliviese-Pronto*** **®**	Llevar un control semanal en donde se pueda validar si las acciones tomada fueron eficaces	3
Hacer cambios al sistema de gestión de la seguridad de la información	***Aliviese-Pronto*** **®**	En caso de que el sistema de gestión de la seguridad de la información no se adapte a las necesidades o se empiecen a evidenciar fallas se citara a comité para realizar los respectivos cambios y correcciones	3

ANEXO C

1. Lineamientos generales

Requerimiento ISO 27018	Responsabilidad	Implementación	Valoración
Los derechos de los clientes a la hora de acceder y borrar datos importantes	***Aliviese-Pronto*** ®	El usuario realizara una solicitud de la información que desea eliminar o modificar con copia de su documento de identidad	2
No utilizar los datos para marketing y publicidad	***Aliviese-Pronto*** ®	Las bases de datos son para uso exclusivo de la plataforma ***Aliviese-Pronto*** ®	4
Notificaciones del cliente en caso de realizar una solicitud de divulgación de los datos	***Aliviese-Pronto*** ®	Si en el algún momento se tuviese que divulgar los datos personales se notificara al usuario mediante el correo electrónico inscrito	4
Notificar al cliente inmediatamente en caso de que se produzca una violación de los datos	***Aliviese-Pronto*** ®	Se realizará la notificación vía correo electrónico y mediante llamada telefónica	3
Gestionar los documentos para las políticas y procedimientos en la nube	***Aliviese-Pronto*** ®	Se encuentra toda la documentación del servicio disponible de acuerdo a los permisos otorgados	3

Establecer acuerdos de confidencialidad para todas las personas que pueden acceder a los datos personales.	***Aliviese-Pronto ®***	Todos los empleados deben firmar un acuerdo de confidencialidad para proteger la información que se maneja dentro de la compañía	4
Será necesario contar con una autorización para utilizar los datos fuera de las instalaciones.	***Aliviese-Pronto ®***	En caso de ser necesario se enviará correo electrónico con formato digital el cual deberá ser diligenciado por el usuario	2
Restringir la utilización de los medios de comunicación que no tienen capacidad de cifrado	***Aliviese-Pronto ®***	La información de datos del usuario solo podrá transmitirse mediante un dispositivo que tenga cifrado	3
Utilizar identificaciones únicas para los clientes de la nube	***Aliviese-Pronto ®***	Cada usuario cuanta con una cuenta de red única	4
Revelar al cliente de la nube en que países se almacenan sus datos	***Aliviese-Pronto ®***	El usuario realizara una solicitud de la información vía correo electrónico para revelar dicha información	4

2. Proteja los datos del titular de la tarjeta que fueron almacenados

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos. También se deberían considerar otros métodos eficaces para proteger los datos almacenados oportunidades para mitigar posibles riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario; truncar los datos del titular de la tarjeta si no se necesita el PAN (número de cuenta principal) completo y no

enviar el PAN (número de cuenta principal) utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea.

1. Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.

Requisitos de ISO 27018	**Responsabilidad**	**Implementación**	**Valoración**
Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos.	Cliente	En cuanto los datos del titular de la tarjeta se guardan únicamente el número de la tarjeta de crédito digitado a la hora del registro, esto con el fin de facilitar al usuario el proceso de compra, NUNCA se almacena código de seguridad, ni clave de la tarjeta.	4

3. No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). Si se reciben datos de autenticación confidenciales, convierta todos los datos en irrecuperables al finalizar el proceso de autorización.

Requisitos ISO 27018	**Responsabilidad**	**Implementación**	**Valoración**
No almacene contenido completo de ninguna pista (de la banda magnética ubicada en el reverso de la tarjeta, datos equivalentes que están en un chip o en cualquier otro dispositivo)	Cliente	Únicamente se almacena el número de tarjeta digitado por el usuario a la hora del registro	4
No almacene el valor o código de validación de tarjetas (número de tres o cuatro dígitos impreso en el anverso o reverso de una tarjeta de pago que se utiliza para verificar las transacciones de tarjetas ausentes) después de la autorización.	Cliente	Este código de seguridad SIEMPRE debe ser digitado por el usuario cada vez que desee realizar una compra.	4

3.3. Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

Requisitos ISO 27018	Responsabilidad	Implementación	Valoración
Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Todas las políticas de seguridad se entregan al personal cuando firman contrato con la entidad.	4

3.Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.

La información confidencial se debe cifrar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación siguen siendo los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.

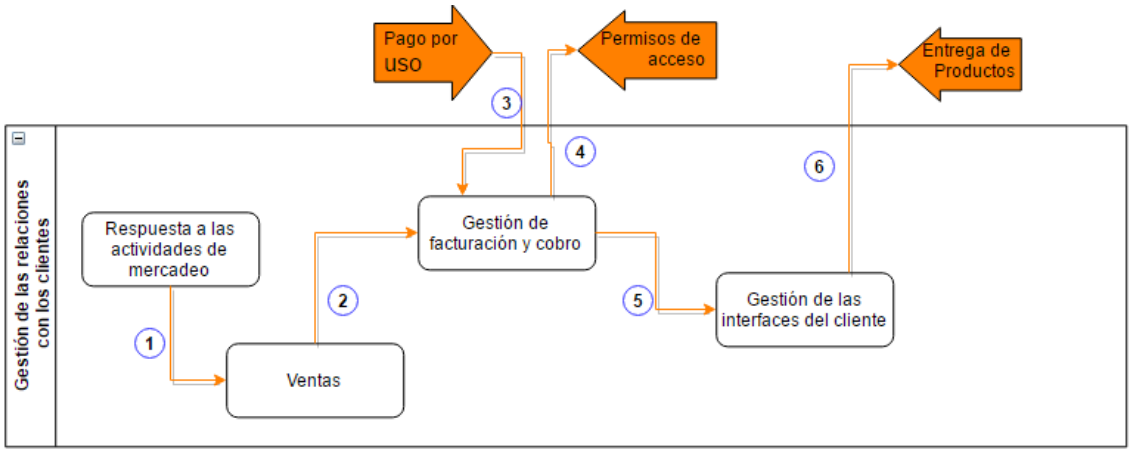
2. Implemente un software antivirus en todos los sistemas que, generalmente, se ven afectados por software malicioso (en especial, computadoras personales y servidores).

Requisitos ISO 27018	Responsabilidad	Implementación	Valoración
Asegúrese de que los programas de antivirus puedan detectar y eliminar todos los tipos de software malicioso conocidos y proteger a los sistemas contra estos.	Cliente	Se utiliza el antimalware de Microsoft Azure en todos los servicios.	3
Para aquellos sistemas que no suelen verse afectados por software maliciosos, lleve a cabo evaluaciones periódicas para identificar y evaluar las amenazas de malware que	Cliente	Cada mes se debe realizar un scanero de los servidores para validar el diagnostico que es generado de	3

pueden aparecer a fin de determinar si es necesario o no implementar un software antivirus en dichos sistemas.		cada dispositivo, máquina virtual.	
Asegúrese de que los mecanismos de antivirus cumplan con lo siguiente: Estén actualizados. Ejecuten análisis periódicos.	Microsoft Azure	Se encarga de mantener actualizados los antivirus instalados, genera reportes periódicamente y envía alertas según lo configurado	3
Asegúrese de que las políticas de seguridad y los procedimientos operativos que protegen los sistemas estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.	Cliente	Todas las políticas de seguridad y procedimientos operativos se entregan al personal cuando firman contrato con la entidad.	4

ANEXO D

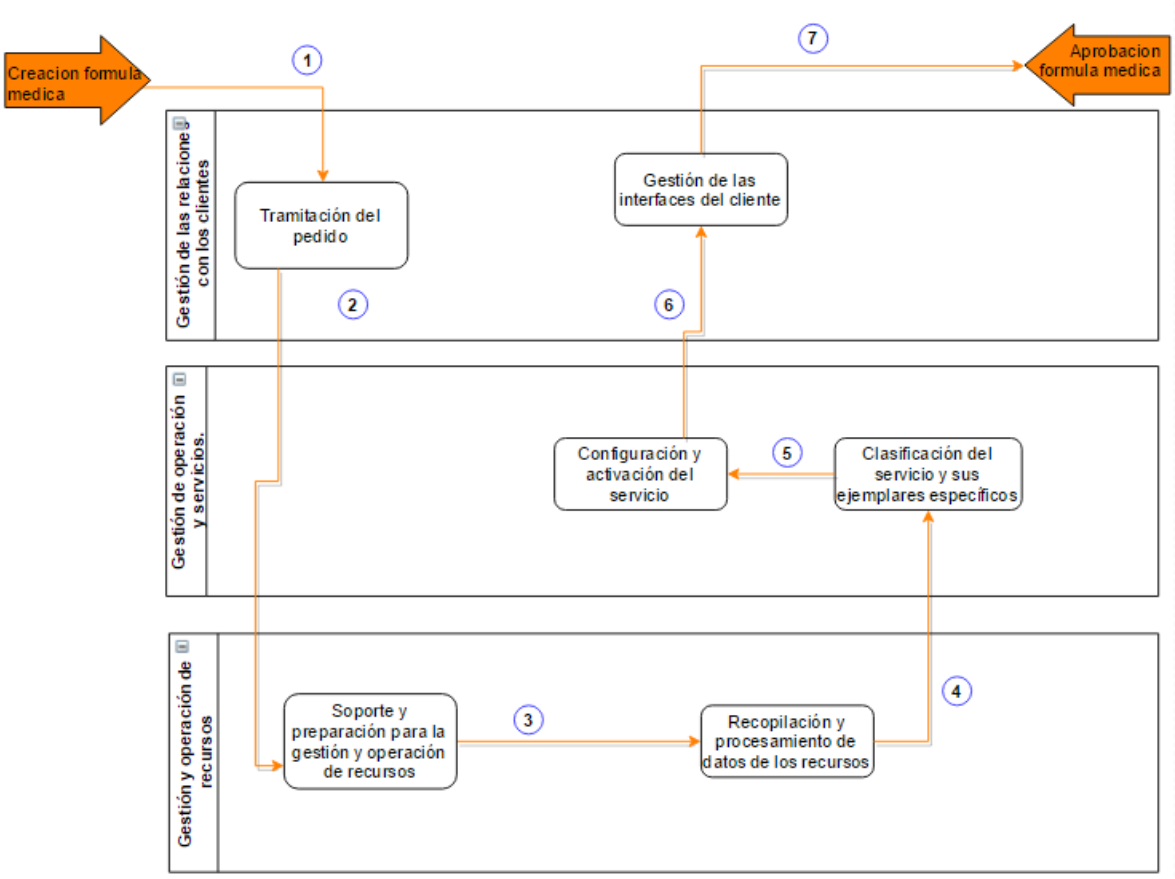
Procesos de las farmacias en *Aliviese-Pronto* ®



1. La farmacia recibe los resultados de las actividades de marketing realizadas.
2. La farmacia adquiere los accesos a la plataforma Aliviese Pronto
3. La farmacia realiza el pago mensual por uso de Aliviese Pronto
4. El personal solicitado es registrado a la plataforma Aliviese Pronto
5. El personal accede a la plataforma.
6. Se visualizan las actividades segun la asignacion y los permisos de cada rol

ANEXO E

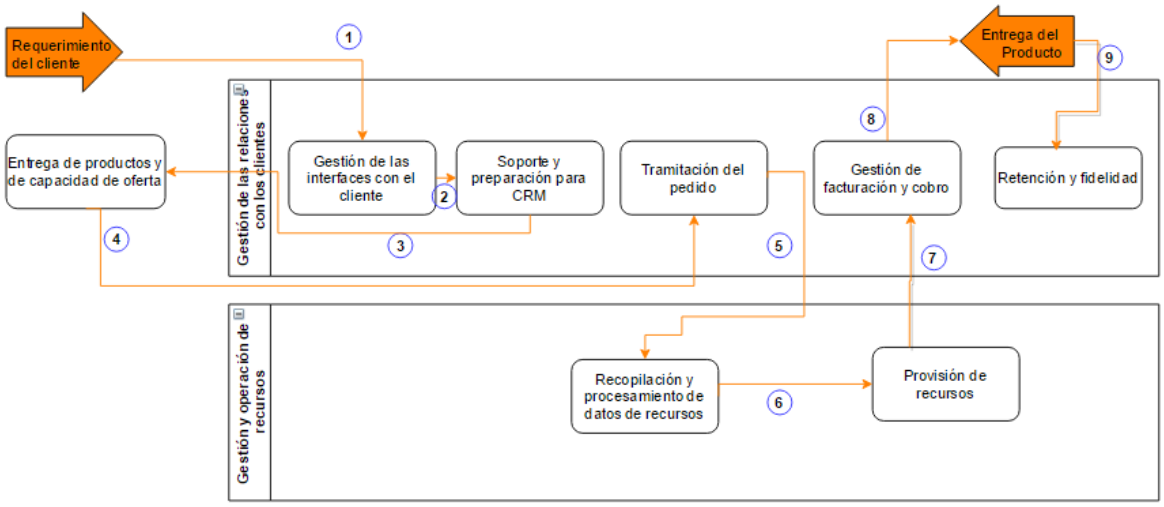
Procesos del médico en *Aliviese-Pronto* ®



1. El Doctor encargado de la consulta elabora la formula medica del usuario.
2. El Doctor ingresa a la plataforma de Aliviese Pronto e ingresa la formula medica. Las formulas medicas son recibidas y se procede a preparar y alistar los recursos.
3. La información de los productos requeridos es reunida y es puesta en linea por el Farmaceuta.
4. Los productos son categorizados por usuario y numero de orden medica.
5. Con la orden de pedido, se el servicio
6. Se ponen en orden los productos según la formula medica del usuario.
7. Los produtos y su formula medica son revisados y aprobados

ANEXO F

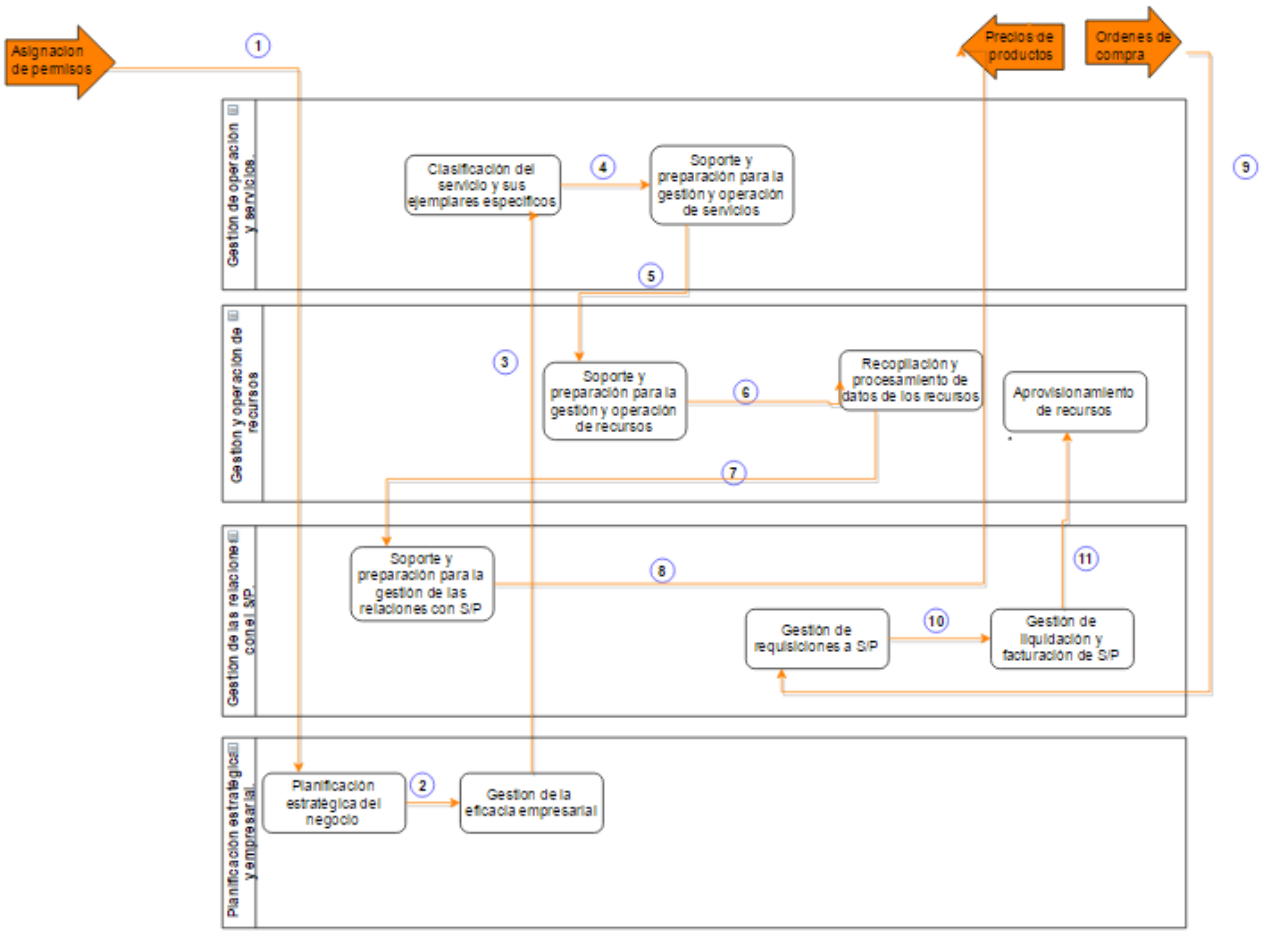
Procesos del usuario en *Aliviese-Pronto* ®



1. El cliente manifiesta su necesidad de adquirir un servicio
2. El farmaceuta orienta la necesidad del cliente a una solución adecuada para él
3. El farmaceuta realiza una consulta a la capacidad de oferta
4. Al ser posible ofrecer el servicio, se tramita el pedido
5. Con la orden de pedido, se reune la información de los recursos necesarios para prestar el servicio
6.
7. Una vez el servicio está listo y probado, se genera la factura y se establece el medio de pago
8. Se procede a entregar el servicio funcionando
9. En caso de ser necesario, se realiza la solución a problemas del servicio

ANEXO G

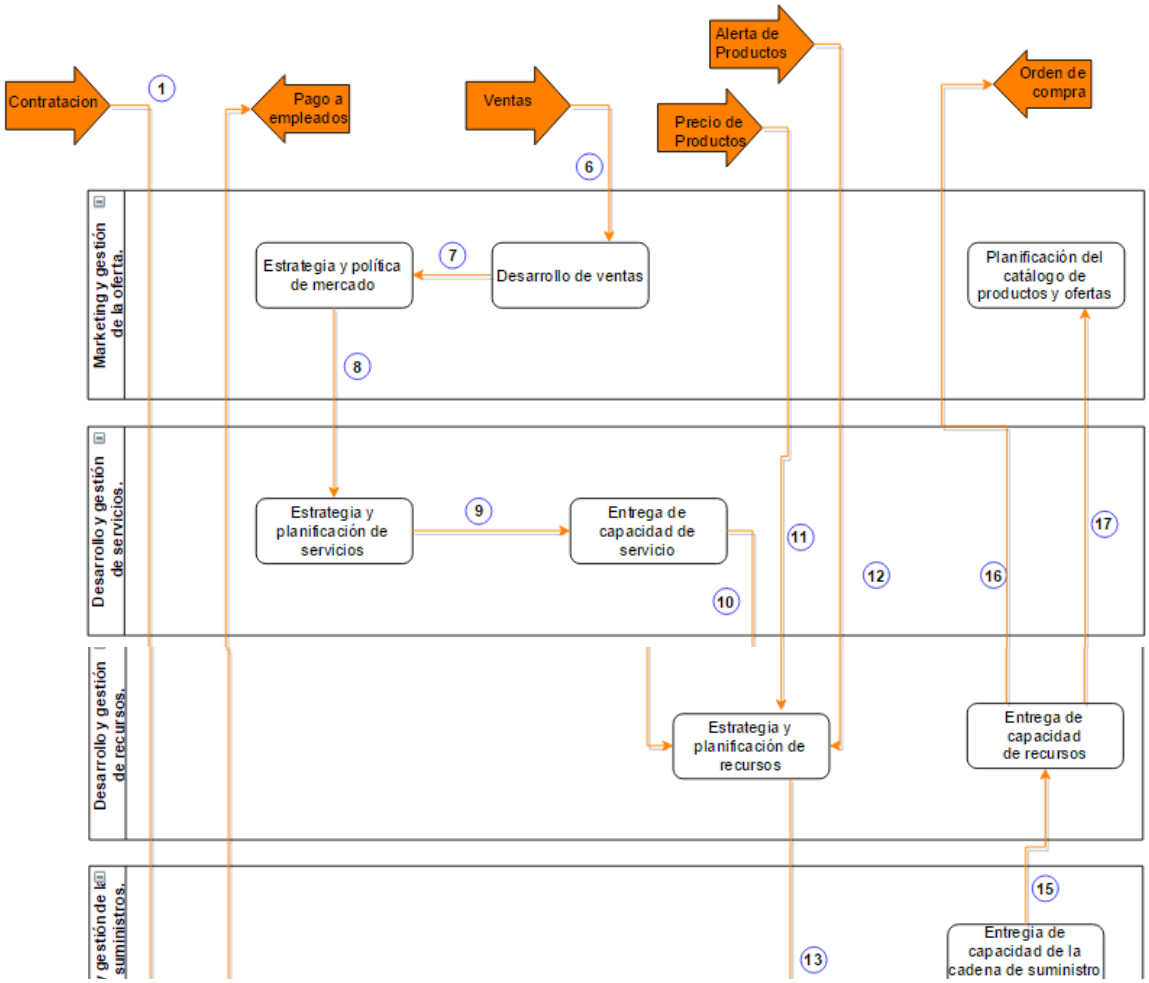
Procesos del administrador en *Aliviese-Pronto* ®



1. El administrador de la farmacia ingresa a la plataforma y realiza registros de los funcionarios.
2. El administrador realiza estrategias internas y distribuye funciones.
3. El administrador controla el inventario de productos
4. El administrador de la farmacia provee a todos los funcionarios los accesos y recursos necesarios de acuerdo al rol de trabajo.
5. El administrador de la farmacia mantiene contacto con los suministradores para mantener el inventario
6. El administrador de la farmacia mantiene actualizados los precios de los productos
7. El administrador recibe del gerente una orden de compra de nuevos productos en el inventario.
8. El admiistrador realiza el pedido a los suministradores de los productos solicitados por el gerente.
9. Una ves facturado el pedido se aprovisionan los produc

ANEXO H

Procesos del gerente en *Aliviese-Pronto* ®



1. Se realiza la contratación de personal calificado.
2. Dependiendo de la estrategia interna se establece un salario para cada rol.
3. Planeacion de estrategias de venta y control interno en la farmacia
4. Se realiza un control de desempeño de actividades para cada uno de los funcionarios
5. Se realiza el pago de nomina a los funcionarios de la farmacia según el contrato.
6. La plataforma Aliviese Pronto cuenta con un registro y estaditica del numero de productos y formulas medicas despachadas.
7. El gerente de la farmacia estudia y documenta las ventas totales en un periodo determinado.
8. Teniendo el personal adecuado y la planeacion y estudio se procede a planificar los productos
9. Se revisan los precios de los productos en el inventario.
10. Se tienen en cuenta las alertas generadas en la plataforma por la falta de productos
11. El gerente realiza la planeacion de la cantidad de productos.
12. Se estudian los libros contables para determinar la adquisicion de nuevos productos
13. El gerente se comunica con el proveedor y genera la orden de compra
14. Depende los nuevos productos y las estadísticas analizadas por el gerente se modifica el catalc de productos de la farmacia

Referencias

7. Chimbo, K. O., Aveiga, H. L., Yanez, R. M., & Parra, M. A. (28 de Abril de 2016). *La importancia del uso de las cloud computing en las empresas publicas y privada*. Obtenido de Eumed.net: http://www.eumed.net/ce/2016/2/icloud.html
8. Maidana, E. A. (12 de Marzo de 2014). *Puro Marketing*. Obtenido de ¿Qué es un Producto Mínimo Viable y como lo puedes desarrollar?: http://www.puromarketing.com/13/19295/producto-minimo-viable-como-puedes-desarrollar.html
9. Migesa Microsoft. (29 de Junio de 2015). *Migesa Soluciones Microsoft*. Obtenido de Descubre los diferenciadores que hacen a Microsoft la mejor opción para convertirse en el proveedor de nube de tu empresa.: http://www.migesamicrosoft.com/3-razones-para-usar-la-nube-de-microsoft/
10. TMForum. (09 de Octubre de 2007). *TMForum*. Obtenido de Bussiness Process Framework (eTOM): https://www.tmforum.org/business-process-framework/
11. Gartner, Inc. (28 de Septiembre de 2015). *Gartner*. Obtenido de About Gartner: http://www.gartner.com/technology/about.jsp
12. PCI Security Standards Council. (16 de Abril de 2016). *PCI Security Standards*. Obtenido de Document Library: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
13. PMI Project Management Institute. (27 de Julio de 2016). *PMI Project Management Institute*. Obtenido de PMBOK® Guide and Standards : https://www.pmi.org/pmbok-guide-standards
14. ISO. (09 de Julio de 2014). *ISO*. Obtenido de ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally (PII) in public clouds acting as PII processors: http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
15. ISO . (29 de Septiembre de 2013). *ISO*. Obtenido de ISO/IEC 27001:2013: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534
16. NIST National Institute of Standards and Technology U.S. Departmen of Commerce. (26 de Septiembre de 2011). *NIST National Institute of Standards and Technology U.S.* Obtenido de Special Publication 800-145 The NIST definition of Cloud Computing: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
17. Microsoft Azure . (06 de Mayo de 2016). *Microsft Trust Center*. Obtenido de Compliance industry-verified conformity with global standars: https://www.microsoft.com/en-us/trustcenter/Compliance/
18. World Health Organization. (13 de Octubre de 2016). *World Health Organization*. Obtenido de Fact Files: http://www.who.int/features/factfiles/en/
19. Health Information Privacy U.S. Department of Health & Human Service. (14 de Agosto de 2012). *HHS.gov Health Information Privacy U.S. Department of Health & Human Service*. Obtenido de The HIPAA Privacy Rule: https://www.hhs.gov/hipaa/for-professionals/privacy/
20. Health Information Privacy U.S. Department of Health & Human Service. (26 de Febrero de 2013). *HHS.gov Health Information Privacy U.S. Department of Health &*

Human Service. Obtenido de What is PHI?: http://www.hhs.gov/answers/hipaa/what-is-phi/index.html

21. Search Health IT. (17 de Febrero de 2009). *TechTarget*. Obtenido de HITECH Act (Health Information Technology for Economic and Clinical Health Act): http://searchhealthit.techtarget.com/definition/HITECH-Act

22. Vault rankings & reviews. (14 de Octubre de 2015). *Valut*. Obtenido de CVS PHARMACY, INC.: http://www.vault.com/company-profiles/retail/cvs-pharmacy,-inc/company-overview.aspx

23. Japsen, B. (30 de Julio de 2015). *Forbes*. Obtenido de Forbes / Pharma & Healthcare: http://www.forbes.com/sites/brucejapsen/2015/07/30/cvs-and-ibms-watson-partner-to-predict-patient-health-needs/#6096fb5d68ac

24. The Pulse on Health, Science and Technology. (18 de Febrero de 2016). *The Pulse on Health, Science and Technology - GE Healthcare*. Obtenido de Cloud Computing Can Transform the Healthcare Sector: http://newsroom.gehealthcare.com/cloud-computing-can-transform-the-healthcare-sector/

25. QuintilesIMS . (25 de Diciembre de 2014). *QuintilesIMS* . Obtenido de IMS Health Colombia: http://www.imshealth.com:90/es_CO/country-homepage-content/colombia

26. Diario Farma . (11 de Julio de 2016). *Diario Farma la informacion clave de la farmacia y del medicamento*. Obtenido de IMS Health potenciará su 'Big Data Factory' con Cloudera Enterprise: http://www.diariofarma.com/2016/07/11/ims-health-potenciara-su-big-data-factory-con-cloudera-enterprise

27. INCOCREDITO. (18 de Junio de 2016). *PCI Security Standard Council*. Obtenido de Que es la norma de seguridad PCI-DSS?: http://www.normapci.com.co/index.php/

28. PCI Security Standard Council. (13 de Mayo de 2016). *Norma PCI* . Obtenido de Norma PCI Requisitos y procedimientos de evaluación de seguridad V 3.2.: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

29. Centro de protección de datos personales Defensoria del pueblo de la ciudad de Buenos Aires. (23 de Octubre de 2015). *Centro de protección de datos personales Defensoria del pueblo de la ciudad de Buenos Aires*. Obtenido de ¿Qué son los datos sensible?: http://www.cpdp.gov.ar/index.php?view=items&cid=1%3Afcat_cpdp&id=7%3Afac_Qué+son+los+datos+sensibles&option=com_quickfaq&Itemid=72

30. Microsoft. (27 de Noviembre de 2011). *Microsoft Trust Center*. Obtenido de ISO/EICE 27001:2013 Information Security Management Standards: https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001

31. Microsoft. (09 de Diciembre de 2015). *ISO/EICE 27018 Code of Practice por Protecting Personal Data in the Cloud*. Obtenido de https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27018

32. Normas ISO. (29 de Febrero de 2015). *NORMAS ISO Asesoría, Formación & Sistemas de Gestión*. Obtenido de Análisis de la Norma ISO / IEC 27018 2014 Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud : http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal

33. Microsoft Azure. (12 de Octubre de 2016). *Microsoft Azure - Productos*. Obtenido de Base de datos SQL: https://azure.microsoft.com/es-es/services/sql-database/

34. Microsoft Azure. (19 de Agosto de 2016). *Microsoft Azure - Documentación* . Obtenido de Copias de seguridad y restauración para SQL Server en Máquinas virtuales de

Azure: https://azure.microsoft.com/es-es/documentation/articles/virtual-machines-windows-sql-backup-recovery/

35. S. S. (19 de Septiembre de 2016). *Microsoft Azure - Documentación*. Obtenido de Administración de Bases de datos SQL de Azure con el Portal de Azure: https://azure.microsoft.com/es-es/documentation/articles/sql-database-manage-portal/

36. Dial, J. (27 de Abril de 2016). *Microsoft Azure - Documentación*. Obtenido de Direcciones IP en Azure: https://azure.microsoft.com/es-es/documentation/articles/virtual-network-ip-addresses-overview-arm/

37. Dial, J. (11 de Febrero de 2016). *Microsoft Azure - Documentación*. Obtenido de ¿Qué es un grupo de seguridad de red?: https://azure.microsoft.com/es-es/documentation/articles/virtual-networks-nsg/

38. Vilcinskas, M. (23 de Agosto de 2016). *Microsft Azure - Documentación*. Obtenido de ¿Qué es Azure Active Directory?: https://azure.microsoft.com/es-es/documentation/articles/active-directory-whatis/

39. Dial, J. (04 de Febrero de 2016). *Microsoft Azure - Documentación*. Obtenido de Cómo administrar grupos de seguridad de red con el Portal de Azure: https://azure.microsoft.com/es-es/documentation/articles/virtual-networks-create-nsg-arm-pportal/

40. Narumoto, M. (13 de Julio de 2016). *Microsoft Azure - Documentación* . Obtenido de Lista de comprobación de escalabilidad: https://azure.microsoft.com/es-es/documentation/articles/best-practices-scalability-checklist/

41. Microsoft Azure. (12 de Julio de 2016). *Microsoft Azure - Documentación*. Obtenido de Contratos de nivel de servicio: https://azure.microsoft.com/es-es/support/legal/sla/

42. Microsoft Azure. (05 de Febrero de 2016). *Microsoft Azure - Documentación*. Obtenido de Azure DNS: https://azure.microsoft.com/en-us/services/dns/

43. De George, A. (06 de Septiembre de 2016). *Microsft Azure - Documentación* . Obtenido de Cómo escalar automáticamente un servicio en la nube: https://azure.microsoft.com/es-es/documentation/articles/cloud-services-how-to-scale/

44. Poggemeyer, L. (15 de agosto de 2016). *Mixrosoft Azure - Disponibilidad*. Obtenido de Calcular el uso del ancho de banda de red de Azure RemoteApp: https://azure.microsoft.com/es-es/documentation/articles/remoteapp-bandwidth/